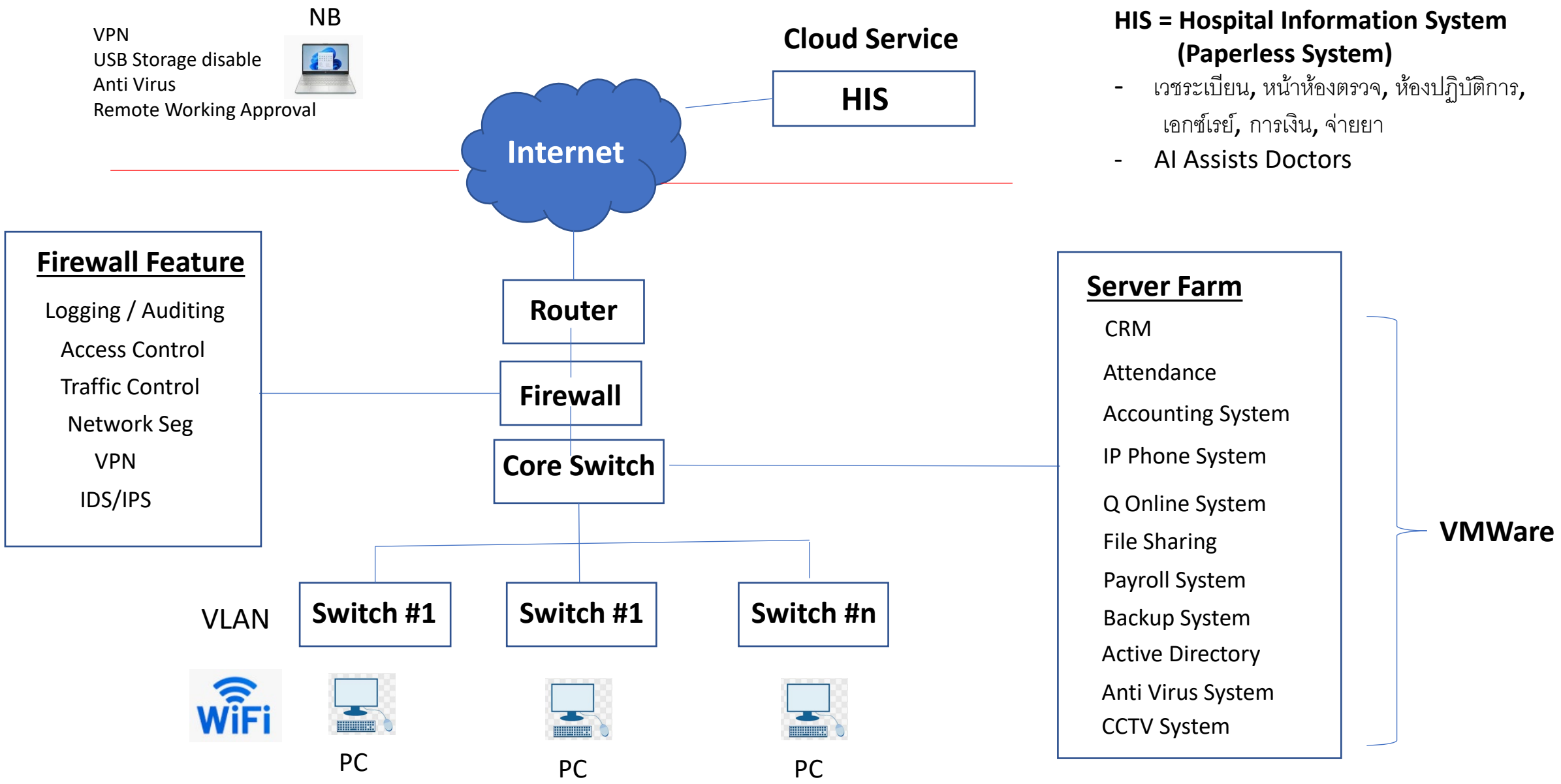
เอกสารประกอบการเรียนการสอน

หลักสูตรผู้นำการปฏิบัติ

(Lead Implementer)

กรณีศึกษาในการทำระบบ : ระบบโรงพยาบาล (CII)



HIS = Hospital Information System (Paperless System)

- เวชระเบียน, หน้าห้องตรวจ, ห้องปฏิบัติการ, เอกซ์เรย์, การเงิน, จ่ายยา
- AI Assists Doctors

ประมวลแนวทางปฏิบัติ

1. ประมวลแนวทางปฏิบัติ

1. แผนการตรวจสอบ (Cybersecurity Audit Plan) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
   1.1 > จัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)
   1.2 > รายงานการตรวจสอบ (Audit Report), NIST SP 800-53A
   1.3 > แผนการตรวจสอบ 1 ปี หรือ > 1 ปี
2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
   2.1 > กำหนดนโยบายการบริหารความเสี่ยง (Cybersecurity Risk Management Policy)
   2.2 > การประเมินความเสี่ยง (Cybersecurity Risk Assessment)
   2.3 > การจัดการความเสี่ยง (Cybersecurity Risk Treatment)
   2.4 > กำหนดดัชนีวัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI)
   2.5 > การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)
   2.6 > รายงานการประเมินความเสี่ยง (Risk Assessment Reporting), SP 800-30
3. แผนการรับมือภัยคุกคามทางไซเบอร์ (IR Plan) พร้อมรายงานการแจ้งเหตุการณ์

1

แผนการตรวจสอบ

(Cybersecurity Audit Plan)

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Logo	**ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Audit Plan -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	CSMS-Audit Plan -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.44, ม.54), ประมวลและกรอบ [ข้อ 17.1, ข้อ 17.1(ก), ข้อ 17.1(ข), ข้อ 17.1(ค), ข้อ 17.2, ข้อ 17.3, ข้อ 17.4, ข้อ 17.5]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่ามีการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์ในองค์กรอย่างต่อเนื่องและมีประสิทธิภาพ โดยเป็นไปตามมาตรฐานและข้อกำหนดที่กำหนดไว้ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับองค์กร รวมถึงการตรวจสอบกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ บริการที่สำคัญ และการปฏิบัติตามข้อกำหนดของกฎหมายและมาตรฐานที่เกี่ยวข้อง

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้ตรวจสอบทางด้านไซเบอร์ (Cybersecurity Auditors)**: รับผิดชอบในการดำเนินการตรวจสอบทั้งภายในและภายนอก โดยตรวจสอบการรักษาความมั่นคงปลอดภัยของระบบทางด้านไซเบอร์และกระบวนการต่าง ๆ ตามขอบเขตที่กำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	CSMS-Audit Plan -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **คณะกรรมการขององค์กรที่ได้รับการมอบหมาย (Cybersecurity Management Committee: CMC)**: รับผิดชอบในการอนุมัติแผนการตรวจสอบ ติดตามผลการตรวจสอบ และกำหนดแนวทางในการดำเนินการแก้ไขหากพบข้อบกพร่อง
- **หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)**: รับผิดชอบในการดำเนินการตามแผนการตรวจสอบที่ได้รับการอนุมัติ และดำเนินการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบ

4. ขั้นตอนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Process Steps)

4.1 การวางแผนการตรวจสอบ (Audit Planning)

- **4.1.1 การกำหนดขอบเขตการตรวจสอบ**
  - **ขั้นตอน**: กำหนดขอบเขตของการตรวจสอบตามที่ระบุไว้ในแนวปฏิบัติ รวมถึงกระบวนการจัดทำและบริการที่สำคัญ และการปฏิบัติตามกฎหมาย พรบ ไซเบอร์และมาตรฐานที่เกี่ยวข้อง
- **4.1.2 การแต่งตั้งผู้ตรวจสอบ**
  - **ขั้นตอน**: แต่งตั้งผู้ตรวจสอบที่มีความรู้และความเชี่ยวชาญในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ทั้งจากภายในหรือภายนอกองค์กร เพื่อร่วมดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	CSMS-Audit Plan -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4.2 การดำเนินการตรวจสอบ (Audit Execution)

- **4.2.1 การตรวจสอบกระบวนการและบริการที่สำคัญ**
  - **ขั้นตอน:** ผู้ตรวจสอบดำเนินการตรวจสอบกระบวนการจัดทำการตรวจสอบพร้อมวิเคราะห์ผลกระทบ (BIA) และบริการที่สำคัญขององค์กรตามขอบเขตที่กำหนดไว้
- **4.2.2 การตรวจสอบการปฏิบัติตามกฎหมาย พรบ ไซเบอร์ และมาตรฐานอื่นๆ ที่เกี่ยวข้อง**
  - **ขั้นตอน:** ผู้ตรวจสอบตรวจสอบการปฏิบัติตาม พรบ ไซเบอร์ และมาตรฐานการปฏิบัติงานที่เกี่ยวข้อง รวมถึงการปฏิบัติตามข้อกำหนดขององค์กรและหน่วยงานควบคุมหรือกำกับดูแล

4.3 การรายงานผลการตรวจสอบ (Audit Reporting)

- **4.3.1 การจัดทำรายงานการตรวจสอบ**
  - **ขั้นตอน:** ผู้ตรวจสอบจัดทำรายงานสรุปผลการตรวจสอบ รวมถึงข้อบกพร่องที่พบและข้อเสนอแนะในการปรับปรุง
- **4.3.2 การส่งรายงานผลการตรวจสอบ**
  - **ขั้นตอน:** หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบต่อสำนักงานภายในกำหนด 30 วันหลังจากที่ดำเนินการตรวจสอบเสร็จสิ้น และส่งสำเนาให้กับหน่วยงานควบคุมหรือกำกับดูแล

4.4 การดำเนินการแก้ไขข้อบกพร่อง (Corrective Action Implementation)

- **4.4.1 การจัดทำแผนการดำเนินการแก้ไข**
  - **ขั้นตอน:** หากพบข้อบกพร่องหรือการไม่ปฏิบัติตามในการตรวจสอบ องค์กรจะต้องจัดทำแผนการดำเนินการแก้ไขโดยระบุรายละเอียดการแก้ไขและระยะเวลาที่จะดำเนินการ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan Procedure)	รหัสเอกสาร	CSMS-Audit Plan -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **4.4.2 การติดตามและรายงานผลการแก้ไข**
  - **ขั้นตอน:** ติดตามผลการดำเนินการแก้ไข และรายงานผลการแก้ไขต่อคณะกรรมการขององค์กรที่ได้รับมอบหมายเป็นประจำ และหน่วยงานควบคุมหรือกำกับดูแล ภายในระยะเวลาที่กำหนด

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review**)

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานการตรวจสอบ (Audit Program / Plan)
2. รายงานการตรวจสอบ (Audit Reporting), NIST SP 800-53A Rev. 5
3. ผลการดำเนินการแก้ไข และรายงานผลการแก้ไข
4. แผนการตรวจสอบระยะเวลา 1 ปี (Annual Audit Plan) หรือ เกินกว่า 1 ปี (Multi-Year Audit Plan)
5. รายงานหรือเอกสารแสดงการจัดทำ BIA

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure**	**รหัสเอกสาร**	**CSMS-BIA -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure	รหัสเอกสาร	CSMS-BIA -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure

อ้างอิง : พรบ ไซเบอร์ (ม.44, ม.54), ประมวลและกรอบ [ข้อ 17.1, ข้อ 17.1(ก), ข้อ 17.1(ข), ข้อ 17.1(ค), ข้อ 17.2, ข้อ 17.3, ข้อ 17.4, ข้อ 17.5]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อระบุและวิเคราะห์ผลกระทบทางธุรกิจที่อาจเกิดขึ้นจากเหตุการณ์ที่ไม่คาดคิด รวมถึงการหยุดชะงักในการดำเนินงาน เพื่อกำหนดลำดับความสำคัญของกระบวนการและระบบที่สำคัญ และเพื่อกำหนดกลยุทธ์ในการรักษาความต่อเนื่องทางธุรกิจ

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมการวิเคราะห์ผลกระทบทางธุรกิจของทุกกระบวนการ ระบบ และทรัพยากรที่เกี่ยวข้องกับการดำเนินงานขององค์กร เพื่อประเมินระดับผลกระทบและกำหนดกลยุทธ์ในการจัดการความเสี่ยงและการฟื้นฟูการดำเนินงาน

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้จัดการโครงการ BIA (BIA Project Manager)**: รับผิดชอบในการจัดทำแผนการวิเคราะห์ผลกระทบทางธุรกิจ ควบคุมการดำเนินงาน และรายงานผลการวิเคราะห์
- **ทีมวิเคราะห์ผลกระทบ (Impact Analysis Team)**: รับผิดชอบในการรวบรวมข้อมูล วิเคราะห์ผลกระทบ และจัดทำรายงาน BIA

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **ผู้บริหารองค์กร (Senior Management)**: รับผิดชอบในการอนุมัติผลการวิเคราะห์ BIA และสนับสนุนการดำเนินการตามกลยุทธ์ที่กำหนด

4. ขั้นตอนการจัดทำและวิเคราะห์ผลกระทบทางธุรกิจ (BIA Process Steps)

4.1 การวางแผนและการเริ่มต้น (Planning and Initiation)

- **4.1.1 กำหนดวัตถุประสงค์และขอบเขต**
  - **ขั้นตอน**: กำหนดวัตถุประสงค์ ขอบเขต และเกณฑ์ในการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงทรัพยากรที่เกี่ยวข้อง ซึ่งวัตถุประสงค์คือการประเมินผลกระทบจากการหยุดชะงักของระบบเครือข่ายที่ใช้ในการบริการลูกค้า ขอบเขตครอบคลุมกระบวนการทั้งหมดที่เกี่ยวข้องกับการให้บริการลูกค้าและการจัดการข้อมูลลูกค้า
- **4.1.2 การจัดตั้งทีมวิเคราะห์ผลกระทบ**
  - **ขั้นตอน**: แต่งตั้งทีมวิเคราะห์ผลกระทบที่ประกอบด้วยบุคลากรจากหน่วยงานต่าง ๆ ในองค์กรที่มีความเชี่ยวชาญในกระบวนการที่เกี่ยวข้อง เช่น ฝ่าย IT, ฝ่ายการเงิน, ฝ่ายปฏิบัติการ, และฝ่ายบริหารความเสี่ยง

4.2 การรวบรวมข้อมูล (Data Collection)

- **4.2.1 การระบุและจัดลำดับความสำคัญของกระบวนการ**
  - **ขั้นตอน**: ระบุและจัดลำดับความสำคัญของกระบวนการทางธุรกิจที่สำคัญ โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้นต่อองค์กร โดยกระบวนการเหล่านี้ถูกจัดเป็นกระบวนการที่มีความสำคัญสูงสุด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure	รหัสเอกสาร	CSMS-BIA -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **4.2.2 การรวบรวมข้อมูลจากหน่วยงานที่เกี่ยวข้อง**
  - **ขั้นตอน:** รวบรวมข้อมูลจากหน่วยงานที่เกี่ยวข้องเกี่ยวกับกระบวนการ ระบบ และทรัพยากรที่ใช้ในกระบวนการ เพื่อประเมินผลกระทบจากการหยุดชะงัก

4.3 การวิเคราะห์และประเมินผลกระทบ (Analysis and Impact Evaluation)

- **4.3.1 การประเมินผลกระทบที่อาจเกิดขึ้น (Impact Analysis)**
  - **ขั้นตอน:** วิเคราะห์ผลกระทบทางการเงิน ด้านชื่อเสียง ด้านกฎหมาย และผลกระทบอื่น ๆ ที่อาจเกิดขึ้นจากการหยุดชะงักของกระบวนการและระบบ หากระบบการประมวลผลธุรกรรมการเงินล่ม อาจส่งผลให้บริษัทสูญเสียรายได้และเกิดความเสียหายด้านชื่อเสียง
- **4.3.2 การกำหนดเกณฑ์เวลาที่สำคัญ (Critical Timeframes)**
  - **ขั้นตอน:** กำหนดเกณฑ์เวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), และ Recovery Point Objective (RPO) สำหรับกระบวนการที่สำคัญ ซึ่งหมายความว่าระบบต้องฟื้นฟูให้ใช้งานได้ภายในเวลาที่กำหนดไว้

4.4 การจัดทำรายงานและข้อเสนอแนะ (Reporting and Recommendations)

- **4.4.1 การจัดทำรายงาน BIA**
  - **ขั้นตอน:** จัดทำรายงานสรุปผลการวิเคราะห์ BIA ที่รวมถึงผลกระทบที่ประเมินได้ ข้อสังเกต และข้อเสนอแนะในการจัดการความเสี่ยงและการฟื้นฟูกระบวนการ เช่นรายงาน BIA ต้องระบุว่าการหยุดชะงักของระบบเครือข่ายหลักจะส่งผลกระทบทางการเงินอย่างมีนัยสำคัญ และเสนอให้จัดตั้งระบบสำรองเพื่อให้สามารถฟื้นฟูการทำงานได้ภายใน 2 ชั่วโมง เป็นต้น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure	รหัสเอกสาร	CSMS-BIA -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **4.4.2 การนำเสนอผลการวิเคราะห์**
  - **ขั้นตอน:** นำเสนอผลการวิเคราะห์ต่อผู้บริหารองค์กรและคณะกรรมการที่เกี่ยวข้อง เพื่อพิจารณาและอนุมัติแผนการดำเนินการตามข้อเสนอแนะ เนื่องจาก บางอย่างต้องมีการอนุมัติการลงทุนด้วย

4.5 การดำเนินการตามข้อเสนอแนะ (Implementation of Recommendations)

- **4.5.1 การดำเนินการตามแผนการฟื้นฟู**
  - **ขั้นตอน:** ดำเนินการตามแผนการฟื้นฟูที่ได้รับอนุมัติ รวมถึงการจัดตั้งระบบสำรอง การทดสอบระบบ และการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ
- **4.5.2 การติดตามและประเมินผล**
  - **ขั้นตอน:** ติดตามและประเมินผลการดำเนินการตามแผน BIA เพื่อปรับปรุงและปรับแผนให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) Procedure	รหัสเอกสาร	CSMS-BIA -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. เอกสารแสดงการจัดทำ BIA
2. รายงานผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA Report)

1. ข้อมูลทั่วไป

- **ชื่อองค์กร:** บริษัท XYZ จำกัด
- **วันที่รายงาน:** 8 กันยายน 2567
- **ชื่อผู้จัดทำรายงาน:** นางสาว A
- **ทีมวิเคราะห์ที่เกี่ยวข้อง:** ฝ่ายความเสี่ยง, ฝ่าย IT, ฝ่ายการเงิน, ฝ่ายปฏิบัติการ, ฝ่ายทรัพยากรบุคคล

2. วัตถุประสงค์ของการวิเคราะห์ (Objective)

รายงานนี้จัดทำขึ้นเพื่อวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ที่ไม่คาดคิดต่อกระบวนการสำคัญขององค์กร และเพื่อกำหนดลำดับความสำคัญในการฟื้นฟูการดำเนินงานในกรณีที่เกิดการหยุดชะงัก

3. ขอบเขตของการวิเคราะห์ (Scope)

- **กระบวนการที่ครอบคลุม**
    1. การให้บริการลูกค้า
    2. การประมวลผลคำสั่งซื้อ
    3. ระบบการจัดการคลังสินค้า
    4. ระบบการจัดการการเงิน
    5. การสรรหาและจัดการทรัพยากรบุคคล
- **ระบบและทรัพยากรที่เกี่ยวข้อง:** ฐานข้อมูลลูกค้า, ระบบ ERP, ระบบ CRM, ระบบบัญชี, เซิร์ฟเวอร์หลัก, เครือข่ายอินเทอร์เน็ต

4. รายการกระบวนการที่สำคัญและผลการวิเคราะห์ (Key Processes and Impact Analysis)

	กระบวนการทางธุรกิจ	ผลกระทบทางการเงิน	ผลกระทบด้านชื่อเสียง	ผลกระทบด้านกฎหมาย	MTPD	RTO	RPO	ข้อเสนอแนะ
1	ระบบให้บริการลูกค้า (CRM)	3 ล้านบาท/วัน	สูง	ปรับเงิน 500,000 บาท	24 ชม.	4 ชม.	1 ชม.	จัดทำระบบสำรองและเพิ่มทีมสนับสนุน
2	ระบบโรงพยาบาล (HIS)	2 ล้านบาท/วัน	ปานกลาง	ไม่มี	48 ชม.	8 ชม.	2 ชม.	ปรับปรุงระบบสำรองข้อมูลและขั้นตอนการทำงาน
3	ระบบการจัดการคลังสินค้า (INV)	1.5 ล้านบาท/วัน	ต่ำ	ไม่มี	72 ชม.	12 ชม.	4 ชม.	ใช้เทคโนโลยี IoT เพื่อติดตามสต็อก
4	ระบบการจัดการการเงิน (ACCT)	5 ล้านบาท/วัน	สูง	ปรับเงิน 1 ล้านบาท	24 ชม.	6 ชม.	1 ชม.	เพิ่มมาตรการความปลอดภัยไซเบอร์และสำรองข้อมูล
5	การสรรหาและจัดการทรัพยากรบุคคล (HRM/Payroll)	500,000 บาท/วัน	ปานกลาง	ปรับเงิน 200,000 บาท	96 ชม.	24 ชม.	8 ชม.	ใช้ระบบ HRM ที่มีความเสถียรและสำรองข้อมูลอัตโนมัติ

คำอธิบายเพิ่มเติม

- **ผลกระทบทางการเงิน:** มูลค่าความเสียหายทางการเงินที่อาจเกิดขึ้น หากกระบวนการหยุดชะงัก
- **ผลกระทบด้านชื่อเสียง:** ระดับความเสียหายต่อความเชื่อมั่นของลูกค้า (สูง, ปานกลาง, ต่ำ)
- **ผลกระทบด้านกฎหมาย:** การละเมิดกฎหมายหรือข้อบังคับที่อาจเกิดขึ้น รวมถึงค่าปรับ
- **MTPD (Maximum Tolerable Period of Disruption)**: ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก
- **RTO (Recovery Time Objective)**: ระยะเวลาในการกู้คืนระบบ
- **RPO (Recovery Point Objective)**: ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหาย
- **ข้อเสนอแนะ:** แนวทางในการปรับปรุงและลดความเสี่ยง

5. สรุปผลการวิเคราะห์ (Summary of Findings)

- **ผลกระทบที่อาจเกิดขึ้น:** หากเกิดการหยุดชะงักในระบบการจัดการการเงินและการให้บริการลูกค้า จะส่งผลกระทบทางการเงินและชื่อเสียงอย่างมาก
- **กระบวนการที่มีความสำคัญสูงสุด**
  - **การให้บริการลูกค้า:** เป็นหัวใจหลักของธุรกิจที่ต้องรักษาความต่อเนื่อง
  - **ระบบการจัดการการเงิน:** ส่งผลโดยตรงต่อการดำเนินงานทางการเงินและการปฏิบัติตามกฎหมาย
- **ข้อเสนอแนะสำหรับการจัดการความเสี่ยง**
  - จัดทำและทดสอบแผนสำรองข้อมูลและการกู้คืนระบบอย่างสม่ำเสมอ
  - เพิ่มมาตรการความปลอดภัยไซเบอร์เพื่อป้องกันการโจมตีที่อาจทำให้ระบบหยุดชะงัก
  - จัดอบรมพนักงานเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน

6. แผนการดำเนินการและติดตามผล (Action Plan and Follow-up)

- **แผนการดำเนินการ**
  1. **ระบบให้บริการลูกค้า:** เพิ่มทีมสนับสนุนและจัดทำระบบสำรองข้อมูลที่สามารถกู้คืนได้ภายใน 4 ชั่วโมง
  2. **ระบบการจัดการการเงิน:** ปรับปรุงระบบความปลอดภัยและทดสอบแผนกู้คืนข้อมูลทุกไตรมาส
  3. **ระบบโรงพยาบาล:** ปรับปรุงขั้นตอนการทำงานและใช้ระบบอัตโนมัติเพื่อลดเวลาการกู้คืน
  4. **ระบบการจัดการคลังสินค้า:** นำเทคโนโลยี IoT มาใช้เพื่อติดตามและจัดการสต็อกแบบเรียลไทม์
  5. **การสรรหาและจัดการทรัพยากรบุคคล:** ใช้ระบบ HRM ที่มีการสำรองข้อมูลอัตโนมัติและเสถียร
- **การติดตามผล**
  1. **ฝ่าย IT:** รับผิดชอบการปรับปรุงระบบและการทดสอบแผนกู้คืน
  2. **ฝ่ายความเสี่ยง:** ติดตามและรายงานความคืบหน้าต่อผู้บริหาร
  3. **ฝ่ายบริหาร:** ประเมินผลและให้คำแนะนำเพิ่มเติม
- **วันที่ประเมินซ้ำ:** 8 กันยายน 2568

7. ภาคผนวก (Appendices)

- **ข้อมูลที่เกี่ยวข้องเพิ่มเติม**
  - รายละเอียดของระบบและทรัพยากรที่ใช้ในแต่ละกระบวนการ
  - ผลการประเมินความเสี่ยงเพิ่มเติมสำหรับแต่ละกระบวนการ
- **รายชื่อผู้เข้าร่วมการวิเคราะห์**
  - นางสาว A (ฝ่าย IT)
  - นาย B (ฝ่ายการเงิน)
  - นางสาว C (ฝ่ายความเสี่ยง)

แผนการตรวจสอบประเมิน

(Cybersecurity Audit Plan)

แผนการตรวจสอบภายใน ประจำปี 2568

	หน่วยรับตรวจ	ประเภทการตรวจ							ระยะเวลาการตรวจสอบ				หมายเหตุ
		ประมวลแนวทางปฏิบัติ	Govern	Identify	Protect	Detect	Respond	Recover	Q1	Q2	Q3	Q4	
1	รพ 1 และศูนย์คอมพิวเตอร์	X	X	X	X	X	X	X	X				สัมภาษณ์ผู้บริหาร
2	รพ 2 และศูนย์คอมพิวเตอร์	X	X	X		X		X		X			สัมภาษณ์ผู้บริหาร
3	สนง 1 และศูนย์คอมพิวเตอร์	X	X	X	X		X	X			X		สัมภาษณ์ผู้บริหาร
4	สนง 2	X	X		X	X		X				X	

Logo

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วัตถุประสงค์การตรวจประเมิน(Objective):	เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อ: 1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 2) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ 3) นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 4) ตรวจความพร้อมของเอกสารหลักฐานที่เกี่ยวข้องฯ
เกณฑ์/มาตรฐานที่ใช้ในการตรวจประเมิน (Audit Criteria):	**1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562** **2) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** **3) นโยบาย ประมวลผลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** **4) มาตรฐานควบคุม ตาม พ.ร.บ.ไซเบอร์ 2562**
ขอบเขตที่ตรวจประเมิน(Scope of Audit):	การรักษาความมั่นคงปลอดภัยไซเบอร์ (ชื่อหน่วยงาน) ซึ่งประกอบไปด้วย **ขอบเขตบริการที่สำคัญดังต่อไปนี้ (อ้างอิงเอกสารแนบ1 : ผลการวิเคราะห์ผลกระทบทางธุรกิจ(Business Impact Analysis: BIA)** 1. บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ xxx 2. บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ xxx 3. บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ xxx 4. บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ xxx รวมถึงสิ่งอำนวยความสะดวกพื้นฐาน (Facilities) ระบบเครือข่าย(Network) ที่สนับสนุนการให้บริการดังกล่าวของ (ชื่อหน่วยงานและสถานที่ตั้ง) ศูนย์คอมพิวเตอร์ อาคาร_____กรม____ถนน_____อำเภอ_____ จังหวัด_____

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
15 มิ.ย. 2568	09.00 – 09.15	Opening Meeting (ประชุมชี้แจงแผนการตรวจสอบประเมิน)	Auditor Team	All participants	
15 มิ.ย. 2568	09.15 – 10.30	**Govern, สัมภาษณ์ผู้บริหาร [มาตรา 44, นโยบายบริหารจัดการทางไซเบอร์ และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]** • นโยบาย CSMS , โครงสร้าง CSMS และการกำหนดบทบาทหน้าที่ • ทิศทางการบริหารจัดการ • วิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ • ทิศทางการบริหารจัดการ • การกำหนดขอบเขตของระบบการจัดการความมั่นคงปลอดภัยไซเบอร์ • ความเป็นผู้นำและความมุ่งมั่น • ความสอดคล้องด้านวิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ • ปัจจัยภายในภายนอกที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กร • ความคาดหวังของผู้มีส่วนได้ส่วนเสีย • การสนับสนุนทรัพยากรที่จำเป็น • การทบทวนของฝ่ายบริหาร • การส่งเสริมการปรับปรุงพัฒนาอย่างต่อเนื่อง		ผู้บริหาร (Top Management CSMS)	

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
15 มิ.ย. 2568	10.30 – 11.00	**การควบคุมเอกสาร [มาตรา 44]** • ตรวจสอบการควบคุมเอกสาร • กระบวนการในการควบคุมเอกสารและการประกาศใช้เอกสาร การสื่อสารถึงหน่วยงานที่เกี่ยวข้อง		CSMR และ คณะทำงานด้านการบริหารจัดการและควบคุมเอกสาร	
15 มิ.ย. 2568	10.30 – 11.00	**Identify [มาตรา 44 และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]** **Asset Management** • ดูวิธีการจัดการทรัพย์สิน, ดูหลักฐานทะเบียนทรัพย์สิน **Risk Assessment and Risk Management Strategy** • ดูวิธีการประเมินความเสี่ยงไซเบอร์ของบริการที่สำคัญ, ดูความถี่ในการประเมินความเสี่ยง อย่างน้อย ปีละ1 ครั้ง, ดูทะเบียนความเสี่ยง **Vulnerability Assessment and Penetration Testing** • ดูวิธีการประเมินช่องโหว่ของการบริการที่สำคัญ, ดูวิธีการทดสอบเจาะระบบ รวมถึงผลการทดสอบ, ดูใบรับรองจากผู้ให้บริการทดสอบเจาะระบบ, ดูรายงานสรุปผลการเจาะระบบ **Third Part Management** • ดูข้อตกลงระดับการให้บริการ (SLA), ดูเงื่อนไขของสัญญาจ้าง, ดูการประเมินความเสี่ยงที่เกี่ยวข้องกับการบริการ, ดูผลการตรวจสอบผู้ให้บริการ		CSMR และ ทีมงานที่เกี่ยวข้อง	

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
15 มิ.ย. 2568	11.00 – 12.00	**<u>Protect [มาตรา 44 และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]</u>** **<u>Access Control</u>** • ตรวจสอบดูสิทธิ์การเข้าถึง ของบุคคลและอุปกรณ์, ดู Logs of all access, ตรวจสอบดูการเข้าถึง Interface เช่น USB, Serial Port **<u>System Hardening</u>** • ดูมาตรฐานการกำหนดค่าขั้นต่ำด้านไซเบอร์, ดูกระบวนการจัดการเปลี่ยนแปลงหรือกระบวนการ **<u>Remote Connection</u>** • ดูมาตรฐานการเชื่อมต่อระยะไกล, ดูเทคนิคการพิสูจน์ตัวตนที่ใช้, ดูการเข้ารหัส (https, ssh, scp), ทดสอบการใช้คำสั่งระบบ เช่น Telnet or shell script **<u>Removable Storage Media</u>** • ตรวจสอบดูการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้, ทดสอบ USB Port ใช้งานได้หรือไม่, มีการขออนุญาตในการใช้สื่อบันทึก, ทดสอบว่าสื่อบันทึกมีการเข้ารหัสหรือไม่ **<u>Cybersecurity Awareness</u>** • ดูแผนงานการสร้างความตระหนักรู้ สำหรับ พนักงาน ผู้รับเหมาและ 3 rd party, ดูหลักฐานการอบรมเกี่ยวกับ CSMS / กฎหมาย พรบ ไซเบอร์, ดูว่ามีการสื่อสารอย่างสม่ำเสมอ อย่างไร, ดูว่ามีการทบทวนแผนงานในการสร้างตระหนักรู้หรือไม่ และอย่างน้อย ปีละ 1 ครั้ง		CSMR และ ทีมงานที่เกี่ยวข้อง	

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
		Information Sharing • ตรวจสอบดูขั้นตอนเพื่อแบ่งปันข้อมูล, ดูแนวทางและรูปแบบในการแบ่งปันข้อมูล		-	
15 มิ.ย. 2568	12.00 – 13.00	**พักกลางวัน**			
15 มิ.ย. 2568	14.00 – 14.30	**Detect [มาตรา 44 และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]** **Cyber Threat Detection and Monitoring** • ตรวจสอบดูกลไกและกระบวนการตรวจจับเหตุการณ์ทางไซเบอร์, ดูการจัดประเภทและวิเคราะห์เหตุการณ์, ดูว่ามรการทบทวนกลไกและกระบวนการ อย่างน้อย ปีละ 1 ครั้ง หรือไม่		CSMR และ ทีมงานที่เกี่ยวข้อง	
15 มิ.ย. 2568	14.30 – 15.30	**Respond [มาตรา 44 และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]** **Cybersecurity Incident Response Plan** • ดูแผนการรับมือภัยคุกคามทางไซเบอร์, ดูความถี่ ในการสื่อสาร ฝึกซ้อม ทบทวนและปรับปรุง อย่างน้อย ปีละ 1 ครั้งหรือไม่ **Crisis Communication Plan** • ดูแผนการสื่อสารในภาวะวิกฤต, ดูว่ามีการจัดตั้งทีมสื่อสารในภาวะวิกฤตหรือไม่, ดูมีการฝึกซ้อมแผนการสื่อสารหรือไม่ และมีความถี่อย่างน้อย ปีละ 1 ครั้ง		CSMR และ ทีมงานที่เกี่ยวข้อง	

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ
		Cybersecurity Exercise • ดูหลักฐานว่ามีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์		-	
15 มิ.ย. 2568	15.30 – 16.00	**Recover [มาตรา 44 และมาตรการควบคุม ตาม พรบ ไซเบอร์ 2562]** **Cybersecurity Resilience and Recovery** • ดูแผนความต่อเนื่องทางธุรกิจ (BCP) • ดูหลักฐานการสอบทานแผนของผู้ให้บริการภายนอก • ดูหลักฐานการฝึกซ้อม BCP, ความถี่ 1 ครั้งต่อปี		CSMR และ ทีมงานที่เกี่ยวข้อง	
15 มิ.ย. 2568	16.00 – 16.30	**Auditor Time ประชุมคณะผู้ตรวจการประเมิน**			
15 มิ.ย. 2568	16.30 – 17.00	**Close Meeting** **สรุปผลการตรวจสอบประเมินภายใน ร่วมกับทีมผู้ตรวจประเมินและผู้ที่รับการตรวจ**	Auditor Team	All participants	

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) ประจำปี 2568 ครั้งที่ 1

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน(Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจประเมิน	หมายเหตุ

ผู้จัดทำ/ตรวจสอบ
ลงนาม : ( ) ประธานคณะกรรมการตรวจสอบภายใน(Lead Auditor)
วันที่ :

ผู้อนุมัติ
ลงนาม : ( ) ผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์
วันที่ :

ตัวอย่างรายงานสิ่งที่พบเจอทั้งหมด (Audit Finding)

*** แนะนำให้ใช้ Compliance Audit Checklist เพื่อความสะดวก ***

	สิ่งที่พบเจอ (Audit Finding)	ผลการประเมิน	ความคิดเห็นและข้อเสนอแนะของผู้ตรวจสอบ
1	(Controls No. xx), ช่วงเวลาที่กำหนดในการจัดการฝึกอบรมแผนสำรองหลังจากเข้ารับหน้าที่ความรับผิดชอบตามแผนสำรองได้รับการกำหนดหรือไม่	S	นโยบายการวางแผนแผนสำรองของระบบ ABC ระบุช่วงเวลา (ที่กำหนดโดยองค์กร) เป็น 4 สัปดาห์
2	(Controls No. xx), ความถี่ในการจัดการฝึกอบรมให้กับผู้ใช้ระบบที่มีบทบาทหรือหน้าที่ความรับผิดชอบตามแผนสำรองได้รับการกำหนดหรือไม่	S	นโยบายการวางแผนแผนสำรองของระบบ ABC ระบุความถี่เป็นประจำทุกปี
3	(Controls No. xx), ความถี่ในการทบทวนและปรับปรุงเนื้อหาการฝึกอบรมแผนสำรองได้รับการกำหนดหรือไม่	S	นโยบายการวางแผนแผนสำรองของระบบ ABC ระบุความถี่เป็นประจำทุกปี

S = Satisfied, O = Non - Satisfied

เพิ่มเติม : -

- ผู้ประเมินพบว่าระบบ ABC มีการกำหนดช่วงเวลาและความถี่ที่ชัดเจนในการฝึกอบรมแผนสำรอง รวมถึงการทบทวนเนื้อหาเป็นประจำทุกปี อย่างไรก็ตาม การฝึกอบรมที่สอดคล้องกับการเปลี่ยนแปลงของระบบและเหตุการณ์ที่จำเป็นในการทบทวนยังขาดหลักฐานและการกำหนดที่ชัดเจน
- **ข้อเสนอแนะ**: ควรจัดทำแผนการจัดการฝึกอบรมที่ครอบคลุมถึงการเปลี่ยนแปลงระบบ และกำหนดเหตุการณ์ที่จำเป็นในการทบทวนและปรับปรุงเนื้อหาการฝึกอบรมแผนสำรอง

รายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Audit Report)

(อ้างอิง Appendix E, NIST SP 800-53A Rev. 5)

ชื่อระบบ: ระบบบริหารจัดการโรงพยาบาล (HIS – Hospital Information System)

การจัดหมวดหมู่ความมั่นคงปลอดภัย: ความลับสูง (High Confidentiality), ความถูกต้องปานกลาง (Moderate Integrity), ความพร้อมใช้งานสูง (High Availability)

สถานที่และวันที่ประเมิน: อาคารศูนย์ข้อมูล, วันที่ 1-3 กันยายน 2567

ชื่อผู้ตรวจสอบ: 1. นายก้องภพ Lead Auditor, 2. นายหรรษา Auditor

ผลการประเมินก่อนหน้า: ประเมินล่าสุดเมื่อเดือนมีนาคม 2567, พบช่องโหว่ในกระบวนการควบคุมการเข้าถึง

รายละเอียดการตรวจสอบ

ตัวควบคุม: การควบคุมการเข้าถึงระยะไกล (Remote Access Control), Control No. xx

วัตถุประสงค์: ตรวจสอบว่าได้มีการจำกัดและอนุญาตการเข้าถึงระยะไกลอย่างเหมาะสม

วิธีการประเมิน:

1. ตรวจสอบเอกสารการควบคุม
2. สัมภาษณ์ผู้ดูแลระบบเครือข่าย
3. ทดสอบการเข้าถึงระยะไกล

ผลการประเมิน:

ผ่านการประเมิน (S - Satisfied): ระบบมีการจัดการการเข้าถึงระยะไกลที่เหมาะสมตามที่ระบุไว้ในนโยบายและการตรวจสอบการทำงานจริง

ความคิดเห็นของผู้ประเมิน: กระบวนการควบคุมการเข้าถึงระยะไกลดำเนินการได้อย่างสมบูรณ์ และมีระบบป้องกันความเสี่ยงการเข้าถึงที่ไม่ได้รับอนุญาตได้อย่างมีประสิทธิภาพ

คำแนะนำ: ควรพิจารณาการอัปเดตระบบป้องกันการเข้าถึงอัตโนมัติเพื่อรองรับการขยายตัวในอนาคต

ตัวควบคุม: การจัดการช่องโหว่ (Vulnerability Management), Control No. xx

วัตถุประสงค์: ระบุและแก้ไขช่องโหว่ในระบบอย่างสม่ำเสมอ

วิธีการประเมิน:

1. ตรวจสอบเอกสารการจัดการช่องโหว่
2. สัมภาษณ์ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์
3. ทดสอบการสแกนหาช่องโหว่

ผลการประเมิน:

ไม่ผ่านการประเมิน (O): พบช่องโหว่ที่ไม่ได้รับการแก้ไขภายในระยะเวลาที่กำหนด

ความคิดเห็นของผู้ประเมิน: จำเป็นต้องมีการตอบสนองที่รวดเร็วขึ้นในการแก้ไขช่องโหว่ ความล่าช้าอาจก่อให้เกิดความเสี่ยง

คำแนะนำ: แนะนำให้จัดทำกระบวนการที่มีการตอบสนองที่ชัดเจนและรวดเร็วขึ้นในการจัดการช่องโหว่

สรุปผลการประเมิน

ผ่านการประเมิน: การควบคุมการเข้าถึงระยะไกล Control No. xx

ไม่ผ่านการประเมิน: การจัดการช่องโหว่ Control No. xx

ข้อเสนอแนะ:

ปรับปรุงระบบการควบคุมการเข้าถึงระยะไกลให้รองรับผู้ใช้เพิ่มเติม

เร่งกระบวนการตอบสนองในการจัดการช่องโหว่ให้รวดเร็วขึ้น

2

การประเมินความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Risk Assessment)

2.1 > กำหนดนโยบายการบริหารความเสี่ยง (Cybersecurity Risk Management Policy)

Logo	**นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)**	**รหัสเอกสาร**	**CSMS-Policy-02**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

1. วัตถุประสงค์ (Objective)

วัตถุประสงค์ของนโยบายนี้คือเพื่อกำหนดกรอบการทำงานสำหรับการระบุ ประเมิน และบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้แน่ใจว่าโครงสร้างพื้นฐานและบริการที่สำคัญได้รับการปกป้องจากภัยคุกคามไซเบอร์ นโยบายนี้สอดคล้องกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย โดยเฉพาะ **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และ **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงหน่วยงาน แผนก และพันธมิตรภายนอกทั้งหมดที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งรวมถึง …

- โครงสร้างพื้นฐานสำคัญด้านสารสนเทศ
- ข้อมูลและเครือข่ายที่สำคัญ
- ผู้ให้บริการและผู้จำหน่ายภายนอก

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)	รหัสเอกสาร	CSMS-Policy-02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

3. หลักการบริหารความเสี่ยง (Risk Management Principle)

องค์กรจะใช้หลักการดังต่อไปนี้ในการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

- **การระบุความเสี่ยงเชิงรุก**: การระบุความเสี่ยงด้านไซเบอร์ผ่านการประเมินอย่างสม่ำเสมอและการวิเคราะห์ข้อมูลภัยคุกคาม
- **การประเมินความเสี่ยง**: การประเมินผลกระทบและความเป็นไปได้ของความเสี่ยงที่ระบุ โดยเน้นที่ภัยคุกคามที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานหรือข้อมูลสำคัญ
- **การลดความเสี่ยง**: ดำเนินการลดหรือขจัดความเสี่ยง โดยจัดลำดับความสำคัญของภัยคุกคาม
- **การติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง**: การติดตามและทบทวนความเสี่ยงด้านไซเบอร์มีการกระทำอย่างต่อเนื่อง หรืออย่างน้อย ปีละ 1 ครั้ง โดยผ่านระบบอัตโนมัติและการตรวจสอบด้วยตนเองอย่างสม่ำเสมอ

4. ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

นโยบายนี้จะสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

- **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**: ปฏิบัติตามข้อกำหนดในการปกป้องโครงสร้างพื้นฐานสำคัญและการรายงานเหตุการณ์
- **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**: เป็นการพัฒนาความมั่นคงปลอดภัยทางทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติและเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ทีมงานด้านความมั่นคงปลอดภัยไซเบอร์**: รับผิดชอบในการดำเนินการประเมินความเสี่ยง ดำเนินมาตรการแก้ไข และติดตามความเสี่ยงอย่างต่อเนื่อง
- **ฝ่ายบริหาร**: ต้องมั่นใจว่าการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ถูกรวมเข้ากับกรอบการบริหารจัดการทั่วไปและรายงานความสอดคล้องกับหน่วยงานที่เกี่ยวข้อง
- **เจ้าหน้าที่กำกับดูแล**: รับผิดชอบในการตรวจสอบและให้แน่ใจว่าปฏิบัติตามกฎหมายและระเบียบข้อบังคับตามที่ระบุใน **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

6. กระบวนการระบุและประเมินความเสี่ยง (Risk Identification and Risk Assessment)

- **ทะเบียนความเสี่ยง**: จะมีการบันทึกความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดในทะเบียนความเสี่ยง โดยจะมีการประเมินแต่ละความเสี่ยง เช่น
    - **ความเป็นไปได้**: ความน่าจะเป็นที่ความเสี่ยงจะเกิดขึ้น
    - **ผลกระทบ**: ความเสียหายหรือการรบกวนที่อาจเกิดขึ้นจากความเสี่ยง
    - **มาตรการควบคุม**: ขั้นตอนที่มีอยู่ในปัจจุบัน สามารถเพื่อบรรเทาความเสี่ยงนั้นๆ
- **การจัดประเภทความเสี่ยง**: ความเสี่ยงจะถูกจัดหมวดหมู่ตามระดับ เช่น สูง กลาง ต่ำ ตามความรุนแรงที่ประเมิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

7. การจัดการความเสี่ยง (Risk Treatment)

- **การหลีกเลี่ยง**: ความเสี่ยงที่สามารถหลีกเลี่ยงได้จะถูกขจัดออกโดยการเปลี่ยนแปลงระบบหรือกระบวนการในการปฏิบัติ
- **การลดความเสี่ยง**: ลดความเสี่ยงโดยการดำเนินมาตรการควบคุมเพิ่มเติม เช่น การเข้ารหัสไฟล์ วางไฟร์วอลล์ และฝึกอบรมพนักงาน
- **การยอมรับ**: มีการกำหนดความเสี่ยงในระดับต่ำที่ยอมรับได้ โดยไม่ต้องมีมาตรการเพิ่มเติม
- **การโอนความเสี่ยง**: โอนความเสี่ยงให้หน่วยงานหรือองค์กรภายนอก โดยการทำสัญญาหรือประกันภัยในกรณีที่เหมาะสม

8. การตอบสนองและรายงานเหตุการณ์ (Response and Incident Reporting)

- ทุกเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์จะต้องรายงานต่อทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ทันที
- เหตุการณ์ที่รุนแรงที่ส่งผลต่อโครงสร้างพื้นฐานสำคัญจะถูกส่งต่อไปยังผู้บริหารระดับสูงและหน่วยงานควบคุมหรือกำกับดูแล ตาม **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

9. การปรับปรุงอย่างต่อเนื่อง (Continuously Improvement)

- จะมีการตรวจสอบและประเมินผลนโยบายฯอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ากรอบการบริหารความเสี่ยงนั้นยังคงมีประสิทธิภาพ
- นโยบายฯนี้จะได้รับการปรับปรุงเพื่อให้ทันกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์

10. การปฏิบัติตามและการกำกับดูแล (Operate and Governance)

นโยบายฯนี้จะได้รับการตรวจสอบอย่างต่อเนื่องเพื่อให้สอดคล้องกับยุทธศาสตร์ไซเบอร์แห่งชาติหรือนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) รวมถึงข้อกำหนดของ **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** การไม่ปฏิบัติตามนโยบายนี้จะมีบทลงโทษตามข้อกำหนดขององค์กร

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

2.2 > การประเมินความเสี่ยง (Cybersecurity Risk Assessment)

2.3 > การจัดการความเสี่ยง (Cybersecurity Risk Treatment)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) และการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Treatment)							วันที่ทำการประเมิน : 1/05/67	ผู้ทำการประเมินความเสี่ยง : ทีมประเมินความเสี่ยง	
	ระบุความเสี่ยง (Risk Identification)	การวิเคราะห์ความเสี่ยง (Risk Analyst)	การประเมินความเสี่ยง (Risk Evaluation) / โอกาสที่จะเกิดขึ้น	ความรุนแรงของเหตุการณ์ (Severity of the event)		การจัดการความเสี่ยง (Risk Treatment)	เจ้าของความเสี่ยง (Owner Risk)	ความเสี่ยงที่เหลือ (Residual Risk)	สถานะของการจัดการความเสี่ยง (Risk Managed Status)
1	ความเสี่ยงจากการโจมตีแบบฟิชชิ่ง (Phishing Attacks)	การโจมตีแบบฟิชชิ่งสามารถทำให้ผู้โจมตีเข้าถึงข้อมูลสำคัญขององค์กรได้ โดยการหลอกลวงให้พนักงานเปิดเผยข้อมูลที่เป็นความลับ เช่น รหัสผ่าน หรือข้อมูลส่วนบุคคล	สูง (High)	สูง (High)	1	ฝึกอบรมพนักงานให้ความรู้เกี่ยวกับ CSMS Awareness และ Cyber Attack ทุกรูปแบบ โดยเฉพาะฟิชชิ่ง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ติดตั้งระบบกรองอีเมลที่มีความสามารถในการตรวจจับและบล็อกอีเมลฟิชชิ่ง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ดำเนินการตรวจสอบและทดสอบการรับรู้ของพนักงานเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
2	ความเสี่ยงจากการโจมตี (DDoS, Distributed Denial of Service Attacks)	การโจมตี DDoS สามารถทำให้บริการออนไลน์ขององค์กรล่มและไม่สามารถให้บริการแก่ลูกค้าได้	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบป้องกันการโจมตี DDoS (DDoS Mitigation)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้บริการ CDN (Content Delivery Network) ที่มีการป้องกัน DDoS ในตัว	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการรับส่งข้อมูลเครือข่ายเป็นระยะ ๆ เพื่อระบุพฤติกรรมที่ผิดปกติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
3	ความเสี่ยงจากการขโมยข้อมูล (Data Theft)	การขโมยข้อมูลที่สำคัญ เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน อาจทำให้เกิดความเสียหายอย่างรุนแรงต่อองค์กร	ปานกลาง (Medium)	สูง (High)	1	เข้ารหัสข้อมูลทั้งหมดที่เก็บในระบบฐานข้อมูล	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงข้อมูลสำคัญเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้ระบบการยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
4	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่ได้รับการอัปเดต (Outdated Software)	ซอฟต์แวร์ที่ไม่ได้รับการอัปเดตอาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้เพื่อเข้าถึงระบบหรือข้อมูลที่สำคัญได้	สูง (High)	ปานกลาง (Medium)	1	จัดตั้งนโยบายการอัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้เครื่องมือจัดการการแพตช์ซอฟต์แวร์อัตโนมัติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

					3	ตรวจสอบและทดสอบซอฟต์แวร์ที่ใช้งานในระบบอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
5	ความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)	การเข้าถึงระบบโดยไม่ได้รับอนุญาตสามารถทำให้เกิดการโจมตีหรือการขโมยข้อมูลจากระบบขององค์กรได้	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบการยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication - 2FA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงระบบเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ทบทวนสิทธิ์การเข้าถึงของผู้ใช้ในระบบอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
6	ความเสี่ยงจากการโจมตีผ่านเครือข่ายไร้สาย (Wireless Network Attacks)	การโจมตีผ่านเครือข่ายไร้สายอาจทำให้ข้อมูลที่ถูกส่งผ่านเครือข่ายถูกดักฟังหรือถูกขโมย	ปานกลาง (Medium)	ปานกลาง (Medium)	1	ติดตั้งระบบการเข้ารหัสข้อมูลในเครือข่ายไร้สาย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงเครือข่ายไร้สายเฉพาะผู้ใช้ที่ได้รับอนุญาต	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้ระบบตรวจสอบการเข้าถึงเครือข่ายไร้สายเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
7	ความเสี่ยงจากการโจมตีแบบ Zero-Day (Zero-Day Attacks)	การโจมตีแบบ Zero-Day เป็นการโจมตีที่ใช้ช่องโหว่ที่ยังไม่เคยถูกค้นพบมาก่อน ทำให้ไม่มีการป้องกันโดยเฉพาะสำหรับช่องโหว่นั้น	ปานกลาง (Medium)	สูง (High)	1	ใช้ระบบการป้องกันที่มีการอัปเดตช่องโหว่อย่างต่อเนื่อง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ตรวจสอบระบบเครือข่ายและการใช้งานซอฟต์แวร์เพื่อระบุพฤติกรรมที่ผิดปกติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
8	ความเสี่ยงจากการใช้รหัสผ่านที่ไม่ปลอดภัย (Weak Passwords)	การใช้รหัสผ่านที่ไม่ปลอดภัยหรือรหัสผ่านที่สามารถเดาได้ง่ายทำให้ผู้โจมตีสามารถเข้าถึงระบบได้ง่ายขึ้น	สูง (High)	ปานกลาง (Medium)	1	กำหนดนโยบายการตั้งรหัสผ่านที่มีความซับซ้อนและบังคับให้เปลี่ยนรหัสผ่านเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้การยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication - 2FA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการใช้งานรหัสผ่านในระบบเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
9	ความเสี่ยงจากการเข้าถึงอุปกรณ์ IoT ที่ไม่ได้รับการควบคุม (Uncontrolled IoT Devices)	อุปกรณ์ IoT ที่ไม่ได้รับการควบคุมหรืออัปเดตสามารถเป็นจุดเริ่มต้นของการโจมตีในระบบเครือข่ายขององค์กร	ปานกลาง (Medium)	ปานกลาง (Medium)	1	จำกัดการเข้าถึงอุปกรณ์ IoT และการเชื่อมต่อกับเครือข่ายองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	อัปเดตซอฟต์แวร์ของอุปกรณ์ IoT อย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ติดตั้งระบบการตรวจสอบการใช้งานอุปกรณ์ IoT ในองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

10	**ความเสี่ยงจากการรั่วไหลของข้อมูลลูกค้า (Customer Data Leakage)**	ข้อมูลลูกค้าที่รั่วไหลอาจทำให้เกิดความเสียหายต่อความเชื่อมั่นของลูกค้าและภาพลักษณ์ขององค์กร	**ปานกลาง** (Medium)	**สูง** (High)	**1**	เข้ารหัสข้อมูลลูกค้าทั้งหมดที่จัดเก็บและส่งผ่านในระบบ	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					2	จำกัดการเข้าถึงข้อมูลลูกค้าเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					3	ตรวจสอบการเข้าถึงและการใช้งานข้อมูลลูกค้าอย่างสม่ำเสมอ	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
11	**ความเสี่ยงจากการโจมตีผ่านการใช้งาน Remote Access (Remote Access Attacks)**	การใช้งาน Remote Access อาจทำให้ผู้โจมตีสามารถเข้าถึงระบบขององค์กรจากภายนอกได้หากไม่มีการรักษาความปลอดภัยที่เหมาะสม	**สูง** (High)	**ปานกลาง** (Medium)	**1**	ใช้การยืนยันตัวตนแบบสองขั้นตอน (2FA) สำหรับการเข้าถึงระยะไกล	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					2	จำกัดการใช้งาน Remote Access เฉพาะผู้ที่มีความจำเป็นเท่านั้น	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					3	ตรวจสอบการใช้งาน Remote Access อย่างสม่ำเสมอ	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
12	**ความเสี่ยงจากการโจมตีผ่านแอปพลิเคชันที่ไม่ได้รับการตรวจสอบ (Unvetted Applications)**	แอปพลิเคชันที่ไม่ได้รับการตรวจสอบหรือทดสอบก่อนใช้งานอาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้โจมตีระบบได้	**ปานกลาง** (Medium)	**สูง** (High)	**1**	ตรวจสอบและทดสอบแอปพลิเคชันทั้งหมดก่อนที่จะนำไปใช้งานในระบบ	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					2	ห้ามใช้งานแอปพลิเคชันที่ไม่ได้รับการอนุมัติจากฝ่าย IT	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					3	ทบทวนการใช้งานแอปพลิเคชันในองค์กรเป็นระยะ ๆ	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
13	**ความเสี่ยงจากการโจมตีผ่านซอฟต์แวร์ที่ไม่ปลอดภัย (Insecure Software)**	ซอฟต์แวร์ที่ไม่ได้รับการพัฒนาตามมาตรฐานความปลอดภัยอาจมีช่องโหว่ที่สามารถนำไปสู่การโจมตีได้	**ปานกลาง** (Medium)	**สูง** (High)	**1**	ใช้แนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Lifecycle - SSDLC)	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					2	ทดสอบความปลอดภัยของซอฟต์แวร์ก่อนที่จะนำไปใช้งาน	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)
					3	จัดทำการตรวจสอบซอฟต์แวร์เป็นระยะเพื่อระบุช่องโหว่ที่อาจเกิดขึ้น	CSMR	**น้อย** (Low)	**ดำเนินการแล้ว** (1/04/67)

14	**ความเสี่ยงจากการโจมตีผ่านเว็บไซต์ขององค์กร (Website Attacks)**	เว็บไซต์ขององค์กรอาจเป็นเป้าหมายของการโจมตี เช่น การโจมตี SQL Injection, XSS, หรือการโจมตีแบบอื่น ๆ ที่สามารถทำให้ข้อมูลรั่วไหลหรือเว็บไซต์ล่ม	ปานกลาง (Medium)	สูง (High)	1	ทดสอบความปลอดภัยของเว็บไซต์ด้วยการทดสอบการเจาะระบบ (Penetration Testing)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้เครื่องมือ Web Application Firewall (WAF) เพื่อป้องกันการโจมตีทางเว็บ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	อัปเดตแพลตฟอร์มและปลั๊กอินของเว็บไซต์เป็นประจำ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
15	**ความเสี่ยงจากการรั่วไหลของข้อมูลผ่านอุปกรณ์พกพา (Mobile Device Data Leakage)**	อุปกรณ์พกพาที่ใช้ในองค์กรอาจเป็นช่องทางในการรั่วไหลของข้อมูล หากไม่ได้รับการควบคุมและจัดการที่เหมาะสม	ปานกลาง (Medium)	สูง (High)	1	ใช้ระบบ Mobile Device Management (MDM) เพื่อควบคุมการใช้งานอุปกรณ์พกพาในองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	บังคับใช้การเข้ารหัสข้อมูลบนอุปกรณ์พกพา	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	จำกัดการเข้าถึงข้อมูลสำคัญจากอุปกรณ์พกพาเฉพาะผู้ที่มีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
16	**ความเสี่ยงจากการใช้เครือข่ายสาธารณะ (Public Network Usage Risks)**	การใช้เครือข่ายสาธารณะในการเชื่อมต่อเข้าถึงระบบขององค์กรอาจทำให้ข้อมูลถูกดักฟังหรือขโมยได้ง่ายขึ้น	ปานกลาง (Medium)	ปานกลาง (Medium)	1	ห้ามการเข้าถึงระบบองค์กรผ่านเครือข่ายสาธารณะหากไม่มีการใช้ VPN	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	บังคับใช้การเข้ารหัสข้อมูลสำหรับการเชื่อมต่อผ่านเครือข่ายสาธารณะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ฝึกอบรมพนักงานเกี่ยวกับความเสี่ยงและแนวทางปฏิบัติที่ปลอดภัยในการใช้เครือข่ายสาธารณะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
17	**ความเสี่ยงจากการโจมตีทางกายภาพ (Physical Security Breaches)**	การโจมตีทางกายภาพ เช่น การเข้าถึงห้องเซิร์ฟเวอร์หรือศูนย์ข้อมูลโดยไม่ได้รับอนุญาต อาจทำให้ข้อมูลและระบบที่สำคัญถูกทำลายหรือขโมย	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบควบคุมการเข้าถึงทางกายภาพ (Physical Access Control Systems - PACS)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้ระบบกล้องวงจรปิด (CCTV) และการตรวจสอบการเข้าถึงทางกายภาพ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

					3	ตรวจสอบและบันทึกการเข้าถึงทางกายภาพของพนักงานและผู้เยี่ยมชมเป็นประจำ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
18	ความเสี่ยงจากการโจมตีผ่าน **Social Engineering (Social Engineering Attacks)**	การโจมตีผ่าน Social Engineering อาจทำให้ผู้โจมตีสามารถหลอกลวงพนักงานเพื่อเข้าถึงข้อมูลหรือระบบขององค์กร	สูง (High)	ปานกลาง (Medium)	1	ฝึกอบรมพนักงานเกี่ยวกับการระบุและป้องกันการโจมตีแบบ Social Engineering	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ติดตั้งระบบยืนยันตัวตนที่เข้มงวดในการเข้าถึงข้อมูลหรือระบบ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ทดสอบความรู้และความสามารถของพนักงานในการระบุการโจมตีแบบ Social Engineering เป็นระยะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
19	ความเสี่ยงจากการขาดการสำรองข้อมูลที่เพียงพอ (**Inadequate Data Backup)**	การขาดการสำรองข้อมูลที่เพียงพออาจทำให้ข้อมูลสูญหายถาวรหากเกิดเหตุการณ์ที่ไม่คาดฝัน เช่น การโจมตีทางไซเบอร์หรือการล่มของเซิร์ฟเวอร์	ปานกลาง (Medium)	สูง (High)	1	จัดทำการสำรองข้อมูลอย่างสม่ำเสมอและเก็บรักษาข้อมูลสำรองในสถานที่ที่ปลอดภัย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ทดสอบการกู้คืนข้อมูลจากการสำรองอย่างสม่ำเสมอเพื่อยืนยันความถูกต้อง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้การเข้ารหัสข้อมูลสำหรับการสำรองข้อมูลเพื่อป้องกันการรั่วไหล	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
20	ความเสี่ยงจากการขาดการทดสอบความปลอดภัยเป็นระยะ (**Lack of Regular Security Testing)**	การขาดการทดสอบความปลอดภัยเป็นระยะอาจทำให้ช่องโหว่ที่มีอยู่ในระบบไม่ได้รับการระบุและแก้ไขทันเวลา	ปานกลาง (Medium)	สูง (High)	1	กำหนดแผนการทดสอบความปลอดภัยเป็นระยะ เช่น การทดสอบการเจาะระบบและการสแกนหาช่องโหว่	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จัดทำรายงานและแผนการแก้ไขปัญหาจากผลการทดสอบความปลอดภัย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบและปรับปรุงมาตรการความปลอดภัยตามผลการทดสอบเป็นระยะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

2.4 > กำหนดดัชนีวัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI)

		จัดทำโดย : ทีมประเมินความเสี่ยง | 1/ 05/67

ตารางการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI) สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์

	รายละเอียด	**KRI**	**เกณฑ์ที่ยอมรับได้**
1	**จำนวนเหตุการณ์การโจมตีที่สำเร็จ (Number of Successful Cyber Attacks)**	จำนวนการโจมตีที่สำเร็จต่อเดือน	0 ครั้งต่อเดือน
2	**จำนวนการพยายามเข้าถึงโดยไม่ได้รับอนุญาต (Number of Unauthorized Access Attempts)**	จำนวนการพยายามเข้าถึงที่ถูกบล็อกต่อเดือน	น้อยกว่า 10 ครั้งต่อวัน
3	**ระยะเวลาตอบสนองต่อเหตุการณ์ (Incident Response Time)**	เวลาที่ใช้ในการเริ่มการตอบสนองตั้งแต่ได้รับแจ้ง	น้อยกว่า 30 นาที
4	**เปอร์เซ็นต์การอัปเดตแพตช์ความปลอดภัย (Percentage of Security Patch Updates)**	เปอร์เซ็นต์ของระบบที่อัปเดตแพตช์ล่าสุด	มากกว่า 95%
5	**จำนวนการรายงานเหตุการณ์ไซเบอร์จากพนักงาน (Number of Cybersecurity Incidents Reported by Employees)**	จำนวนรายงานเหตุการณ์ไซเบอร์จากพนักงาน	อย่างน้อย 5 รายงานต่อเดือน
6	**จำนวนบัญชีที่ไม่ใช้งานแต่ยังเปิดอยู่ (Number of Inactive but Open User Accounts)**	จำนวนบัญชีที่ไม่ใช้งานเกิน 30 วันแต่ยังไม่ปิด	0 บัญชี
7	**จำนวนการรั่วไหลของข้อมูล (Number of Data Breaches)**	จำนวนการรั่วไหลของข้อมูลต่อเดือน	0 ครั้งต่อเดือน
8	**เปอร์เซ็นต์พนักงานที่ผ่านการฝึกอบรมด้านไซเบอร์ (Percentage of Employees Trained in Cybersecurity)**	เปอร์เซ็นต์พนักงานที่ผ่านการฝึกอบรมในรอบปี	มากกว่า 90%

9	**ระยะเวลาที่ใช้ในการกู้คืนระบบหลังเหตุการณ์ (System Recovery Time After Incident)**	เวลากู้คืนระบบหลังเกิดเหตุการณ์	ภายใน 4 ชั่วโมง
10	**จำนวนช่องโหว่ที่ตรวจพบในการตรวจสอบความปลอดภัย (Number of Vulnerabilities Detected in Security Audits)**	จำนวนช่องโหว่ที่ตรวจพบจากการตรวจสอบต่อไตรมาส	น้อยกว่า 5 ช่องต่อไตรมาส
11	**จำนวนการหยุดชะงักของระบบที่เกิดจากเหตุการณ์ไซเบอร์ (Number of System Downtimes Due to Cyber Incidents)**	จำนวนการหยุดชะงักต่อเดือน	น้อยกว่า 1 ครั้งต่อเดือน
12	**จำนวนการแจ้งเตือนที่เป็นเท็จ (Number of False Positive Security Alerts)**	จำนวนการแจ้งเตือนที่เป็นเท็จต่อเดือน	น้อยกว่า 5 ครั้งต่อเดือน
13	**จำนวนการใช้งานบัญชีผู้ใช้ที่ไม่มีการอนุญาต (Number of Unauthorized User Account Accesses)**	จำนวนการเข้าถึงบัญชีผู้ใช้โดยไม่ได้รับอนุญาตต่อเดือน	0 ครั้งต่อเดือน
14	**เปอร์เซ็นต์ของข้อมูลสำคัญที่เข้ารหัส (Percentage of Sensitive Data Encrypted)**	เปอร์เซ็นต์ของข้อมูลสำคัญที่ถูกเข้ารหัส	มากกว่า 98%
15	**จำนวนการตอบสนองต่อการทดสอบเจาะระบบที่ล้มเหลว (Number of Failed Responses to Penetration Testing)**	จำนวนเหตุการณ์ที่ตอบสนองไม่สำเร็จต่อการทดสอบเจาะระบบ	น้อยกว่า 1 ครั้งต่อการทดสอบ
16	**จำนวนการเรียกใช้งานบัญชีผู้ใช้โดยไม่ได้รับอนุญาต (Number of Unauthorized Privileged User Actions)**	จำนวนการเรียกใช้งานโดยผู้ใช้ที่มีสิทธิพิเศษโดยไม่ได้รับอนุญาต	0 ครั้งต่อเดือน

17	**เปอร์เซ็นต์ของข้อมูลสำรองที่ตรวจสอบความถูกต้อง (Percentage of Validated Data Backups)**	เปอร์เซ็นต์ของข้อมูลสำรองที่ผ่านการตรวจสอบและสามารถกู้คืนได้	มากกว่า 99%
18	**จำนวนการใช้งานอุปกรณ์ USB ที่ไม่ได้รับอนุญาต (Number of Unauthorized USB Device Usages)**	จำนวนการใช้อุปกรณ์ USB ที่ไม่ได้รับอนุญาตต่อเดือน	0 ครั้งต่อเดือน
19	**จำนวนเหตุการณ์ที่เกี่ยวข้องกับการละเมิดความปลอดภัยของพนักงาน (Number of Employee Security Breaches)**	จำนวนเหตุการณ์ความปลอดภัยที่เกิดจากการละเมิดโดยพนักงาน	น้อยกว่า 1 ครั้งต่อไตรมาส
20	**จำนวนการขอเข้าถึงระบบโดยผู้ให้บริการภายนอก (Number of External Vendor System Access Requests)**	จำนวนการขอเข้าถึงระบบโดยผู้ให้บริการภายนอกต่อเดือน	น้อยกว่า 5 ครั้งต่อเดือน

2.6 > รายงานการประเมินความเสี่ยง

(Risk Assessment Reporting)

, SP 800-30

รายงานการประเมินความเสี่ยง (Risk Assessment Report)

(อ้างอิง Appendix K, NIST SP 800-30 Rev. 1)

วันที่ทำประเมิน: 15 กันยายน 2567

ผู้จัดทำรายงาน : นาย สุรศักดิ์ มั่นคง

ชื่อระบบ: ระบบจัดการข้อมูลลูกค้า (Customer Data Management System - CDMS)

---

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน: 15 กันยายน 2567

วัตถุประสงค์: การประเมินความเสี่ยงของระบบจัดการข้อมูลลูกค้า (CDMS) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่สำคัญและหาวิธีการควบคุมที่เหมาะสม

ขอบเขต:

Tier 3 (ระดับระบบข้อมูล): ประเมินการปกป้องความลับของข้อมูลลูกค้า ระบบจัดการข้อมูลลูกค้า (CDMS) ตั้งอยู่ในศูนย์ข้อมูลหลักขององค์กร

ประเภทของการประเมิน: การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม: ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ ปานกลาง

จำนวนความเสี่ยงที่ระบุ:

ความเสี่ยงต่ำ: 5 รายการ

ความเสี่ยงปานกลาง: 3 รายการ

ความเสี่ยงสูง: 1 รายการ

---

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบ CDMS ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูลลูกค้า
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบ CDMS รวมถึงการจัดการข้อมูลลูกค้าที่มีความสำคัญ
3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

2.2 ข้อสมมติและข้อจำกัดในการประเมิน

สมมติว่าข้อมูลทั้งหมดที่ให้มาสำหรับการประเมินเป็นข้อมูลที่ถูกต้องและครบถ้วน ข้อจำกัดของการประเมินคือไม่สามารถเข้าถึงเซิร์ฟเวอร์เสมือนจริงที่ใช้สำรองข้อมูลได้

2.3 การยอมรับความเสี่ยง

องค์กรมีนโยบายรับความเสี่ยงในระดับ ปานกลาง โดยยอมรับความเสี่ยงบางส่วนเพื่อรักษาประสิทธิภาพในการดำเนินงาน

2.4 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

---

3. รายละเอียดความเสี่ยง (Detailed Risk Assessment)

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม
1	การเข้าถึงข้อมูลลูกค้าโดยไม่ได้รับอนุญาต (Unauthorized Access to Customer Data)	สูง	การสูญเสียความลับของข้อมูลลูกค้าและการละเมิดข้อมูลที่สำคัญ	การควบคุมการเข้าถึงโดยการยืนยันตัวตนสองชั้น	เพิ่มการทดสอบการเจาะระบบทุก 6 เดือน
2	การจัดเก็บข้อมูลสำรองไม่ถูกต้อง (Improper Backup Storage)	ปานกลาง	ข้อมูลสูญหายและไม่สามารถกู้คืนได้	การควบคุมการเข้าถึงโดยการยืนยันตัวตนสองชั้น	ตรวจสอบระบบการสำรองข้อมูลเพิ่มเติม
3	ความล่าช้าในการอัปเดตซอฟต์แวร์ (Delayed Software Updates)	ต่ำ	ระบบมีช่องโหว่ที่อาจถูกโจมตี	มีการอัปเดตเป็นประจำทุกไตรมาส	แนะนำให้ลดระยะเวลาการอัปเดตลงเป็นรายเดือน

---

4. ภาคผนวกสนับสนุน (Supporting Appendices)

4.1 ผลการประเมินโดยละเอียด

ระบบ CDMS ได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตผ่านการควบคุมการเข้าถึงที่เหมาะสม อย่างไรก็ตาม จำเป็นต้องทดสอบและอัปเดตมาตรการเป็นระยะเพื่อป้องกันภัยคุกคามใหม่ ๆ

4.2 ระยะเวลาความถูกต้องของการประเมิน

ผลการประเมินนี้มีอายุการใช้งาน 1 ปี หรือจนกว่าจะมีการเปลี่ยนแปลงระบบ

4.3 การจำแนกความเสี่ยง

ภัยคุกคามที่เกิดจากบุคคลภายนอก (Adversarial Threats): โจมตีด้วยการพยายามเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

ภัยคุกคามที่ไม่เกิดจากบุคคลภายนอก (Non-Adversarial Threats): การสูญหายของข้อมูลจากข้อผิดพลาดในการจัดเก็บข้อมูล

3

แผนการรับมือภัยคุกคามทางไซเบอร์ พร้อมรายงานการแจ้งเหตุการณ์

(Cybersecurity Incident Response Plan)

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure : CIRP)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58) , ประมวลและกรอบ [ข้อ 24.1.1]

1. วัตถุประสงค์ (Objective)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จัดทำขึ้นเพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายเพื่อป้องกัน, จำกัดขอบเขตความเสียหาย, และฟื้นฟูระบบให้กลับมาทำงานตามปกติได้อย่างรวดเร็ว

2. ขอบเขต (Scope)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้ใช้สำหรับเหตุการณ์ภัยคุกคามที่ส่งผลกระทบต่อระบบสำคัญขององค์กร ทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS) โดยมีการครอบคลุมถึงการรับมือกับ …

- การโจมตีทางไซเบอร์ เช่น Malware, Ransomware, Phishing, Distributed Denial of Service (DDoS) หรืออื่นๆ
- การโจมตีทางช่องโหว่ความปลอดภัยในระบบ
- การโจมตีการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

3. โครงสร้างทีมรับมือเหตุการณ์ทางไซเบอร์ (Incident Response Team Structure)

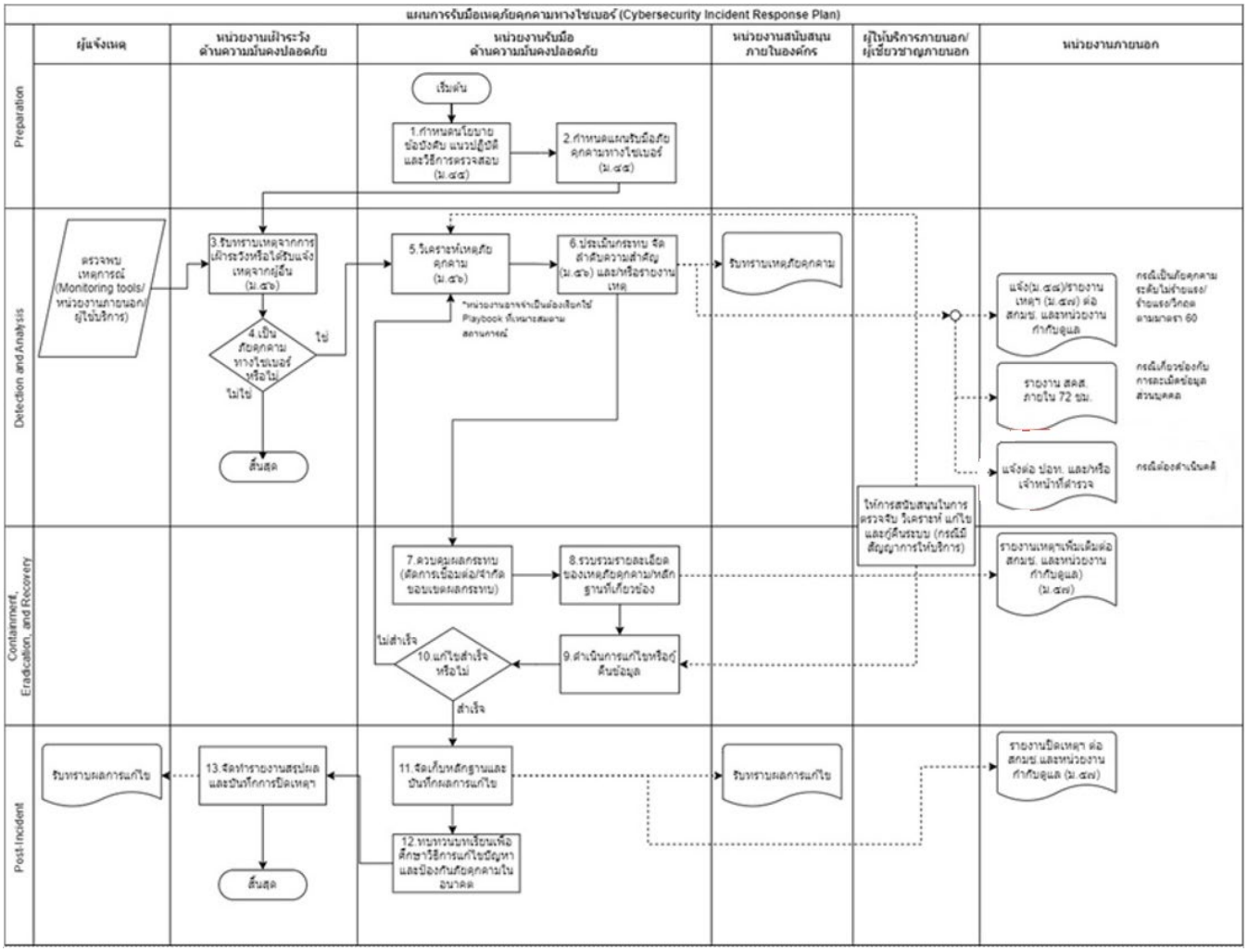
ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

	ตำแหน่ง	หน้าที่และความรับผิดชอบ	รายละเอียดการติดต่อ
1	**หัวหน้าทีม (Team Leader)**	รับผิดชอบการจัดการภาพรวมของเหตุการณ์, การตัดสินใจที่สำคัญ	โทร: 081-xxx-xxxx, อีเมล: a@abc.com
2	**ผู้จัดการด้าน IT**	รับผิดชอบการประเมินระบบ, การกู้คืนระบบและการจำกัดขอบเขต	โทร: 081-xxx-xxxx, อีเมล: b@abc.com
3	**ผู้จัดการด้านความปลอดภัย**	ประสานงานกับผู้เชี่ยวชาญภายนอกและหน่วยงานที่เกี่ยวข้อง	โทร: 081-xxx-xxxx, อีเมล: c@abc.com
4	**ผู้จัดการด้านกฎหมาย**	ให้คำปรึกษาด้านกฎหมายและจัดการด้านการรายงานภายใต้ พ.ร.บ. ไซเบอร์	โทร: 081-xxx-xxxx, อีเมล: d@abc.com
5	**เจ้าหน้าที่ด้านการสื่อสาร**	สื่อสารภายในองค์กรและแจ้งข้อมูลต่อสื่อและหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานอื่นๆ ที่เกี่ยวข้อง	โทร: 081-xxx-xxxx, อีเมล: e@abc.com
6	**ผู้เชี่ยวชาญด้านไซเบอร์ (Cyber Technical Expert)**	วิเคราะห์หลักฐานและตรวจสอบการโจมตีเพื่อแก้ไขปัญหา	โทร: 081-xxx-xxxx, อีเมล: f@abc.com

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)



เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ขั้นตอนการรายงานเหตุการณ์

1. **การตรวจพบเหตุการณ์**: หากมีการตรวจพบเหตุการณ์ความผิดปกติ เช่น การเข้าถึงระบบที่ไม่ได้รับอนุญาต หรือระบบถูกโจมตี ทีม IT จะต้องรายงานต่อหัวหน้าทีมทันที
2. **การประเมินเบื้องต้น**: หัวหน้าทีมและผู้จัดการด้าน IT จะทำการประเมินความร้ายแรงของเหตุการณ์และประสานงานกับทีมรับมือเหตุการณ์
3. **การจำกัดขอบเขต** : ทีม IT จะทำการจำกัดขอบเขตของเหตุการณ์เพื่อป้องกันการกระจายผลกระทบต่อระบบเพิ่มเติม
4. **การแจ้งต่อหน่วยงานที่เกี่ยวข้อง**
    - **หน่วยงานภายใน**: แจ้งหัวหน้าหน่วยงานต่าง ๆ ที่เกี่ยวข้อง
    - **หน่วยงานภายนอก**: หากเป็นเหตุการณ์สำคัญ ให้รายงานต่อหน่วยงานควบคุมหรือกำกับดูแล หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) ตาม พ.ร.บ. ไซเบอร์ ภายใน 24 ชั่วโมง
5. **การดำเนินการกู้คืน (Recovery)**: หลังจากจำกัดขอบเขตเหตุการณ์ ทีม IT จะเริ่มกระบวนการกู้คืนระบบตามแผนที่กำหนดไว้ เช่น การกู้คืนข้อมูลจากระบบสำรอง
6. **การทบทวนเหตุการณ์ (Post-Incident Review)**: หลังจากเหตุการณ์สิ้นสุด ทีมรับมือจะจัดทำรายงานการทบทวนเพื่อวิเคราะห์สาเหตุและปรับปรุงแผนการป้องกัน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

5. เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activation Criteria and Procedures)

เกณฑ์การเรียกใช้งาน

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จะถูกเรียกใช้งานเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น

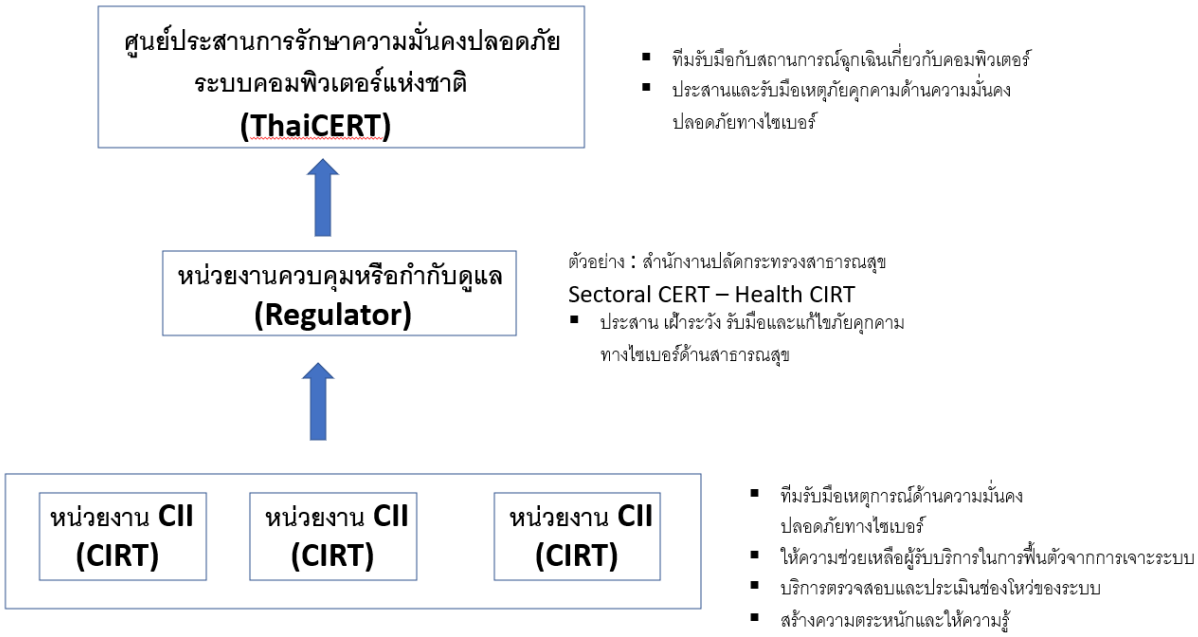
- การโจมตีทางไซเบอร์
- การรั่วไหลของข้อมูลสำคัญ
- การเข้าถึงระบบโดยไม่ได้รับอนุญาต

ขั้นตอนการเรียกใช้งาน

1. แจ้งเตือนทีม **Cyber Incident Response Team (CIRT)** ผ่านโทรศัพท์และอีเมล
2. เปิดใช้แผนการตอบสนอง โดยทีมรับมือเริ่มดำเนินการตามขั้นตอนที่กำหนด
3. แจ้งเตือนบุคลากรที่เกี่ยวข้องภายในองค์กรถึงสถานการณ์ฉุกเฉิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only



6. ขั้นตอนจำกัดขอบเขต (Containment)

ขั้นตอนการจำกัดขอบเขต

1. แยกระบบที่ได้รับผลกระทบออกจากเครือข่ายหลักเพื่อป้องกันการแพร่กระจายไปยังระบบอื่น
2. ประเมินความเสียหายและระบุว่ามีระบบใดที่เกี่ยวข้อง
3. ดำเนินการแก้ไขเบื้องต้น เช่น การปิดพอร์ตที่ถูกโจมตีหรือการบล็อก IP ที่มีพฤติกรรมไม่พึงประสงค์
4. เก็บข้อมูลสำคัญจากระบบที่ได้รับผลกระทบเพื่อใช้ในกระบวนการสอบสวน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

7. การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

ขั้นตอนการกู้คืน

1. ตรวจสอบและซ่อมแซมระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าไม่มีช่องโหว่ที่ยังไม่ได้รับการแก้ไข
2. ฟื้นฟูระบบโดยการกู้คืนข้อมูลจากระบบสำรองล่าสุด (Backup)
3. ทดสอบระบบทั้งหมดเพื่อยืนยันว่าระบบปลอดภัยและสามารถทำงานได้ปกติ
4. ตรวจสอบการทำงานของระบบสำรองเพื่อให้แน่ใจว่าข้อมูลที่กู้คืนครบถ้วน

8. ขั้นตอนในการสอบสวน (Investigation)

ขั้นตอนการสอบสวน

1. เก็บหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อก การจับภาพหน้าจอ การตรวจสอบข้อมูลเครือข่าย
2. วิเคราะห์สาเหตุของเหตุการณ์ เช่น ตรวจสอบวิธีการที่ผู้โจมตีใช้ในการเข้าถึงระบบ
3. ระบุผู้ที่อาจรับผิดชอบต่อเหตุการณ์ เช่น การระบุที่อยู่ IP หรือการตรวจสอบพฤติกรรมที่ผิดปกติ
4. จัดทำรายงานการสอบสวนและเสนอแนวทางการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

9. การเก็บรักษาหลักฐาน (Preservation of Evidence)

การจัดเก็บหลักฐาน

1. บันทึกข้อมูลจากระบบที่ได้รับผลกระทบ เช่น ล็อกไฟล์ การจับภาพหน้าจอ และอุปกรณ์เครือข่ายที่เกี่ยวข้อง
2. จัดเก็บอุปกรณ์ที่มีหลักฐานไว้ในที่ปลอดภัยเพื่อป้องกันการดัดแปลง เช่น จัดเก็บในตู้ที่มีการล็อกและการควบคุมการเข้าถึง
3. ทำรายการหลักฐานทั้งหมดที่ถูกเก็บรวบรวม พร้อมระบุวันที่และเวลาที่ได้รับหลักฐาน

10. ระเบียบวิธีการมีส่วนร่วมกับบุคคลภายนอก (Engagement Protocols)

ผู้ที่เกี่ยวข้อง

- **บริษัทที่ปรึกษา** : บริษัท A โทร. 02-111-XXXX
- **หน่วยงานบังคับใช้กฎหมาย**: นาย C โทร. 02-111-XXXX

ขั้นตอนการมีส่วนร่วม

1. ติดต่อบุคคลภายนอกตามความจำเป็น เช่น บริษัทที่ปรึกษา สำหรับการวิเคราะห์หาสาเหตุ
2. ประสานงานกับหน่วยงานบังคับใช้กฎหมาย หากมีความจำเป็นในการดำเนินคดี
3. ส่งมอบหลักฐานที่เกี่ยวข้องให้กับผู้เชี่ยวชาญภายนอก พร้อมรายการหลักฐานทั้งหมดเพื่อใช้ในการตรวจสอบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

11. กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

ขั้นตอนการทบทวน

1. จัดประชุมทีม CIRT ภายใน 7 วันหลังจากเหตุการณ์สิ้นสุด เพื่อประเมินกระบวนการตอบสนอง
2. ประเมินผลการดำเนินการ เช่น ความเร็วในการตอบสนอง, การกู้คืนระบบ, และการจำกัดขอบเขตเหตุการณ์
3. ระบุข้อบกพร่องและข้อเสนอแนะสำหรับการปรับปรุงกระบวนการตอบสนอง
4. เสนอมาตรการปรับปรุงแผนรับมือภัยคุกคาม เพื่อให้มีประสิทธิภาพมากขึ้นในการป้องกันเหตุการณ์ในอนาคต

12. การสื่อสารและการทบทวนแผน (Communication and Plan Review)

การสื่อสารแผน

- สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้กับบุคลากรที่เกี่ยวข้องทั้งหมดผ่านการอบรมและเอกสารแผน
- จัดอบรมพนักงานอย่างสม่ำเสมอเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน

การทบทวนแผน

- ทบทวนแผนการรับมือภัยคุกคามทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมทางไซเบอร์
- ปรับปรุงแผนตามผลการทบทวนและการฝึกซ้อมแผนรับมือภัยคุกคาม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์
2. โครงสร้างทีมรับมือเหตุการณ์
3. รายงานสรุปเหตุการณ์
4. แผนการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : ทีมเฝ้าระวังทางไซเบอร์ (SOC)

จัดทำเมื่อ : 1 ตุลาคม 2567

รายงานการแจ้งเหตุการณ์ภัยคุกคามทางไซเบอร์

(Incident Report: Ransomware Attack)

1. ข้อมูลทั่วไป (General Information)

- **ชื่อเหตุการณ์:** การโจมตีด้วย Ransomware
- **วันที่และเวลาที่ตรวจพบเหตุการณ์:** 8 กันยายน 2567, เวลา 10:30 น.
- **ผู้รายงาน:** นายสมชาย (IT Security Team)
- **ประเภทของเหตุการณ์:** การโจมตีด้วย Ransomware
- **ระบบที่ได้รับผลกระทบ:** ระบบฐานข้อมูลลูกค้า (CRM), ระบบสำรองข้อมูล
- **หน่วยงานที่เกี่ยวข้อง:** ฝ่าย IT, ฝ่ายกฎหมาย, ฝ่ายปฏิบัติการ

2. ขั้นตอนการเรียกใช้งาน (Activation)

- **เกณฑ์การเรียกใช้งาน:** พบการโจมตี Ransomware ที่เข้ารหัสข้อมูลทั้งหมดในระบบ CRM และระบบสำรองข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต
- **ขั้นตอนการเรียกใช้งาน**
    1. **แจ้งเตือนทีม CIRT:** ทีม IT ตรวจพบเหตุการณ์และแจ้งเตือนทีม CIRT ผ่านอีเมลและโทรศัพท์
    2. **Activate แผนการตอบสนอง:** หัวหน้าทีม CIRT อนุมัติการเปิดใช้แผนการตอบสนองภัยคุกคามทางไซเบอร์
    3. **แจ้งผู้บริหารและบุคลากรที่เกี่ยวข้อง:** แจ้งผู้บริหารและทีมกฎหมายเกี่ยวกับเหตุการณ์และเริ่มกระบวนการตอบสนอง

3. ขั้นตอนการจำกัดขอบเขต (Containment)

- **เวลาเริ่มต้นการจำกัดขอบเขต:** 8 กันยายน 2567, เวลา 11:00 น.
- **ขั้นตอนที่ดำเนินการ**
    1. **แยกระบบ CRM** ออกจากเครือข่ายภายในทันที เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังระบบอื่น
    2. **บล็อก IP** และผู้ใช้งานที่เกี่ยวข้องกับการโจมตีเพื่อจำกัดการเข้าถึงที่ไม่ได้รับอนุญาต
    3. **ประเมินระบบที่เกี่ยวข้อง:** ตรวจสอบว่าเซิร์ฟเวอร์สำรองข้อมูลถูกโจมตีและได้รับการเข้ารหัสข้อมูล
    4. **แก้ไขเบื้องต้น:** ปิดการทำงานของพอร์ตที่ถูกโจมตีและใช้ระบบสำรองสำหรับการดำเนินการบางส่วน

4. ขั้นตอนการกู้คืนระบบ (Recovery Process)

- **เวลาเริ่มต้นการกู้คืนระบบ:** 8 กันยายน 2567, เวลา 13:00 น.
- **ขั้นตอนการดำเนินการ**
    1. **ซ่อมแซมระบบที่ได้รับผลกระทบ:** ทีม IT ซ่อมแซมระบบ CRM ที่ถูกเข้ารหัส โดยการนำซอฟต์แวร์ความปลอดภัยมาใช้ในการลบ Ransomware
    2. **กู้คืนข้อมูลจากระบบสำรอง:** กู้คืนข้อมูลที่ไม่ได้รับผลกระทบจากการสำรองข้อมูลที่ได้รับการปกป้อง
    3. **ทดสอบระบบ:** ทีม IT ทดสอบระบบทั้งหมดเพื่อให้แน่ใจว่าไม่มีมัลแวร์หลงเหลืออยู่ และระบบสามารถทำงานได้ตามปกติ
    4. **เปิดใช้งานระบบอีกครั้ง:** เปิดใช้งานระบบ CRM และแจ้งให้ผู้ใช้งานทราบว่าระบบพร้อมใช้งานอีกครั้ง

5. ขั้นตอนการสอบสวน (Investigation)

- **เวลาเริ่มต้นการสอบสวน:** 9 กันยายน 2567, เวลา 09:00 น.
- **ขั้นตอนการสอบสวน**
    1. **เก็บรวบรวมหลักฐาน:** ทีมสอบสวน เก็บรวบรวมหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อกของเซิร์ฟเวอร์, การตรวจสอบการเข้าถึงเครือข่าย
    2. **วิเคราะห์สาเหตุของเหตุการณ์:** วิเคราะห์ว่าการโจมตีเริ่มต้นจากช่องโหว่ใดและวิธีที่ผู้โจมตีใช้ เช่น การเปิดอีเมลที่มีลิงก์อันตราย
    3. **ระบุผู้รับผิดชอบ:** ตรวจสอบการเชื่อมต่อจากภายนอกและ IP ที่เกี่ยวข้องกับการโจมตี เพื่อระบุผู้โจมตี
    4. **จัดทำรายงานการสอบสวน:** ทีมสอบสวน จัดทำรายงานสรุปสาเหตุและกระบวนการโจมตี พร้อมแนวทางการป้องกันเหตุการณ์ในอนาคต

6. การเก็บรักษาหลักฐาน (Preservation of Evidence)

- **เวลาเริ่มต้นการเก็บรักษาหลักฐาน:** 9 กันยายน 2567, เวลา 10:30 น.
- **ขั้นตอนการเก็บรักษาหลักฐาน**
    1. **บันทึกข้อมูล:** เก็บล็อกไฟล์ทั้งหมดและการจับภาพหน้าจอจากระบบที่ถูกโจมตี
    2. **จัดเก็บอุปกรณ์สำคัญ:** จัดเก็บอุปกรณ์ที่เกี่ยวข้อง เช่น เซิร์ฟเวอร์ที่มีการโจมตีในตู้เซฟที่มีการควบคุมการเข้าถึง
    3. **ทำรายการหลักฐาน:** ทำรายการหลักฐานที่ถูกเก็บไว้ และลงบันทึกวันเวลาที่ได้รับและจัดเก็บหลักฐาน
    4. **ส่งมอบหลักฐานให้บุคคลภายนอก:** หากมีความจำเป็นในการดำเนินคดี ให้ประสานงานกับหน่วยงานบังคับใช้กฎหมายและส่งมอบหลักฐานให้กับผู้ที่เกี่ยวข้อง

7. ข้อสรุปและการดำเนินการเพิ่มเติม

- **การทบทวนและปรับปรุง**
    1. ทีม CIRT ได้จัดประชุมเพื่อทบทวนเหตุการณ์ ภายใน 7 วันหลังเหตุการณ์สิ้นสุด
    2. ผลการทบทวนระบุข้อบกพร่องในการตอบสนอง เช่น การตรวจจับที่ล่าช้าและการแจ้งเตือนผู้ใช้งานที่ไม่เพียงพอ
    3. เสนอการปรับปรุงแผนการตอบสนองต่อเหตุการณ์เพื่อป้องกันการโจมตีที่คล้ายคลึงในอนาคต

8. รายละเอียดเพิ่มเติม (Appendices)

- รายชื่อผู้ที่เกี่ยวข้องในเหตุการณ์
    - นาย A , หน่วยงาน …. , ติดต่อ ….
    - นาย B , หน่วยงาน …. , ติดต่อ ….
    - นาย C , หน่วยงาน …. , ติดต่อ ….
- ล็อกไฟล์และหลักฐานทางดิจิทัลที่เกี่ยวข้อง
    - Audit Logging of Firewall

กรอบมาตรฐาน

2. กรอบมาตรฐาน

Govern

1. Cybersecurity Management System Policy (CSMS Policy)
2. Cybersecurity Risk Management Policy
3. Security Baseline Configuration Standard Policy
4. Remote Connection Policy
5. Removable Storage Media Policy
6. Information Sharing Policy

Identify

1. Asset Management Procedure
2. Risk Assessment and Risk Management Strategy Procedure
3. Vulnerability Assessment and Penetration Testing Procedure
4. Third Part Management Procedure

Respond

1. Cybersecurity Incident Response Plan
2. Crisis Communication Plan Procedure
3. Cybersecurity Exercise Procedure

Protect

1. Access Control Management Procedure
2. System Hardening Procedure
3. Remote Connection Procedure
4. Removable Storage Media Procedure
5. Cybersecurity Awareness Procedure
6. Information Sharing Procedure
7. Change Management Process Procedure

Recover

1. Cybersecurity Resilience and Recovery Procedure
2. Business Continuity Plan Procedure / Manual

Detect

1. Cyber Threat Detection and Monitoring Procedure

GOVERN

Govern

1. Cybersecurity Management System Policy (CSMS Policy)
2. Cybersecurity Risk Management Policy
3. Security Baseline Configuration Standard Policy
4. Remote Connection Policy
5. Removable Storage Media Policy
6. Information Sharing Policy

Logo	**นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)**	**รหัสเอกสาร**	**CSMS-Policy-01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ส.ค. 2568**
		ชั้นความลับเอกสารของเอกสาร	**Public**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.45, ม.46, ม.54, ม.56), นโยบาย [ข้อ 1.1, ข้อ 1.3, ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2], ประมวลและกรอบ [ข้อ 18]

1. วัตถุประสงค์ (Objective)

นโยบายนี้จัดทำขึ้นเพื่อกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ในองค์กร โดยมีวัตถุประสงค์เพื่อปกป้องทรัพย์สินสารสนเทศ โครงสร้างพื้นฐาน และข้อมูลที่มีความสำคัญจากภัยคุกคามทางไซเบอร์ รวมถึงการสร้างความมั่นใจในการดำเนินธุรกิจขององค์กรอย่างต่อเนื่องและปลอดภัย

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมทุกระบบ ข้อมูล โครงสร้างพื้นฐานสารสนเทศ และกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในองค์กร รวมถึงพนักงาน ผู้บริหาร ผู้ใช้งาน ผู้ให้บริการ และผู้ที่มีส่วนเกี่ยวข้องทั้งหมดในองค์กร

3. ความสอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (Alignment with Cybersecurity Policy and Plan)

- องค์กรจะดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้มั่นใจว่าการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สอดคล้องกับกฎหมาย ข้อบังคับ และมาตรการที่เกี่ยวข้อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

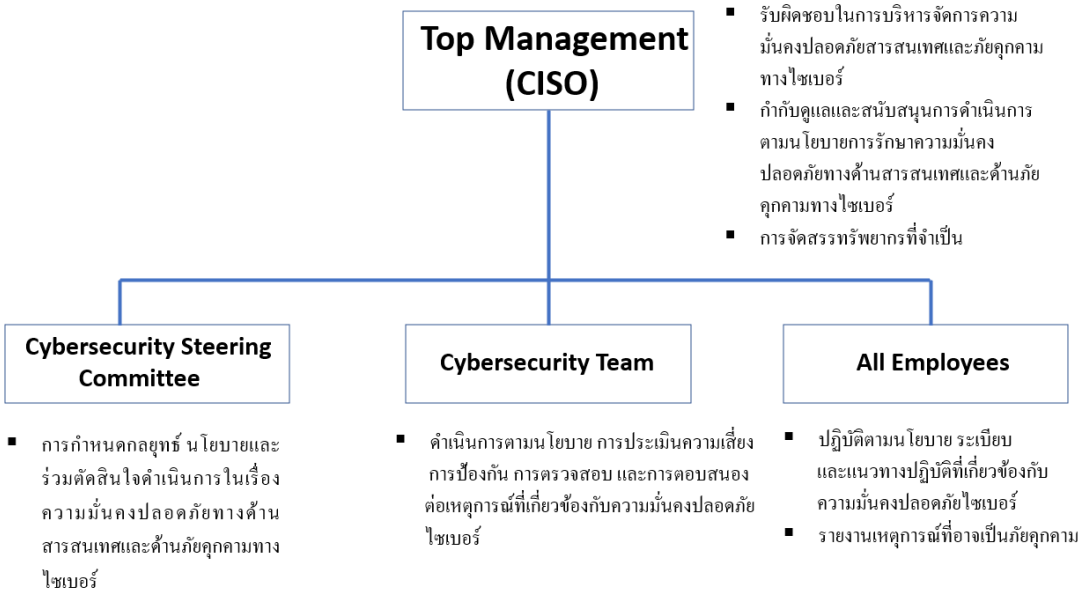
Logo	นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)	รหัสเอกสาร	CSMS-Policy-01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ส.ค. 2568
		ชั้นความลับเอกสารของเอกสาร	Public

- นโยบายนี้ได้รับการออกแบบมาเพื่อสนับสนุนและเสริมสร้างมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจส่งผลกระทบต่อการดำเนินงานและความมั่นคงปลอดภัยของหน่วยงานที่รับผิดชอบ

4. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

โครงสร้างคณะทำงานระบบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSMS Organization Structure Chart)

Cybersecurity Management System Organization Chart



*** ควรมีการระบุชื่อ ผู้ที่อยู่ในแต่ละกลุ่มด้วย ***

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- 4.1 ผู้บริหารระดับสูง (Top Management - CISO): รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์ พร้อมทั้งกำกับดูแลและสนับสนุนการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศและด้านภัยคุกคามทางไซเบอร์ รวมถึงการจัดสรรทรัพยากรที่จำเป็น,

CISO – Chief Information Security Officer มีความเป็นอิสระจากงานด้านการปฏิบัติงาน (IT Operation) และงานด้านพัฒนาระบบสารสนเทศ (IT Development)

- 4.2 คณะกรรมการบริหารจัดการและกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Steering Committee): รับผิดชอบในการกำหนดกลยุทธ์ นโยบาย และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยทางด้านสารสนเทศและด้านภัยคุกคามทางไซเบอร์
- 4.3 ทีมรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Team): รับผิดชอบในการดำเนินการตามนโยบาย การประเมินความเสี่ยง การป้องกัน การตรวจสอบ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- 4.4 พนักงานทุกคน (All Employees): มีหน้าที่ในการปฏิบัติตามนโยบาย ระเบียบ และแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงการรายงานเหตุการณ์ที่อาจเป็นภัยคุกคาม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management)

- 5.1 การประเมินความเสี่ยง (Risk Assessment): องค์กรจะดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อระบุ วิเคราะห์ และประเมินค่าความเสี่ยงที่อาจเกิดขึ้น
- 5.2 การจัดการความเสี่ยง (Risk Treatment): องค์กรจะดำเนินการควบคุมและลดความเสี่ยงโดยใช้มาตรการป้องกันที่เหมาะสม เพื่อให้ความเสี่ยงเหลืออยู่ในระดับที่ยอมรับได้

6. มาตรการการป้องกัน รับมือ และลดความเสี่ยง (Prevention, Response, and Risk Mitigation Measures)

- 6.1 การป้องกัน (Prevention): องค์กรจะนำมาตรการป้องกันที่ทันสมัยและเหมาะสมมาใช้ เพื่อปกป้องข้อมูลและโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์ เช่น การใช้ไฟร์วอลล์ การเข้ารหัสข้อมูล และการควบคุมการเข้าถึง
- 6.2 การรับมือ (Incident Response): องค์กรจะพัฒนาและนำแผนตอบสนองต่อเหตุการณ์ทางไซเบอร์มาใช้ เพื่อให้สามารถรับมือและจัดการกับเหตุการณ์ทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ
- 6.3 การลดความเสี่ยง (Risk Mitigation): องค์กรจะดำเนินการลดความเสี่ยงที่ระบุไว้ให้เหลือน้อยที่สุด โดยการปรับปรุงมาตรการป้องกันและการฝึกอบรมพนักงานอย่างสม่ำเสมอ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

7. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

- 7.1 การเข้าถึงข้อมูล (Data Access Control): องค์กรจะกำหนดมาตรการควบคุมการเข้าถึงข้อมูลให้เป็นไปตามหลักการสิทธิ์น้อยที่สุด (Least Privilege) และจำเป็นต้องทราบ (Need to Know) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- 7.2 การเข้ารหัสข้อมูล (Data Encryption): ข้อมูลที่มีความสำคัญและข้อมูลส่วนบุคคลจะต้องถูกเข้ารหัสทั้งขณะเก็บรักษาและขณะส่งผ่านเครือข่าย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

8. การรักษาความมั่นคงปลอดภัยของระบบ (System Security)

- 8.1 การป้องกันระบบ (System Protection): องค์กรจะดำเนินการติดตั้งและบำรุงรักษามาตรการป้องกันระบบ เช่น ไฟร์วอลล์ การตรวจจับและป้องกันการบุกรุก (IDS/IPS) และซอฟต์แวร์ป้องกันมัลแวร์
- 8.2 การจัดการแพตช์และอัปเดต (Patch Management and Updates): ระบบและซอฟต์แวร์ทั้งหมดจะต้องได้รับการอัปเดตแพตช์และการรักษาความปลอดภัยอย่างสม่ำเสมอ เพื่อลดช่องโหว่ที่อาจถูกใช้ในการโจมตี

9. การบริหารจัดการเหตุการณ์ทางไซเบอร์ (Cyber Incident Management)

- 9.1 การตรวจจับเหตุการณ์ (Incident Detection): องค์กรจะใช้เครื่องมือและระบบตรวจสอบเพื่อเฝ้าระวังและตรวจจับเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้นอย่างต่อเนื่อง
- 9.2 การตอบสนองต่อเหตุการณ์ (Incident Response): องค์กรจะพัฒนาและดำเนินการตามแผนตอบสนองต่อเหตุการณ์ทางไซเบอร์ (Incident Response Plan) ซึ่งรวมถึงการกักกัน การวิเคราะห์ และการฟื้นฟูระบบที่ได้รับผลกระทบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- 9.3 การรายงานเหตุการณ์ (Incident Reporting): เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์จะต้องถูกรายงานต่อผู้บริหารและหน่วยงานที่เกี่ยวข้องตามขั้นตอนที่กำหนด

10. การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

- 10.1 การฝึกอบรมพนักงาน (Employee Training): องค์กรจะจัดฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพนักงานทุกคนอย่างสม่ำเสมอ เพื่อให้พนักงานมีความรู้และทักษะในการปฏิบัติตามนโยบายและการป้องกันภัยคุกคามทางไซเบอร์
- 10.2 การสร้างความตระหนัก (Awareness Campaigns): องค์กรจะดำเนินการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ผ่านการสื่อสารและกิจกรรมต่าง ๆ เพื่อให้พนักงานตระหนักถึงความสำคัญของการรักษาความปลอดภัยข้อมูลและระบบ

11. การปฏิบัติตามกฎหมายและมาตรฐาน (Compliance with Laws and Standards)

- 11.1 การปฏิบัติตามข้อกำหนด (Regulatory Compliance): องค์กรจะปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด
- 11.2 การประเมินและตรวจสอบ (Assessment and Audits): องค์กรจะดำเนินการประเมินและตรวจสอบภายในเป็นระยะเพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างเหมาะสม

12. การจัดทำเอกสารและการจัดเก็บข้อมูล (Documentation and Record Keeping)

- 12.1 การจัดทำเอกสาร (Documentation): องค์กรจะดำเนินการจัดทำเอกสารที่เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วนและถูกต้อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- 12.2 การจัดเก็บและเข้าถึงข้อมูล (Record Keeping and Access): เอกสารและข้อมูลทั้งหมดจะถูกจัดเก็บอย่างปลอดภัย และจะต้องสามารถเข้าถึงได้เมื่อจำเป็นสำหรับการตรวจสอบหรือใช้งานในอนาคต

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)**	**รหัสเอกสาร**	**CSMS-Policy-02**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

1. วัตถุประสงค์ (Objective)

วัตถุประสงค์ของนโยบายนี้คือเพื่อกำหนดกรอบการทำงานสำหรับการระบุ ประเมิน และบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้แน่ใจว่าโครงสร้างพื้นฐานและบริการที่สำคัญได้รับการปกป้องจากภัยคุกคามไซเบอร์ นโยบายนี้สอดคล้องกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย โดยเฉพาะ **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และ **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงหน่วยงาน แผนก และพันธมิตรภายนอกทั้งหมดที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งรวมถึง …

- โครงสร้างพื้นฐานสำคัญด้านสารสนเทศ
- ข้อมูลและเครือข่ายที่สำคัญ
- ผู้ให้บริการและผู้จำหน่ายภายนอก

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

3. หลักการบริหารความเสี่ยง (Risk Management Principle)

องค์กรจะใช้หลักการดังต่อไปนี้ในการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

- **การระบุความเสี่ยงเชิงรุก**: การระบุความเสี่ยงด้านไซเบอร์ผ่านการประเมินอย่างสม่ำเสมอและการวิเคราะห์ข้อมูลภัยคุกคาม
- **การประเมินความเสี่ยง**: การประเมินผลกระทบและความเป็นไปได้ของความเสี่ยงที่ระบุ โดยเน้นที่ภัยคุกคามที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานหรือข้อมูลสำคัญ
- **การลดความเสี่ยง**: ดำเนินการลดหรือขจัดความเสี่ยง โดยจัดลำดับความสำคัญของภัยคุกคาม
- **การติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง**: การติดตามและทบทวนความเสี่ยงด้านไซเบอร์มีการกระทำอย่างต่อเนื่อง หรืออย่างน้อย ปีละ 1 ครั้ง โดยผ่านระบบอัตโนมัติและการตรวจสอบด้วยตนเองอย่างสม่ำเสมอ

4. ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

นโยบายนี้จะสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

- **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**: ปฏิบัติตามข้อกำหนดในการปกป้องโครงสร้างพื้นฐานสำคัญและการรายงานเหตุการณ์
- **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**: เป็นการพัฒนาความมั่นคงปลอดภัยทางทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติและเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ทีมงานด้านความมั่นคงปลอดภัยไซเบอร์**: รับผิดชอบในการดำเนินการประเมินความเสี่ยง ดำเนินมาตรการแก้ไข และติดตามความเสี่ยงอย่างต่อเนื่อง
- **ฝ่ายบริหาร**: ต้องมั่นใจว่าการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ถูกรวมเข้ากับกรอบการบริหารจัดการทั่วไปและรายงานความสอดคล้องกับหน่วยงานที่เกี่ยวข้อง
- **เจ้าหน้าที่กำกับดูแล**: รับผิดชอบในการตรวจสอบและให้แน่ใจว่าปฏิบัติตามกฎหมายและระเบียบข้อบังคับตามที่ระบุใน **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

6. กระบวนการระบุและประเมินความเสี่ยง (Risk Identification and Risk Assessment)

- **ทะเบียนความเสี่ยง**: จะมีการบันทึกความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดในทะเบียนความเสี่ยง โดยจะมีการประเมินแต่ละความเสี่ยง เช่น
    - **ความเป็นไปได้**: ความน่าจะเป็นที่ความเสี่ยงจะเกิดขึ้น
    - **ผลกระทบ**: ความเสียหายหรือการรบกวนที่อาจเกิดขึ้นจากความเสี่ยง
    - **มาตรการควบคุม**: ขั้นตอนที่มีอยู่ในปัจจุบัน สามารถเพื่อบรรเทาความเสี่ยงนั้นๆ
- **การจัดประเภทความเสี่ยง**: ความเสี่ยงจะถูกจัดหมวดหมู่ตามระดับ เช่น สูง กลาง ต่ำ ตามความรุนแรงที่ประเมิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

7. การจัดการความเสี่ยง (Risk Treatment)

- **การหลีกเลี่ยง**: ความเสี่ยงที่สามารถหลีกเลี่ยงได้จะถูกขจัดออกโดยการเปลี่ยนแปลงระบบหรือกระบวนการในการปฏิบัติ
- **การลดความเสี่ยง**: ลดความเสี่ยงโดยการดำเนินมาตรการควบคุมเพิ่มเติม เช่น การเข้ารหัสไฟล์ วางไฟร์วอลล์ และฝึกอบรมพนักงาน
- **การยอมรับ**: มีการกำหนดความเสี่ยงในระดับต่ำที่ยอมรับได้ โดยไม่ต้องมีมาตรการเพิ่มเติม
- **การโอนความเสี่ยง**: โอนความเสี่ยงให้หน่วยงานหรือองค์กรภายนอก โดยการทำสัญญาหรือประกันภัยในกรณีที่เหมาะสม

8. การตอบสนองและรายงานเหตุการณ์ (Response and Incident Reporting)

- ทุกเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์จะต้องรายงานต่อทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ทันที
- เหตุการณ์ที่รุนแรงที่ส่งผลต่อโครงสร้างพื้นฐานสำคัญจะถูกส่งต่อไปยังผู้บริหารระดับสูงและหน่วยงานควบคุมหรือกำกับดูแล ตาม **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

9. การปรับปรุงอย่างต่อเนื่อง (Continuously Improvement)

- จะมีการตรวจสอบและประเมินผลนโยบายฯอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ากรอบการบริหารความเสี่ยงนั้นยังคงมีประสิทธิภาพ
- นโยบายฯนี้จะได้รับการปรับปรุงเพื่อให้ทันกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์

10. การปฏิบัติตามและการกำกับดูแล (Operate and Governance)

นโยบายฯนี้จะได้รับการตรวจสอบอย่างต่อเนื่องเพื่อให้สอดคล้องกับยุทธศาสตร์ไซเบอร์แห่งชาติหรือนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) รวมถึงข้อกำหนดของ **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** การไม่ปฏิบัติตามนโยบายนี้จะมีบทลงโทษตามข้อกำหนดขององค์กร

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

IDENTIFY

Identify

1. กระบวนการจัดการทรัพย์สิน
   (**Asset Management Procedure**)
   - ทะเบียนทรัพย์สิน, ตรวจปีละ **1** ครั้ง
   - การประเมินความเสี่ยงทรัพย์สินและการบริการที่สำคัญ, ตรวจปีละ **1** ครั้ง
2. กระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง
   (**Risk Assessment and Risk Management Strategy Procedure**)
   - ทะเบียนความเสี่ยง, ตรวจปีละ **1** ครั้ง
   - การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์, ตรวจปีละ **1** ครั้ง
3. กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ

(**Vulnerability Assessment and Penetration Testing Procedure**)

- การประเมินช่องโหว่ แยกตาม **IT (Information Technology)** และ **ICS (Industrial Control System)**
  - Host Security Assessment, Network Security Assessment and Architecture Security Review
- ขั้นตอนการทดสอบเจาะระบบ **(Penetration Testing)** ใช้ **Outsource** ได้, ตรวจปีละ **1** ครั้ง
- รายงานสรุปผลการทดสอบเจาะระบบ

Identify

ประเมินช่องโหว่ของบริการที่สำคัญ

1. ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
2. ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

ต้องพิจารณา 3 ด้าน

- การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

Identify

4. กระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)

- กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของผู้ให้บริการภายนอก
- ข้อตกลงระดับการให้บริการ **(SLA)**
- เงื่อนไขของสัญญากับผู้ให้บริการภายนอก
- การประเมินความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ **(Risk Assessment for services and product supply chain)**

1. กระบวนการจัดการทรัพย์สิน

(Asset Management Procedure)

Logo	**ระเบียบกระบวนการจัดการทรัพย์สิน (Asset Management Procedure)**	**รหัสเอกสาร**	**CSMS-Identify -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดการทรัพย์สิน (Asset Management Procedure)	รหัสเอกสาร	CSMS-Identify -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการจัดการทรัพย์สิน (Asset Management Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.1.1, ข้อ 21.1.2, ข้อ 21.1.3, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1, ข้อ 21.3.2, ข้อ 21.3.3, ข้อ 21.3.9]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าทรัพย์สินของบริการที่สำคัญขององค์กรได้รับการจัดการอย่างเหมาะสมและมีการบันทึกข้อมูลที่ครบถ้วนและเป็นปัจจุบัน รวมถึงการระบุ การติดตาม และการประเมินความเสี่ยงของทรัพย์สินเหล่านี้อย่างสม่ำเสมอ

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมทรัพย์สินทุกประเภทที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ระบบเครือข่าย และทรัพยากรทางเทคโนโลยีสารสนเทศอื่น ๆ ที่มีความสำคัญต่อการดำเนินงานขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการกำกับดูแลและสนับสนุนการดำเนินการตามกระบวนการจัดการทรัพย์สิน
- **ทีม IT (IT Team)**: รับผิดชอบในการจัดทำ ดูแลรักษา และอัปเดตทะเบียนทรัพย์สิน รวมถึงการตรวจสอบและประเมินความเสี่ยงของทรัพย์สิน
- **ผู้ใช้งานระบบ (System Users)**: มีหน้าที่ในการรายงานการเปลี่ยนแปลงที่เกิดขึ้นกับทรัพย์สินที่ใช้งานต่อทีม IT เพื่อให้มีการอัปเดตข้อมูลในทะเบียนทรัพย์สิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. การจัดทำและดูแลทะเบียนทรัพย์สิน (Inventory Management)

- **4.1 การจัดทำทะเบียนทรัพย์สิน (Asset Inventory List)**
  - **ขั้นตอน**
    - จัดทำทะเบียนทรัพย์สินที่ระบุรายละเอียดของทรัพย์สินทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร
    - ข้อมูลที่ต้องบันทึกในทะเบียนทรัพย์สิน ได้แก่
      - ชื่อหรือคำอธิบายของทรัพย์สิน
      - ฟังก์ชันที่สำคัญของทรัพย์สิน
      - การจัดลำดับความสำคัญของทรัพย์สิน
      - เจ้าของหรือผู้ดำเนินการทรัพย์สิน
      - ตำแหน่งทางกายภาพของทรัพย์สิน
      - การเชื่อมต่อและการพึ่งพาของทรัพย์สินบนระบบ/เครือข่าย
- **4.2 การดูแลและอัปเดตทะเบียนทรัพย์สิน**
  - **ขั้นตอน**
    - ดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยมีการตรวจสอบและอัปเดตข้อมูลทุกครั้งที่มีการเปลี่ยนแปลง เช่น การเพิ่ม การย้าย หรือการกำจัดทรัพย์สิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. การระบุขอบเขตเครือข่ายและระบบคอมพิวเตอร์ (Network and System Scope Identification)

- **ขั้นตอน**
  - ระบุและกำหนดขอบเขตของเครือข่ายที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน รวมถึงระบบคอมพิวเตอร์ที่มีการเชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

6. การตรวจสอบและปรับปรุงทะเบียนทรัพย์สิน (Inventory Review and Update)

- **6.1 การตรวจสอบประจำปี**
  - **ขั้นตอน**
    - ดำเนินการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าข้อมูลในทะเบียนเป็นปัจจุบันและถูกต้อง
- **6.2 การปรับปรุงทะเบียนเมื่อมีการเปลี่ยนแปลง**
  - **ขั้นตอน**
    - หากมีการเปลี่ยนแปลงทรัพย์สินหรือบริการที่สำคัญ ต้องทำการอัปเดตข้อมูลในทะเบียนทรัพย์สินทันที

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดการทรัพย์สิน (Asset Management Procedure)	รหัสเอกสาร	CSMS-Identify -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

7. การประเมินความเสี่ยงของทรัพย์สินและบริการที่สำคัญ (Asset and System service Risk Assessment)

- **ขั้นตอน**
  - ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของทรัพย์สินและของบริการที่สำคัญในทะเบียนอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบและระบุความเสี่ยงที่อาจเกิดขึ้น รวมถึงการพิจารณามาตรการการจัดการความเสี่ยงที่เหมาะสม

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review**)

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายการทรัพย์สินทั้งหมด (Asset Inventory List
2. ทะเบียนทรัพย์สิน (Asset Register)
3. เอกสารการประเมินความเสี่ยงของทรัพย์สิน (Risk Assessment of Critical Asset Inventory List)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

ทะเบียนทรัพย์สิน (Asset Register)

วันที่จัดทำ : 1/05/2567

จัดทำโดย : นาย สุรศักดิ์ มั่นคง

1. ทะเบียนทรัพย์สิน (Asset Register)

ควรแสดงทรัพย์สินที่สามารถถูกโจมตีหรือมีส่วนเป็นช่องโหว่ที่ทำให้เกิดการโจมตีทางไซเบอร์

ลำดับที่	ชื่อ/คำอธิบายของทรัพย์สิน (Asset Name/Description)	ฟังก์ชันที่สำคัญของทรัพย์สิน (Key Function of Asset)	การระบุและจัดลำดับความสำคัญ (Identification & Prioritization	เจ้าของ/ผู้ดำเนินการ (Owner/Operator)	ตำแหน่งทางกายภาพ (Physical Location)	การขึ้นต่อกันของทรัพย์สิน (Asset Dependencies)
1	PC 001	ใช้สำหรับการดำเนินงาน	กลาง (Medium)	นาย A	ฝ่ายบัญชี ตึก 1	ระบบเครือข่ายภายใน
2	PC 002	ใช้สำหรับการดำเนินงาน	กลาง (Medium)	นาย B	ฝ่ายซ่อมบำรุง ตึก 2	ระบบเครือข่ายภายใน
3	Server 001	ประมวลผลการทำงาน	สูง (Critical)	หน่วยงาน IT	ห้องคอมพิวเตอร์	ระบบไฟฟ้าสำรอง, ระบบเครือข่ายภายใน
4	Database Server 001	เก็บข้อมูลของลูกค้า	สูง (Critical)	หน่วยงาน IT	ห้องคอมพิวเตอร์	
5	Notebook 001	ใช้สำหรับการดำเนินงานระดับสูง	กลาง (Medium)	นาย C	ใช้งานที่บ้านและสำนักงาน	ต่อระบบ VPN, เครือข่ายภายใน
6	ระบบควบคุมเครือข่าย (Network System)	จัดการการเชื่อมต่อและการรักษาความปลอดภัยของเครือข่าย	สูง (Critical)	นาง B	ห้องควบคุม, อาคาร B, ชั้น 2	ต่อระบบไฟฟ้าสำรอง, ระบบฐานข้อมูลและเครือข่ายภายใน
7	ระบบไฟร์วอลล์ (Firewall System)	ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตจากภายนอก	สูง (Critical)	นาย E	ห้องควบคุม, อาคาร C, ชั้น 2	ต่อระบบเครือข่ายภายใน, เครือข่ายภายนอก
8	ระบบเครือข่ายไร้สาย (Wireless Network System)	ให้บริการการเชื่อมต่อเครือข่ายไร้สายสำหรับพนักงาน	กลาง (Medium)	นาย J	อาคาร A, ทุกชั้น	ต่อระบบไฟฟ้าสำรอง, ระบบเครือข่ายหลัก

2. ทะเบียนทรัพย์สินที่เป็นของบริการที่สำคัญ (Asset for System service Inventory)

แนะนำให้เอาระบบ Application ขององค์กรมาใส่ ซึ่งถือว่าเป็นระบบบริการที่สำคัญ ที่สามารถถูกโจมตีหรือมีส่วนเป็นช่องโหว่ที่ทำให้เกิดการโจมตีทางไซเบอร์

ลำดับที่	ชื่อ/คำอธิบายของทรัพย์สิน (Asset Name/Description)	ฟังก์ชันที่สำคัญของทรัพย์สิน (Key Function of Asset)	การระบุและจัดลำดับความสำคัญ (Identification & Prioritization	เจ้าของ/ผู้ดำเนินการ (Owner/Operator)	ตำแหน่งทางกายภาพ (Physical Location)	การขึ้นต่อกันของทรัพย์สิน (Asset Dependencies)
1	ระบบ HIS (HIS System)	บริการผู้ป่วยทั้งหมด	สูง (Critical)	นาย D	ห้องเซิร์ฟเวอร์, อาคาร A, ชั้นใต้ดิน	ต่อกับบริการคลาวด์
2	ระบบอีเมลองค์กร (Email System)	จัดการการส่งและรับอีเมลทั้งหมดในองค์กร	สูง (Critical)	นาย F	ห้องเซิร์ฟเวอร์, อาคาร A, ชั้น 3	ต่อระบบเครือข่ายภายใน, อินเทอร์เน็ต
3	ระบบจัดการเอกสาร (Document Management System)	เก็บและจัดการเอกสารสำคัญขององค์กร	กลาง (Medium)	นาย G	ห้องควบคุมเอกสาร, อาคาร B, ชั้น 2	ต่อระบบไฟฟ้าสำรอง, ระบบสำรองข้อมูล
4	ระบบการบัญชี (Accounting System)	จัดการบัญชีการเงินและงบประมาณขององค์กร	สูง (Critical)	นาย H	ห้องการเงิน, อาคาร B, ชั้น 2	ต่อระบบฐานข้อมูล, ระบบสำรองข้อมูล

2. กระบวนการการประเมินความเสี่ยง และกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk MGT Strategy Procedure)

Logo	**ระเบียบกระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)**	**รหัสเอกสาร**	**CSMS-Identify -02**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)**	**รหัสเอกสาร**	**CSMS-Identify -02**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

ระเบียบกระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้มีวัตถุประสงค์เพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญขององค์กร และเพื่อกำหนดกลยุทธ์ในการจัดการความเสี่ยงเพื่อป้องกันหรือลดผลกระทบจากความเสี่ยงเหล่านั้น

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับทรัพย์สิน ข้อมูล ระบบ โครงสร้างพื้นฐาน และบริการที่สำคัญขององค์กร รวมถึงการจัดทำและปรับปรุงทะเบียนความเสี่ยง

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้จัดการความเสี่ยง (Risk Manager)**: รับผิดชอบในการกำกับดูแลการดำเนินการตามกระบวนการประเมินและจัดการความเสี่ยง รวมถึงการตัดสินใจเกี่ยวกับกลยุทธ์การจัดการความเสี่ยงที่สำคัญ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **ทีมจัดการความเสี่ยง (Risk Management Team)**: รับผิดชอบในการดำเนินการประเมินความเสี่ยง การจัดทำทะเบียนความเสี่ยง และการพัฒนากลยุทธ์ในการจัดการความเสี่ยง
- **เจ้าของความเสี่ยง (Risk Owner)**: รับผิดชอบในการติดตามและจัดการความเสี่ยงที่ตนรับผิดชอบตามที่ระบุไว้ในทะเบียนความเสี่ยง

4. การประเมินความเสี่ยง (Risk Assessment)

4.1 การระบุความเสี่ยง (Risk Identification)

- **4.1.1 การระบุภัยคุกคามและช่องโหว่**
  - **ขั้นตอน**: ระบุภัยคุกคามทางไซเบอร์และช่องโหว่ที่อาจส่งผลกระทบต่อระบบและกระบวนการที่สำคัญ รวมถึงความเสี่ยงที่เกิดจากกระบวนการปฏิบัติงาน บุคลากร หรือปัจจัยภายนอก โดยการระบุว่ามีความเสี่ยงจากการโจมตีทางไซเบอร์ต่างๆ ต่อระบบเครือข่ายหลัก หรือช่องโหว่จากการใช้งานซอฟต์แวร์ที่ไม่ได้รับการอัปเดต
- **4.1.2 การจัดทำรายการความเสี่ยง**
  - **ขั้นตอน**: จัดทำรายการความเสี่ยงที่ระบุได้ โดยจัดลำดับความสำคัญตามความรุนแรงและโอกาสที่ความเสี่ยงจะเกิดขึ้น โดยจัดลำดับความเสี่ยงที่สูงสุดเป็นความเสี่ยงจากการโจมตีทางไซเบอร์ ที่อาจทำให้ระบบเครือข่ายล่มเป็นเวลานาน

4.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

- **4.2.1 การวิเคราะห์ผลกระทบและโอกาส**
  - **ขั้นตอน**: วิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงที่ระบุและโอกาสที่ความเสี่ยงจะเกิดขึ้น รวมถึงผลกระทบทางการเงิน ด้านชื่อเสียง ด้านกฎหมาย และอื่น ๆ โดยการวิเคราะห์ว่าการโจมตีทางไซเบอร์ อาจทำให้เว็บไซต์ขององค์กรไม่สามารถให้บริการได้ และเกิดความเสียหายทางการเงินและชื่อเสียงอย่างมาก

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)	รหัสเอกสาร	CSMS-Identify -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **4.2.2 การจัดลำดับความสำคัญของความเสี่ยง**
  - **ขั้นตอน:** จัดลำดับความสำคัญของความเสี่ยงตามผลกระทบและโอกาสที่เกิดขึ้น เพื่อกำหนดลำดับการดำเนินการจัดการความเสี่ยง โดยความเสี่ยงจากการโจมตีทางไซเบอร์ ถูกจัดลำดับเป็นความเสี่ยงสูงสุด เนื่องจากมีผลกระทบทางการเงินและชื่อเสียงสูง

4.3 การประเมินค่าความเสี่ยง (Risk Evaluation)

- **4.3.1 การประเมินโอกาสและผลกระทบ**
  - **ขั้นตอน:** ประเมินโอกาสที่ความเสี่ยงจะเกิดขึ้นและผลกระทบต่อการดำเนินงานและธุรกิจ รวมถึงกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) โดยประเมินว่าโอกาสที่การโจมตีทางไซเบอร์ จะเกิดขึ้นมีสูง และผลกระทบที่เกิดขึ้นอาจทำให้ระบบหยุดทำงานเป็นเวลานาน ซึ่งเกินกว่าระดับความเสี่ยงที่ยอมรับได้ขององค์กร

4.4 การจัดการความเสี่ยง (Risk Treatment)

- **4.4.1 การกำหนดแนวทางการจัดการความเสี่ยง**
  - **ขั้นตอน:** กำหนดแนวทางจัดการความเสี่ยง เช่น การหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การโอนความเสี่ยง หรือการยอมรับความเสี่ยง โดยคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ
- **4.4.2 การกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (KRI)**
  - **ขั้นตอน:** กำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง

4.5 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

- **4.5.1 การติดตามความเสี่ยงอย่างต่อเนื่อง**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)	รหัสเอกสาร	CSMS-Identify -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **ขั้นตอน:** มีกระบวนการที่มีประสิทธิภาพในการติดตามความเสี่ยงและทบทวนการจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้แน่ใจว่าความเสี่ยงยังคงอยู่ภายใต้ระดับที่ยอมรับได้และมี รายงานผลให้กับคณะทำงานที่เกี่ยวข้องรับทราบ

- **4.5.2 การทบทวนและปรับปรุงแนวทางการจัดการความเสี่ยง**
  - **ขั้นตอน:** ทบทวนแนวทางการจัดการความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ เพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพในการจัดการความเสี่ยง หรือหลังจากเกิดการโจมตีทางไซเบอร์ ให้ทำการทบทวนแนวทางการป้องกันและเสนอแนะการปรับปรุงแนวทางป้องกันเพิ่มเติม

4.6 การรายงานความเสี่ยง (Risk Assessment Reporting)

- **4.6.1 การรายงานระดับความเสี่ยงและผลการจัดการความเสี่ยง**
  - **ขั้นตอน:** รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ
- **4.6.2 การทบทวนและปรับปรุงระเบียบวิธีปฏิบัติ**
  - **ขั้นตอน:** ทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ อย่างมีนัยสำคัญ

5. การจัดทำทะเบียนความเสี่ยง (Risk Register)

- **ขั้นตอน**
  - จัดทำและปรับปรุงทะเบียนความเสี่ยงหลังการประเมินความเสี่ยงทุกครั้ง โดยรายละเอียดที่ต้องบันทึกในทะเบียนความเสี่ยง ได้แก่
    - วันที่ระบุความเสี่ยง (Date the Risk is Identified)
    - คำอธิบายของความเสี่ยง (Description of the Risk)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

6. การพัฒนากลยุทธ์เพื่อจัดการความเสี่ยง (Risk Management Strategy)

- **6.1 การพัฒนากลยุทธ์การเพื่อจัดการความเสี่ยง**
  - **ขั้นตอน**
    - พัฒนากลยุทธ์ในการจัดการความเสี่ยงที่เหมาะสมเพื่อลดผลกระทบจากความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยอาจใช้วิธีการต่าง ๆ เช่น การป้องกันความเสี่ยง (Risk Avoidance) การลดความเสี่ยง (Risk Reduction) การถ่ายโอนความเสี่ยง (Risk Transfer) หรือการยอมรับความเสี่ยง (Risk Acceptance) โดยการใช้การเข้ารหัสข้อมูลเพื่อลดความเสี่ยงจากการถูกโจมตีแบบ Man-in-the-Middle
- **6.2 การติดตามและปรับปรุงกลยุทธ์การจัดการความเสี่ยง**
  - **ขั้นตอน**
    - ติดตามผลการจัดการความเสี่ยงและปรับปรุงกลยุทธ์การจัดการความเสี่ยงตามความเหมาะสม โดยพิจารณาจากสถานะของการจัดการความเสี่ยงและความเสี่ยงที่เหลือ (Residual Risk) และดำเนินการปรับปรุงมาตรการความปลอดภัยเพิ่มเติมหลังจากพบว่าการควบคุมความเสี่ยงที่ใช้อยู่ยังไม่เพียงพอ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ทะเบียนความเสี่ยง (Risk Register)
2. เอกสารการประเมินความเสี่ยงและการจัดการความเสี่ยง (Risk Assessment and Risk Treatment)
3. ดัชนีวัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI)
4. รายงานการประเมินความเสี่ยง (Risk Assessment Report), NIST SP 800-30

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

ทะเบียนความเสี่ยง (Risk Register)

ประจำปี : 2567	ผู้บันทึกทะเบียนความเสี่ยง : นายสุรศักดิ์ มั่นคง

ลำดับที่	วันที่ระบุความเสี่ยง	คำอธิบายของความเสี่ยง	โอกาสที่จะเกิดขึ้น	ความรุนแรงของเหตุการณ์	การจัดการความเสี่ยง	เจ้าของความเสี่ยง	สถานะของการจัดการความเสี่ยง	ความเสี่ยงที่เหลือ
1	1/8/2567	การโจมตีแบบ DDoS ที่อาจทำให้ระบบเครือข่ายหยุดทำงาน	สูง (High)	สูง (High)	การติดตั้งระบบป้องกัน DDoS	เจ้าหน้าที่ IT	กำลังดำเนินการ (In Progress)	ต่ำ (Low)
2	15/09/2567	ช่องโหว่ในซอฟต์แวร์เก่าไม่ได้รับการอัปเดต	ปานกลาง (Medium)	สูง (High)	การอัปเดตแพตช์ซอฟต์แวร์	เจ้าหน้าที่ IT	สำเร็จ (Completed)	ต่ำ (Low)
3	22/10/2567	ความเสี่ยงจากการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต	ต่ำ (Low)	ปานกลาง (Medium)	การใช้การเข้ารหัสข้อมูล	ผู้จัดการฐานข้อมูล	กำลังดำเนินการ (In Progress)	ต่ำ (Low)
4	25/12/2567	การสูญเสียข้อมูลเนื่องจากการสำรองข้อมูลไม่สม่ำเสมอ	ปานกลาง (Medium)	สูง (High)	การตั้งค่าการสำรองข้อมูลอัตโนมัติ	เจ้าหน้าที่ IT	กำลังดำเนินการ (In Progress)	ต่ำ (Low)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) และการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Treatment)							วันที่ทำการประเมิน : 1/05/67	ผู้ทำการประเมินความเสี่ยง : ทีมประเมินความเสี่ยง	
	ระบุความเสี่ยง (Risk Identification)	การวิเคราะห์ความเสี่ยง (Risk Analyst)	การประเมินความเสี่ยง (Risk Evaluation) / โอกาสที่จะเกิดขึ้น	ความรุนแรงของเหตุการณ์ (Severity of the event)		การจัดการความเสี่ยง (Risk Treatment)	เจ้าของความเสี่ยง (Owner Risk)	ความเสี่ยงที่เหลือ (Residual Risk)	สถานะของการจัดการความเสี่ยง (Risk Managed Status)
1	ความเสี่ยงจากการโจมตีแบบฟิชชิ่ง (Phishing Attacks)	การโจมตีแบบฟิชชิ่งสามารถทำให้ผู้โจมตีเข้าถึงข้อมูลสำคัญขององค์กรได้ โดยการหลอกลวงให้พนักงานเปิดเผยข้อมูลที่เป็นความลับ เช่น รหัสผ่าน หรือข้อมูลส่วนบุคคล	สูง (High)	สูง (High)	1	ฝึกอบรมพนักงานให้ความรู้เกี่ยวกับ CSMS Awareness และ Cyber Attack ทุกรูปแบบ โดยเฉพาะฟิชชิ่ง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ติดตั้งระบบกรองอีเมลที่มีความสามารถในการตรวจจับและบล็อกอีเมลฟิชชิ่ง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ดำเนินการตรวจสอบและทดสอบการรับรู้ของพนักงานเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
2	ความเสี่ยงจากการโจมตี (DDoS, Distributed Denial of Service Attacks)	การโจมตี DDoS สามารถทำให้บริการออนไลน์ขององค์กรล่มและไม่สามารถให้บริการแก่ลูกค้าได้	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบป้องกันการโจมตี DDoS (DDoS Mitigation)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้บริการ CDN (Content Delivery Network) ที่มีการป้องกัน DDoS ในตัว	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการรับส่งข้อมูลเครือข่ายเป็นระยะ ๆ เพื่อระบุพฤติกรรมที่ผิดปกติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
3	ความเสี่ยงจากการขโมยข้อมูล (Data Theft)	การขโมยข้อมูลที่สำคัญ เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน อาจทำให้เกิดความเสียหายอย่างรุนแรงต่อองค์กร	ปานกลาง (Medium)	สูง (High)	1	เข้ารหัสข้อมูลทั้งหมดที่เก็บในระบบฐานข้อมูล	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงข้อมูลสำคัญเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้ระบบการยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
4	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่ได้รับการอัปเดต (Outdated Software)	ซอฟต์แวร์ที่ไม่ได้รับการอัปเดตอาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้เพื่อเข้าถึงระบบหรือข้อมูลที่สำคัญได้	สูง (High)	ปานกลาง (Medium)	1	จัดตั้งนโยบายการอัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้เครื่องมือจัดการการแพตช์ซอฟต์แวร์อัตโนมัติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

					3	ตรวจสอบและทดสอบซอฟต์แวร์ที่ใช้งานในระบบอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
5	ความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)	การเข้าถึงระบบโดยไม่ได้รับอนุญาตสามารถทำให้เกิดการโจมตีหรือการขโมยข้อมูลจากระบบขององค์กรได้	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบการยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication - 2FA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงระบบเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ทบทวนสิทธิ์การเข้าถึงของผู้ใช้ในระบบอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
6	ความเสี่ยงจากการโจมตีผ่านเครือข่ายไร้สาย (Wireless Network Attacks)	การโจมตีผ่านเครือข่ายไร้สายอาจทำให้ข้อมูลที่ถูกส่งผ่านเครือข่ายถูกดักฟังหรือถูกขโมย	ปานกลาง (Medium)	ปานกลาง (Medium)	1	ติดตั้งระบบการเข้ารหัสข้อมูลในเครือข่ายไร้สาย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงเครือข่ายไร้สายเฉพาะผู้ใช้ที่ได้รับอนุญาต	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้ระบบตรวจสอบการเข้าถึงเครือข่ายไร้สายเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
7	ความเสี่ยงจากการโจมตีแบบ Zero-Day (Zero-Day Attacks)	การโจมตีแบบ Zero-Day เป็นการโจมตีที่ใช้ช่องโหว่ที่ยังไม่เคยถูกค้นพบมาก่อน ทำให้ไม่มีการป้องกันโดยเฉพาะสำหรับช่องโหว่นั้น	ปานกลาง (Medium)	สูง (High)	1	ใช้ระบบการป้องกันที่มีการอัปเดตช่องโหว่อย่างต่อเนื่อง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ตรวจสอบระบบเครือข่ายและการใช้งานซอฟต์แวร์เพื่อระบุพฤติกรรมที่ผิดปกติ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
8	ความเสี่ยงจากการใช้รหัสผ่านที่ไม่ปลอดภัย (Weak Passwords)	การใช้รหัสผ่านที่ไม่ปลอดภัยหรือรหัสผ่านที่สามารถเดาได้ง่ายทำให้ผู้โจมตีสามารถเข้าถึงระบบได้ง่ายขึ้น	สูง (High)	ปานกลาง (Medium)	1	กำหนดนโยบายการตั้งรหัสผ่านที่มีความซับซ้อนและบังคับให้เปลี่ยนรหัสผ่านเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้การยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication - 2FA)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการใช้งานรหัสผ่านในระบบเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
9	ความเสี่ยงจากการเข้าถึงอุปกรณ์ IoT ที่ไม่ได้รับการควบคุม (Uncontrolled IoT Devices)	อุปกรณ์ IoT ที่ไม่ได้รับการควบคุมหรืออัปเดตสามารถเป็นจุดเริ่มต้นของการโจมตีในระบบเครือข่ายขององค์กร	ปานกลาง (Medium)	ปานกลาง (Medium)	1	จำกัดการเข้าถึงอุปกรณ์ IoT และการเชื่อมต่อกับเครือข่ายองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	อัปเดตซอฟต์แวร์ของอุปกรณ์ IoT อย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ติดตั้งระบบการตรวจสอบการใช้งานอุปกรณ์ IoT ในองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

10	**ความเสี่ยงจากการรั่วไหลของข้อมูลลูกค้า (Customer Data Leakage)**	ข้อมูลลูกค้าที่รั่วไหลอาจทำให้เกิดความเสียหายต่อความเชื่อมั่นของลูกค้าและภาพลักษณ์ขององค์กร	ปานกลาง (Medium)	สูง (High)	1	เข้ารหัสข้อมูลลูกค้าทั้งหมดที่จัดเก็บและส่งผ่านในระบบ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการเข้าถึงข้อมูลลูกค้าเฉพาะผู้ที่มีสิทธิ์และมีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการเข้าถึงและการใช้งานข้อมูลลูกค้าอย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
11	**ความเสี่ยงจากการโจมตีผ่านการใช้งาน Remote Access (Remote Access Attacks)**	การใช้งาน Remote Access อาจทำให้ผู้โจมตีสามารถเข้าถึงระบบขององค์กรจากภายนอกได้หากไม่มีการรักษาความปลอดภัยที่เหมาะสม	สูง (High)	ปานกลาง (Medium)	1	ใช้การยืนยันตัวตนแบบสองขั้นตอน (2FA) สำหรับการเข้าถึงระยะไกล	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จำกัดการใช้งาน Remote Access เฉพาะผู้ที่มีความจำเป็นเท่านั้น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบการใช้งาน Remote Access อย่างสม่ำเสมอ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
12	**ความเสี่ยงจากการโจมตีผ่านแอปพลิเคชันที่ไม่ได้รับการตรวจสอบ (Unvetted Applications)**	แอปพลิเคชันที่ไม่ได้รับการตรวจสอบหรือทดสอบก่อนใช้งานอาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้โจมตีระบบได้	ปานกลาง (Medium)	สูง (High)	1	ตรวจสอบและทดสอบแอปพลิเคชันทั้งหมดก่อนที่จะนำไปใช้งานในระบบ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ห้ามใช้งานแอปพลิเคชันที่ไม่ได้รับการอนุมัติจากฝ่าย IT	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ทบทวนการใช้งานแอปพลิเคชันในองค์กรเป็นระยะ ๆ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
13	**ความเสี่ยงจากการโจมตีผ่านซอฟต์แวร์ที่ไม่ปลอดภัย (Insecure Software)**	ซอฟต์แวร์ที่ไม่ได้รับการพัฒนาตามมาตรฐานความปลอดภัยอาจมีช่องโหว่ที่สามารถนำไปสู่การโจมตีได้	ปานกลาง (Medium)	สูง (High)	1	ใช้แนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Lifecycle - SSDLC)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ทดสอบความปลอดภัยของซอฟต์แวร์ก่อนที่จะนำไปใช้งาน	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	จัดทำการตรวจสอบซอฟต์แวร์เป็นระยะเพื่อระบุช่องโหว่ที่อาจเกิดขึ้น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

14	**ความเสี่ยงจากการโจมตีผ่านเว็บไซต์ขององค์กร (Website Attacks)**	เว็บไซต์ขององค์กรอาจเป็นเป้าหมายของการโจมตี เช่น การโจมตี SQL Injection, XSS, หรือการโจมตีแบบอื่น ๆ ที่สามารถทำให้ข้อมูลรั่วไหลหรือเว็บไซต์ล่ม	ปานกลาง (Medium)	สูง (High)	1	ทดสอบความปลอดภัยของเว็บไซต์ด้วยการทดสอบการเจาะระบบ (Penetration Testing)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้เครื่องมือ Web Application Firewall (WAF) เพื่อป้องกันการโจมตีทางเว็บ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	อัปเดตแพลตฟอร์มและปลั๊กอินของเว็บไซต์เป็นประจำ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
15	**ความเสี่ยงจากการรั่วไหลของข้อมูลผ่านอุปกรณ์พกพา (Mobile Device Data Leakage)**	อุปกรณ์พกพาที่ใช้ในองค์กรอาจเป็นช่องทางในการรั่วไหลของข้อมูล หากไม่ได้รับการควบคุมและจัดการที่เหมาะสม	ปานกลาง (Medium)	สูง (High)	1	ใช้ระบบ Mobile Device Management (MDM) เพื่อควบคุมการใช้งานอุปกรณ์พกพาในองค์กร	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	บังคับใช้การเข้ารหัสข้อมูลบนอุปกรณ์พกพา	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	จำกัดการเข้าถึงข้อมูลสำคัญจากอุปกรณ์พกพาเฉพาะผู้ที่มีความจำเป็น	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
16	**ความเสี่ยงจากการใช้เครือข่ายสาธารณะ (Public Network Usage Risks)**	การใช้เครือข่ายสาธารณะในการเชื่อมต่อเข้าถึงระบบขององค์กรอาจทำให้ข้อมูลถูกดักฟังหรือขโมยได้ง่ายขึ้น	ปานกลาง (Medium)	ปานกลาง (Medium)	1	ห้ามการเข้าถึงระบบองค์กรผ่านเครือข่ายสาธารณะหากไม่มีการใช้ VPN	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	บังคับใช้การเข้ารหัสข้อมูลสำหรับการเชื่อมต่อผ่านเครือข่ายสาธารณะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ฝึกอบรมพนักงานเกี่ยวกับความเสี่ยงและแนวทางปฏิบัติที่ปลอดภัยในการใช้เครือข่ายสาธารณะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
17	**ความเสี่ยงจากการโจมตีทางกายภาพ (Physical Security Breaches)**	การโจมตีทางกายภาพ เช่น การเข้าถึงห้องเซิร์ฟเวอร์หรือศูนย์ข้อมูลโดยไม่ได้รับอนุญาต อาจทำให้ข้อมูลและระบบที่สำคัญถูกทำลายหรือขโมย	ปานกลาง (Medium)	สูง (High)	1	ติดตั้งระบบควบคุมการเข้าถึงทางกายภาพ (Physical Access Control Systems - PACS)	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ใช้ระบบกล้องวงจรปิด (CCTV) และการตรวจสอบการเข้าถึงทางกายภาพ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

					3	ตรวจสอบและบันทึกการเข้าถึงทางกายภาพของพนักงานและผู้เยี่ยมชมเป็นประจำ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
18	ความเสี่ยงจากการโจมตีผ่าน **Social Engineering (Social Engineering Attacks)**	การโจมตีผ่าน Social Engineering อาจทำให้ผู้โจมตีสามารถหลอกลวงพนักงานเพื่อเข้าถึงข้อมูลหรือระบบขององค์กร	สูง (High)	ปานกลาง (Medium)	1	ฝึกอบรมพนักงานเกี่ยวกับการระบุและป้องกันการโจมตีแบบ Social Engineering	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ติดตั้งระบบยืนยันตัวตนที่เข้มงวดในการเข้าถึงข้อมูลหรือระบบ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ทดสอบความรู้และความสามารถของพนักงานในการระบุการโจมตีแบบ Social Engineering เป็นระยะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
19	ความเสี่ยงจากการขาดการสำรองข้อมูลที่เพียงพอ (**Inadequate Data Backup)**	การขาดการสำรองข้อมูลที่เพียงพออาจทำให้ข้อมูลสูญหายถาวรหากเกิดเหตุการณ์ที่ไม่คาดฝัน เช่น การโจมตีทางไซเบอร์หรือการล่มของเซิร์ฟเวอร์	ปานกลาง (Medium)	สูง (High)	1	จัดทำการสำรองข้อมูลอย่างสม่ำเสมอและเก็บรักษาข้อมูลสำรองในสถานที่ที่ปลอดภัย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	ทดสอบการกู้คืนข้อมูลจากการสำรองอย่างสม่ำเสมอเพื่อยืนยันความถูกต้อง	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ใช้การเข้ารหัสข้อมูลสำหรับการสำรองข้อมูลเพื่อป้องกันการรั่วไหล	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
20	ความเสี่ยงจากการขาดการทดสอบความปลอดภัยเป็นระยะ (**Lack of Regular Security Testing)**	การขาดการทดสอบความปลอดภัยเป็นระยะอาจทำให้ช่องโหว่ที่มีอยู่ในระบบไม่ได้รับการระบุและแก้ไขทันเวลา	ปานกลาง (Medium)	สูง (High)	1	กำหนดแผนการทดสอบความปลอดภัยเป็นระยะ เช่น การทดสอบการเจาะระบบและการสแกนหาช่องโหว่	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					2	จัดทำรายงานและแผนการแก้ไขปัญหาจากผลการทดสอบความปลอดภัย	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)
					3	ตรวจสอบและปรับปรุงมาตรการความปลอดภัยตามผลการทดสอบเป็นระยะ	CSMR	น้อย (Low)	ดำเนินการแล้ว (1/04/67)

รายงานการประเมินความเสี่ยง (Risk Assessment Report)

(อ้างอิง Appendix K, NIST SP 800-30 Rev. 1)

วันที่ทำประเมิน: 15 กันยายน 2567

ผู้จัดทำรายงาน : นาย สุรศักดิ์ มั่นคง

ชื่อระบบ: ระบบจัดการข้อมูลลูกค้า (Customer Data Management System - CDMS)

---

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน: 15 กันยายน 2567

วัตถุประสงค์: การประเมินความเสี่ยงของระบบจัดการข้อมูลลูกค้า (CDMS) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่สำคัญและหาวิธีการควบคุมที่เหมาะสม

ขอบเขต:

Tier 3 (ระดับระบบข้อมูล): ประเมินการปกป้องความลับของข้อมูลลูกค้า ระบบจัดการข้อมูลลูกค้า (CDMS) ตั้งอยู่ในศูนย์ข้อมูลหลักขององค์กร

ประเภทของการประเมิน: การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม: ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ ปานกลาง

จำนวนความเสี่ยงที่ระบุ:

ความเสี่ยงต่ำ: 5 รายการ

ความเสี่ยงปานกลาง: 3 รายการ

ความเสี่ยงสูง: 1 รายการ

---

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบ CDMS ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูลลูกค้า
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบ CDMS รวมถึงการจัดการข้อมูลลูกค้าที่มีความสำคัญ
3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

2.2 ข้อสมมติและข้อจำกัดในการประเมิน

สมมติว่าข้อมูลทั้งหมดที่ให้มาสำหรับการประเมินเป็นข้อมูลที่ถูกต้องและครบถ้วน ข้อจำกัดของการประเมินคือไม่สามารถเข้าถึงเซิร์ฟเวอร์เสมือนจริงที่ใช้สำรองข้อมูลได้

2.3 การยอมรับความเสี่ยง

องค์กรมีนโยบายรับความเสี่ยงในระดับ ปานกลาง โดยยอมรับความเสี่ยงบางส่วนเพื่อรักษาประสิทธิภาพในการดำเนินงาน

2.4 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

---

3. รายละเอียดความเสี่ยง (Detailed Risk Assessment)

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม
1	การเข้าถึงข้อมูลลูกค้าโดยไม่ได้รับอนุญาต (Unauthorized Access to Customer Data)	สูง	การสูญเสียความลับของข้อมูลลูกค้าและการละเมิดข้อมูลที่สำคัญ	การควบคุมการเข้าถึงโดยการยืนยันตัวตนสองชั้น	เพิ่มการทดสอบการเจาะระบบทุก 6 เดือน
2	การจัดเก็บข้อมูลสำรองไม่ถูกต้อง (Improper Backup Storage)	ปานกลาง	ข้อมูลสูญหายและไม่สามารถกู้คืนได้	การควบคุมการเข้าถึงโดยการยืนยันตัวตนสองชั้น	ตรวจสอบระบบการสำรองข้อมูลเพิ่มเติม
3	ความล่าช้าในการอัปเดตซอฟต์แวร์ (Delayed Software Updates)	ต่ำ	ระบบมีช่องโหว่ที่อาจถูกโจมตี	มีการอัปเดตเป็นประจำทุกไตรมาส	แนะนำให้ลดระยะเวลาการอัปเดตลงเป็นรายเดือน

---

4. ภาคผนวกสนับสนุน (Supporting Appendices)

4.1 ผลการประเมินโดยละเอียด

ระบบ CDMS ได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตผ่านการควบคุมการเข้าถึงที่เหมาะสม อย่างไรก็ตาม จำเป็นต้องทดสอบและอัปเดตมาตรการเป็นระยะเพื่อป้องกันภัยคุกคามใหม่ ๆ

4.2 ระยะเวลาความถูกต้องของการประเมิน

ผลการประเมินนี้มีอายุการใช้งาน 1 ปี หรือจนกว่าจะมีการเปลี่ยนแปลงระบบ

4.3 การจำแนกความเสี่ยง

ภัยคุกคามที่เกิดจากบุคคลภายนอก (Adversarial Threats): โจมตีด้วยการพยายามเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

ภัยคุกคามที่ไม่เกิดจากบุคคลภายนอก (Non-Adversarial Threats): การสูญหายของข้อมูลจากข้อผิดพลาดในการจัดเก็บข้อมูล

3. กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)

=

Logo	**ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)**	**รหัสเอกสาร**	**CSMS-Identify -03**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นเอกสารของความลับ	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) ที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร รวมถึงการดำเนินการทดสอบเจาะระบบเพื่อประเมินความเสี่ยงและการควบคุมความปลอดภัย

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมการประเมินช่องโหว่และการทดสอบเจาะระบบสำหรับระบบเทคโนโลยีสารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรมที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร โดยรวมถึงการตรวจสอบความมั่นคงปลอดภัยของโฮสต์ เครือข่าย สถาปัตยกรรม และแอปพลิเคชัน

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ทีมความมั่นคงปลอดภัยสารสนเทศ (IT Security Team)**: รับผิดชอบในการดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบ รวมถึงการติดตามและแก้ไขช่องโหว่ที่พบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

- **ผู้ให้บริการทดสอบเจาะระบบ (Penetration Testing Service Providers)**: รับผิดชอบในการดำเนินการทดสอบเจาะระบบตามขอบเขตที่กำหนด โดยต้องมีการรับรองและได้รับประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม
- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและสนับสนุนการดำเนินการตามกระบวนการ รวมถึงการตรวจสอบและประเมินผล

4. การประเมินช่องโหว่ (Vulnerability Assessment)

- **4.1 การประเมินช่องโหว่ตามหลักการบริหารความเสี่ยง**
  - **ขั้นตอน:** ดำเนินการประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรมตามหลักการบริหารความเสี่ยงที่องค์กรกำหนด เพื่อระบุจุดอ่อนและการควบคุมที่จำเป็น โดยการประเมินความเสี่ยงความมั่นคงปลอดภัยของโฮสต์เพื่อหาช่องโหว่ที่อาจถูกโจมตีได้
- **4.2 การตรวจสอบขอบเขตของการประเมินช่องโหว่**
  - **ขั้นตอน:** ตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่ครอบคลุมถึงการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม โดยการตรวจสอบว่าได้ทำการประเมินความมั่นคงปลอดภัยของเครือข่ายทั้งหมดที่เชื่อมต่อกับระบบที่สำคัญ
- **4.3 การประเมินช่องโหว่ก่อนการเปลี่ยนแปลงระบบสำคัญ**
  - **ขั้นตอน:** ทำการประเมินช่องโหว่ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบที่สำคัญหรือเชื่อมต่อระบบใหม่ รวมถึงการเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี โดยการประเมินช่องโหว่ก่อนการอัปเกรดซอฟต์แวร์ในระบบควบคุมเครื่องจักรในอุตสาหกรรม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

5. การทดสอบเจาะระบบ (Penetration Testing)

- **5.1 การดำเนินการทดสอบเจาะระบบตามความเสี่ยง**
  - **ขั้นตอน:** พิจารณาดำเนินการทดสอบเจาะระบบสำหรับบริการที่สำคัญ โดยเฉพาะอย่างยิ่งระบบที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบที่อาจเกิดขึ้นจากการทดสอบ โดยเฉพาะการทดสอบเจาะระบบของแอปพลิเคชันที่มีการเข้าถึงจากภายนอกผ่านอินเทอร์เน็ต
- **5.2 การตรวจสอบขอบเขตของการทดสอบเจาะระบบ**
  - **ขั้นตอน:** ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบครอบคลุมถึงโฮสต์ เครือข่าย และแอปพลิเคชันของระบบที่เป็นบริการที่สำคัญ โดยเฉพาะระบบที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง
- **5.3 ความถี่ในการทดสอบเจาะระบบ**
  - **ขั้นตอน:** พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ เพื่อประเมินความถูกต้องของระบบรักษาความมั่นคงปลอดภัย ตัวอย่างเช่น การทดสอบเจาะระบบของระบบควบคุมเครื่องจักรหลังการปรับปรุงเทคโนโลยีใหม่
- **5.4 การรับรองผู้ทดสอบเจาะระบบ**
  - **ขั้นตอน:** ตรวจสอบให้แน่ใจว่าผู้ทดสอบเจาะระบบมีการรับรองและประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม และผู้ทดสอบต้องเป็นอิสระจากระบบที่ทำการทดสอบ เช่น การใช้ผู้ทดสอบเจาะระบบที่ได้รับการรับรองจากองค์กรมาตรฐานสากล เช่น CEH – Certificated Ethical Hacker, OSCP – Offensive Security Certificated Professional

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

- **5.5 การควบคุมการทดสอบเจาะระบบโดยองค์กร/หน่วยงานที่รับผิดชอบ**
  - **ขั้นตอน:** ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดดำเนินการภายใต้การดูแลขององค์กร/หน่วยงานที่รับผิดชอบ โดยต้องมีทีมงานภายในองค์กรควบคุมและตรวจสอบการทดสอบเจาะระบบที่ดำเนินการโดยผู้ให้บริการภายนอก

6. การติดตามและจัดการช่องโหว่ (Vulnerability Management)

- **6.1 การติดตามและจัดการช่องโหว่**
  - **ขั้นตอน:** สร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ ซึ่งมีการใช้ระบบติดตามการแก้ไขช่องโหว่ (Vulnerability Management System) เพื่อรับประกันว่าช่องโหว่ทั้งหมดถูกแก้ไขตามกำหนดเวลา

7. การรายงานผลการทดสอบเจาะระบบ (Penetration Testing Reporting)

- **ขั้นตอน:** หากได้รับการร้องขอจากหน่วยงานควบคุมหรือกำกับดูแล ทางหน่วยงานโครงสร้างพื้นฐานสำคัญต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน 30 วันหลังจากได้รับการร้องขอ โดยรูปแบบของรายงานให้เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

ต่อไปนี้ เป็นกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Process)

1. การประเมินช่องโหว่ (Vulnerability Assessment)

- **1.1 ขอบเขตของการประเมินช่องโหว่**
  - ประเมินช่องโหว่ของ **ระบบเทคโนโลยีสารสนเทศ (IT System)** ที่ให้บริการสำคัญ
  - ประเมินช่องโหว่ของ **ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)**
- **1.2 รายการที่ต้องตรวจสอบ**
  - **การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)**
  - **การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)**
  - **การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)**
- **1.3 ระยะเวลาในการดำเนินการ**
  - ดำเนินการประเมินอย่างน้อย **ปีละ 1 ครั้ง** หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

2. การทดสอบเจาะระบบ (Penetration Testing)

- **2.1 ขอบเขตของการทดสอบเจาะระบบ**
  - ทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ
  - ทดสอบเจาะระบบของระบบที่เชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing Systems)
- **2.2 การทดสอบเจาะระบบเป็นประจำ**
  - พิจารณาดำเนินการทดสอบเจาะระบบ **ปีละ 1 ครั้ง** หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ หรือการเปลี่ยนเทคโนโลยี
- **2.3 การรับรองผู้ทดสอบเจาะระบบ**
  - ผู้ทดสอบเจาะระบบต้องมีการรับรองและได้รับประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม
- **2.4 การดำเนินการทดสอบเจาะระบบ**
  - ทดสอบเจาะระบบทั้งหมดดำเนินการภายใต้การดูแลขององค์กร/หน่วยงาน และควบคุมโดยผู้ทดสอบที่เป็นอิสระจากระบบที่ถูกทดสอบ

3. การติดตามและจัดการกับช่องโหว่ (Vulnerability Management)

- **3.1 กระบวนการติดตาม**
  - สร้างกระบวนการเพื่อติดตามและจัดการช่องโหว่ที่ระบุในผลการประเมินและการทดสอบเจาะระบบ
- **3.2 การแก้ไขช่องโหว่**
  - ตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

=

Logo	ระเบียบกระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นเอกสารของความลับ	Internal Use Only

- **3.3 รายงานผลการทดสอบ**
  - หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานโครงสร้างพื้นฐานสำคัญต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน **30 วัน** หลังจากได้รับหนังสือร้องขอ

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review**)

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายงาน/ผลการทดสอบเจาะระบบ
2. รายงาน/ผลการประเมินช่องโหว่
3. เอกสารการประเมินความเสี่ยง ทั้ง 3 ด้าน (Host Security, Network Security, Architecture Security)
4. Vulnerability Management System

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเจาะระบบ (Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเจาะระบบ (Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

1. วัตถุประสงค์ (Objective)

การทดสอบเจาะระบบมีวัตถุประสงค์เพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT System) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) เพื่อให้สามารถดำเนินการแก้ไขปัญหาเหล่านั้นได้ก่อนที่จะถูกโจมตีจริง

2. ขอบเขตของการทดสอบ (Scope of Testing)

การทดสอบจะครอบคลุมระบบและส่วนประกอบต่อไปนี้

- ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) Systems)
- ระบบควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS)
- โครงสร้างพื้นฐานทางเครือข่าย (Network Infrastructure)
- แอปพลิเคชันและบริการที่เชื่อมต่ออินเทอร์เน็ต (Internet-facing Applications and Services)
- ฐานข้อมูล (Database)
- ระบบควบคุมการเข้าถึง (Access Control System)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

3. ทีมที่รับผิดชอบ (Responsibility)

- **ผู้ทดสอบเจาะระบบ (Penetration Tester):** ทีมความมั่นคงปลอดภัยหรือผู้ให้บริการภายนอกที่ได้รับการรับรอง
- **ผู้ประสานงาน (Coordinator):** ผู้จัดการหรือหัวหน้าทีมที่มีหน้าที่ดูแลและประสานงานกับทีมต่าง ๆ
- **เจ้าของระบบ (System Owner):** เจ้าของหรือผู้ดูแลระบบที่ได้รับการทดสอบ

4. ขั้นตอนการทดสอบ (Testing Procedure)

4.1 การวางแผนและการเตรียมการ (Planning and Preparation)

- **กำหนดขอบเขตการทดสอบ (Define Scope):** ระบุระบบและส่วนประกอบที่ต้องการทดสอบ เช่น ระบบฐานข้อมูล, ระบบควบคุมเครื่องจักร, หรือระบบเครือข่าย โดยในการทดสอบนี้ ขอบเขตครอบคลุมถึงระบบฐานข้อมูลของลูกค้า ระบบเครือข่ายที่ใช้ในการสื่อสาร และแอปพลิเคชันที่เชื่อมต่อกับอินเทอร์เน็ต
- **จัดทำเอกสารการอนุญาต (Obtain Authorization):** ขอกำหนดการอนุญาตจากเจ้าของระบบหรือผู้บริหารที่เกี่ยวข้องเพื่อดำเนินการทดสอบ ซึ่งต้องได้รับอนุญาตจากฝ่าย IT และผู้จัดการฝ่ายความมั่นคงสารสนเทศในการดำเนินการทดสอบเจาะระบบ
- **เตรียมเครื่องมือและทรัพยากร (Prepare Tools and Resources):**ตรวจสอบเครื่องมือที่จะใช้ในการทดสอบให้มีความพร้อมใช้ เช่น เครื่องมือสำหรับการสแกนช่องโหว่ (Nessus) และเครื่องมือสำหรับการทดสอบการเจาะระบบ (Metasploit)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเจาะระบบ (Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4.2 การสแกนและการรวบรวมข้อมูล (Scanning and Information Gathering)

- **สแกนหาช่องโหว่ (Vulnerability Scanning):** ใช้เครื่องมือสแกนหาช่องโหว่ (Nessus) ในระบบเครือข่ายหรือเซิร์ฟเวอร์ฐานข้อมูลเพื่อหาช่องโหว่ การตั้งค่าการเข้าถึง
- **รวบรวมข้อมูลเกี่ยวกับระบบเป้าหมาย (Information Gathering):** รวบรวมข้อมูลที่จำเป็นเกี่ยวกับระบบที่กำลังทดสอบ เช่น ที่อยู่ IP, โดเมน, และบริการที่เปิดใช้งาน รวมถึงพอร์ตที่เปิดใช้งาน

4.3 การวิเคราะห์และการทดสอบช่องโหว่ (Analysis and Exploitation)

- **วิเคราะห์ผลการสแกน (Analyze Scan Results):** ตรวจสอบผลการสแกนเพื่อระบุช่องโหว่ที่ควรดำเนินการทดสอบเพิ่มเติม เช่น มีช่องโหว่ในระบบฐานข้อมูลที่เปิดให้เข้าถึงได้หรือไม่ โดยไม่ได้รับอนุญาตผ่านพอร์ตที่ไม่ได้เข้ารหัส
- **ทดสอบการเจาะระบบ (Exploitation Testing):** ดำเนินการทดสอบเจาะระบบโดยใช้เครื่องมือเฉพาะเพื่อยืนยันและประเมินความรุนแรงของช่องโหว่ที่พบ โดยใช้เครื่องมือ Metasploit ในการเจาะระบบฐานข้อมูลผ่านช่องโหว่ที่พบ และดูว่าสามารถเข้าถึงข้อมูลสำคัญได้หรือไม่

4.4 การรายงานและการสรุปผล (Reporting and Conclusion)

- **จัดทำรายงานผลการทดสอบ (Create Testing Report):** สรุปผลการทดสอบที่ดำเนินการ ช่องโหว่ที่พบ ความรุนแรง และแนวทางการแก้ไข ซึ่งการจัดทำรายงานนั้นต้อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

ระบุว่าได้พบช่องโหว่ที่รุนแรงในระบบฐานข้อมูลหรืออื่นๆและพร้อมการนำเสนอการปรับปรุง ด้วย เช่น การตั้งค่าไฟร์วอลล์และการเข้ารหัสข้อมูล เป็นต้น

2. **เสนอแนะการแก้ไข (Provide Remediation Recommendations):** ให้คำแนะนำเกี่ยวกับวิธีการแก้ไขช่องโหว่ที่พบในการทดสอบ
    - **สรุปผลการทดสอบกับผู้เกี่ยวข้อง (Conclude Testing with Stakeholders):** สรุปผลการทดสอบและข้อเสนอแนะให้กับทีมงานที่เกี่ยวข้องและเจ้าของระบบรับทราบ หรืออาจจัดประชุมสรุปผลการทดสอบกับทีม IT และผู้จัดการฝ่ายความมั่นคงสารสนเทศ ก็ได้ เพื่อดำเนินการแก้ไขช่องโหว่ตามข้อเสนอแนะ

4.5 การติดตามผลการแก้ไข (Follow-Up on Remediation)

1. **ตรวจสอบการแก้ไขช่องโหว่ (Verify Remediation):** ทดสอบช่องโหว่ที่ได้รับการแก้ไขแล้วอีกครั้ง เพื่อยืนยันว่าได้ทำการแก้ไขอย่างถูกต้องและไม่มีความเสี่ยงอีกต่อไป

5. สรุปและการปิดโครงการ (Summary and Closure)

1. **ปิดโครงการทดสอบเจาะระบบ (Project Closure):** สรุปโครงการและปิดโครงการหลังจากได้ดำเนินการทดสอบเจาะระบบและแก้ไขช่องโหว่ทั้งหมดแล้ว
2. **จัดเก็บเอกสาร (Documentation Storage):** จัดเก็บรายงานผลการทดสอบและเอกสารที่เกี่ยวข้องอย่างปลอดภัย เพื่อใช้เป็นข้อมูลอ้างอิงในอนาคต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเจาะระบบ (Penetration Testing Procedure)	รหัสเอกสาร	CSMS-Identify -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review**)

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนรวมถึงขอบเขตการทดสอบเจาะระบบ
2. เอกสารที่ได้รับการอนุญาตในการเจาะระบบ
3. ผลการทดสอบช่องโหว่
4. รายงานผลการทดสอบ
5. รายงานผลการติดตามการแก้ไข
6. เอกสารสรุปปิดโครงการ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : ทีมประเมินความเสี่ยง (ช่องโหว่)

วันที่ทำการประเมินช่องโหว่ : 1/05/2567

รายงานการประเมินช่องโหว่ พร้อมกับระบุความรุนแรงและการแก้ไข (Vulnerability Assessment and Treatment)

แบ่งการประเมินช่องโหว่ ออกเป็น 2 ดังนี้

1. ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
2. ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

ซึ่งขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

1. การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
2. การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
3. การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

---

1. ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) System)

1.1 การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

	ช่องโหว่ที่พบ	ความรุนแรง	การแก้ไข | เสร็จเมื่อไหร่
1	ระบบปฏิบัติการไม่ได้รับการอัปเดตเป็นเวอร์ชันล่าสุด	สูง (High)	อัปเดตระบบปฏิบัติการและซอฟต์แวร์ทั้งหมดให้เป็นเวอร์ชันล่าสุด | 1 กันยายน 2567
2	ใช้รหัสผ่านที่ไม่ซับซ้อนสำหรับผู้ใช้ระดับสูง	สูง (High)	กำหนดนโยบายการตั้งรหัสผ่านที่ซับซ้อนและบังคับให้เปลี่ยนรหัสผ่านเป็นระยะ | 1 กันยายน 2567
3	ไม่มีการติดตั้งซอฟต์แวร์ป้องกันไวรัส	สูง (High)	ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่ได้รับการอัปเดตอย่างสม่ำเสมอ | 1 กันยายน 2567
4	บัญชีผู้ใช้มีสิทธิ์เกินความจำเป็น	กลาง (Medium)	ตรวจสอบและปรับลดสิทธิ์ของผู้ใช้ให้ตรงกับความจำเป็นในการใช้งาน | 1 กันยายน 2567
5	ไม่มีระบบล็อกอินแบบสองชั้น (2FA)	สูง (High)	ติดตั้งระบบล็อกอินแบบสองชั้น (2FA) เพื่อเพิ่มความปลอดภัย | 1 กันยายน 2567
6	ใช้ซอฟต์แวร์ที่ไม่ได้รับการสนับสนุนจากผู้ผลิต	สูง (High)	อัปเกรดหรือเปลี่ยนซอฟต์แวร์เป็นเวอร์ชันที่ได้รับการสนับสนุน | 1 กันยายน 2567

7	เก็บข้อมูลสำคัญในพื้นที่ที่ไม่ได้เข้ารหัส	สูง (High)	เข้ารหัสข้อมูลสำคัญทั้งหมดที่เก็บในระบบ | 1 กันยายน 2567
8	ไม่มีการตรวจสอบสิทธิ์การเข้าถึงไฟล์และระบบเป็นประจำ	กลาง (Medium)	จัดทำการตรวจสอบสิทธิ์การเข้าถึงไฟล์และระบบเป็นประจำ | 1 กันยายน 2567
9	ไฟล์ที่อนุญาตให้เข้าถึงได้โดยผู้ใช้ทั่วไป	สูง (High)	จำกัดการเข้าถึงไฟล์สำคัญเฉพาะผู้ใช้ที่มีสิทธิ์ | 1 กันยายน 2567
10	ไม่มีการลบข้อมูลที่ไม่จำเป็นออกจากระบบ	กลาง (Medium)	จัดทำนโยบายการลบข้อมูลที่ไม่จำเป็นเป็นประจำ | 1 กันยายน 2567

1.2 การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

	ช่องโหว่ที่พบ	**ความรุนแรง**	**การแก้ไข | เสร็จเมื่อไหร่**
1	การตั้งค่าไฟร์วอลล์ที่ไม่ถูกต้อง	สูง (High)	ปรับปรุงการตั้งค่าไฟร์วอลล์ให้ถูกต้องและจำกัดการเข้าถึงจากภายนอก | 1 กันยายน 2567
2	ใช้ระบบเครือข่ายที่ไม่ได้เข้ารหัส	สูง (High)	ติดตั้งระบบเข้ารหัสข้อมูลสำหรับการสื่อสารผ่านเครือข่าย | 1 กันยายน 2567
3	ไม่มีการใช้ระบบตรวจจับการบุกรุก (IDS/IPS)	สูง (High)	ติดตั้งระบบตรวจจับการบุกรุก (IDS/IPS) เพื่อป้องกันการโจมตี | 1 กันยายน 2567
4	เปิดใช้งานพอร์ตที่ไม่จำเป็น	กลาง (Medium)	ปิดการใช้งานพอร์ตที่ไม่จำเป็นและจำกัดพอร์ตที่ต้องใช้งานจริงเท่านั้น | 1 กันยายน 2567
5	ไม่มีการแบ่งแยกเครือข่ายระหว่างส่วนที่สำคัญและไม่สำคัญ	สูง (High)	จัดทำการแบ่งแยกเครือข่ายระหว่างส่วนที่สำคัญและส่วนที่ไม่สำคัญ | 1 กันยายน 2567
6	ใช้โปรโตคอลที่ไม่ปลอดภัย เช่น FTP แทน SFTP	กลาง (Medium)	เปลี่ยนมาใช้โปรโตคอลที่ปลอดภัย เช่น SFTP ในการถ่ายโอนไฟล์ | 1 กันยายน 2567
7	ไม่มีการควบคุมการเข้าถึงเครือข่ายไร้สายอย่างเข้มงวด	สูง (High)	ตั้งค่าการควบคุมการเข้าถึงเครือข่ายไร้สายให้เข้มงวดมากขึ้น | 1 กันยายน 2567
8	ไม่มีการตั้งค่า VPN สำหรับการเข้าถึงระยะไกล	สูง (High)	ติดตั้งและกำหนดใช้งาน VPN สำหรับการเข้าถึงระบบจากภายนอก | 1 กันยายน 2567
9	ใช้ DNS ที่ไม่ได้รับการรักษาความปลอดภัย	กลาง (Medium)	เปลี่ยนมาใช้ DNS ที่มีการรักษาความปลอดภัยและติดตั้ง DNSSEC | 1 กันยายน 2567
10	ไม่มีการตรวจสอบการตั้งค่าความปลอดภัยของเครือข่าย	กลาง (Medium)	จัดทำการตรวจสอบการตั้งค่าความปลอดภัยของเครือข่ายเป็นประจำ | 1 กันยายน 2567

1.3 การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

	ช่องโหว่ที่พบ	ความรุนแรง	การแก้ไข | เสร็จเมื่อไหร่
1	ไม่มีการแบ่งแยกเครือข่ายระหว่างส่วนที่สำคัญและไม่สำคัญ	สูง (High)	จัดทำการแบ่งแยกเครือข่ายระหว่างส่วนที่สำคัญและไม่สำคัญ | 1 กันยายน 2567
2	ไม่มีการแยกข้อมูลสำคัญออกจากระบบทั่วไป	สูง (High)	แยกข้อมูลสำคัญออกจากระบบทั่วไปเพื่อเพิ่มความปลอดภัย | 1 กันยายน 2567
3	การออกแบบระบบที่ไม่มีการสำรองข้อมูลเพียงพอ	สูง (High)	เพิ่มการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลเป็นประจำ | 1 กันยายน 2567
4	ไม่มีการควบคุมการเข้าถึงระหว่างส่วนต่างๆ ของระบบ	สูง (High)	จัดทำการควบคุมการเข้าถึงระหว่างส่วนต่างๆ ของระบบอย่างเข้มงวด | 1 กันยายน 2567
5	การใช้ระบบที่มีการพึ่งพาอุปกรณ์หรือซอฟต์แวร์เก่า	กลาง (Medium)	อัปเกรดหรือเปลี่ยนอุปกรณ์และซอฟต์แวร์ที่เก่าและไม่มีการสนับสนุน | 1 กันยายน 2567
6	ไม่มีการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรมเป็นประจำ	กลาง (Medium)	จัดทำการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรมเป็นระยะ ๆ | 1 กันยายน 2567
7	ขาดการควบคุมการเข้าถึงและการตรวจสอบภายในระบบ	สูง (High)	ติดตั้งระบบควบคุมการเข้าถึงและการตรวจสอบกิจกรรมภายในระบบ | 1 กันยายน 2567
8	ไม่มีการแบ่งแยกเครือข่ายสำหรับการทดสอบและการผลิต	สูง (High)	จัดทำเครือข่ายแยกระหว่างการทดสอบและการผลิตเพื่อป้องกันการรั่วไหลของข้อมูล | 1 กันยายน 2567
9	ขาดการเข้ารหัสข้อมูลในส่วนที่สำคัญของระบบ	สูง (High)	ติดตั้งการเข้ารหัสข้อมูลในส่วนที่สำคัญของระบบ | 1 กันยายน 2567
10	การออกแบบที่ไม่มีการกู้คืนระบบหลังจากเกิดเหตุขัดข้อง	สูง (High)	จัดทำแผนการกู้คืนระบบและทดสอบแผนเป็นประจำ | 1 กันยายน 2567

2. ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

2.1 การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

	ช่องโหว่ที่พบ	ความรุนแรง	การแก้ไข | เสร็จเมื่อไหร่
1	ใช้ซอฟต์แวร์เวอร์ชันเก่าที่มีช่องโหว่ด้านความปลอดภัย	สูง (High)	อัปเกรดซอฟต์แวร์เป็นเวอร์ชันที่มีการแก้ไขช่องโหว่ | 1 กันยายน 2567
2	ระบบปฏิบัติการของเครื่องจักรไม่มีการอัปเดต	สูง (High)	อัปเดตระบบปฏิบัติการของเครื่องจักรและติดตั้งแพตช์ความปลอดภัย | 1 กันยายน 2567
3	ไม่มีการตรวจสอบความมั่นคงปลอดภัยของโฮสต์เป็นประจำ	กลาง (Medium)	จัดทำการตรวจสอบความมั่นคงปลอดภัยของโฮสต์เป็นประจำ | 1 กันยายน 2567
4	ไม่มีการจำกัดสิทธิ์การเข้าถึงระบบควบคุมเครื่องจักร	สูง (High)	กำหนดสิทธิ์การเข้าถึงระบบควบคุมเครื่องจักรเฉพาะผู้ที่จำเป็น | 1 กันยายน 2567
5	การใช้บัญชีผู้ใช้ร่วมกันระหว่างหลายบุคคล	สูง (High)	ห้ามใช้บัญชีผู้ใช้ร่วมกันและให้มีการตรวจสอบการใช้บัญชีอย่างเข้มงวด | 1 กันยายน 2567
6	ไม่มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสในเครื่องควบคุม	กลาง (Medium)	ติดตั้งซอฟต์แวร์ป้องกันไวรัสในเครื่องควบคุมเครื่องจักร | 1 กันยายน 2567
7	ระบบควบคุมไม่มีการเข้ารหัสในการส่งข้อมูล	สูง (High)	ติดตั้งการเข้ารหัสข้อมูลในระบบควบคุมเพื่อป้องกันการโจมตี | 1 กันยายน 2567
8	ขาดการสำรองข้อมูลระบบควบคุมอย่างสม่ำเสมอ	กลาง (Medium)	จัดทำการสำรองข้อมูลของระบบควบคุมเป็นประจำ | 1 กันยายน 2567
9	การตั้งค่าระบบควบคุมเครื่องจักรที่ไม่ปลอดภัย	สูง (High)	ปรับปรุงการตั้งค่าระบบควบคุมเครื่องจักรให้ปลอดภัยมากขึ้น | 1 กันยายน 2567
10	การไม่จัดการกับช่องโหว่ที่ระบุในระบบควบคุมเครื่องจักร	สูง (High)	ดำเนินการแก้ไขช่องโหว่ที่ระบุและตรวจสอบเป็นระยะ | 1 กันยายน 2567

2.2 การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

	ช่องโหว่ที่พบ	ความรุนแรง	การแก้ไข | เสร็จเมื่อไหร่
1	การสื่อสารระหว่างเครื่องจักรไม่ได้เข้ารหัส	สูง (High)	ติดตั้งการเข้ารหัสในการสื่อสารระหว่างเครื่องจักรและระบบควบคุม | 1 กันยายน 2567
2	ไม่มีการใช้ไฟร์วอลล์ระหว่างระบบควบคุมและเครือข่ายทั่วไป	สูง (High)	ติดตั้งไฟร์วอลล์เพื่อแยกระบบควบคุมจากเครือข่ายทั่วไป | 1 กันยายน 2567
3	การเปิดใช้งานพอร์ตที่ไม่จำเป็นในระบบควบคุม	กลาง (Medium)	ปิดพอร์ตที่ไม่จำเป็นในระบบควบคุมและจำกัดพอร์ตที่จำเป็นต้องใช้งาน | 1 กันยายน 2567
4	ไม่มีการตรวจสอบการเข้าถึงเครือข่ายของระบบควบคุม	สูง (High)	ติดตั้งระบบตรวจสอบการเข้าถึงเครือข่ายของระบบควบคุม | 1 กันยายน 2567
5	การใช้โปรโตคอลที่ไม่ปลอดภัยในระบบควบคุม	กลาง (Medium)	เปลี่ยนไปใช้โปรโตคอลที่มีความปลอดภัยในการสื่อสาร | 1 กันยายน 2567
6	ขาดการแบ่งแยกเครือข่ายสำหรับระบบควบคุมเครื่องจักร	สูง (High)	แยกเครือข่ายสำหรับระบบควบคุมเครื่องจักรเพื่อเพิ่มความปลอดภัย | 1 กันยายน 2567
7	การเปิดใช้งานการเข้าถึงจากภายนอกในระบบควบคุม	สูง (High)	ปิดการเข้าถึงจากภายนอกและกำหนดนโยบายเข้มงวดในการเข้าถึง | 1 กันยายน 2567
8	ไม่มีการควบคุมการเข้าถึงเครือข่ายไร้สายในพื้นที่โรงงาน	สูง (High)	ติดตั้งระบบควบคุมการเข้าถึงเครือข่ายไร้สายที่มีความปลอดภัยสูง | 1 กันยายน 2567
9	การตั้งค่าเครือข่ายที่ไม่ปลอดภัยสำหรับระบบควบคุม	สูง (High)	ปรับปรุงการตั้งค่าเครือข่ายให้มีความปลอดภัยสูงขึ้น | 1 กันยายน 2567
10	ไม่มีการตรวจสอบการตั้งค่าความปลอดภัยของระบบควบคุม	กลาง (Medium)	จัดทำการตรวจสอบการตั้งค่าความปลอดภัยของระบบควบคุมเป็นระยะ ๆ | 1 กันยายน 2567

2.3 การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

	ช่องโหว่ที่พบ	ความรุนแรง	การแก้ไข | เสร็จเมื่อไหร่
1	ไม่มีการแบ่งแยกเครือข่ายระหว่างส่วนควบคุมและส่วนทั่วไป	สูง (High)	จัดทำการแบ่งแยกเครือข่ายระหว่างส่วนควบคุมและส่วนทั่วไป | 1 กันยายน 2567
2	ไม่มีการแยกข้อมูลสำคัญออกจากระบบทั่วไป	สูง (High)	แยกข้อมูลสำคัญออกจากระบบทั่วไปเพื่อเพิ่มความปลอดภัย | 1 กันยายน 2567
3	การออกแบบระบบควบคุมที่ไม่มีการสำรองข้อมูลเพียงพอ	สูง (High)	เพิ่มการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลในระบบควบคุมเครื่องจักร | 1 กันยายน 2567
4	ขาดการควบคุมการเข้าถึงระหว่างส่วนต่างๆ ของระบบควบคุม	สูง (High)	ติดตั้งระบบควบคุมการเข้าถึงและการตรวจสอบกิจกรรมภายในระบบควบคุม | 1 กันยายน 2567
5	การใช้ระบบควบคุมที่มีการพึ่งพาอุปกรณ์หรือซอฟต์แวร์เก่า	กลาง (Medium)	อัปเกรดหรือเปลี่ยนอุปกรณ์และซอฟต์แวร์ที่เก่าและไม่มีการสนับสนุน | 1 กันยายน 2567
6	ไม่มีการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรมเป็นประจำ	กลาง (Medium)	จัดทำการตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรมเป็นระยะ ๆ | 1 กันยายน 2567
7	ขาดการควบคุมการเข้าถึงและการตรวจสอบภายในระบบควบคุม	สูง (High)	ติดตั้งระบบควบคุมการเข้าถึงและการตรวจสอบกิจกรรมภายในระบบควบคุม | 1 กันยายน 2567
8	การไม่แยกระบบควบคุมระหว่างการทดสอบและการผลิต	สูง (High)	จัดทำเครือข่ายแยกระหว่างการทดสอบและการผลิตในระบบควบคุมเครื่องจักร | 1 กันยายน 2567
9	ขาดการเข้ารหัสข้อมูลในส่วนที่สำคัญของระบบควบคุม	สูง (High)	ติดตั้งการเข้ารหัสข้อมูลในส่วนที่สำคัญของระบบควบคุมเครื่องจักร | 1 กันยายน 2567
10	การออกแบบที่ไม่มีการกู้คืนระบบควบคุมหลังจากเกิดเหตุขัดข้อง	สูง (High)	จัดทำแผนการกู้คืนระบบควบคุมและทดสอบแผนเป็นประจำ | 1 กันยายน 2567

รายงานสรุปผลการทดสอบเจาะระบบ (Penetration Testing Report Summary)

จัดทำโดย : นาย สุรศักดิ์ มั่นคง

จัดทำเมื่อ : 15/09/2567

---

1. ข้อมูลทั่วไป (General Information)

- **ชื่อหน่วยงาน:** บริษัท/องค์กร ...
- **วันที่ทดสอบ:** 01/09/2567 - 05/09/2567
- **ทีมทดสอบ:** ทีมความมั่นคงปลอดภัยไซเบอร์ / ผู้ให้บริการภายนอก
- **ผู้ประสานงาน:** นาย A , หัวหน้าทีมรักษาความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ
- **เจ้าของระบบที่ทดสอบ:** นาย B , ผู้จัดการฝ่าย IT

2. วัตถุประสงค์ของการทดสอบ (Objective of Testing)

การทดสอบเจาะระบบครั้งนี้มีวัตถุประสงค์เพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงระบบเทคโนโลยีสารสนเทศ (IT System) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) ของบริษัท ... เพื่อให้สามารถดำเนินการแก้ไขช่องโหว่เหล่านั้นได้ก่อนที่จะเกิดการโจมตีจริง

3. ขอบเขตของการทดสอบ (Scope of Testing)

การทดสอบเจาะระบบครอบคลุมระบบและส่วนประกอบต่อไปนี้

- ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) System)
- ระบบควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)
- โครงสร้างพื้นฐานทางเครือข่าย (Network Infrastructure)
- แอปพลิเคชันและบริการที่เชื่อมต่ออินเทอร์เน็ต (Internet-facing Applications and Services)
- ฐานข้อมูลลูกค้า (Customer Database)

- ระบบควบคุมการเข้าถึง (Access Control System)

ผลการทดสอบ (Testing Results) - แนะนำควรเป็นระบบ Application ทั้งหมดที่อยู่ในองค์กร

ลำดับที่	ระบบที่ทดสอบ (System Tested)	ช่องโหว่ที่พบ (Vulnerabilities Found)	ความรุนแรง (Severity)	การแก้ไขที่แนะนำ (Recommended Remediation)	สถานะการแก้ไข (Remediation Status)
1	ระบบฐานข้อมูลลูกค้า (Customer Database)	พบการเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต	สูง (High)	ติดตั้งการยืนยันตัวตนสองชั้น (2FA) และเข้ารหัสข้อมูล	แก้ไขแล้วเสร็จ 15/09/2567
2	ระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS)	พบช่องโหว่ในการสื่อสารระหว่างระบบและเครื่องจักร	สูง (High)	ติดตั้งการเข้ารหัสในการสื่อสารและตรวจสอบการเข้าถึง	แก้ไขแล้วเสร็จ 15/09/2567
3	ระบบเครือข่าย (Network Infrastructure)	พบการตั้งค่าไฟร์วอลล์ที่ไม่ปลอดภัย	กลาง (Medium)	ปรับปรุงการตั้งค่าไฟร์วอลล์และกำหนดนโยบายการเข้าถึง	แก้ไขแล้วเสร็จ 15/09/2567
4	แอปพลิเคชันภายนอก (Internet-facing Applications)	พบช่องโหว่ SQL Injection	สูง (High)	ปรับปรุงโค้ดเพื่อป้องกัน SQL Injection	แก้ไขแล้วเสร็จ 15/09/2567
5	ระบบควบคุมการเข้าถึง (Access Control System)	พบการตั้งค่าการเข้าถึงที่ไม่ปลอดภัย	กลาง (Medium)	แก้ไขการตั้งค่าและตรวจสอบสิทธิ์การเข้าถึงเป็นประจำ	แก้ไขแล้วเสร็จ 15/09/2567
6	ระบบสำรองข้อมูล (Backup System)	พบว่าข้อมูลสำรองไม่มีการเข้ารหัส	สูง (High)	เข้ารหัสข้อมูลสำรองและเก็บในที่ปลอดภัย	แก้ไขแล้วเสร็จ 15/09/2567
7	ระบบอีเมลองค์กร (Email System)	พบช่องโหว่ในการส่งอีเมลฟิชชิ่ง	สูง (High)	ติดตั้งระบบกรองอีเมลฟิชชิ่งและการฝึกอบรมผู้ใช้	แก้ไขแล้วเสร็จ 15/09/2567
8	ระบบควบคุมการเข้า-ออกสถานที่ (Physical Access Control System)	พบการตั้งค่าไม่ปลอดภัยในระบบควบคุมการเข้าถึงทางกายภาพ	กลาง (Medium)	ปรับปรุงการตั้งค่าและติดตั้งการตรวจสอบการเข้าถึง	แก้ไขแล้วเสร็จ 15/09/2567
9	ระบบจัดการข้อมูลลูกค้า (Customer Information Management System)	พบช่องโหว่ในการป้องกันการรั่วไหลของข้อมูลลูกค้า	สูง (High)	เข้ารหัสข้อมูลลูกค้าและจำกัดการเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง	แก้ไขแล้วเสร็จ 15/09/2567
10	ระบบจัดการสิทธิ์ผู้ใช้ (User Account Management System)	พบช่องโหว่ในการจัดการสิทธิ์ของผู้ใช้	กลาง (Medium)	ปรับปรุงการจัดการสิทธิ์และตรวจสอบการเข้าถึงอย่างสม่ำเสมอ	แก้ไขแล้วเสร็จ 15/09/2567

สรุปผลการทดสอบ (Summary of Findings)

1. **ระบบฐานข้อมูลลูกค้า (Customer Database)**
    - พบว่ามีการเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต ซึ่งเป็นช่องโหว่ที่มีความรุนแรงสูง (High)
    - แนะนำให้ติดตั้งระบบการยืนยันตัวตนแบบสองชั้น (2FA) และเข้ารหัสข้อมูลที่จัดเก็บในฐานข้อมูลเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
2. **ระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS)**
    - พบช่องโหว่ในการสื่อสารระหว่างระบบควบคุมและเครื่องจักร ไม่มีการเข้ารหัส ทำให้เสี่ยงต่อการโจมตี
    - แนะนำให้ติดตั้งการเข้ารหัสในการสื่อสารและตรวจสอบการเข้าถึงเพื่อเพิ่มความปลอดภัยของระบบ
3. **ระบบเครือข่าย (Network Infrastructure)**
    - พบการตั้งค่าไฟร์วอลล์ที่ไม่ปลอดภัย ทำให้บริการบางส่วนสามารถเข้าถึงได้จากเครือข่ายภายนอก
    - แนะนำให้ปรับปรุงการตั้งค่าไฟร์วอลล์และกำหนดนโยบายการเข้าถึงอย่างเข้มงวดเพื่อป้องกันการโจมตีจากภายนอก
4. **แอปพลิเคชันภายนอก (Internet-facing Applications)**
    - พบช่องโหว่ SQL Injection ในแอปพลิเคชันภายนอก ซึ่งมีความรุนแรงสูง (High)
    - แนะนำให้ปรับปรุงโค้ดของแอปพลิเคชันเพื่อป้องกันการโจมตีแบบ SQL Injection ที่อาจทำให้ข้อมูลถูกขโมยหรือถูกแก้ไข
5. **ระบบควบคุมการเข้าถึง (Access Control System)**
    - พบว่าการตั้งค่าการเข้าถึงไม่ปลอดภัยในระบบควบคุมการเข้าถึง มีความรุนแรงปานกลาง (Medium)
    - แนะนำให้แก้ไขการตั้งค่าและทำการตรวจสอบสิทธิ์การเข้าถึงอย่างสม่ำเสมอเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
6. **ระบบสำรองข้อมูล (Backup System)**
    - พบว่าข้อมูลสำรองไม่มีการเข้ารหัส ทำให้เสี่ยงต่อการถูกเข้าถึงหรือขโมยข้อมูล
    - แนะนำให้เข้ารหัสข้อมูลสำรองทั้งหมดและจัดเก็บในพื้นที่ที่มีความปลอดภัยสูงเพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
7. **ระบบอีเมลองค์กร (Corporate Email System)**
    - พบช่องโหว่ที่ทำให้ผู้ใช้สามารถส่งอีเมลฟิชชิ่งได้ง่าย ซึ่งอาจนำไปสู่การโจมตีแบบฟิชชิ่ง
    - แนะนำให้ติดตั้งระบบกรองอีเมลฟิชชิ่งและทำการฝึกอบรมผู้ใช้เกี่ยวกับการรับรู้และป้องกันฟิชชิ่ง
8. **ระบบควบคุมการเข้า-ออกสถานที่ (Physical Access Control System)**
    - พบการตั้งค่าที่ไม่ปลอดภัยในระบบควบคุมการเข้าถึงทางกายภาพ ทำให้เสี่ยงต่อการบุกรุกสถานที่

- แนะนำให้ปรับปรุงการตั้งค่าและติดตั้งระบบตรวจสอบการเข้าถึงเพื่อเพิ่มความปลอดภัย

9. **ระบบจัดการข้อมูลลูกค้า (Customer Information Management System)**
    - พบช่องโหว่ในการป้องกันการรั่วไหลของข้อมูลลูกค้า ซึ่งมีความรุนแรงสูง (High)
    - แนะนำให้เข้ารหัสข้อมูลลูกค้าและจำกัดการเข้าถึงเฉพาะผู้ที่มีความจำเป็น เพื่อป้องกันการรั่วไหลของข้อมูล
10. **ระบบจัดการสิทธิ์ผู้ใช้ (User Account Management System)**

- พบช่องโหว่ในการจัดการสิทธิ์ของผู้ใช้ ทำให้สิทธิ์การเข้าถึงของบางผู้ใช้ไม่ถูกต้องหรือเกินความจำเป็น
- แนะนำให้ปรับปรุงการจัดการสิทธิ์และตรวจสอบการเข้าถึงอย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

การติดตามและตรวจสอบผลการแก้ไข (Follow-Up and Verification)

หลังจากดำเนินการแก้ไขช่องโหว่ที่ระบุแล้ว ทีมความมั่นคงปลอดภัยไซเบอร์จะทำการทดสอบซ้ำเพื่อยืนยันว่าช่องโหว่เหล่านั้นได้รับการแก้ไขอย่างถูกต้อง และระบบบริการที่สำคัญดังกล่าว มีความปลอดภัยจากการคุกคามทางไซเบอร์

สรุปผลการทดสอบกับผู้บริหาร (Conclusion with Stakeholders)

ในที่ประชุมร่วมกับทีมงานและผู้บริหารที่เกี่ยวข้อง ได้มีการสรุปผลการทดสอบและแผนการแก้ไขช่องโหว่ที่พบ เพื่อให้มั่นใจว่าระบบทั้งหมดจะได้รับการป้องกันอย่างเหมาะสมต่อความเสี่ยงที่อาจเกิดขึ้น

ลงชื่อ: นาย A , หัวหน้าทีมรักษาความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ

ลงวันที่ 15 กันยายน 2567

4. กระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)

Logo	**ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)**	**รหัสเอกสาร**	**CSMS-Identify-05**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	รหัสเอกสาร	CSMS-Identify-05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.4.1, ข้อ 21.4.2, ข้อ 21.4.3, ข้อ 21.4.4]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าผู้ให้บริการภายนอกที่เข้ามาเกี่ยวข้องกับบริการที่สำคัญขององค์กรสามารถปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด และเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการภายนอก

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในการจัดทำข้อตกลงและสัญญากับผู้ให้บริการภายนอก รวมถึงการตรวจสอบความถูกต้องและการปฏิบัติตามข้อกำหนดเหล่านั้น

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการกำกับดูแลและตรวจสอบให้แน่ใจว่ามีการจัดการผู้ให้บริการภายนอกอย่างเหมาะสมและปฏิบัติ ตาม พรบ ไซเบอร์ รวมถึงการอนุมัติข้อตกลงและสัญญาที่เกี่ยวข้อง
- **ทีมจัดการผู้ให้บริการภายนอก (Third Party Management Team)**: รับผิดชอบในการดำเนินการตามกระบวนการทั้งหมดที่เกี่ยวข้องกับผู้ให้บริการภายนอก รวมถึงการกำหนดข้อกำหนด การตรวจสอบและการเจรจาต่อรองสัญญา

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	รหัสเอกสาร	CSMS-Identify-05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **ผู้ให้บริการภายนอก (Third Party Providers)**: มีหน้าที่ในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในสัญญาหรือข้อตกลงกับองค์กร

4. การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Requirements)

- **4.1 การกำหนดข้อกำหนดในข้อตกลงระดับการให้บริการ (SLA) หรือสัญญากับผู้ให้บริการภายนอก**
  - **ขั้นตอน**: กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในข้อตกลงระดับการให้บริการ (SLA) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก เพื่อป้องกันและลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง การจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องมีการระบุข้อกำหนดที่ชัดเจนเกี่ยวกับการป้องกันข้อมูลที่สำคัญ เช่น การเข้ารหัสข้อมูล และการควบคุมการเข้าถึง รวมถึงพิจารณาใบรับรองที่ผู้ให้การบริการภายนอก ควรต้องมี เช่น ISO, NIST Cybersecurity จากหน่วยงานที่รับรอง โดยให้สอดคล้องกับวัตถุประสงค์ของโครงการที่ทำ
- **4.2 ประเภทของผู้ให้บริการภายนอก**
  - **ขั้นตอน**: ระบุประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญขององค์กร โดยพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ด้วย เนื่องจากอาจมีการเข้าถึงข้อมูลที่มีความสำคัญสูงขององค์กร
- **4.3 ภาระหน้าที่ของผู้ให้บริการภายนอก**
  - **ขั้นตอน**: ระบุภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญขององค์กรจากภัยคุกคามทางไซเบอร์ เช่น ผู้ให้บริการภายนอกต้องมีตรวจสอบระบบความปลอดภัยของตนเองอย่างสม่ำเสมอ หรือ ดำเนินการอัปเดตระบบรักษาความปลอดภัยทุกครั้งที่มีการเปลี่ยนแปลงเทคโนโลยี ให้รับทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	รหัสเอกสาร	CSMS-Identify-05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **4.4 การจัดการความเสี่ยงในห่วงโซ่อุปทาน (Supply Chain Risk Management)**
  - **ขั้นตอน**: ระบุความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานของผลิตภัณฑ์ และกำหนดมาตรการในการควบคุมความเสี่ยงเหล่านี้ โดยการการตรวจสอบแหล่งที่มาของการบริการ ในผลิตภัณฑ์ที่ผู้ให้บริการภายนอกจัดหามาให้ เพื่อป้องกันการใช้ส่วนประกอบหรือส่วนที่เกี่ยวข้องที่ไม่ได้มาตรฐานหรือมีความเสี่ยง
- **4.5 สิทธิ์ในการตรวจสอบ (Audit Rights)**
  - **ขั้นตอน**: ระบุสิทธิ์ขององค์กรในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดที่ระบุไว้ในสัญญา

5. การตรวจสอบความถูกต้องและความสอดคล้อง (Verification and Compliance)

- **5.1 การตรวจสอบความถูกต้องของผู้ให้บริการภายนอก**
  - **ขั้นตอน**: พิจารณาดำเนินการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา เช่น การตรวจสอบโดยบุคคลที่สาม (Site reference) และการตรวจสอบมาตรฐานของผลิตภัณฑ์
- **5.2 การเจรจาต่อรองเงื่อนไขของสัญญาจ้าง**
  - **ขั้นตอน**: พิจารณาเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับข้อกำหนดทางกฎหมายปัจจุบันหรือข้อบังคับใหม่ที่อาจเกิดขึ้นในอนาคต เช่น มีการประกาศใช้กฎหมายใหม่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

6. การติดตามและปรับปรุงกระบวนการ (Monitoring and Process Improvement)

- **ขั้นตอน**: ดำเนินการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอ และปรับปรุงกระบวนการจัดการผู้ให้บริการตามความเหมาะสม เพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดด้านความ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการจัดการผู้ให้บริการภายนอก (Third Party Management Procedure)	รหัสเอกสาร	CSMS-Identify-05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

มั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดยต้องมีการจัดทำรายงานผลการตรวจสอบกับผู้ให้บริการภายนอกเป็นรายไตรมาส

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ข้อตกลงระดับการให้บริการ (SLA)
2. เงื่อนไขของสัญญากับผู้ให้บริการภายนอก
3. หลักฐานการทำการประเมินความเสี่ยงไซเบอร์ที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
4. หลักฐานการทำการตรวจสอบระบบความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการภายนอก
5. ใบรับรองตามมาตรฐานสากลต่างๆ เช่น ISO/IEC 27001 (ISMS), ISO/IEC 29110 (Software Engineer), ISO 9001 (Quality), ISO 14001 (Environment), ISO 45001 (Safety)
6. ใบรับรองทางไซเบอร์ เช่น NIST Cybersecurity Management System

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : นาย สุรศักดิ์ มั่นคง

จัดทำเมื่อ : 15 / 09 / 2567

ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการภายนอก (Cybersecurity Requirements for Third-Party Providers)

1. การเข้าถึงข้อมูล (Data Access)

- **ข้อกำหนด**
  - ผู้ให้บริการภายนอกต้องจำกัดการเข้าถึงข้อมูลสำคัญเฉพาะบุคคลที่มีความจำเป็นต้องใช้เท่านั้น (Need-to-Know Basis)
  - ต้องมีการยืนยันตัวตน (Authentication) และการตรวจสอบสิทธิ์ (Authorization) สำหรับการเข้าถึงข้อมูลทุกครั้ง
  - ระบบการเข้าถึงต้องใช้การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA)

2. การจัดเก็บข้อมูล (Data Storage)

- **ข้อกำหนด**
  - ข้อมูลสำคัญทั้งหมดต้องถูกเข้ารหัสทั้งในระหว่างการจัดเก็บ (Data-at-Rest) และการส่งผ่าน (Data-in-Transit)
  - ผู้ให้บริการภายนอกต้องจัดให้มีการสำรองข้อมูล (Data Backup) อย่างสม่ำเสมอและจัดเก็บในสถานที่ที่ปลอดภัย
  - ต้องมีมาตรการป้องกันการเข้าถึงข้อมูลสำรองที่ไม่ได้รับอนุญาต

3. การสื่อสารข้อมูล (Data Communication)

- **ข้อกำหนด**
    - การสื่อสารข้อมูลระหว่างหน่วยงานและผู้ให้บริการภายนอกต้องใช้การเข้ารหัสที่มีมาตรฐานสากล เช่น TLS/SSL
    - ผู้ให้บริการต้องใช้ VPN ที่ปลอดภัยสำหรับการสื่อสารข้อมูลที่มีความสำคัญกับองค์กรหรือหน่วยงาน
    - ห้ามใช้โปรโตคอลหรือวิธีการสื่อสารที่ไม่ได้รับการอนุมัติจากฝ่ายความมั่นคงปลอดภัยไซเบอร์ขององค์กรหรือหน่วยงาน

4. การจัดการความปลอดภัย (Security Management)

- **ข้อกำหนด**
    - ผู้ให้บริการภายนอกต้องดำเนินการตามแนวปฏิบัติที่ดีที่สุดในด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การใช้การอัปเดตซอฟต์แวร์และแพตช์ความปลอดภัยอย่างสม่ำเสมอ
    - ต้องมีการตรวจสอบและบันทึกการเข้าถึงข้อมูลและระบบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
    - ผู้ให้บริการต้องมีการตรวจสอบภายในและการทดสอบความปลอดภัย (Security Testing) เป็นระยะ ๆ

5. การจัดการเหตุการณ์ความปลอดภัย (Incident Management)

- **ข้อกำหนด**
    - ผู้ให้บริการภายนอกต้องรายงานเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นทันทีแก่องค์กรหรือหน่วยงาน (ไม่เกิน 24 ชั่วโมง)
    - ต้องมีแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) ที่สอดคล้องกับนโยบายขององค์กรหรือหน่วยงาน
    - ผู้ให้บริการต้องร่วมมือกับองค์กรหรือหน่วยงานในการตรวจสอบและแก้ไขปัญหาที่เกิดขึ้นจากเหตุการณ์ความไม่ปลอดภัยทางไซเบอร์

6. การตรวจสอบและการปฏิบัติตามข้อกำหนด (Audit and Compliance)

- **ข้อกำหนด**
    - ผู้ให้บริการต้องยอมรับการตรวจสอบความมั่นคงปลอดภัยจากองค์กรหรือหน่วยงานหรือบุคคลที่สามตามที่องค์กรหรือหน่วยงานกำหนด
    - ผู้ให้บริการต้องจัดให้มีการตรวจสอบภายในและการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ
    - องค์กรหรือหน่วยงานมีสิทธิ์ในการตรวจสอบและประเมินความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการตลอดระยะเวลาของสัญญา

จัดทำโดย : นาย สุรศักดิ์ มั่นคง

จัดทำเมื่อ : 15 / 09 / 2567

ข้อตกลงระดับการให้บริการ (Service Level Agreement - SLA)

1. บทนำ (Introduction)

ข้อตกลงระดับการให้บริการฉบับนี้จัดทำขึ้นระหว่าง **บริษัท ABC จำกัด** ("ลูกค้า") และ **บริษัท XYZ จำกัด** ("ผู้ให้บริการ") เพื่อกำหนดข้อกำหนดและมาตรฐานการให้บริการ รวมถึงความคาดหวังในด้านคุณภาพของบริการ ความมั่นคงปลอดภัย และการจัดการเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการให้บริการ **ระบบจัดการฐานข้อมูลลูกค้า (Customer Database Management System)**

2. ขอบเขตของบริการ (Scope of Services)

- ผู้ให้บริการจะให้บริการ **การจัดการและดูแลรักษาระบบฐานข้อมูลลูกค้า** ของบริษัท ABC ซึ่งรวมถึง
  - การตรวจสอบและบำรุงรักษาฐานข้อมูลอย่างสม่ำเสมอ
  - การสำรองข้อมูล (Data Backup) เป็นประจำทุกวัน
  - การให้การสนับสนุนและการแก้ไขปัญหาฐานข้อมูลตามที่กำหนดในข้อตกลงนี้

3. ระดับการให้บริการ (Service Levels)

- **เวลาการให้บริการ (Service Availability)**
  - ผู้ให้บริการต้องรับประกันความพร้อมใช้งานของระบบฐานข้อมูลอย่างน้อย **99.5%** ต่อเดือน
  - กำหนดเวลาที่ให้บริการ: **24 ชั่วโมงต่อวัน, 7 วันต่อสัปดาห์**
- **เวลาตอบสนอง (Response Time)**
  - ผู้ให้บริการต้องตอบสนองต่อคำขอการสนับสนุนภายใน **1 ชั่วโมง** นับจากเวลาที่ได้รับแจ้งปัญหา
  - กำหนดเวลาการแก้ไขปัญหา:
    - ปัญหาระดับวิกฤติ (Critical): ภายใน **4 ชั่วโมง**

- ปัญหาระดับสำคัญ (Major): ภายใน **8 ชั่วโมง**
- ปัญหาระดับปานกลาง (Minor): ภายใน **24 ชั่วโมง**

- **การจัดการเหตุการณ์ (Incident Management)**
  - ผู้ให้บริการต้องรายงานเหตุการณ์ทางไซเบอร์หรือการหยุดชะงักของบริการภายใน **30 นาที** นับจากเวลาที่เกิดเหตุการณ์
  - ต้องดำเนินการแก้ไขและป้องกันการเกิดซ้ำของเหตุการณ์ที่เกิดขึ้นโดยเร็วที่สุด

4. ข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements)

- **การเข้าถึงข้อมูล (Data Access)**
  - ผู้ให้บริการต้องใช้การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA) ในการเข้าถึงระบบฐานข้อมูลของลูกค้า
  - การเข้าถึงข้อมูลจะต้องได้รับการจำกัดให้เฉพาะพนักงานของผู้ให้บริการที่มีความจำเป็นต้องใช้เท่านั้น
- **การจัดเก็บและการสื่อสารข้อมูล (Data Storage and Communication)**
  - ข้อมูลที่จัดเก็บในฐานข้อมูลและส่งผ่านต้องถูกเข้ารหัสด้วยมาตรฐาน AES-256 และ TLS/SSL ตามลำดับ
  - การสื่อสารข้อมูลทั้งหมดระหว่างผู้ให้บริการและลูกค้าจะต้องดำเนินการผ่าน VPN ที่ปลอดภัย
- **การตรวจสอบและการปฏิบัติตามข้อกำหนด (Audit and Compliance)**
  - ผู้ให้บริการต้องยอมรับการตรวจสอบความมั่นคงปลอดภัยโดยลูกค้าหรือบุคคลที่สามที่ลูกค้าแต่งตั้ง อย่างน้อยปีละหนึ่งครั้ง
  - ผู้ให้บริการต้องปฏิบัติตาม พรบ ไซเบอร์ 2562 ในการจัดการความมั่นคงปลอดภัยทางไซเบอร์

5. การตรวจสอบประสิทธิภาพ (Performance Monitoring)

- ผู้ให้บริการต้องจัดทำรายงานการตรวจสอบประสิทธิภาพการให้บริการและความมั่นคงปลอดภัยเป็นประจำทุกเดือน รายงานต้องครอบคลุมถึง
    - ระดับการให้บริการที่เป็นไปตาม SLA (เช่น ความพร้อมใช้งานของระบบ)
    - เหตุการณ์ที่เกิดขึ้นและวิธีการแก้ไข
    - การอัปเดตและการปรับปรุงที่ดำเนินการในเดือนนั้น ๆ
    - การพบเจอเหตุการณ์หรือภัยคุกคามทางไซเบอร์

6. บทลงโทษและการชดเชย (Penalties and Compensation)

- หากผู้ให้บริการไม่สามารถปฏิบัติตามระดับการให้บริการที่กำหนดไว้ใน SLA ลูกค้ามีสิทธิ์ในการเรียกร้องการชดเชย เช่น
    - ส่วนลดค่าบริการรายเดือน **10%** หากความพร้อมใช้งานของระบบต่ำกว่า 99.5% แต่ไม่ต่ำกว่า 98%
    - ยกเว้นค่าบริการในเดือนนั้นหากความพร้อมใช้งานของระบบต่ำกว่า 98%

7. การแก้ไขและการทบทวนข้อตกลง (Amendments and Review)

- ข้อตกลงนี้สามารถแก้ไขได้ตามความจำเป็น โดยต้องได้รับการเห็นชอบจากทั้งสองฝ่าย การแก้ไขต้องถูกบันทึกและแนบไว้เป็นภาคผนวกของข้อตกลงนี้
- ข้อตกลงนี้จะได้รับการทบทวนเป็นประจำทุกปีเพื่อให้มั่นใจว่าสอดคล้องกับความต้องการของลูกค้าและข้อกำหนดทางกฎหมาย

8. เงื่อนไขและระยะเวลาของสัญญา (Terms and Duration)

- ข้อตกลงนี้มีผลบังคับใช้ตั้งแต่วันที่ **1 มกราคม 2567** ถึงวันที่ **31 ธันวาคม 2567** หรือจนกว่าจะมีการยกเลิกหรือแก้ไขตามข้อตกลง
- การยกเลิกข้อตกลงต้องแจ้งล่วงหน้าอย่างน้อย **30 วัน** เป็นลายลักษณ์อักษรเท่านั้น

9. ลายเซ็นต์ (Signatures)

- **บริษัท ABC จำกัด**
  - **ชื่อ:** นาย A
  - **ตำแหน่ง:** ผู้อำนวยการฝ่าย IT
  - **วันที่:** 15 ตุลาคม 2567
- **บริษัท XYZ จำกัด**
  - **ชื่อ:** นางสาว B
  - **ตำแหน่ง:** ผู้จัดการฝ่ายบริการลูกค้า
  - **วันที่:** 15 ตุลาคม 2567

จัดทำโดย : นาย สุรศักดิ์ มั่นคง

จัดทำเมื่อ : 15 / 09 / 2567

เงื่อนไขของสัญญา (Contract Terms) กับผู้ให้บริการภายนอก

1. ขอบเขตของบริการ (Scope of Services)

- **รายละเอียดบริการ:** ผู้ให้บริการ **บริษัท XYZ จำกัด** ตกลงที่จะให้บริการ **การจัดการและดูแลรักษาระบบเครือข่ายองค์กร** ของ **บริษัท ABC จำกัด** โดยบริการนี้รวมถึง
    - การตรวจสอบและบำรุงรักษาระบบเครือข่ายให้พร้อมใช้งานตลอดเวลา
    - การจัดการระบบความปลอดภัยเครือข่าย เช่น การติดตั้งและอัปเดตไฟร์วอลล์
    - การให้คำปรึกษาและการสนับสนุนทางเทคนิคตามความต้องการของลูกค้า
- **ขอบเขตงาน:** ผู้ให้บริการจะต้องดำเนินการทุกด้านที่เกี่ยวข้องกับ **การติดตั้ง, การบำรุงรักษา, การตรวจสอบ, และการแก้ไขปัญหา** เพื่อให้มั่นใจว่าระบบเครือข่ายของลูกค้าทำงานได้อย่างต่อเนื่องและปลอดภัยจากภัยคุกคามทางไซเบอร์

2. ระยะเวลาของสัญญา (Contract Duration)

- สัญญานี้มีผลบังคับใช้ตั้งแต่วันที่ **1 มกราคม 2567** และสิ้นสุดในวันที่ **31 ธันวาคม 2567**
- การต่ออายุสัญญาจะต้องได้รับความเห็นชอบจากทั้งสองฝ่าย และการต่ออายุสัญญาจะต้องดำเนินการล่วงหน้าก่อนวันสิ้นสุดสัญญา **30 วัน**

3. ค่าบริการและการชำระเงิน (Fees and Payment)

- **ค่าบริการ:** ลูกค้าตกลงที่จะชำระค่าบริการรายเดือนให้แก่ผู้ให้บริการเป็นจำนวนเงิน **100,000 บาท** ต่อเดือน
- **เงื่อนไขการชำระเงิน:** การชำระเงินจะต้องดำเนินการภายใน **30 วัน** หลังจากวันที่ได้รับใบแจ้งหนี้จากผู้ให้บริการ
- **ค่าปรับล่าช้า:** หากลูกค้าไม่สามารถชำระเงินตามกำหนด ลูกค้าจะต้องชำระดอกเบี้ยค่าปรับ **1.5% ต่อเดือน** ของยอดค้างชำระ

4. ข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Requirements)

- ผู้ให้บริการต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงป้องกันข้อมูลรั่วไหล เช่น การเข้ารหัสข้อมูล, การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA) และการควบคุมการเข้าถึงข้อมูล (Access Control)
- ผู้ให้บริการต้องยอมรับการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ จากลูกค้าหรือตัวแทนที่ลูกค้าแต่งตั้งเป็นระยะ ๆ เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดที่ตกลงกันไว้

5. การจัดการเหตุการณ์และการรายงาน (Incident Management and Reporting)

- ผู้ให้บริการต้องรายงานเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่เกิดขึ้นทันทีภายใน **24 ชั่วโมง** นับจากเวลาที่พบเหตุการณ์
- ผู้ให้บริการต้องร่วมมือกับลูกค้าในการตรวจสอบและแก้ไขปัญหาที่เกิดขึ้นจากเหตุการณ์ และจัดทำรายงานสรุปผลการตรวจสอบให้แก่ลูกค้า

6. การยกเลิกสัญญา (Termination)

- **การยกเลิกโดยลูกค้า:** ลูกค้ามีสิทธิ์ในการยกเลิกสัญญานี้ได้หากผู้ให้บริการไม่สามารถปฏิบัติตามข้อกำหนดที่ระบุในสัญญา หรือหากมีการละเมิดข้อตกลงที่ร้ายแรง ลูกค้าต้องแจ้งเป็นลายลักษณ์อักษรล่วงหน้า **30 วัน**
- **การยกเลิกโดยผู้ให้บริการ:** ผู้ให้บริการสามารถยกเลิกสัญญาได้หากลูกค้าไม่ปฏิบัติตามข้อกำหนดการชำระเงินหรือเงื่อนไขที่ระบุในสัญญา โดยต้องแจ้งเป็นลายลักษณ์อักษรล่วงหน้า **30 วัน**

7. การรักษาความลับ (Confidentiality)

- ผู้ให้บริการต้องเก็บรักษาข้อมูลทั้งหมดที่ได้รับจากลูกค้าถือว่าเป็นความลับ และไม่เปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สามโดยไม่ได้รับความยินยอมจากลูกค้า
- ข้อกำหนดการรักษาความลับนี้ยังคงมีผลบังคับใช้ต่อไปแม้หลังจากสิ้นสุดสัญญา

8. ข้อพิพาทและการระงับข้อพิพาท (Dispute Resolution)

- หากเกิดข้อพิพาทใด ๆ ขึ้นระหว่างคู่สัญญา ทั้งสองฝ่ายจะต้องพยายามแก้ไขข้อพิพาทดังกล่าวด้วยการเจรจาในเบื้องต้น
- หากไม่สามารถแก้ไขข้อพิพาทได้โดยการเจรจา ข้อพิพาทจะถูกส่งดำเนินการในขั้นศาลต่อไป ตามที่ตกลงกันไว้ในสัญญาฉบับนี้

9. การเปลี่ยนแปลงและการแก้ไขสัญญา (Amendments)

- การเปลี่ยนแปลงหรือแก้ไขสัญญาต้องได้รับความเห็นชอบจากทั้งสองฝ่ายเป็นลายลักษณ์อักษรเท่านั้น
- การเปลี่ยนแปลงหรือแก้ไขสัญญาจะต้องแนบไว้เป็นภาคผนวกของสัญญาฉบับนี้

10. ลายเซ็นต์และวันที่ (Signatures and Date)

- **บริษัท XYZ จำกัด**
  - **ชื่อ:** นางสาว A
  - **ตำแหน่ง:** ผู้จัดการฝ่ายบริการลูกค้า
  - **วันที่:** 1 ธันวาคม 2567
- **บริษัท ABC จำกัด**
  - **ชื่อ:** นาย C
  - **ตำแหน่ง:** ผู้อำนวยการฝ่าย IT
  - **วันที่:** 1 ธันวาคม 2567

จัดทำโดย : ทีมประเมินความเสี่ยง (ส่วนบริการและห่วงโซ่อุปทานผลิตภัณฑ์)

วันที่ทำการประเมิน : 1 กันยายน 2567

การประเมินความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ (Risk Assessment for Services and Product Supply Chain)

ลำดับที่	ความเสี่ยง (Risk)	คำอธิบายความเสี่ยง (Description)	โอกาสที่จะเกิดขึ้น (Likelihood)	ความรุนแรงของผลกระทบ (Impact Severity)	การจัดการความเสี่ยง (Risk Mitigation)	เจ้าของความเสี่ยง (Risk Owner)	สถานะ (Status)
1	การหยุดชะงักของห่วงโซ่อุปทาน (Supply Chain Disruption)	การหยุดชะงักในกระบวนการจัดหาวัตถุดิบหรือบริการจากผู้ให้บริการอาจทำให้เกิดความล่าช้าในการผลิตหรือการให้บริการ	ปานกลาง (Medium)	สูง (High)	- ทำแผนสำรองสำหรับการจัดหาจากผู้ให้บริการรายอื่น, - ทำสัญญากับผู้ให้บริการหลายราย	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
2	การขาดความโปร่งใสในห่วงโซ่อุปทาน (Lack of Supply Chain Transparency)	ขาดข้อมูลที่ชัดเจนเกี่ยวกับแหล่งที่มาของวัตถุดิบหรือบริการ ซึ่งอาจส่งผลต่อคุณภาพของผลิตภัณฑ์และการปฏิบัติตามข้อกำหนด	สูง (High)	ปานกลาง (Medium)	- ใช้เทคโนโลยีบล็อกเชนในการติดตามห่วงโซ่อุปทาน, - กำหนดข้อกำหนดในการรายงานสถานะของห่วงโซ่อุปทาน	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
3	การไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดทางกฎหมาย (Non-Compliance with Standards or Regulations)	ผู้ให้บริการในห่วงโซ่อุปทานไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดทางกฎหมาย อาจส่งผลให้เกิดบทลงโทษทางกฎหมาย	ต่ำ (Low)	สูง (High)	- ตรวจสอบและประเมินความสามารถของผู้ให้บริการตามข้อกำหนด, - ทำสัญญาที่ชัดเจนระบุว่าต้องปฏิบัติตามมาตรฐาน	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
4	ความเสี่ยงต่อคุณภาพผลิตภัณฑ์จากการใช้วัตถุดิบที่มีคุณภาพต่ำ (Risk of Low-Quality Materials)	การใช้วัตถุดิบหรือผลิตภัณฑ์จากผู้ให้บริการที่มีคุณภาพต่ำอาจส่งผลต่อคุณภาพของสินค้าสุดท้าย	ปานกลาง (Medium)	ปานกลาง (Medium)	- ตรวจสอบคุณภาพวัตถุดิบก่อนการสั่งซื้อ, - ทำสัญญากับผู้ให้บริการที่ผ่านการรับรองคุณภาพ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
5	ความเสี่ยงจากการพึ่งพาผู้ให้บริการรายเดียว (Dependency on Single Supplier)	การพึ่งพาผู้ให้บริการหรือผู้ผลิตรายเดียวอาจทำให้เกิดความเสี่ยงในการหยุดชะงักของบริการหากเกิดปัญหากับผู้ให้บริการรายนั้น	สูง (High)	ปานกลาง (Medium)	- หาผู้ให้บริการรายอื่นเป็นสำรอง, - กระจายการสั่งซื้อไปยังผู้ให้บริการหลายราย	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
6	การโจมตีทางไซเบอร์ต่อห่วงโซ่อุปทาน (Cyberattacks on Supply Chain)	ผู้ให้บริการในห่วงโซ่อุปทานอาจตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ ซึ่งอาจ	ปานกลาง (Medium)	สูง (High)	- กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญา, - ตรวจสอบ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567

		นำไปสู่การเข้าถึงข้อมูลที่เป็นความลับ			ความปลอดภัยของระบบของผู้ให้บริการ		
7	ความเสี่ยงด้านความยั่งยืนจากการจัดหาวัตถุดิบ (Sustainability Risks in Material Sourcing)	การจัดหาวัตถุดิบที่ไม่มีความยั่งยืนอาจส่งผลกระทบต่อภาพลักษณ์และการปฏิบัติตามนโยบายความยั่งยืนขององค์กร	ต่ำ (Low)	ปานกลาง (Medium)	- เลือกผู้ให้บริการที่มีนโยบายด้านความยั่งยืน, - ตรวจสอบและประเมินห่วงโซ่อุปทานในด้านความยั่งยืน	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
8	การขาดการสนับสนุนทางเทคนิคจากผู้ให้บริการ (Lack of Technical Support from Suppliers)	การขาดการสนับสนุนทางเทคนิคที่เพียงพอจากผู้ให้บริการอาจส่งผลต่อการแก้ไขปัญหาหรือการบำรุงรักษาผลิตภัณฑ์	ปานกลาง (Medium)	ปานกลาง (Medium)	- กำหนดในสัญญาว่าผู้ให้บริการต้องมีทีมสนับสนุนทางเทคนิค, - ประเมินการให้บริการหลังการขาย	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
9	ความเสี่ยงจากการจัดการสินค้าคงคลังไม่ดี (Inventory Management Risks)	การจัดการสินค้าคงคลังที่ไม่ดีอาจนำไปสู่การขาดแคลนวัตถุดิบหรือการผลิตเกินความต้องการ	สูง (High)	ปานกลาง (Medium)	- ใช้ระบบการจัดการสินค้าคงคลังที่ทันสมัย, - ตรวจสอบระดับสินค้าคงคลังเป็นระยะ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
10	ความเสี่ยงจากการเปลี่ยนแปลงของตลาด (Market Volatility Risks)	การเปลี่ยนแปลงในตลาด เช่น ราคาวัตถุดิบหรือผลิตภัณฑ์ที่ผันผวน อาจส่งผลต่อความสามารถในการจัดหา	ปานกลาง (Medium)	ปานกลาง (Medium)	- ทำสัญญาซื้อขายล่วงหน้าเพื่อลดความเสี่ยงจากการเปลี่ยนแปลงของราคา, - ติดตามแนวโน้มของตลาดอย่างใกล้ชิด	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
11	การหยุดชะงักในการขนส่งสินค้า (Transportation Disruption)	การขนส่งสินค้าหรือวัตถุดิบที่ล่าช้าหรือหยุดชะงักเนื่องจากปัญหาทางโลจิสติกส์ เช่น สภาพอากาศไม่เอื้ออำนวย อาจทำให้เกิดความล่าช้าในกระบวนการผลิต	ปานกลาง (Medium)	สูง (High)	- เลือกผู้ให้บริการขนส่งที่มีความน่าเชื่อถือ, - มีแผนสำรองสำหรับการขนส่งฉุกเฉิน	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
12	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายของรัฐบาล (Government Policy Changes)	การเปลี่ยนแปลงนโยบายหรือกฎระเบียบของรัฐบาลที่กระทบต่อห่วงโซ่อุปทาน อาจทำให้เกิดข้อจำกัดในการจัดหาวัตถุดิบหรือบริการ	ต่ำ (Low)	ปานกลาง (Medium)	- ติดตามการเปลี่ยนแปลงนโยบายของรัฐบาลอย่างใกล้ชิด, - ทำสัญญาที่มีความยืดหยุ่นในการปรับตัวต่อการเปลี่ยนแปลง	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
13	การสูญเสียความลับทางการค้าในห่วงโซ่อุปทาน (Loss of Trade Secrets in Supply Chain)	การเปิดเผยข้อมูลที่เป็นความลับแก่ผู้ให้บริการในห่วงโซ่อุปทานอาจนำไปสู่การสูญเสียความได้เปรียบทางการค้า	ปานกลาง (Medium)	สูง (High)	- ทำสัญญารักษาความลับ (NDA) กับผู้ให้บริการ, - จำกัดการเข้าถึงข้อมูลสำคัญเฉพาะผู้ที่มีความจำเป็น	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
14	ความเสี่ยงจากการขาดมาตรการด้านสิ่งแวดล้อมของผู้ให้บริการ	ผู้ให้บริการในห่วงโซ่อุปทานที่ไม่ปฏิบัติตามมาตรการด้านสิ่งแวดล้อม	ต่ำ (Low)	ปานกลาง (Medium)	- เลือกผู้ให้บริการที่ปฏิบัติตามมาตรการด้านสิ่งแวดล้อม, -	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567

	(Environmental Compliance Risks)	อาจทำให้เกิดปัญหาทางกฎหมายและภาพลักษณ์			ตรวจสอบการปฏิบัติตามมาตรการด้านสิ่งแวดล้อมเป็นระยะ		
15	ความเสี่ยงจากการละเมิดสิทธิแรงงานในห่วงโซ่อุปทาน (Labor Rights Violations in Supply Chain)	การละเมิดสิทธิแรงงานโดยผู้ให้บริการในห่วงโซ่อุปทานอาจทำให้องค์กรต้องเผชิญกับปัญหาทางกฎหมายและภาพลักษณ์	ต่ำ (Low)	สูง (High)	- ทำสัญญาที่ชัดเจนเกี่ยวกับการปฏิบัติตามกฎหมายแรงงาน, - ตรวจสอบการปฏิบัติตามสิทธิแรงงานของผู้ให้บริการ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
16	ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยี (Technological Changes Risks)	การเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วอาจทำให้ผลิตภัณฑ์หรือบริการที่ได้รับจากห่วงโซ่อุปทานล้าสมัยหรือไม่สอดคล้องกับความต้องการตลาด	ปานกลาง (Medium)	ปานกลาง (Medium)	- เลือกผู้ให้บริการที่มีความสามารถในการปรับตัวต่อเทคโนโลยีใหม่ ๆ, - ทำสัญญาที่มีความยืดหยุ่นในการปรับปรุงเทคโนโลยี	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
17	ความเสี่ยงจากการขาดการฝึกอบรมและความรู้ในห่วงโซ่อุปทาน (Lack of Training and Knowledge in Supply Chain)	การขาดการฝึกอบรมและความรู้เกี่ยวกับผลิตภัณฑ์หรือบริการของผู้ให้บริการในห่วงโซ่อุปทานอาจส่งผลต่อคุณภาพและประสิทธิภาพ	ปานกลาง (Medium)	ปานกลาง (Medium)	- จัดการฝึกอบรมและพัฒนาความรู้ให้กับผู้ให้บริการ, - กำหนดมาตรฐานการฝึกอบรมในสัญญา	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
18	ความเสี่ยงจากการขาดการตรวจสอบคุณภาพอย่างสม่ำเสมอ (Lack of Regular Quality Checks)	การขาดการตรวจสอบคุณภาพอย่างสม่ำเสมอในห่วงโซ่อุปทานอาจนำไปสู่การลดลงของคุณภาพผลิตภัณฑ์หรือบริการ	สูง (High)	ปานกลาง (Medium)	- จัดทำแผนการตรวจสอบคุณภาพเป็นระยะ, - ทำสัญญาที่ระบุว่าผู้ให้บริการต้องรับการตรวจสอบคุณภาพ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
19	ความเสี่ยงจากการเปลี่ยนแปลงความต้องการของตลาด (Market Demand Changes Risks)	การเปลี่ยนแปลงความต้องการของตลาดอย่างรวดเร็วอาจทำให้สินค้าหรือบริการที่ได้รับจากห่วงโซ่อุปทานไม่สามารถตอบสนองได้	ปานกลาง (Medium)	ปานกลาง (Medium)	- ทำการวิจัยตลาดเป็นระยะ, - ทำสัญญาที่มีความยืดหยุ่นในการปรับตัวต่อการเปลี่ยนแปลงของตลาด	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567
20	ความเสี่ยงจากการขาดแคลนแรงงานในห่วงโซ่อุปทาน (Labor Shortages in Supply Chain)	การขาดแคลนแรงงานในห่วงโซ่อุปทานอาจทำให้เกิดความล่าช้าในการผลิตหรือการจัดหาบริการ	ปานกลาง (Medium)	สูง (High)	- ทำสัญญาที่กำหนดข้อกำหนดด้านแรงงานขั้นต่ำ, - ตรวจสอบสถานะการจ้างงานในห่วงโซ่อุปทานเป็นระยะ	ทีมความเสี่ยง	ดำเนินการแล้วเสร็จ | 1ธันวาคม 2567

PROTECT

1. กระบวนการการควบคุมการเข้าถึง

(Access Control Procedure)

Logo	ระเบียบกระบวนการการจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	CSMS-Protect -05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	รหัสเอกสาร	CSMS-Protect -05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43), ประมวลและกรอบ [ข้อ 22.1.1, ข้อ 22.1.2, ข้อ 22.1.3, ข้อ 22.1.4]

1. วัตถุประสงค์ (Objective)

กระบวนการนี้จัดทำขึ้นเพื่อการจัดการตัวตนและการควบคุมกำกับดูแลการเข้าถึงบริการที่สำคัญขององค์กร ทั้งนี้เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยไซเบอร์ และให้มั่นใจว่าการบริหารจัดการตัวตนของบุคลากรเป็นไปอย่างมีประสิทธิภาพ

2. ขอบเขต (Scope)

กระบวนการนี้ครอบคลุมถึงการจัดการตัวตนและการควบคุมกำกับดูแลการเข้าถึง สำหรับบุคลากร อุปกรณ์และอินเทอร์เฟซ รวมถึงการตรวจสอบและจัดเก็บบันทึกการเข้าถึงบริการที่สำคัญขององค์กร เพื่อให้แน่ใจว่าการเข้าถึงเหล่านี้เป็นไปตามข้อกำหนดที่กำหนดไว้ นอกจากนี้ยังรวมถึงการบริหารจัดการวงจรชีวิตของตัวตนในระบบ (Identity Lifecycle Management)

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management):** กำกับดูแลให้มีนโยบายและแนวปฏิบัติในการจัดการตัวตนและการควบคุมการเข้าถึง
- **ผู้ดูแลระบบ (System Administrators):** รับผิดชอบการจัดการบัญชีผู้ใช้ กำหนดสิทธิ์และตรวจสอบการเข้าถึงระบบเป็นประจำ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **พนักงาน (Employee):** ปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการเข้าถึงบริการที่สำคัญขององค์กร

4. การจัดการตัวตน (Identity Management)

4.1 การสร้างตัวตน (Identity Creation)

- ขั้นตอน
  - บุคลากรที่ต้องการเข้าถึงระบบต้องได้รับการลงทะเบียนตัวตนในระบบโดยมีการยืนยันข้อมูลจากแหล่งที่เชื่อถือได้ เช่น ฐานข้อมูลทรัพยากรบุคคล (HR Database)
  - ใช้การตรวจสอบตัวตนสองปัจจัย (Two-Factor Authentication) ในการลงทะเบียนและเข้าใช้งานระบบที่มีข้อมูลสำคัญ

4.2 การบริหารวงจรชีวิตตัวตน (Identity Lifecycle Management)

- ขั้นตอน
  - มีการกำหนดวงจรชีวิตของตัวตนในระบบ ตั้งแต่การลงทะเบียน การใช้งาน การปรับเปลี่ยนสิทธิ์ จนถึงการยกเลิกการเข้าถึงเมื่อบุคลากรออกจากองค์กร
  - ตรวจสอบสิทธิ์การเข้าถึงของพนักงานทุก 6 เดือนเพื่อให้แน่ใจว่าสอดคล้องกับหน้าที่งาน

4.3 การยกเลิกตัวตน (Identity Deactivation)

- ขั้นตอน
  - เมื่อพนักงานลาออกหรือไม่มีความจำเป็นต้องเข้าถึงระบบ ระบบต้องดำเนินการยกเลิกบัญชีผู้ใช้งานภายใน 24 ชั่วโมง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- ตรวจสอบให้แน่ใจว่าไม่มีบัญชีที่ไม่ได้ใช้งานหรือบัญชีซ้ำซ้อนในระบบ

5. การจำกัดการเข้าถึง (Access Restrictions)

5.1 การจำกัดการเข้าถึงบริการที่สำคัญ

- ขั้นตอน
  - การเข้าถึงบริการที่สำคัญถูกจำกัดเฉพาะบุคลากรที่ได้รับอนุญาต อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาตเท่านั้น
  - ระบบต้องมีการตรวจสอบสิทธิ์การเข้าถึงเป็นระยะเพื่อให้แน่ใจว่าผู้ใช้ยังคงมีความจำเป็นในการเข้าถึง

5.2 การใช้เทคนิคการตรวจสอบสิทธิ์

- ขั้นตอน
  - กำหนดให้ใช้การตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-Factor Authentication, MFA) ในการเข้าถึงระบบที่สำคัญ
  - ใช้มาตรการเข้ารหัสข้อมูลการยืนยันตัวตนเพื่อป้องกันการถูกดักฟังหรือขโมยข้อมูล

6. การบันทึกและตรวจสอบการเข้าถึง (Access Logging and Monitoring)

6.1 การเก็บรักษาบันทึกการเข้าถึง

- ขั้นตอน
  - เก็บรักษาบันทึกของการเข้าถึงทั้งหมดและตรวจสอบเป็นระยะเพื่อหากิจกรรมที่ผิดปกติ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- ใช้ระบบบันทึกการเข้าถึงอัตโนมัติและแจ้งเตือนเมื่อมีพฤติกรรมที่ผิดปกติ

6.2 ความสม่ำเสมอในการตรวจสอบบันทึก

- ขั้นตอน
  - ตรวจสอบบันทึกการเข้าถึงของระบบเครือข่ายภายในทุกวัน และการตรวจสอบบันทึกการเข้าถึงข้อมูลสำคัญอย่างน้อยรายสัปดาห์

7. การควบคุมการเข้าถึงอินเทอร์เฟซและการเข้าถึงทางลอจิคอล (Interface and Logical Access Control)

7.1 การควบคุมการเข้าถึงอินเทอร์เฟซ

- ขั้นตอน
  - ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ เช่น USB และพอร์ตอนุกรม ต้องถูกควบคุมและดำเนินการภายใต้การดูแลขององค์กรที่เกี่ยวข้องเท่านั้น
  - ตั้งค่าข้อจำกัดในการใช้งานพอร์ต USB บนอุปกรณ์คอมพิวเตอร์ที่ใช้ในองค์กร

7.2 การเข้าถึงทางลอจิคอล

- ขั้นตอน
  - กำกับดูแลการเข้าถึงทางลอจิคอลของบริการที่สำคัญ โดยให้ดำเนินการในสถานที่ที่ได้รับอนุญาตและอยู่ภายใต้การควบคุมขององค์กร
  - กำหนดให้การเข้าถึงระบบจัดการข้อมูลต้องทำจากภายในองค์กรเท่านั้น และห้ามเข้าถึงจากภายนอกองค์กร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. หลักฐาน Logs of Access
2. หลักฐานสิทธิ์การเข้าถึงระบบ (User Permission Matrix)
3. หลักฐานการจัดการตัวตน (Identity Users)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

2. กระบวนการการทำให้ระบบมีความแข็งแกร่ง

(System Hardening Procedure)

Logo	ระเบียบกระบวนการการทำให้ระบบมีความแข็งแกร่ง (System Hardening Procedure)	รหัสเอกสาร	CSMS-Protect -07
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการทำให้ระบบมีความแข็งแกร่ง (System Hardening Procedure)	รหัสเอกสาร	CSMS-Protect -07
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการทำให้ระบบมีความแข็งแกร่ง (System Hardening Procedure)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ 22.2.4]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร เพื่อป้องกันภัยคุกคามทางไซเบอร์และรักษาความมั่นคงปลอดภัยของบริการที่สำคัญ

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและกำกับดูแลการดำเนินการตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team)**: รับผิดชอบในการพัฒนามาตรฐานการกำหนดค่าขั้นต่ำ ตรวจสอบการปฏิบัติตามมาตรฐาน และดำเนินการตรวจสอบและปรับปรุงมาตรฐานตามความเหมาะสม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **ผู้ใช้งานระบบ (System Users)**: มีหน้าที่ในการปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการใช้งานระบบตามมาตรฐานที่กำหนด

4. การกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

- **4.1 การพัฒนามาตรฐานการกำหนดค่าขั้นต่ำ**
  - **ขั้นตอน**: พัฒนามาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่เกี่ยวข้อง โดยให้สอดคล้องกับโปรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยการกำหนดนโยบายการเข้าถึงที่ใช้หลักการสิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- **4.2 องค์ประกอบหลักของมาตรฐานการกำหนดค่าขั้นต่ำ**
  - **ขั้นตอน**: มาตรฐานการกำหนดค่าขั้นต่ำต้องครอบคลุมถึงองค์ประกอบความมั่นคงปลอดภัยที่สำคัญ เช่น
    - สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
    - การแบ่งแยกหน้าที่ (Separation of Duties)
    - การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
    - การลบบัญชีที่ไม่ได้ใช้
    - การลบบริการและแอปพลิเคชันที่ไม่จำเป็น
    - การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
    - การป้องกันมัลแวร์
    - การอัปเดตซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัย

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **4.3 การใช้งานมาตรฐานการกำหนดค่าขั้นต่ำ**
  - **ขั้นตอน**: ตรวจสอบให้แน่ใจว่ามาตรฐานการกำหนดค่าขั้นต่ำถูกใช้งานก่อนที่จะเชื่อมต่อทรัพย์สินใด ๆ หรือก่อนการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ โดยการตรวจสอบมาตรฐานการกำหนดค่าของเซิร์ฟเวอร์ก่อนการนำไปใช้งานจริง
- **4.4 การตรวจสอบและปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำ**
  - **ขั้นตอน**: ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ โดยการทบทวนและปรับปรุงมาตรฐานการกำหนดค่าขั้นต่ำตามการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามใหม่ ๆ

5. การจัดการเปลี่ยนแปลง (Change Management Process)

- **5.1 การอนุญาตและตรวจสอบการเปลี่ยนแปลง**
  - **ขั้นตอน**: จัดทำกระบวนการจัดการเปลี่ยนแปลงเพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน โดยการทบทวนการเปลี่ยนแปลงระบบโดยคณะกรรมการความมั่นคงปลอดภัยก่อนที่จะอนุมัติการเปลี่ยนแปลง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. นโยบายมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)
2. กระบวนการจัดการเปลี่ยนแปลง (Change Management Process)
3. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	รหัสเอกสาร	CSMS-Policy-03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	รหัสเอกสาร	CSMS-Policy-03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ 22.2.4]

1. วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับการกำหนดค่าระบบสารสนเทศ เพื่อป้องกันความเสี่ยงและลดช่องโหว่ที่อาจเกิดขึ้นจากการกำหนดค่าระบบที่ไม่ปลอดภัย

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการกำหนดค่าระบบทั้งหมดในองค์กร รวมถึงเซิร์ฟเวอร์, คอมพิวเตอร์, อุปกรณ์เครือข่าย และแอปพลิเคชันที่ใช้งานภายในองค์กร

3. หลักการรักษาความมั่นคงปลอดภัย (Security Principles)

องค์กรต้องปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้:

1. **สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)**
    - ระบบฐานข้อมูลขององค์กรจะต้องถูกกำหนดให้พนักงานแต่ละคนเข้าถึงข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับหน้าที่ของตนเท่านั้น เช่น เจ้าหน้าที่ฝ่ายการเงินจะสามารถเข้าถึงข้อมูลการเงิน แต่ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลของพนักงานได้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

2. **การแบ่งแยกหน้าที่ (Separation of Duties)**
   - ในองค์กรนั้นจะต้องมีการแบ่งแยกหน้าที่กันอย่างชัดเจน
3. **การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน**
   - องค์กรกำหนดให้ผู้ใช้ทุกคนต้องตั้งรหัสผ่านที่ประกอบด้วยอักษรพิมพ์ใหญ่, อักษรพิมพ์เล็ก, ตัวเลข และอักขระพิเศษ และต้องมีความยาวอย่างน้อย 12 ตัวอักษร
4. **การลบบัญชีที่ไม่ได้ใช้**
   - บัญชีของพนักงานที่ลาออกจะถูกลบออกจากระบบภายใน 24 ชั่วโมงหลังจากที่พนักงานคนนั้นออกจากองค์กร เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
5. **การลบบริการและแอปพลิเคชันที่ไม่จำเป็น**
   - เซิร์ฟเวอร์ขององค์กรจะถูกกำหนดค่าให้ลบคอมไพเลอร์ (Compiler) และแอปพลิเคชันที่ไม่จำเป็น เช่น แอปพลิเคชันที่ใช้สำหรับการทดสอบหรือสนับสนุนจากผู้ให้บริการภายนอก เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากช่องโหว่ในแอปพลิเคชันเหล่านั้น
6. **การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน**
   - ในการตั้งค่าเครือข่ายขององค์กร พอร์ตที่ไม่ได้ใช้งาน เช่น พอร์ต FTP จะถูกปิดเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากการเข้าถึงผ่านพอร์ตเหล่านั้น
7. **การป้องกันมัลแวร์ (Malware Protection)**
   - คอมพิวเตอร์ทุกเครื่องในองค์กรจะต้องติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์เป็นประจำ รวมถึงมีการสแกนระบบแบบอัตโนมัติทุกสัปดาห์
8. **การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบ**
   - เซิร์ฟเวอร์ขององค์กรจะได้รับการอัปเดตซอฟต์แวร์และติดตั้งแพตช์ความมั่นคงปลอดภัยที่ปล่อยออกมาโดยผู้ผลิตซอฟต์แวร์ภายใน 48 ชั่วโมงหลังจากที่แพตช์เหล่านั้นถูกปล่อยออกมา เพื่อป้องกันการโจมตีจากช่องโหว่ที่เป็นที่รู้จัก

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. การตรวจสอบและการปฏิบัติตามนโยบาย (Audit and Compliance)

องค์กรต้องดำเนินการตรวจสอบการปฏิบัติตามนโยบายนี้อย่างสม่ำเสมอ โดยการตรวจสอบการตั้งค่าระบบและการใช้งานสิทธิ์ต่าง ๆ และรายงานผลการตรวจสอบต่อผู้บริหารที่เกี่ยวข้อง นโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป

5. การฝ่าฝืนนโยบาย (Policy Violations)

ผู้ใช้งานใดที่ฝ่าฝืนนโยบายนี้จะต้องได้รับการพิจารณาและอาจต้องรับโทษตามมาตรการที่กำหนดไว้ในกฎระเบียบขององค์กร

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย นาย A , Cybersecurity Administrator

จัดทำเมื่อ : 1 ตุลาคม 2567

ตรวจสอบเมื่อ : 1 ธันวาคม 2567

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

1. สำหรับระบบปฏิบัติการ (Operating Systems)

1. **การจำกัดสิทธิพิเศษการเข้าถึง (Least Access Privilege)**
    - บัญชีผู้ใช้ทั่วไปไม่มีสิทธิ์ติดตั้งหรือเปลี่ยนแปลงซอฟต์แวร์
    - บัญชีผู้ใช้ชั่วคราว เช่น นักศึกษาฝึกงาน ได้รับสิทธิ์เข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการทำงาน
    - ผู้ดูแลระบบฐานข้อมูลสามารถจัดการฐานข้อมูลแต่ไม่สามารถเข้าถึงข้อมูลส่วนตัวได้
    - บัญชีผู้ดูแลระบบจะถูกใช้เฉพาะงานที่จำเป็นเท่านั้น
    - บัญชีผู้ใช้งานทั่วไปไม่สามารถเข้าถึงฟีเจอร์ระบบปฏิบัติการขั้นสูงได้
    - จำกัดการเข้าถึงไฟล์ระบบที่สำคัญสำหรับผู้ใช้ทั่วไป
    - ผู้ดูแลระบบไม่สามารถเข้าถึงข้อมูลที่ละเอียดอ่อนของผู้ใช้
    - บัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 30 วันจะถูกล็อก
    - ผู้ใช้ทั่วไปไม่สามารถเปลี่ยนแปลงการตั้งค่าด้านความมั่นคงของระบบได้
    - การจำกัดสิทธิ์การเข้าถึงทรัพยากรเฉพาะงานที่ได้รับอนุมัติเท่านั้น
2. **การบังคับใช้นโยบายรหัสผ่าน (Password Complexity Enforcement)**
    - รหัสผ่านต้องมีความยาวอย่างน้อย 12 ตัวอักษร
    - ต้องผสมผสานตัวอักษรพิมพ์ใหญ่, พิมพ์เล็ก, ตัวเลข, และอักขระพิเศษ
    - รหัสผ่านต้องเปลี่ยนทุก 90 วัน
    - ระบบปฏิเสธรหัสผ่านง่าย ๆ เช่น "123456" หรือ "password"
    - การล็อกบัญชีหลังจากพยายามเข้าสู่ระบบไม่สำเร็จเกิน 5 ครั้ง
    - บัญชีจะถูกล็อกหากมีการเข้าสู่ระบบจากหลายอุปกรณ์พร้อมกัน
    - ห้ามใช้รหัสผ่านเดิมซ้ำใน 3 ครั้งล่าสุด

- มีการตรวจสอบความแข็งแรงของรหัสผ่านก่อนอนุญาตให้ใช้
- การบังคับใช้รหัสผ่านแบบไม่สามารถแชร์รหัสผ่านกับผู้ใช้อื่นได้
- แจ้งเตือนผู้ใช้ก่อนรหัสผ่านหมดอายุ 10 วัน

3. **การจัดการบัญชีผู้ใช้ที่ไม่ได้ใช้งาน (Removal of Unused Accounts)**
    - ลบบัญชีที่ไม่มีการใช้งานเกิน 90 วัน
    - บัญชีผู้ใช้ชั่วคราวจะถูกลบทันทีหลังจากสิ้นสุดโครงการ
    - ลบบัญชีผู้ดูแลระบบที่ไม่ได้ใช้งานภายใน 30 วัน
    - ลบบัญชีที่ถูกสร้างขึ้นโดยไม่ได้รับอนุมัติจากผู้ดูแลระบบ
    - การลบบัญชีผู้ใช้งานที่ซ้ำซ้อนหรือไม่มีความจำเป็น
    - บัญชีที่ถูกล็อกนานกว่า 90 วันจะถูกลบ
    - ลบบัญชีที่ไม่มีการเข้าสู่ระบบเกิน 60 วัน
    - ลบบัญชีผู้ใช้งานที่มีสิทธิ์เกินความจำเป็น
    - การแจ้งเตือนและยืนยันการลบบัญชีที่ไม่มีการใช้งาน
    - บัญชีผู้ใช้งานเก่าจะถูกลบภายใน 24 ชั่วโมงหลังการยืนยันลาออก

4. **การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน (Disabling Unused Network Ports)**
    - ปิดพอร์ต SSH ที่ไม่ได้ใช้งาน
    - ปิดพอร์ต Telnet บนเซิร์ฟเวอร์ทั้งหมด
    - ปิดพอร์ต SMB ที่ไม่ได้ใช้งานในระบบ Windows
    - ปิดพอร์ต HTTP ที่ไม่ได้ใช้งานบนเซิร์ฟเวอร์
    - ปิดพอร์ต FTP ที่ไม่ได้ใช้งาน
    - ปิดพอร์ต RDP ที่ไม่ได้ใช้งาน
    - ปิดพอร์ต SNMP ที่ไม่ได้ใช้งาน
    - ปิดพอร์ตที่ไม่ได้เชื่อมต่อบนสวิตช์เครือข่าย
    - ปิดพอร์ตที่ไม่จำเป็นในอุปกรณ์ IoT
    - การจัดการพอร์ตที่เปิดใช้งานโดยมีการตรวจสอบความปลอดภัยเป็นประจำ

5. **การติดตั้งแพตช์และอัปเดตซอฟต์แวร์ (Patch and Software Updates)**
    - อัปเดตระบบปฏิบัติการภายใน 48 ชั่วโมงหลังจากมีการปล่อยแพตช์
    - ทดสอบแพตช์ในระบบทดสอบก่อนนำไปใช้ในระบบจริง
    - ติดตั้งแพตช์ความมั่นคงปลอดภัยภายใน 24 ชั่วโมงหลังการปล่อยแพตช์
    - อัปเดตซอฟต์แวร์แอปพลิเคชันภายใน 72 ชั่วโมงหลังการปล่อยอัปเดต
    - ตรวจสอบและติดตั้งอัปเดตอัตโนมัติจากผู้ผลิตซอฟต์แวร์
    - ตรวจสอบการอัปเดตซอฟต์แวร์โอเพ่นซอร์สที่ใช้งาน
    - ติดตั้งแพตช์ในระบบคลาวด์ตามการปล่อยอัปเดตจากผู้ให้บริการ
    - แจ้งเตือนผู้ใช้งานเมื่อมีการปล่อยอัปเดตใหม่
    - ตรวจสอบให้แน่ใจว่าทุกระบบได้รับการติดตั้งแพตช์ที่จำเป็น
    - ทบทวนการอัปเดตเป็นระยะเพื่อให้แน่ใจว่าระบบปลอดภัย

2. สำหรับแอปพลิเคชัน (Applications)

1. **การจำกัดสิทธิพิเศษการเข้าถึง (Least Access Privilege)**
    - พนักงานขายสามารถเข้าถึงข้อมูลลูกค้าและสถานะคำสั่งซื้อ แต่ไม่สามารถแก้ไขข้อมูลได้
    - บัญชีผู้ใช้ทั่วไปสามารถเข้าถึงแอปพลิเคชันที่จำเป็นต่อการทำงานเท่านั้น
    - ผู้จัดการบัญชีสามารถเข้าถึงและจัดการข้อมูลทางการเงิน แต่ไม่สามารถเข้าถึงข้อมูลที่ไม่เกี่ยวข้องได้
    - การจัดการสิทธิ์ในแอปพลิเคชันจะถูกตรวจสอบเป็นประจำ
    - ผู้ดูแลระบบแอปพลิเคชันสามารถจัดการการตั้งค่า แต่ไม่สามารถเข้าถึงข้อมูลผู้ใช้
    - การเข้าถึงระบบคลาวด์จำกัดเฉพาะโฟลเดอร์ที่เกี่ยวข้องกับงานที่ทำ
    - ผู้ใช้อุปกรณ์พกพาสามารถเข้าถึงเฉพาะแอปพลิเคชันที่จำเป็น
    - การจัดการสิทธิ์การเข้าถึงในไฟล์แอปพลิเคชันการเงินสำหรับผู้ใช้ที่จำเป็น
    - การจำกัดการเข้าถึงข้อมูลแผนกอื่นในแอปพลิเคชันการจัดการ
    - การจัดการสิทธิ์ในการเข้าถึงแอปพลิเคชันการจัดการข้อมูลเฉพาะแผนก

2. **การลบแอปพลิเคชันที่ไม่จำเป็น (Removal of Unnecessary Applications)**
   - ลบแอปพลิเคชันที่ไม่ได้รับการอัปเดตเป็นเวลานาน
   - ลบแอปพลิเคชันทดสอบหลังจากการทดสอบเสร็จสิ้น
   - ลบแอปพลิเคชันสนับสนุนจากผู้ให้บริการภายนอกหลังจากไม่ใช้งาน
   - ลบคอมไพเลอร์ที่ไม่ได้ใช้งานจากเซิร์ฟเวอร์การผลิต
   - ลบซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าที่ไม่ได้ใช้งาน
   - ลบบริการเว็บที่ไม่ได้ใช้งาน
   - ลบบริการ FTP ที่ไม่ได้ใช้งาน
   - ลบซอฟต์แวร์ที่ไม่มีผู้ใช้และไม่มีความจำเป็น
   - ลบบริการอีเมลที่ไม่ได้ใช้งาน
   - ลบบริการระบบที่มีความซ้ำซ้อนกับบริการอื่น

3. สำหรับอุปกรณ์เครือข่าย (Network Devices)

1. **การจำกัดสิทธิพิเศษการเข้าถึง (Least Access Privilege)**
   - ผู้ดูแลระบบเครือข่ายสามารถจัดการเครือข่าย แต่ไม่สามารถเข้าถึงข้อมูลบนเซิร์ฟเวอร์
   - ผู้ใช้ทั่วไปไม่สามารถแก้ไขการตั้งค่าเครือข่ายได้
   - ผู้ใช้อุปกรณ์พกพาสามารถเข้าถึงเฉพาะเครือข่ายที่จำเป็น
   - การจำกัดการเข้าถึงไฟล์เซิร์ฟเวอร์สำหรับผู้ใช้ที่ได้รับอนุญาตเท่านั้น
   - ผู้ใช้ทั่วไปไม่สามารถแก้ไขการตั้งค่าเครือข่ายขั้นสูง
   - บัญชีผู้ใช้เครือข่ายที่ไม่ได้ใช้งานเกิน 30 วันจะถูกล็อก
   - ผู้ใช้ไม่สามารถเข้าถึงการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย
   - การจัดการสิทธิ์การเข้าถึงในไฟร์วอลล์สำหรับผู้ดูแลระบบเท่านั้น
   - ผู้ใช้ทั่วไปไม่สามารถเข้าถึงการจัดการพอร์ตเครือข่ายได้
   - การจำกัดการเข้าถึงในโฟลเดอร์ข้อมูลเครือข่ายเฉพาะผู้มีสิทธิ์เท่านั้น

2. การป้องกันมัลแวร์ (Malware Protection)

- ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ในทุกอุปกรณ์เครือข่าย
- สแกนระบบเครือข่ายโดยอัตโนมัติทุกสัปดาห์เพื่อตรวจจับมัลแวร์
- บล็อกการดาวน์โหลดไฟล์ที่น่าสงสัยหรือเป็นอันตราย
- การตรวจสอบอีเมลที่เข้ามาเพื่อตรวจจับมัลแวร์
- การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ในอุปกรณ์พกพา
- การใช้เทคโนโลยี Sandboxing สำหรับไฟล์จากภายนอก
- การตรวจสอบและป้องกันมัลแวร์ในระบบคลาวด์
- การใช้ซอฟต์แวร์ป้องกันมัลแวร์แบบเรียลไทม์ในเครือข่าย
- ตรวจสอบมัลแวร์ในเซิร์ฟเวอร์อีเมล
- การฝึกอบรมพนักงานเรื่องการป้องกันมัลแวร์

3. การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน (Disabling Unused Ports)

- ปิดพอร์ต SSH ที่ไม่ได้ใช้งาน
- ปิดพอร์ต Telnet บนเซิร์ฟเวอร์ทั้งหมด
- ปิดพอร์ต SMB ที่ไม่ได้ใช้งานในระบบ Windows
- ปิดพอร์ต HTTP ที่ไม่ได้ใช้งานบนเซิร์ฟเวอร์
- ปิดพอร์ต FTP ที่ไม่ได้ใช้งาน
- ปิดพอร์ต RDP ที่ไม่ได้ใช้งาน
- ปิดพอร์ต SNMP ที่ไม่ได้ใช้งาน
- ปิดพอร์ตที่ไม่ได้เชื่อมต่อบนสวิตช์เครือข่าย
- ปิดพอร์ตที่ไม่จำเป็นในอุปกรณ์ IoT
- การจัดการพอร์ตที่เปิดใช้งานโดยมีการตรวจสอบความปลอดภัยเป็นประจำ

Logo	**ระเบียบกระบวนการจัดการเปลี่ยนแปลง (Change Management Process Procedure)**	**รหัสเอกสาร**	**CSMS-Protect -07**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการจัดการเปลี่ยนแปลง (Change Management Process Procedure)	รหัสเอกสาร	CSMS-Protect -07
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการจัดการเปลี่ยนแปลง (Change Management Process Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.2.5]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ รวมถึงการควบคุมการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นในระบบหรือกระบวนการขององค์กร เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเหล่านั้นได้รับการดำเนินการอย่างเหมาะสม ลดความเสี่ยงที่อาจเกิดขึ้น และรักษาความมั่นคงปลอดภัยทางไซเบอร์ในการดำเนินงานขององค์กรหรือหน่วยงาน

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมการเปลี่ยนแปลงทุกประเภทสำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดในระบบ

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้ร้องขอการเปลี่ยนแปลง (Change Requester)**: รับผิดชอบในการระบุความจำเป็นในการเปลี่ยนแปลงและจัดทำเอกสารการร้องขอ
- **คณะกรรมการจัดการการเปลี่ยนแปลง (Change Advisory Board: CAB)**: รับผิดชอบในการประเมิน อนุมัติ หรือปฏิเสธการเปลี่ยนแปลง
- **ผู้ดำเนินการเปลี่ยนแปลง (Change Implementer)**: รับผิดชอบในการดำเนินการเปลี่ยนแปลงตามแผนที่ได้รับอนุมัติ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. ขั้นตอนการจัดการเปลี่ยนแปลง (Change Management Process Steps)

4.1 การร้องขอการเปลี่ยนแปลง (Change Request)

- **4.1.1 ระบุความต้องการในการเปลี่ยนแปลง**
  - **ขั้นตอน**: บุคลากรหรือหน่วยงานที่พบว่ามีความจำเป็นต้องเปลี่ยนแปลงระบบหรือกระบวนการจะต้องระบุความต้องการในการเปลี่ยนแปลง พร้อมเหตุผลและรายละเอียดที่เกี่ยวข้อง เช่น ทีม IT ร้องขอการเปลี่ยนแปลงเพื่ออัปเดตซอฟต์แวร์ระบบให้เป็นเวอร์ชันล่าสุดเพื่อลดความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์
- **4.1.2 ส่งเอกสารการร้องขอ**
  - **ขั้นตอน**: ผู้ร้องขอจัดทำเอกสารการร้องขอการเปลี่ยนแปลง (Change Request Document) ที่รวมถึงวัตถุประสงค์ของการเปลี่ยนแปลง รายละเอียดการเปลี่ยนแปลง ผลกระทบที่คาดการณ์และทรัพยากรที่จำเป็น แล้วส่งไปยังคณะกรรมการจัดการการเปลี่ยนแปลง (CAB) เช่น ทีม IT จัดทำเอกสารการร้องขออัปเดตซอฟต์แวร์ โดยระบุว่าอัปเดตนี้จะช่วยแก้ไขช่องโหว่ความปลอดภัยที่พบในระบบปัจจุบัน

4.2 การประเมินและอนุมัติการเปลี่ยนแปลง (Change Evaluation and Approval)

- **4.2.1 การประเมินการเปลี่ยนแปลง**
  - **ขั้นตอน**: คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) จะทำการประเมินความเสี่ยง ผลกระทบต่อระบบและกระบวนการปัจจุบัน ต้นทุน และทรัพยากรที่จำเป็นในการดำเนินการ เช่น คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) ประเมินว่าการอัปเดตซอฟต์แวร์จะใช้เวลา

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4 ชั่วโมงในการดำเนินการ และอาจทำให้ระบบต้องหยุดให้บริการในช่วงเวลานั้น แต่จะช่วยลดความเสี่ยงจากการถูกโจมตี

- **4.2.2 การอนุมัติหรือปฏิเสธการเปลี่ยนแปลง**
  - **ขั้นตอน**: หลังจากการประเมิน คณะกรรมการจัดการการเปลี่ยนแปลง (CAB) จะทำการอนุมัติหรือปฏิเสธการเปลี่ยนแปลง หากได้รับการอนุมัติ จะมีการกำหนดแผนการดำเนินการที่ชัดเจน เช่น กำหนดให้ดำเนินการในช่วงสุดสัปดาห์เมื่อมีผู้ใช้น้อยที่สุด
- **4.2.3 การจัดทำแผนการเปลี่ยนแปลง**
  - **ขั้นตอน**: ผู้ร้องขอการเปลี่ยนแปลงและผู้ดำเนินการเปลี่ยนแปลงร่วมกันจัดทำแผนการดำเนินการเปลี่ยนแปลง ซึ่งรวมถึงเวลาที่จะดำเนินการ ทรัพยากรที่จำเป็น และการเตรียมการสำรอง (Backup) ก่อนดำเนินการ เสมอ

4.3 การดำเนินการเปลี่ยนแปลง (Change Implementation)

- **4.3.1 การสื่อสารการเปลี่ยนแปลง**
  - **ขั้นตอน**: ก่อนเริ่มดำเนินการเปลี่ยนแปลง ต้องมีการสื่อสารแผนการเปลี่ยนแปลงไปยังบุคลากรที่เกี่ยวข้องทุกคน เพื่อให้ทราบถึงการเปลี่ยนแปลงที่จะเกิดขึ้นและการเตรียมความพร้อม โดยการส่งอีเมลแจ้งเตือนผู้ใช้งานทุกคนเกี่ยวกับการหยุดให้บริการระบบในที่กำหนดไว้ เพื่ออัปเดตซอฟต์แวร์ เป็นต้น
- **4.3.2 การดำเนินการตามแผน**
  - **ขั้นตอน**: ผู้ดำเนินการเปลี่ยนแปลงจะดำเนินการเปลี่ยนแปลงตามแผนที่ได้รับอนุมัติ โดยปฏิบัติตามขั้นตอนที่กำหนดอย่างเคร่งครัด และติดตามความคืบหน้าตามแผนที่วางไว้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **4.3.3 การทดสอบและตรวจสอบผลการเปลี่ยนแปลง**
  - **ขั้นตอน**: หลังจากดำเนินการเปลี่ยนแปลง จะต้องทำการทดสอบระบบหรือกระบวนการที่เปลี่ยนแปลงเพื่อให้แน่ใจว่าไม่มีปัญหาเกิดขึ้นและการเปลี่ยนแปลงเป็นไปตามที่คาดหวัง โดยการทดสอบระบบเพื่อตรวจสอบว่าซอฟต์แวร์ทำงานได้อย่างถูกต้องและไม่มีข้อผิดพลาด

4.4 การติดตามและการรายงานผล (Monitoring and Reporting)

- **4.4.1 การติดตามผลหลังการเปลี่ยนแปลง**
  - **ขั้นตอน**: ติดตามผลการเปลี่ยนแปลงในระยะเวลาที่กำหนด เพื่อให้แน่ใจว่าการเปลี่ยนแปลงไม่มีผลกระทบเชิงลบต่อระบบหรือกระบวนการ โดยมีการติดตามผลการทำงานของซอฟต์แวร์ที่อัปเดตใหม่เป็นเวลา 7 วันหลังจากการอัปเดต เพื่อให้แน่ใจว่าไม่มีปัญหาใด ๆ เกิดขึ้น
- **4.4.2 การรายงานผลการเปลี่ยนแปลง**
  - **ขั้นตอน**: รายงานผลการเปลี่ยนแปลงให้กับคณะกรรมการจัดการการเปลี่ยนแปลง (CAB) และผู้บริหาร เพื่อประเมินผลการดำเนินการและตัดสินใจเพิ่มเติมหากมีปัญหาเกิดขึ้น

4.5 การปิดการเปลี่ยนแปลง (Change Closure)

- **4.5.1 การปิดเอกสารการเปลี่ยนแปลง**
  - **ขั้นตอน**: เมื่อการเปลี่ยนแปลงเสร็จสมบูรณ์และผ่านการทดสอบและติดตามผลแล้ว ผู้ดำเนินการเปลี่ยนแปลงจะต้องปิดเอกสารการเปลี่ยนแปลง และบันทึกผลลัพธ์สุดท้ายลงในระบบการจัดการเอกสาร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **4.5.2 การจัดเก็บเอกสารและบทเรียนที่ได้**
  - **ขั้นตอน**: จัดเก็บเอกสารที่เกี่ยวข้องกับการเปลี่ยนแปลง และบันทึกกิจกรรมที่ได้จากการเปลี่ยนแปลงนี้ เพื่อนำไปใช้ในการปรับปรุงกระบวนการในอนาคต

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ใบร้องขอการเปลี่ยนแปลง (Change Management Request Form)
2. รายงานผลการเปลี่ยนแปลง (Change Management report)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

3. กระบวนการการเชื่อมต่อระยะไกล

(Remote Connection Procedure)

Logo	นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)	รหัสเอกสาร	CSMS-Policy -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)	รหัสเอกสาร	CSMS-Policy -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.3.1, ข้อ 22.3.2]

1. วัตถุประสงค์ (Objective)

นโยบายนี้กำหนดแนวทางและข้อกำหนดสำหรับการเชื่อมต่อระยะไกลมายังบริการที่สำคัญขององค์กร เพื่อให้มั่นใจว่าการเข้าถึงจากภายนอกมีความปลอดภัย ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูล

2. ขอบเขต (Scope)

นโยบายนี้ใช้กับพนักงาน ผู้รับเหมา และบุคคลภายนอกที่ต้องการเชื่อมต่อเข้ามายังระบบสารสนเทศขององค์กรจากระยะไกล รวมถึงการเข้าถึงผ่าน VPN, Remote Desktop, และเครื่องมือการเข้าถึงระยะไกลอื่น ๆ ที่ได้รับอนุญาต

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management):** กำกับดูแลให้มีการปฏิบัติตามนโยบายการเชื่อมต่อระยะไกล และอนุมัติแนวทางที่จำเป็นในการรักษาความมั่นคงปลอดภัย
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team):** กำหนดและบังคับใช้นโยบาย รวมถึงตรวจสอบและบันทึกกิจกรรมที่เกี่ยวข้องกับการเข้าถึงระยะไกล
- **ผู้ใช้งานระบบ (Remote Users):** ปฏิบัติตามข้อกำหนดของนโยบายนี้และแจ้งเหตุการณ์ที่ผิดปกติแก่ฝ่าย IT Security

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)	รหัสเอกสาร	CSMS-Policy -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4. แนวปฏิบัติในการเชื่อมต่อระยะไกล (Remote Connection Guidelines)

4.1 ข้อกำหนดทั่วไป

- ผู้ใช้ต้องได้รับการอนุมัติจากฝ่าย IT ก่อนการเข้าถึงระยะไกล
- อุปกรณ์ที่ใช้เชื่อมต่อระยะไกลต้องเป็นอุปกรณ์ที่ได้รับอนุญาตจากองค์กรและต้องติดตั้งซอฟต์แวร์รักษาความปลอดภัย
- การเชื่อมต่อระยะไกลต้องใช้ **VPN และการเข้ารหัสแบบ End-to-End**

4.2 การพิสูจน์ตัวตนและการควบคุมการเข้าถึง

- ผู้ใช้ต้องใช้ **Multi-Factor Authentication (MFA)** ในการเข้าถึงระบบระยะไกล
- ใช้มาตรการ **Least Privilege Access** โดยกำหนดสิทธิ์การเข้าถึงเฉพาะส่วนที่จำเป็น
- มีการตรวจสอบสิทธิ์การเข้าถึงเป็นระยะ และต้องเพิกถอนสิทธิ์ทันทีเมื่อผู้ใช้ออกจากองค์กรหรือหมดหน้าที่ความรับผิดชอบ

4.3 การรักษาความมั่นคงปลอดภัยของข้อมูล

- ห้ามใช้เครือข่ายสาธารณะ (Public Wi-Fi) ในการเข้าถึงบริการที่สำคัญขององค์กร เว้นแต่มีมาตรการป้องกันที่เหมาะสม เช่น VPN
- ห้ามเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กรบนอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อระยะไกล
- ระบบที่รองรับการเข้าถึงระยะไกลต้องมี **Session Timeout** เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการเชื่อมต่อระยะไกล (Remote Connection Policy)	รหัสเอกสาร	CSMS-Policy -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4.4 การบันทึกและการติดตามการเข้าถึง

- ต้องมีการบันทึกกิจกรรมการเข้าถึงระยะไกลทั้งหมดใน **Security Information and Event Management (SIEM)**
- ทีม IT Security ต้องดำเนินการตรวจสอบบันทึกการเข้าถึงเป็นระยะ และมีการแจ้งเตือนเมื่อพบกิจกรรมที่ผิดปกติ
- รายงานการเชื่อมต่อระยะไกลต้องถูกจัดเก็บและตรวจสอบอย่างน้อยปีละ 1 ครั้ง

5. การบังคับใช้และบทลงโทษ (Enforcement and Penalties)

- ผู้ใช้ที่ฝ่าฝืนนโยบายนี้อาจถูกระงับสิทธิ์การเข้าถึงระยะไกล และอาจได้รับโทษทางวินัยตามระเบียบขององค์กร
- องค์กรมีสิทธิ์ตรวจสอบและบังคับใช้นโยบายนี้โดยปรับปรุงให้สอดคล้องกับภัยคุกคามและข้อกำหนดทางกฎหมายที่เปลี่ยนแปลง

นโยบายการเชื่อมต่อระยะไกล (**Policy Review)**

นโยบายการเชื่อมต่อระยะไกล นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเชื่อมต่อระยะไกล (Remote Connection Procedure)	รหัสเอกสาร	CSMS-Protect -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	1 ม.ค. 2568 Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเชื่อมต่อระยะไกล (Remote Connection Procedure)	รหัสเอกสาร	CSMS-Protect -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการเชื่อมต่อระยะไกล (Remote Connection Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.3.1, ข้อ 22.3.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อควบคุมและรักษาความมั่นคงปลอดภัยของการเชื่อมต่อระยะไกลมายังบริการที่สำคัญขององค์กร โดยให้แน่ใจว่ามีมาตรการที่เพียงพอในการป้องกันและตรวจจับการเข้าถึงที่ไม่ได้รับอนุญาต

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกลมายังบริการที่สำคัญ รวมถึงการกำหนดแนวทางปฏิบัติสำหรับการเชื่อมต่อและการควบคุมการไหลของข้อมูล

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและตรวจสอบมาตรการความมั่นคงปลอดภัยสำหรับการเชื่อมต่อระยะไกล
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team)**: รับผิดชอบในการกำหนดและบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล
- **ผู้ใช้งานระบบ (Remote Users)**: มีหน้าที่ปฏิบัติตามนโยบายและแนวทางปฏิบัติที่กำหนดไว้สำหรับการเชื่อมต่อระยะไกล

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการเชื่อมต่อระยะไกล (Remote Connection Procedure)	รหัสเอกสาร	CSMS-Protect -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4. การรักษาความมั่นคงปลอดภัยในการเชื่อมต่อระยะไกล (Remote Connection Security)

- **4.1 มาตรการรักษาความมั่นคงปลอดภัย**
  - **ขั้นตอน**: ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลมายังบริการที่สำคัญมีมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ เช่น การใช้การเข้ารหัส การพิสูจน์ตัวตนที่แข็งแกร่ง และการควบคุมการไหลของข้อมูล โดยมีการใช้ VPN ที่เข้ารหัสการเชื่อมต่อและการยืนยันตัวตนด้วยสองปัจจัย (2FA) สำหรับการเข้าถึงระบบจากระยะไกล
- **4.2 การเปิดใช้งานการเชื่อมต่อ**
  - **ขั้นตอน**: เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น และปิดการเชื่อมต่อเมื่อไม่ใช้งาน โดยการตั้งค่าให้เซิร์ฟเวอร์เปิดใช้งานการเชื่อมต่อระยะไกลเฉพาะในช่วงเวลาทำงานเท่านั้น
- **4.3 การใช้เทคนิคการพิสูจน์ตัวตนที่แข็งแกร่ง**
  - **ขั้นตอน**: ใช้เทคนิคการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยในการส่งข้อมูลและความสมบูรณ์ของข้อความที่แข็งแกร่ง เช่น การใช้โปรโตคอลที่ปลอดภัย SSH สำหรับการเชื่อมต่อระยะไกลเพื่อป้องกันการโจมตีแบบ Man-in-the-Middle
- **4.4 การเข้ารหัสการเชื่อมต่อ**
  - **ขั้นตอน**: ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมดเพื่อป้องกันการดักฟังข้อมูลระหว่างทาง เช่น การใช้ HTTPS สำหรับการเข้าถึงเว็บไซต์ภายในองค์กรจากระยะไกล
- **4.5 ข้อจำกัดในการใช้คำสั่งระบบ (System Commands)**
  - **ขั้นตอน**: ไม่อนุญาตให้เชื่อมต่อระยะไกลเพื่อใช้งานคำสั่งระบบที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน โดยการจำกัดสิทธิ์ในการใช้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

คำสั่งที่เกี่ยวข้องกับการจัดการเซิร์ฟเวอร์ผ่านการเชื่อมต่อระยะไกล เว้นแต่จะได้รับการอนุมัติจากผู้บริหาร

- **4.6 การจำกัดการไหลของข้อมูล**
  - **ขั้นตอน**: จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ เพื่อป้องกันการรั่วไหลของข้อมูลที่ไม่จำเป็น โดยการกำหนดให้สามารถถ่ายโอนข้อมูลเฉพาะไฟล์ที่จำเป็นสำหรับการทำงานเท่านั้นในระหว่างการเชื่อมต่อระยะไกล

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. นโยบาย แนวปฏิบัติในการเชื่อมต่อระยะไกล
2. หลักฐานการขออนุญาตเชื่อมต่อระยะไกล จากการใช้คำสั่งระบบ (Issuing System Commands)
3. รายงานการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. กระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Procedure)

Logo	**นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)**	**รหัสเอกสาร**	**CSMS-Policy -05**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)	รหัสเอกสาร	CSMS-Policy -05
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 2.4.1, ข้อ 22.4.2]

1. วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรการและแนวปฏิบัติสำหรับการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ เช่น USB, External Hard Drive, SD Card และอุปกรณ์จัดเก็บข้อมูลอื่น ๆ เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและการรั่วไหลของข้อมูลสำคัญขององค์กร

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงพนักงานทุกระดับ ผู้รับเหมา และบุคคลภายนอกที่ต้องการใช้งานหรือเชื่อมต่ออุปกรณ์บันทึกข้อมูลแบบถอดได้กับระบบสารสนเทศขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management):** กำกับดูแลให้มีการปฏิบัติตามนโยบายและสนับสนุนมาตรการด้านความมั่นคงปลอดภัย
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team):** บังคับใช้และตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้ พร้อมดำเนินมาตรการรักษาความมั่นคงปลอดภัย
- **พนักงานและผู้ใช้งาน (Employees & Users):** ปฏิบัติตามแนวทางของนโยบายนี้ และรายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการใช้งานสื่อบันทึกข้อมูลแบบถอดได้

4. แนวปฏิบัติในการใช้งานสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Guidelines)

4.1 การอนุญาตและข้อจำกัด

- อุปกรณ์บันทึกข้อมูลแบบถอดได้ต้องได้รับการอนุมัติจากฝ่าย IT ก่อนใช้งาน
- ห้ามใช้อุปกรณ์ส่วนตัวในการถ่ายโอนหรือจัดเก็บข้อมูลขององค์กร เว้นแต่ได้รับอนุญาตเป็นกรณีพิเศษ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- ต้องมีการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลสำคัญที่จัดเก็บในอุปกรณ์บันทึกข้อมูลแบบถอดได้

4.2 การควบคุมการเข้าถึงและการใช้งาน

- จำกัดสิทธิ์การเข้าถึงสื่อบันทึกข้อมูลแบบถอดได้เฉพาะผู้ที่มีความจำเป็นต้องใช้งานเท่านั้น
- ระบบที่รองรับการใช้งานอุปกรณ์แบบถอดได้ต้องมีการเปิดใช้ **Read-Only Mode** เป็นค่าเริ่มต้น และอนุญาตให้เขียนข้อมูลได้เฉพาะอุปกรณ์ที่ได้รับอนุญาต
- ห้ามใช้อุปกรณ์บันทึกข้อมูลแบบถอดได้ที่ไม่มีการตรวจสอบหรือมีแหล่งที่มาไม่แน่ชัด

4.3 มาตรการรักษาความมั่นคงปลอดภัย

- ต้องใช้ซอฟต์แวร์ป้องกันมัลแวร์เพื่อตรวจสอบอุปกรณ์ทุกครั้งก่อนใช้งาน
- อุปกรณ์ที่ไม่ได้ใช้งานเป็นเวลานานต้องถูกลบข้อมูลทั้งหมดก่อนนำมาใช้อีกครั้ง
- ต้องมีระบบบันทึกการใช้งานสื่อบันทึกข้อมูลแบบถอดได้เพื่อให้สามารถตรวจสอบย้อนหลังได้

4.4 การนำออกและการทำลายข้อมูล

- เมื่อเลิกใช้งานอุปกรณ์ ต้องมีการลบข้อมูลอย่างปลอดภัย (Secure Erasure) ตามมาตรฐานขององค์กร
- อุปกรณ์ที่ชำรุดหรือหมดอายุการใช้งานต้องถูกทำลายอย่างปลอดภัย โดยใช้เทคนิคการลบข้อมูลที่ไม่สามารถกู้คืนได้ เช่น **Data Wiping** หรือ **Physical Destruction**

5. การตรวจสอบและบังคับใช้ (Monitoring and Enforcement)

5.1 การตรวจสอบและติดตาม

- ทีม IT Security ต้องมีระบบเฝ้าระวังและตรวจสอบการใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้
- ต้องมีการตรวจสอบบันทึกการใช้งานเป็นระยะ และดำเนินมาตรการตอบสนองหากพบพฤติกรรมที่ผิดปกติ

5.2 การตอบสนองต่อเหตุการณ์ (Incident Response)

- หากพบการใช้งานที่ไม่ได้รับอนุญาต ระบบต้องแจ้งเตือนฝ่าย IT Security ทันที
- ทีม IT มีอำนาจในการยกเลิกสิทธิ์การใช้งานของผู้ใช้ที่ละเมิดนโยบาย

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**นโยบายการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media Policy)**	**รหัสเอกสาร**	**CSMS-Policy -05**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

5.3 การบังคับใช้ข้อกำหนด

- ผู้ใช้ที่ฝ่าฝืนนโยบายนี้อาจถูกระงับสิทธิ์การใช้งานอุปกรณ์บันทึกข้อมูลแบบถอดได้ และอาจได้รับโทษทางวินัยตามระเบียบขององค์กร
- องค์กรมีสิทธิ์ปรับปรุงนโยบายและกระบวนการนี้ให้สอดคล้องกับภัยคุกคามและกฎหมายที่เปลี่ยนแปลง

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Procedure)**	**รหัสเอกสาร**	**CSMS-Protect -03**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Procedure)	รหัสเอกสาร	CSMS-Protect -03
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.4.1, ข้อ 22.4.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อควบคุมและรักษาความมั่นคงปลอดภัยทางไซเบอร์ในการใช้สื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจายของมัลแวร์ไปยังบริการที่สำคัญขององค์กร

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการใช้ การควบคุม และการเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพาที่เชื่อมต่อกับบริการที่สำคัญขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและกำกับดูแลการดำเนินการตามกระบวนการควบคุมการใช้สื่อเก็บข้อมูลแบบถอดได้
- **ทีม IT/รักษาความปลอดภัยสารสนเทศ (IT/Security Team)**: รับผิดชอบในการกำหนดและบังคับใช้มาตรการควบคุม การตรวจสอบ และการเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้
- **ผู้ใช้งานระบบ (System Users)**: มีหน้าที่ปฏิบัติตามนโยบายและแนวทางปฏิบัติที่กำหนดไว้สำหรับการใช้สื่อเก็บข้อมูลแบบถอดได้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. การควบคุมการใช้สื่อเก็บข้อมูลแบบถอดได้ (Control of Removable Storage Media)

- **4.1 การปิดใช้งานพอร์ตเชื่อมต่อภายนอก**
  - **ขั้นตอน**: ให้ทำการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น โดยการตั้งค่าให้พอร์ต USB บนอุปกรณ์คอมพิวเตอร์ภายในองค์กรถูกปิดใช้งานโดยค่าเริ่มต้น และต้องได้รับการอนุญาตจากผู้ดูแลระบบก่อนการเปิดใช้งาน
- **4.2 การใช้งานสื่อเก็บข้อมูลที่ได้รับอนุญาต**
  - **ขั้นตอน**: อนุญาตให้ใช้สื่อเก็บข้อมูลแบบถอดได้เฉพาะที่ได้รับอนุญาตและผ่านการตรวจสอบตามข้อกำหนดที่กำหนดไว้เท่านั้น โดยการจำกัดการใช้งานสื่อเก็บข้อมูลแบบถอดได้ที่ได้รับการจัดหาโดยองค์กรเท่านั้น และป้องกันไม่ให้พนักงานใช้สื่อเก็บข้อมูลส่วนตัว
- **4.3 การตรวจสอบมัลแวร์ก่อนการเชื่อมต่อ**
  - **ขั้นตอน**: ตรวจสอบว่าสื่อเก็บข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญขององค์กร โดยการสแกนหามัลแวร์บนสื่อเก็บข้อมูลก่อนการเชื่อมต่อกับเครือข่ายองค์กร

5. การเข้ารหัสข้อมูลบนสื่อเก็บข้อมูลแบบถอดได้ (Encryption of Data on Removable Storage Media)

- **5.1 การเข้ารหัสข้อมูลที่ละเอียดอ่อน**
  - **ขั้นตอน**: เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญขององค์กรที่จัดเก็บบนสื่อเก็บข้อมูลแบบถอดได้ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยการใช้ซอฟต์แวร์เข้ารหัสข้อมูลเพื่อเข้ารหัสไฟล์สำคัญก่อนที่จะถ่ายโอนข้อมูลไปยังสื่อเก็บข้อมูลแบบถอดได้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **5.2 การตรวจสอบการปฏิบัติตาม**
  - **ขั้นตอน**: ตรวจสอบให้แน่ใจว่าผู้ใช้งานปฏิบัติตามมาตรการการเข้ารหัสข้อมูลและการควบคุมสื่อเก็บข้อมูลแบบถอดได้ตามที่กำหนดไว้ในกระบวนการ มีการตรวจสอบเป็นระยะเพื่อให้แน่ใจว่าสื่อเก็บข้อมูลที่ใช้งานในองค์กรมีการเข้ารหัสข้อมูลตามข้อกำหนด

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. หลักฐานหรือเอกสารที่ใช้ในการร้องขอการเปิด USB Port

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. กระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness Procedure)

Logo	**ระเบียบกระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)**	**รหัสเอกสาร**	**CSMS-Protect -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)**	**รหัสเอกสาร**	**CSMS-Protect -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

ระเบียบกระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 22.5.1, ข้อ 22.5.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อส่งเสริมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย ไซเบอร์แก่พนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการจัดทำแผนงาน การเผยแพร่ และการทบทวนกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรที่เกี่ยวข้องในองค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการสนับสนุนและกำกับดูแลการดำเนินการตามแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
- **ทีมรักษาความปลอดภัยไซเบอร์(Cybersecurity Awareness Team)**: รับผิดชอบในการพัฒนาและดำเนินการตามแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการจัดกิจกรรมและการเผยแพร่ข้อมูล
- **พนักงานและผู้ให้บริการภายนอก (Employees and External Service Providers)**: มีหน้าที่เข้าร่วมกิจกรรมและปฏิบัติตามนโยบายและแนวทางที่ได้รับการอบรมหรือเผยแพร่

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	CSMS-Protect -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4. การจัดทำแผนงานการสร้างความตระหนักรู้ (Development of Cybersecurity Awareness Plan)

- **4.1 กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท**
  - **ขั้นตอน**: จัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกกลุ่ม รวมถึงพนักงานใหม่ ผู้ใช้และผู้บริหาร เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญ และผู้ขายหรือผู้รับเหมา โดยการจัดอบรมความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงานใหม่เมื่อเริ่มงาน และการจัดสัมมนาเชิงปฏิบัติการสำหรับเจ้าหน้าที่ IT เพื่อเรียนรู้เกี่ยวกับภัยคุกคามใหม่ ๆ
- **4.2 การเผยแพร่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์**
  - **ขั้นตอน**: เผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ โดยใช้ช่องทางต่าง ๆ เช่น อีเมล บอร์ดประกาศ และการประชุม โดยการส่งอีเมลแจ้งให้พนักงานทุกคนทราบถึงหน้าที่ในการรักษาความมั่นคงปลอดภัยไซเบอร์ และการกำหนดหน้าที่เฉพาะสำหรับทีม IT
- **4.3 การตระหนักรู้กฎหมายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์**
  - **ขั้นตอน**: จัดทำและเผยแพร่ข้อมูลเกี่ยวกับกฎหมาย กฎ ระเบียบ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้บุคลากรทุกคนตระหนักถึงข้อกำหนดที่ต้องปฏิบัติตาม โดยการการจัดทำคู่มือการปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์ และการอบรมเกี่ยวกับกฎหมายความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง
- **4.4 การสื่อสารและเผยแพร่ข้อมูลอย่างสม่ำเสมอ**
  - **ขั้นตอน**: สื่อสารข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามใหม่ ๆ อย่างสม่ำเสมอและทันท่วงทีผ่านช่องทางที่เหมาะสม เช่น อีเมล บอร์ดข่าวสารภายในองค์กร หรือระบบการ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดการเรียนรู้ โดยการส่งข่าวสารเกี่ยวกับภัยคุกคามไซเบอร์ล่าสุดให้กับพนักงานทุกสัปดาห์ และการจัดทำคอร์สออนไลน์เกี่ยวกับวิธีการบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์

5. การทบทวนแผนงานและการปรับปรุง (Review and Improvement of Awareness Plan)

- **5.1 การทบทวนแผนงานประจำปี**
  - **ขั้นตอน**: ทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีความเกี่ยวข้องกับสถานการณ์ปัจจุบัน
- **5.2 การปรับปรุงเนื้อหาและกิจกรรมตามผลการทบทวน**
  - **ขั้นตอน**: ปรับปรุงเนื้อหาและกิจกรรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการตระหนักรู้และป้องกันภัยคุกคาม โดยการเพิ่มโมดูลการอบรมเกี่ยวกับการป้องกันการโจมตีในรูปแบบต่างๆ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Procedure)	รหัสเอกสาร	CSMS-Protect -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
2. หลักฐานหรือเอกสาร การจัดทำกิจกรรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : นาย สมชาย เอก

จัดทำเมื่อ : 1 ตุลาคม 2567

แผนงานการสร้างความตระหนักรู้ในองค์กร (Cybersecurity Awareness Plan)

1. พนักงานใหม่ (New Employees)

1.1 การฝึกอบรมเบื้องต้นด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมายอื่นที่เกี่ยวข้อง

1. **การฝึกอบรมในห้องเรียน (In-person Training)**
   - **เนื้อหาหลัก:** การใช้รหัสผ่านที่ปลอดภัย, การระบุและป้องกันอีเมลฟิชชิง, การรายงานเหตุการณ์ และบทบาทและความรับผิดชอบตามกฎหมายความมั่นคงปลอดภัยไซเบอร์
   - **ระยะเวลา:** 2 ชั่วโมง
   - **การวัดผล:** ทดสอบความเข้าใจหลังการฝึกอบรม
2. **การฝึกอบรมออนไลน์ (E-learning)**
   - **เนื้อหาหลัก:** วิดีโอสอนเกี่ยวกับข้อกฎหมายสำคัญ, การใช้รหัสผ่าน, การป้องกันภัยคุกคาม, และแบบทดสอบในแต่ละบท
   - **ระยะเวลา:** 1-2 ชั่วโมง
   - **การวัดผล:** คะแนนจากแบบทดสอบออนไลน์
3. **คู่มือการปฏิบัติตามกฎหมายและการใช้งานที่ปลอดภัย (Legal Compliance and Security Handbook)**
   - **เนื้อหาหลัก:** สรุปข้อกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และแนวทางปฏิบัติที่ปลอดภัย
   - **การแจกจ่าย:** แจกคู่มือในวันแรกของการทำงาน

- **การวัดผล:** ไม่มีการทดสอบ

4. **การประชุมแนะนำกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Orientation Meeting)**
    - **เนื้อหาหลัก:** แนะนำพนักงานใหม่เกี่ยวกับกฎหมายและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
    - **ระยะเวลา:** 1 ชั่วโมง
    - **การวัดผล:** การตอบคำถามและทบทวนความเข้าใจ
5. **การฝึกอบรมเชิงปฏิบัติ (Practical Compliance Training)**
    - **เนื้อหาหลัก:** ฝึกอบรมการปฏิบัติตามกฎหมายในสถานการณ์จริง เช่น การจัดการข้อมูลส่วนบุคคล, การปฏิบัติเมื่อพบเหตุการณ์ทางไซเบอร์
    - **ระยะเวลา:** 1.5 ชั่วโมง
    - **การวัดผล:** การปฏิบัติจริงในสถานการณ์จำลอง

2. ผู้ใช้และระดับบริหาร (Users and Management)

2.1 การฝึกอบรมประจำปีด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมาย

1. **สัมมนาออนไลน์ (Webinar)**
    - **เนื้อหาหลัก:** การจัดการการเข้าถึงข้อมูล, การป้องกันการโจมตีไซเบอร์, การอัปเดตกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
    - **ระยะเวลา:** 2 ชั่วโมง
    - **การวัดผล:** แบบทดสอบหลังสัมมนา
2. **การฝึกอบรมเชิงลึกด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (In-depth Legal and Cybersecurity Training)**
    - **เนื้อหาหลัก:** การวิเคราะห์และจัดการความเสี่ยงทางกฎหมายที่เกี่ยวข้องกับไซเบอร์, การตอบสนองต่อเหตุการณ์, การปฏิบัติตามข้อกำหนดทางกฎหมาย
    - **ระยะเวลา:** 3 ชั่วโมง

- **การวัดผล:** การประเมินจากสถานการณ์จำลอง

3. **การแจ้งเตือนภัยคุกคามและการเปลี่ยนแปลงกฎหมาย (Threat and Legal Updates Alerts)**
    - **เนื้อหาหลัก:** การแจ้งเตือนเกี่ยวกับภัยคุกคามใหม่ ๆ และการเปลี่ยนแปลงของกฎหมายที่อาจส่งผลกระทบต่อการปฏิบัติงาน
    - **ระยะเวลา:** ส่งแจ้งเตือนเป็นระยะตามความจำเป็น
    - **การวัดผล:** การตรวจสอบการปรับปรุงการปฏิบัติตามข้อกำหนดใหม่
4. **การฝึกอบรมเฉพาะทาง (Specialized Training)**
    - **เนื้อหาหลัก:** การป้องกันและตอบสนองต่อการโจมตีขั้นสูง, ความรับผิดชอบทางกฎหมายในการปกป้องข้อมูลและระบบสารสนเทศ
    - **ระยะเวลา:** 4 ชั่วโมง
    - **การวัดผล:** การประเมินความเข้าใจและการทดสอบกรณีศึกษา
5. **การประชุมทบทวนกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Legal and Cybersecurity Review Meetings)**
    - **เนื้อหาหลัก:** ทบทวนการปฏิบัติตามกฎหมายและนโยบายความมั่นคงปลอดภัยในปีที่ผ่านมา และวางแผนการปรับปรุง
    - **ระยะเวลา:** 5 ชั่วโมง
    - **การวัดผล:** การวางแผนและดำเนินการตามแผนการปรับปรุงที่ระบุ

3. เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Support Staff)

3.1 การฝึกอบรมเชิงลึกด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์สำหรับ IT และ ICS

1. **การฝึกอบรมเชิงปฏิบัติการและกฎหมาย (Hands-on and Legal Training)**
   - **เนื้อหาหลัก:** การจัดการความปลอดภัยของระบบ SCADA, การควบคุมการเข้าถึงเครือข่าย, การปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
   - **ระยะเวลา:** 5 ชั่วโมง
   - **การวัดผล:** ทดสอบการปฏิบัติจริง
2. **การทดสอบจำลองสถานการณ์และความรู้ด้านกฎหมาย (Simulation Exercises and Legal Knowledge Test)**
   - **เนื้อหาหลัก:** การตอบสนองต่อเหตุการณ์ที่จำลองขึ้น, ทดสอบความรู้ด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติงานในระบบ IT และ ICS
   - **ระยะเวลา:** 3 ชั่วโมง
   - **การวัดผล:** การประเมินความรวดเร็วและประสิทธิภาพในการตอบสนอง
3. **การสัมมนากฎหมายและความเสี่ยง (Legal and Risk Seminar)**
   - **เนื้อหาหลัก:** วิเคราะห์ความเสี่ยงทางกฎหมายที่เกี่ยวข้องกับการจัดการระบบโครงสร้างพื้นฐาน, การป้องกันการโจมตีทางไซเบอร์
   - **ระยะเวลา:** 4 ชั่วโมง
   - **การวัดผล:** การประเมินความเข้าใจและการจัดทำแผนการจัดการความเสี่ยง
4. **การฝึกอบรมการปฏิบัติตามกฎหมายเชิงลึก (In-depth Compliance Training)**
   - **เนื้อหาหลัก:** ฝึกอบรมการปฏิบัติตามกฎหมายในรายละเอียดที่เกี่ยวข้องกับการจัดการระบบสารสนเทศ, การป้องกันการโจมตีที่มีประสิทธิภาพ
   - **ระยะเวลา:** 3 ชั่วโมง

- **การวัดผล:** การประเมินผลการปฏิบัติในสถานการณ์จริง

5. **การประชุมทบทวนกฎหมายที่เกี่ยวข้องกับ ICS (ICS Legal Review Meetings)**
    - **เนื้อหาหลัก:** ทบทวนข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับระบบควบคุมอุตสาหกรรม และปรับปรุงกระบวนการปฏิบัติตาม
    - **ระยะเวลา:** 2 ชั่วโมง
    - **การวัดผล:** การวางแผนและดำเนินการตามข้อเสนอแนะ

4. ผู้ขาย ผู้รับเหมา และผู้ให้บริการภายนอก (Vendors, Contractors, and Service Providers)

4.1 การประชุมและฝึกอบรมด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการภายนอก

1. **การฝึกอบรมกฎหมายและข้อกำหนด (Legal and Compliance Training)**
    - **เนื้อหาหลัก:** ความรับผิดชอบทางกฎหมายในการจัดการข้อมูลและการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับองค์กร, การป้องกันการรั่วไหลของข้อมูล
    - **ระยะเวลา:** 3 ชั่วโมง
    - **การวัดผล:** การลงนามในข้อตกลงการปฏิบัติตามข้อกำหนด
2. **การสัมมนาออนไลน์ด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Online Legal and Cybersecurity Webinars)**
    - **เนื้อหาหลัก:** สรุปข้อกฎหมายที่เกี่ยวข้องกับการให้บริการภายนอก, การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์
    - **ระยะเวลา:** 2 ชั่วโมง
    - **การวัดผล:** การตอบแบบสอบถามหลังสัมมนา

3. **การประชุมเชิงปฏิบัติการด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Legal and Cybersecurity Workshops)**
    - **เนื้อหาหลัก:** ฝึกอบรมและแลกเปลี่ยนความคิดเห็นเกี่ยวกับข้อกำหนดทางกฎหมายในการทำงานร่วมกับองค์กร, การรักษาความปลอดภัยของข้อมูลลูกค้า
    - **ระยะเวลา:** 4 ชั่วโมง
    - **การวัดผล:** การทดสอบความเข้าใจและการประเมินผลการฝึกอบรม
4. **การประชุมรายไตรมาสเกี่ยวกับการปฏิบัติตามกฎหมายและความมั่นคงปลอดภัยไซเบอร์ (Quarterly Compliance and Cybersecurity Meetings)**
    - **เนื้อหาหลัก:** ทบทวนและปรับปรุงการปฏิบัติตามข้อกำหนดทางกฎหมายสำหรับผู้ให้บริการภายนอก, การประเมินความเสี่ยงและการปรับปรุงมาตรการป้องกัน
    - **ระยะเวลา:** 2 ชั่วโมง
    - **การวัดผล:** การติดตามการปรับปรุงที่เกิดขึ้นจริง
5. **การแจ้งเตือนภัยคุกคามและการเปลี่ยนแปลงกฎหมาย (Threat Alerts and Legal Change Notifications)**
    - **เนื้อหาหลัก:** การแจ้งเตือนเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้นและการเปลี่ยนแปลงของกฎหมายที่ส่งผลต่อการให้บริการ, คำแนะนำในการป้องกัน
    - **ระยะเวลา:** ส่งแจ้งเตือนเป็นระยะตามความจำเป็น
    - **การวัดผล:** การตอบสนองต่อภัยคุกคามและการปรับปรุงกระบวนการตามกฎหมายที่เปลี่ยนแปลง

6. กระบวนการการแบ่งปันข้อมูล

(Information Sharing Procedure)

Logo	นโยบายการแบ่งปันข้อมูล (Information Sharing Policy)	รหัสเอกสาร	CSMS-Policy -06
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการแบ่งปันข้อมูล (Information Sharing Policy)	รหัสเอกสาร	CSMS-Policy -06
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

นโยบายการแบ่งปันข้อมูล (Information Sharing Policy)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.6.1]

1. วัตถุประสงค์ (Objective)

นโยบายนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบ เพื่อให้มั่นใจว่าการแบ่งปันข้อมูลเป็นไปอย่างปลอดภัย มีประสิทธิภาพ และสอดคล้องกับข้อกำหนดขององค์กรและกฎหมายที่เกี่ยวข้อง

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ให้กับบุคคลที่เกี่ยวข้อง เช่น หน่วยงานหรือองค์กรที่อยู่ในหน่วยงานควบคุมหรือกำกับดูแลเดียวกัน, ผู้ใช้บริการ, ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management):** อนุมัติและกำกับดูแลการแบ่งปันข้อมูลให้เป็นไปตามนโยบายและข้อกำหนดที่กำหนด
- **ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team):** รวบรวม วิเคราะห์ และแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม
- **ผู้ใช้บริการและผู้รับเหมา (Users and Contractors):** รับทราบข้อมูลที่แบ่งปันและดำเนินการตามมาตรการป้องกันที่ได้รับแจ้ง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	นโยบายการแบ่งปันข้อมูล (Information Sharing Policy)	รหัสเอกสาร	CSMS-Policy -06
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

4. แนวทางปฏิบัติในการแบ่งปันข้อมูล (Guidelines for Information Sharing)

4.1 การรวบรวมและวิเคราะห์ข้อมูล

- ทีมรักษาความปลอดภัยไซเบอร์ต้องรวบรวมข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์ และดำเนินการวิเคราะห์เพื่อระบุผลกระทบที่อาจเกิดขึ้น
- การวิเคราะห์ข้อมูลต้องอ้างอิงจากแหล่งข้อมูลที่น่าเชื่อถือและดำเนินการตามมาตรฐานที่กำหนด

4.2 การแบ่งปันข้อมูลกับบุคคลที่เกี่ยวข้อง

- ข้อมูลที่แบ่งปันต้องเป็นไปตามหลักการ **ความถูกต้อง ครบถ้วน และทันเวลา (Accuracy, Completeness, and Timeliness)**
- ต้องแบ่งปันข้อมูลให้กับบุคคลหรือหน่วยงานที่ได้รับผลกระทบโดยตรงและมีเหตุผลที่เหมาะสมในการรับข้อมูล
- ข้อมูลที่มีความอ่อนไหวต้องแบ่งปันโดยใช้ช่องทางที่ปลอดภัย เช่น การเข้ารหัสอีเมล หรือการใช้ระบบที่ได้รับการรับรองด้านความปลอดภัย

4.3 ข้อจำกัดและข้อกำหนดในการแบ่งปันข้อมูล

- ข้อมูลที่แบ่งปันต้องไม่ละเมิดความเป็นส่วนตัวของบุคคล หรือข้อกำหนดด้านการปกป้องข้อมูลตามกฎหมายที่เกี่ยวข้อง
- ต้องมีการกำหนดระดับของข้อมูลที่สามารถแบ่งปันได้ เช่น:
    - **ข้อมูลสาธารณะ:** สามารถเผยแพร่ได้โดยไม่ต้องได้รับอนุมัติ
    - **ข้อมูลภายใน:** ใช้ภายในองค์กรเท่านั้น
    - **ข้อมูลจำกัด (Restricted):** แบ่งปันเฉพาะบุคคลที่ได้รับอนุญาต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **ข้อมูลลับ (Confidential):** ต้องได้รับการอนุมัติเป็นพิเศษก่อนการแบ่งปัน

4.4 ช่องทางและรูปแบบการแบ่งปันข้อมูล

- ข้อมูลควรถูกแบ่งปันในรูปแบบที่สามารถใช้ได้อย่างมีประสิทธิภาพ เช่น รายงานการวิเคราะห์เหตุการณ์, การแจ้งเตือนภัยคุกคาม หรือเอกสารแนวทางปฏิบัติ
- ควรใช้ช่องทางการสื่อสารที่ปลอดภัย เช่น **Secure Email, VPN, หรือ ระบบภายในองค์กร**
- องค์กรต้องมีระบบแจ้งเตือนภัยคุกคามทางไซเบอร์ เช่น **การแจ้งเตือนผ่านอีเมลหรือแอปพลิเคชันมือถือ**

5. การควบคุมและการรักษาความมั่นคงของข้อมูล (Security and Compliance Controls)

5.1 การควบคุมการเข้าถึงข้อมูลที่แบ่งปัน

- การเข้าถึงข้อมูลที่แบ่งปันต้องได้รับอนุญาตตามระดับของข้อมูลและข้อกำหนดด้านความมั่นคงปลอดภัย
- บุคคลที่ได้รับข้อมูลต้องปฏิบัติตามมาตรการรักษาความปลอดภัยขององค์กร

5.2 การตรวจสอบและติดตาม

- ต้องมีการบันทึกและติดตามการแบ่งปันข้อมูล รวมถึงบุคคลที่ได้รับข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้
- ทีมรักษาความปลอดภัยไซเบอร์ต้องทำการตรวจสอบเป็นระยะ เพื่อให้แน่ใจว่าการแบ่งปันข้อมูลเป็นไปตามข้อกำหนดที่กำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5.3 การรับมือกับการละเมิดนโยบาย

- หากพบว่ามีการแบ่งปันข้อมูลที่ไม่ได้รับอนุญาต หรือมีการใช้ข้อมูลผิดวัตถุประสงค์ ต้องดำเนินมาตรการตอบสนอง เช่น การแจ้งเตือน, การระงับสิทธิ์เข้าถึง หรือการดำเนินการทางกฎหมาย

การทบทวนนโยบาย (**Policy Review)**

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการแบ่งปันข้อมูล (Information Sharing Procedure)	รหัสเอกสาร	CSMS-Protect -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	1 ม.ค. 2568 Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการแบ่งปันข้อมูล (Information Sharing Procedure)	รหัสเอกสาร	CSMS-Protect -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการแบ่งปันข้อมูล (Information Sharing Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 43), ประมวลและกรอบ [ข้อ 22.6.1]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้บุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบสามารถใช้มาตรการป้องกันที่จำเป็นได้อย่างทันท่วงที

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ และมาตรการบรรเทาผลกระทบให้กับบุคคลที่เกี่ยวข้อง เช่น หน่วยงานหรือองค์กรที่อยู่ในหน่วยงานควบคุมหรือกำกับดูแลเดียวกัน, ผู้ใช้บริการ ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญขององค์กร

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและกำกับดูแลการแบ่งปันข้อมูล และตรวจสอบให้แน่ใจว่าการแบ่งปันข้อมูลเป็นไปตามนโยบายและข้อกำหนดที่กำหนด
- **ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team)**: รับผิดชอบในการรวบรวมข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์ รวมถึงมาตรการบรรเทาผลกระทบ และแบ่งปันข้อมูลให้กับบุคคลที่เกี่ยวข้องตามหลักเกณฑ์ที่กำหนด

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **ผู้ใช้บริการและผู้รับเหมา (Users and Contractors)**: มีหน้าที่รับทราบข้อมูลที่แบ่งปันและดำเนินการตามมาตรการป้องกันที่ได้รับแจ้ง

4. การแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคาม (Sharing of Incident and Threat Information)

- **4.1 การรวบรวมและวิเคราะห์ข้อมูล**
  - **ขั้นตอน**: รวบรวมข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดำเนินการวิเคราะห์เพื่อระบุผลกระทบที่อาจเกิดขึ้น โดยเน้นการรวบรวมข้อมูลเกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้นและวิเคราะห์ผลกระทบต่อระบบที่สำคัญ
- **4.2 การแบ่งปันข้อมูลกับบุคคลที่เกี่ยวข้อง**
  - **ขั้นตอน**: แบ่งปันข้อมูลเกี่ยวกับเหตุการณ์หรือภัยคุกคามที่เกิดขึ้น รวมถึงมาตรการบรรเทาผลกระทบที่ดำเนินการแล้ว ให้กับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้บริการ ผู้รับเหมา และเจ้าของระบบคอมพิวเตอร์ โดยการส่งอีเมลแจ้งเตือนผู้ใช้บริการเกี่ยวกับการโจมตีทางไซเบอร์ที่เกิดขึ้น พร้อมแนวทางปฏิบัติเพื่อป้องกันตนเอง

5. แนวทางและรูปแบบในการแบ่งปันข้อมูล (Guidelines and Formats for Information Sharing)

- **5.1 กำหนดแนวทางการแบ่งปันข้อมูล**
  - **ขั้นตอน**: กำหนดแนวทางในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม รวมถึงมาตรการบรรเทาผลกระทบ เพื่อให้มั่นใจว่าการแบ่งปันข้อมูลเป็นไปตามมาตรฐานและมีประสิทธิภาพ โดยการกำหนดนโยบายการแจ้งเตือนภัยคุกคามที่ครอบคลุมถึงการแจ้งเตือนผ่านช่องทางอีเมลและระบบข้อความภายในองค์กร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **5.2 การกำหนดรูปแบบของข้อมูลที่แบ่งปัน**
  - **ขั้นตอน**: กำหนดรูปแบบของข้อมูลที่แบ่งปัน เช่น รายงานการวิเคราะห์เหตุการณ์ รายงานการแจ้งเตือน หรือคู่มือการปฏิบัติตามมาตรการบรรเทาผลกระทบ เพื่อให้ข้อมูลสามารถใช้ได้อย่างมีประสิทธิภาพ โดยการจัดทำรายงานสรุปเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ในรูปแบบไฟล์ PDF ที่มีรายละเอียดเกี่ยวกับเหตุการณ์ ภัยคุกคาม และแนวทางป้องกัน

6. การทบทวนและปรับปรุง (Review and Improvement)

- **6.1 การทบทวนกระบวนการแบ่งปันข้อมูล**
  - **ขั้นตอน**: ทบทวนกระบวนการแบ่งปันข้อมูลเป็นระยะเพื่อให้แน่ใจว่ากระบวนการยังคงมีประสิทธิภาพและเป็นไปตามหลักเกณฑ์ที่กำหนด โดยการทบทวนและปรับปรุงกระบวนการแบ่งปันข้อมูลทุกปี หรือหลังจากเกิดเหตุการณ์สำคัญที่ส่งผลกระทบต่อระบบ
- **6.2 การปรับปรุงแนวทางการแบ่งปันข้อมูลตามผลการทบทวน**
  - **ขั้นตอน**: ปรับปรุงแนวทางและรูปแบบการแบ่งปันข้อมูลตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยการเพิ่มช่องทางการแจ้งเตือนใหม่, ใช้แอปพลิเคชันมือถือในการแจ้งเตือนภัยคุกคามเพื่อเพิ่มความรวดเร็วในการแบ่งปันข้อมูล

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการแบ่งปันข้อมูล (Information Sharing Procedure)	รหัสเอกสาร	CSMS-Protect -04
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. รายชื่อของเอกสารที่สามารถแบ่งปันข้อมูลได้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

DETECT

1. กระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(Cyber Threat Detection and Monitoring Procedure)

Logo	**ระเบียบกระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring Procedure)**	**รหัสเอกสาร**	**CSMS-Detect -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring Procedure)	รหัสเอกสาร	CSMS-Detect -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 56), ประมวลและกรอบ [ข้อ 23.1.1, ข้อ 23.1.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อกำหนดกลไกและกระบวนการในการตรวจจับ จัดประเภท วิเคราะห์ และระบุภัยคุกคามทางไซเบอร์หรือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับบริการที่สำคัญขององค์กร

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับบริการที่สำคัญขององค์กร การจัดประเภทและวิเคราะห์เหตุการณ์ที่ตรวจพบ และการระบุภัยคุกคามที่อาจเกิดขึ้นเพื่อดำเนินการป้องกันและตอบสนองอย่างทันท่วงที

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการกำกับดูแลและตรวจสอบความถูกต้องของกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคาม
- **ทีมรักษาความปลอดภัยไซเบอร์ (Cybersecurity Team)**: รับผิดชอบในการพัฒนากลไกและกระบวนการในการตรวจจับ จัดประเภท วิเคราะห์ และระบุภัยคุกคามทางไซเบอร์ รวมถึงการทบทวนและปรับปรุงกระบวนการตามความจำเป็น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **เจ้าหน้าที่ตรวจสอบและเฝ้าระวัง (Cybersecurity Monitoring Officers)**: มีหน้าที่ในการตรวจสอบและเฝ้าระวังเหตุการณ์ความมั่นคงปลอดภัย ไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ และรายงานผลการตรวจสอบต่อผู้บริหาร

4. การตรวจจับและเฝ้าระวังภัยคุกคาม (Threat Detection and Monitoring)

- **4.1 การสร้างกลไกและกระบวนการตรวจจับภัยคุกคาม**
  - **ขั้นตอน**: พัฒนากลไกและกระบวนการในการตรวจจับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ โดยใช้เครื่องมือและเทคโนโลยีที่เหมาะสม เช่น ระบบตรวจจับการบุกรุก (Intrusion Detection Systems: IDS) รวมถึงการตั้งค่าและปรับแต่งระบบ IDS เพื่อตรวจจับพฤติกรรมที่น่าสงสัยและแจ้งเตือนผู้ดูแลระบบทันทีเมื่อพบกิจกรรมที่อาจเป็นภัยคุกคาม
- **4.2 การจัดประเภทและวิเคราะห์เหตุการณ์ที่ตรวจพบ**
  - **ขั้นตอน**: จัดประเภทและวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ เพื่อระบุระดับความรุนแรงและความเร่งด่วนในการตอบสนอง โดยการวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับการโจมตีแบบฟิชชิ่ง หรืออื่นๆ ที่พบ และจัดประเภทเหตุการณ์เป็นระดับความเสี่ยงสูงเพื่อตอบสนองอย่างเร่งด่วน
- **4.3 การระบุภัยคุกคามและการตอบสนอง**
  - **ขั้นตอน**: ระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อบริการที่สำคัญหรือไม่ และดำเนินการตอบสนองอย่างเหมาะสมตามมาตรการที่กำหนดไว้ โดยการระบุว่าการโจมตีจากบุคคลภายนอกอาจส่งผลกระทบต่อบริการสำคัญขององค์กร และมีการดำเนินการตอบสนองตามแผนการรับมือภัยคุกค

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

5. การทบทวนและปรับปรุงกระบวนการ (Review and Improvement)

- **5.1 การทบทวนกลไกและกระบวนการตรวจจับภัยคุกคาม**
  - **ขั้นตอน**: ทบทวนกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ากระบวนการยังคงมีประสิทธิภาพในการตรวจจับและตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้น รวมถึงการทบทวนและปรับปรุงระบบ IDS (Intrusion Detection Systems) ให้สามารถตรวจจับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ
- **5.2 การปรับปรุงกระบวนการตามผลการทบทวน**
  - **ขั้นตอน**: ปรับปรุงกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามตามผลการทบทวน เพื่อเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยการเพิ่มฟีเจอร์การวิเคราะห์พฤติกรรมผู้ใช้งาน (User Behavior Analytics: UBA) ในระบบตรวจจับภัยคุกคามเพื่อเพิ่มความแม่นยำในการตรวจจับ

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนงานการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
2. รายงานการตรวจจับเหตุการณ์ การจัดประเภทและวิเคราะห์เหตุการณ์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : ทีมเฝ้าระวังภัยคุกคามทางไซเบอร์

จัดทำเมื่อ : 1 ตุลาคม 2567

แผนงานการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(Cyber Threat Detection and Monitoring Plan)

1. วัตถุประสงค์ (Objective)

แผนงานนี้มีวัตถุประสงค์เพื่อกำหนดกลไกและกระบวนการในการตรวจจับ วิเคราะห์ และจัดการกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อบริการที่สำคัญของหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2. ขอบเขต (Scope)

แผนงานนี้ครอบคลุมการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3. กลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Mechanisms and Processes for Cyber Threat Detection and Monitoring)

3.1 การตรวจจับเหตุการณ์ (Event Detection)

- **กลไก**
    - ใช้ระบบ SIEM (Security Information and Event Management) ในการรวบรวมและวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ เพื่อระบุเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
    - ใช้เครื่องมือ IDS/IPS (Intrusion Detection/Prevention System) ในการตรวจจับและป้องกันการโจมตีทางไซเบอร์

- **กระบวนการ**
  - ตั้งค่าการแจ้งเตือนอัตโนมัติเมื่อพบเหตุการณ์ที่น่าสงสัยหรือมีความเสี่ยงสูง
  - จัดทำรายการเหตุการณ์ที่ต้องเฝ้าระวังเป็นพิเศษตามประเภทของภัยคุกคาม

3.2 การจัดประเภทและวิเคราะห์เหตุการณ์ (Event Classification and Analysis)

- **กลไก**
  - จัดทำกระบวนการในการจัดประเภทเหตุการณ์ตามความรุนแรงและผลกระทบที่อาจเกิดขึ้น
  - ใช้ระบบอัตโนมัติในการวิเคราะห์เหตุการณ์และระบุแนวโน้มของภัยคุกคาม
- **กระบวนการ**
  - แยกประเภทเหตุการณ์เป็นกลุ่มตามระดับความรุนแรง เช่น ต่ำ กลาง สูง
  - ใช้ข้อมูลจาก Threat Intelligence เพื่อสนับสนุนการวิเคราะห์และการตอบสนอง

3.3 การระบุและตอบสนองต่อภัยคุกคาม (Threat Identification and Response)

- **กลไก**
  - ใช้ระบบการแจ้งเตือนและการจัดการเหตุการณ์ (Incident Response) เพื่อจัดการกับภัยคุกคามที่ตรวจพบ
  - จัดตั้งทีม CSIRT (Computer Security Incident Response Team) เพื่อรับผิดชอบการตอบสนองต่อภัยคุกคาม
- **กระบวนการ:**
  - ทบทวนและวิเคราะห์เหตุการณ์ที่เกิดขึ้นเพื่อระบุว่าเป็นภัยคุกคามจริงหรือไม่
  - หากพบว่ามีภัยคุกคาม ให้ดำเนินการตามแผนการตอบสนองที่กำหนดไว้ เช่น การกักกัน การวิเคราะห์ การแก้ไข และการฟื้นฟู

4. การทบทวนกลไกและกระบวนการ (Review of Mechanisms and Processes)

- **ความถี่:** ดำเนินการทบทวนกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง
- **ขั้นตอน**
  - ตรวจสอบประสิทธิภาพของกลไกและกระบวนการที่มีอยู่

- ปรับปรุงและอัปเดตตามความจำเป็นเพื่อให้มั่นใจว่ายังคงมีประสิทธิภาพในการเฝ้าระวังและตอบสนองต่อภัยคุกคามใหม่ ๆ
- จัดทำรายงานผลการทบทวนและนำเสนอให้กับผู้บริหารเพื่อการอนุมัติและดำเนินการต่อไป

5. ความรับผิดชอบ (Responsibilities)

- **ทีม IT:** รับผิดชอบการตรวจจับเหตุการณ์และการแจ้งเตือนอัตโนมัติ
- **ทีมความมั่นคงปลอดภัยไซเบอร์:** รับผิดชอบการจัดประเภทและวิเคราะห์เหตุการณ์
- **ทีม CSIRT:** รับผิดชอบการระบุและตอบสนองต่อภัยคุกคาม รวมถึงการทบทวนและปรับปรุงกระบวนการ

6. การบันทึกและรายงาน (Documentation and Reporting)

- **การบันทึก:** จัดทำบันทึกเหตุการณ์ที่เกิดขึ้นและผลการวิเคราะห์ในระบบการจัดการเหตุการณ์
- **การรายงาน:** รายงานผลการตรวจจับและวิเคราะห์เหตุการณ์ให้กับผู้บริหารเป็นระยะ ๆ และเมื่อมีเหตุการณ์สำคัญที่ส่งผลต่อความมั่นคงปลอดภัยไซเบอร์

รายงานการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับบริการที่สำคัญของหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Cyber Threat Detection and Monitoring Report)

วันที่: 1 ตุลาคม 2567

จัดทำโดย : ทีมเฝ้าระวังภัยคุกคามทางไซเบอร์

1. สรุปเหตุการณ์ที่ตรวจพบ

ลำดับ	วันที่ตรวจพบ	ประเภทเหตุการณ์	รายละเอียดเหตุการณ์	การวิเคราะห์เหตุการณ์	การจัดประเภท	ภัยคุกคามที่ระบุได้	บริการที่ได้รับผลกระทบ	การดำเนินการตอบสนอง
1	01/09/2567	การโจมตีแบบ DDoS	การเพิ่มขึ้นของทราฟฟิกที่ผิดปกติจาก IP ต่างประเทศ	การวิเคราะห์พบว่าทราฟฟิกไม่ตรงกับรูปแบบปกติของผู้ใช้งาน	ระดับสูง	พบว่ามีการโจมตีจาก botnet ที่ใช้ DDoS	เว็บไซต์ของหน่วยงานรัฐ	ทำการปิดกั้น IP ที่น่าสงสัยและเพิ่มระดับการตรวจสอบ
2	05/09/2567	Phishing	มีการส่งอีเมลที่หลอกลวงผู้ใช้ให้คลิกลิงก์อันตราย	พบว่าอีเมลถูกส่งจากแหล่งที่ไม่น่าเชื่อถือ	ระดับปานกลาง	พบว่ามีความพยายามในการขโมยข้อมูลส่วนบุคคล	ระบบอีเมลของหน่วยงานรัฐ	แจ้งเตือนผู้ใช้ลบอีเมลและบล็อกโดเมนที่เป็นอันตราย
3	07/09/2567	Malware	มีการตรวจพบไฟล์ที่น่าสงสัยในเซิร์ฟเวอร์	ไฟล์ดังกล่าวมีพฤติกรรมเหมือนมัลแวร์ที่ยังไม่ถูกระบุ	ระดับสูง	พบมัลแวร์ประเภท Ransomware	ระบบการเงินของโครงสร้างพื้นฐานสำคัญ	กักกันไฟล์และเรียกใช้การสแกนเต็มระบบ
4	08/09/2567	Unauthorized Access	ตรวจพบความพยายามในการเข้าสู่ระบบจากผู้ใช้ที่ไม่ได้รับอนุญาต	ความพยายามในการเข้าสู่ระบบมาจาก IP ภายนอกที่ไม่มีสิทธิ์	ระดับสูง	ความพยายามในการเจาะเข้าระบบเพื่อเข้าถึงข้อมูล	ระบบฐานข้อมูลของหน่วยงานรัฐ	ทำการล็อกบัญชีและบล็อก IP

2. ข้อเสนอแนะและการปรับปรุง

- **การเสริมสร้างระบบตรวจสอบ:** แนะนำให้เพิ่มการตรวจสอบทราฟฟิกเพื่อป้องกันการโจมตี DDoS ได้รวดเร็วยิ่งขึ้น
- **การฝึกอบรมผู้ใช้:** ควรเพิ่มการฝึกอบรมการระวังอีเมล phishing และการตรวจสอบความน่าเชื่อถือของอีเมล

RESPOND

1. กระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure : CIRP)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58) , ประมวลและกรอบ [ข้อ 24.1.1]

1. วัตถุประสงค์ (Objective)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จัดทำขึ้นเพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายเพื่อป้องกัน, จำกัดขอบเขตความเสียหาย, และฟื้นฟูระบบให้กลับมาทำงานตามปกติได้อย่างรวดเร็ว

2. ขอบเขต (Scope)

แผนการรับมือภัยคุกคามทางไซเบอร์นี้ใช้สำหรับเหตุการณ์ภัยคุกคามที่ส่งผลกระทบต่อระบบสำคัญขององค์กร ทั้งระบบเทคโนโลยีสารสนเทศ (IT) และระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS) โดยมีการครอบคลุมถึงการรับมือกับ …

- การโจมตีทางไซเบอร์ เช่น Malware, Ransomware, Phishing, Distributed Denial of Service (DDoS) หรืออื่นๆ
- การโจมตีทางช่องโหว่ความปลอดภัยในระบบ
- การโจมตีการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

3. โครงสร้างทีมรับมือเหตุการณ์ทางไซเบอร์ (Incident Response Team Structure)

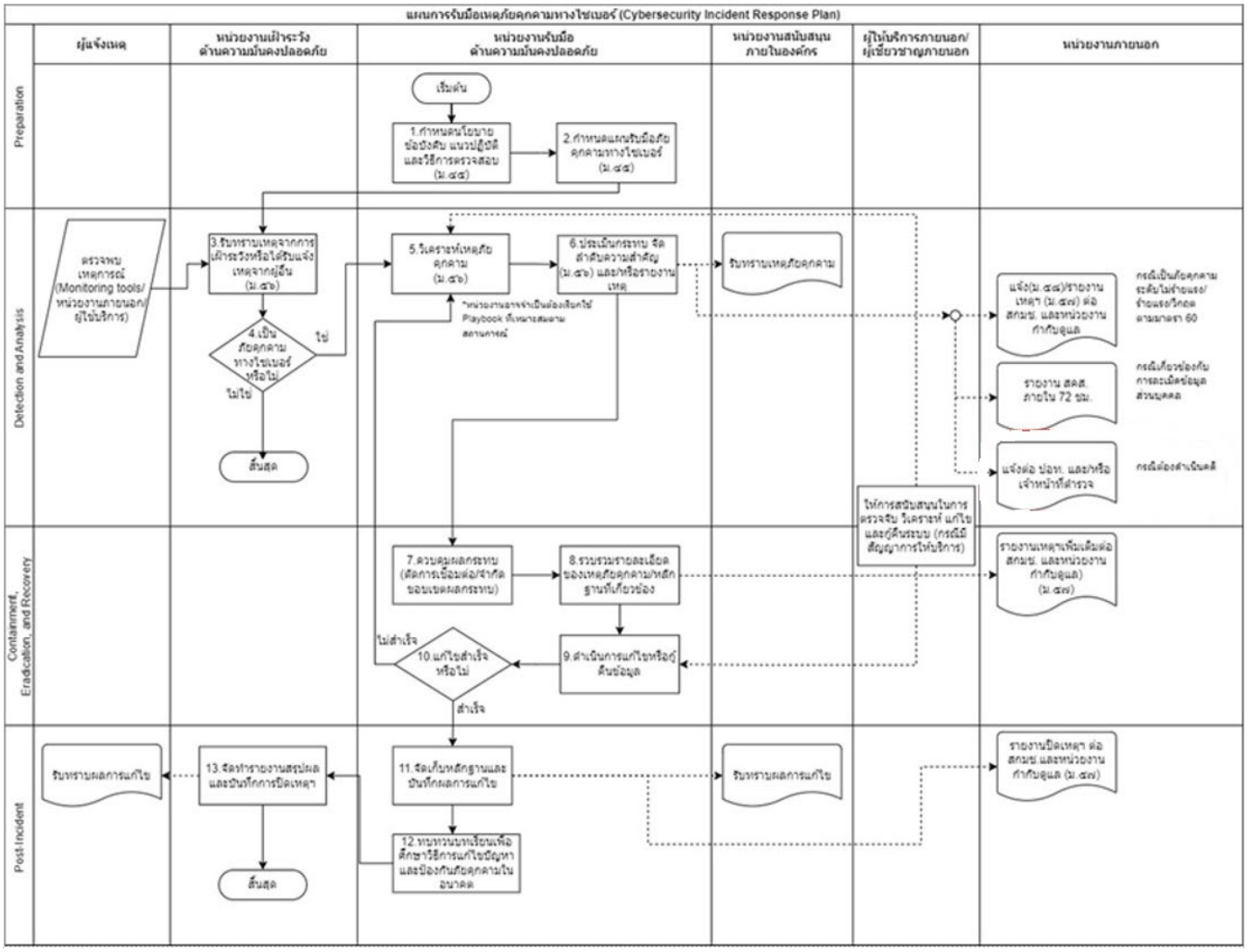
ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

	ตำแหน่ง	หน้าที่และความรับผิดชอบ	รายละเอียดการติดต่อ
1	**หัวหน้าทีม (Team Leader)**	รับผิดชอบการจัดการภาพรวมของเหตุการณ์, การตัดสินใจที่สำคัญ	โทร: 081-xxx-xxxx, อีเมล: a@abc.com
2	**ผู้จัดการด้าน IT**	รับผิดชอบการประเมินระบบ, การกู้คืนระบบและการจำกัดขอบเขต	โทร: 081-xxx-xxxx, อีเมล: b@abc.com
3	**ผู้จัดการด้านความปลอดภัย**	ประสานงานกับผู้เชี่ยวชาญภายนอกและหน่วยงานที่เกี่ยวข้อง	โทร: 081-xxx-xxxx, อีเมล: c@abc.com
4	**ผู้จัดการด้านกฎหมาย**	ให้คำปรึกษาด้านกฎหมายและจัดการด้านการรายงานภายใต้ พ.ร.บ. ไซเบอร์	โทร: 081-xxx-xxxx, อีเมล: d@abc.com
5	**เจ้าหน้าที่ด้านการสื่อสาร**	สื่อสารภายในองค์กรและแจ้งข้อมูลต่อสื่อและหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานอื่นๆ ที่เกี่ยวข้อง	โทร: 081-xxx-xxxx, อีเมล: e@abc.com
6	**ผู้เชี่ยวชาญด้านไซเบอร์ (Cyber Technical Expert)**	วิเคราะห์หลักฐานและตรวจสอบการโจมตีเพื่อแก้ไขปัญหา	โทร: 081-xxx-xxxx, อีเมล: f@abc.com

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)



เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ขั้นตอนการรายงานเหตุการณ์

1. **การตรวจพบเหตุการณ์**: หากมีการตรวจพบเหตุการณ์ความผิดปกติ เช่น การเข้าถึงระบบที่ไม่ได้รับอนุญาต หรือระบบถูกโจมตี ทีม IT จะต้องรายงานต่อหัวหน้าทีมทันที
2. **การประเมินเบื้องต้น**: หัวหน้าทีมและผู้จัดการด้าน IT จะทำการประเมินความร้ายแรงของเหตุการณ์และประสานงานกับทีมรับมือเหตุการณ์
3. **การจำกัดขอบเขต** : ทีม IT จะทำการจำกัดขอบเขตของเหตุการณ์เพื่อป้องกันการกระจายผลกระทบต่อระบบเพิ่มเติม
4. **การแจ้งต่อหน่วยงานที่เกี่ยวข้อง**
    - **หน่วยงานภายใน**: แจ้งหัวหน้าหน่วยงานต่าง ๆ ที่เกี่ยวข้อง
    - **หน่วยงานภายนอก**: หากเป็นเหตุการณ์สำคัญ ให้รายงานต่อหน่วยงานควบคุมหรือกำกับดูแลหรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) ตาม พ.ร.บ. ไซเบอร์ ภายใน 24 ชั่วโมง
5. **การดำเนินการกู้คืน (Recovery)**: หลังจากจำกัดขอบเขตเหตุการณ์ ทีม IT จะเริ่มกระบวนการกู้คืนระบบตามแผนที่กำหนดไว้ เช่น การกู้คืนข้อมูลจากระบบสำรอง
6. **การทบทวนเหตุการณ์ (Post-Incident Review)**: หลังจากเหตุการณ์สิ้นสุด ทีมรับมือจะจัดทำรายงานการทบทวนเพื่อวิเคราะห์สาเหตุและปรับปรุงแผนการป้องกัน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

5. เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activation Criteria and Procedures)

เกณฑ์การเรียกใช้งาน

แผนการรับมือภัยคุกคามทางไซเบอร์นี้จะถูกเรียกใช้งานเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น

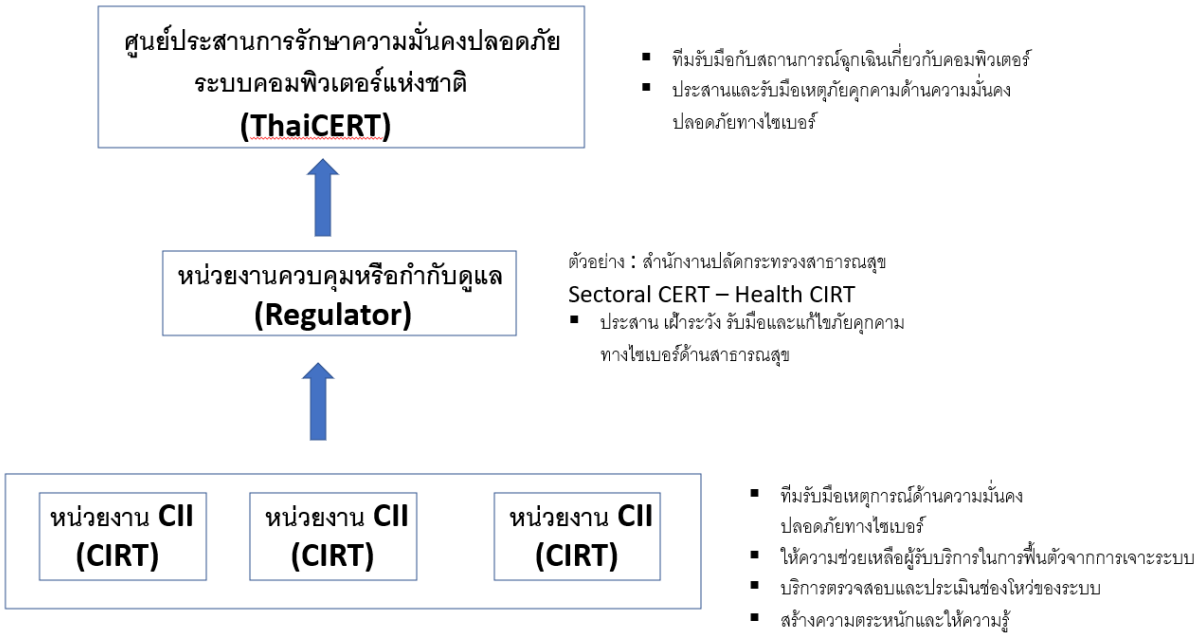
- การโจมตีทางไซเบอร์
- การรั่วไหลของข้อมูลสำคัญ
- การเข้าถึงระบบโดยไม่ได้รับอนุญาต

ขั้นตอนการเรียกใช้งาน

1. แจ้งเตือนทีม **Cyber Incident Response Team (CIRT)** ผ่านโทรศัพท์และอีเมล
2. เปิดใช้แผนการตอบสนอง โดยทีมรับมือเริ่มดำเนินการตามขั้นตอนที่กำหนด
3. แจ้งเตือนบุคลากรที่เกี่ยวข้องภายในองค์กรถึงสถานการณ์ฉุกเฉิน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only



6. ขั้นตอนจำกัดขอบเขต (Containment)

ขั้นตอนการจำกัดขอบเขต

1. แยกระบบที่ได้รับผลกระทบออกจากเครือข่ายหลักเพื่อป้องกันการแพร่กระจายไปยังระบบอื่น
2. ประเมินความเสียหายและระบุว่ามีระบบใดที่เกี่ยวข้อง
3. ดำเนินการแก้ไขเบื้องต้น เช่น การปิดพอร์ตที่ถูกโจมตีหรือการบล็อก IP ที่มีพฤติกรรมไม่พึงประสงค์
4. เก็บข้อมูลสำคัญจากระบบที่ได้รับผลกระทบเพื่อใช้ในกระบวนการสอบสวน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

7. การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

ขั้นตอนการกู้คืน

1. ตรวจสอบและซ่อมแซมระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าไม่มีช่องโหว่ที่ยังไม่ได้รับการแก้ไข
2. ฟื้นฟูระบบโดยการกู้คืนข้อมูลจากระบบสำรองล่าสุด (Backup)
3. ทดสอบระบบทั้งหมดเพื่อยืนยันว่าระบบปลอดภัยและสามารถทำงานได้ปกติ
4. ตรวจสอบการทำงานของระบบสำรองเพื่อให้แน่ใจว่าข้อมูลที่กู้คืนครบถ้วน

8. ขั้นตอนในการสอบสวน (Investigation)

ขั้นตอนการสอบสวน

1. เก็บหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อก การจับภาพหน้าจอ การตรวจสอบข้อมูลเครือข่าย
2. วิเคราะห์สาเหตุของเหตุการณ์ เช่น ตรวจสอบวิธีการที่ผู้โจมตีใช้ในการเข้าถึงระบบ
3. ระบุผู้ที่อาจรับผิดชอบต่อเหตุการณ์ เช่น การระบุที่อยู่ IP หรือการตรวจสอบพฤติกรรมที่ผิดปกติ
4. จัดทำรายงานการสอบสวนและเสนอแนวทางการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

9. การเก็บรักษาหลักฐาน (Preservation of Evidence)

การจัดเก็บหลักฐาน

1. บันทึกข้อมูลจากระบบที่ได้รับผลกระทบ เช่น ล็อกไฟล์ การจับภาพหน้าจอ และอุปกรณ์เครือข่ายที่เกี่ยวข้อง
2. จัดเก็บอุปกรณ์ที่มีหลักฐานไว้ในที่ปลอดภัยเพื่อป้องกันการดัดแปลง เช่น จัดเก็บในตู้ที่มีการล็อกและการควบคุมการเข้าถึง
3. ทำรายการหลักฐานทั้งหมดที่ถูกเก็บรวบรวม พร้อมระบุวันที่และเวลาที่ได้รับหลักฐาน

10. ระเบียบวิธีการมีส่วนร่วมกับบุคคลภายนอก (Engagement Protocols)

ผู้ที่เกี่ยวข้อง

- **บริษัทที่ปรึกษา** : บริษัท A โทร. 02-111-XXXX
- **หน่วยงานบังคับใช้กฎหมาย**: นาย C โทร. 02-111-XXXX

ขั้นตอนการมีส่วนร่วม

1. ติดต่อบุคคลภายนอกตามความจำเป็น เช่น บริษัทที่ปรึกษา สำหรับการวิเคราะห์หาสาเหตุ
2. ประสานงานกับหน่วยงานบังคับใช้กฎหมาย หากมีความจำเป็นในการดำเนินคดี
3. ส่งมอบหลักฐานที่เกี่ยวข้องให้กับผู้เชี่ยวชาญภายนอก พร้อมรายการหลักฐานทั้งหมดเพื่อใช้ในการตรวจสอบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	CSMS-Incident - 01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

11. กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

ขั้นตอนการทบทวน

1. จัดประชุมทีม CIRT ภายใน 7 วันหลังจากเหตุการณ์สิ้นสุด เพื่อประเมินกระบวนการตอบสนอง
2. ประเมินผลการดำเนินการ เช่น ความเร็วในการตอบสนอง, การกู้คืนระบบ, และการจำกัดขอบเขตเหตุการณ์
3. ระบุข้อบกพร่องและข้อเสนอแนะสำหรับการปรับปรุงกระบวนการตอบสนอง
4. เสนอมาตรการปรับปรุงแผนรับมือภัยคุกคาม เพื่อให้มีประสิทธิภาพมากขึ้นในการป้องกันเหตุการณ์ในอนาคต

12. การสื่อสารและการทบทวนแผน (Communication and Plan Review)

การสื่อสารแผน

- สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้กับบุคลากรที่เกี่ยวข้องทั้งหมดผ่านการอบรมและเอกสารแผน
- จัดอบรมพนักงานอย่างสม่ำเสมอเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน

การทบทวนแผน

- ทบทวนแผนการรับมือภัยคุกคามทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมทางไซเบอร์
- ปรับปรุงแผนตามผลการทบทวนและการฝึกซ้อมแผนรับมือภัยคุกคาม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	**ระเบียบกระบวนการแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)**	**รหัสเอกสาร**	**CSMS-Incident - 01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์
2. โครงสร้างทีมรับมือเหตุการณ์
3. รายงานสรุปเหตุการณ์
4. แผนการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : ทีมเฝ้าระวังทางไซเบอร์

จัดทำเมื่อ : 1 ตุลาคม 2567

รายงานการแจ้งเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Report: Ransomware Attack)

1. ข้อมูลทั่วไป (General Information)

- **ชื่อเหตุการณ์:** การโจมตีด้วย Ransomware
- **วันที่และเวลาที่ตรวจพบเหตุการณ์:** 8 กันยายน 2567, เวลา 10:30 น.
- **ผู้รายงาน:** นายสมชาย (IT Security Team)
- **ประเภทของเหตุการณ์:** การโจมตีด้วย Ransomware
- **ระบบที่ได้รับผลกระทบ:** ระบบฐานข้อมูลลูกค้า (CRM), ระบบสำรองข้อมูล
- **หน่วยงานที่เกี่ยวข้อง:** ฝ่าย IT, ฝ่ายกฎหมาย, ฝ่ายปฏิบัติการ

2. ขั้นตอนการเรียกใช้งาน (Activation)

- **เกณฑ์การเรียกใช้งาน:** พบการโจมตี Ransomware ที่เข้ารหัสข้อมูลทั้งหมดในระบบ CRM และระบบสำรองข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต
- **ขั้นตอนการเรียกใช้งาน**
    1. **แจ้งเตือนทีม CIRT:** ทีม IT ตรวจพบเหตุการณ์และแจ้งเตือนทีม CIRT ผ่านอีเมลและโทรศัพท์
    2. **Activate แผนการตอบสนอง:** หัวหน้าทีม CIRT อนุมัติการเปิดใช้แผนการตอบสนองภัยคุกคามทางไซเบอร์
    3. **แจ้งผู้บริหารและบุคลากรที่เกี่ยวข้อง:** แจ้งผู้บริหารและทีมกฎหมายเกี่ยวกับเหตุการณ์และเริ่มกระบวนการตอบสนอง

3. ขั้นตอนการจำกัดขอบเขต (Containment)

- **เวลาเริ่มต้นการจำกัดขอบเขต:** 8 กันยายน 2567, เวลา 11:00 น.
- **ขั้นตอนที่ดำเนินการ**
    1. **แยกระบบ CRM** ออกจากเครือข่ายภายในทันที เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังระบบอื่น
    2. **บล็อก IP** และผู้ใช้งานที่เกี่ยวข้องกับการโจมตีเพื่อจำกัดการเข้าถึงที่ไม่ได้รับอนุญาต

3. **ประเมินระบบที่เกี่ยวข้อง:** ตรวจสอบว่าเซิร์ฟเวอร์สำรองข้อมูลถูกโจมตีและได้รับการเข้ารหัสข้อมูล
4. **แก้ไขเบื้องต้น:** ปิดการทำงานของพอร์ตที่ถูกโจมตีและใช้ระบบสำรองสำหรับการดำเนินการบางส่วน

4. ขั้นตอนการกู้คืนระบบ (Recovery Process)

- **เวลาเริ่มต้นการกู้คืนระบบ:** 8 กันยายน 2567, เวลา 13:00 น.
- **ขั้นตอนการดำเนินการ**
    1. **ซ่อมแซมระบบที่ได้รับผลกระทบ:** ทีม IT ซ่อมแซมระบบ CRM ที่ถูกเข้ารหัส โดยการนำซอฟต์แวร์ความปลอดภัยมาใช้ในการลบ Ransomware
    2. **กู้คืนข้อมูลจากระบบสำรอง:** กู้คืนข้อมูลที่ไม่ได้รับผลกระทบจากการสำรองข้อมูลที่ได้รับการปกป้อง
    3. **ทดสอบระบบ:** ทีม IT ทดสอบระบบทั้งหมดเพื่อให้แน่ใจว่าไม่มีมัลแวร์หลงเหลืออยู่ และระบบสามารถทำงานได้ตามปกติ
    4. **เปิดใช้งานระบบอีกครั้ง:** เปิดใช้งานระบบ CRM และแจ้งให้ผู้ใช้งานทราบว่าระบบพร้อมใช้งานอีกครั้ง

5. ขั้นตอนการสอบสวน (Investigation)

- **เวลาเริ่มต้นการสอบสวน:** 9 กันยายน 2567, เวลา 09:00 น.
- **ขั้นตอนการสอบสวน**
    1. **เก็บรวบรวมหลักฐาน:** ทีมสอบสวน เก็บรวบรวมหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อกของเซิร์ฟเวอร์, การตรวจสอบการเข้าถึงเครือข่าย
    2. **วิเคราะห์สาเหตุของเหตุการณ์:** วิเคราะห์ว่าการโจมตีเริ่มต้นจากช่องโหว่ใดและวิธีที่ผู้โจมตีใช้ เช่น การเปิดอีเมลที่มีลิงก์อันตราย
    3. **ระบุผู้รับผิดชอบ:** ตรวจสอบการเชื่อมต่อจากภายนอกและ IP ที่เกี่ยวข้องกับการโจมตี เพื่อระบุผู้โจมตี
    4. **จัดทำรายงานการสอบสวน:** ทีมสอบสวน จัดทำรายงานสรุปสาเหตุและกระบวนการโจมตี พร้อมแนวทางการป้องกันเหตุการณ์ในอนาคต

6. การเก็บรักษาหลักฐาน (Preservation of Evidence)

- **เวลาเริ่มต้นการเก็บรักษาหลักฐาน:** 9 กันยายน 2567, เวลา 10:30 น.
- **ขั้นตอนการเก็บรักษาหลักฐาน**
    1. **บันทึกข้อมูล:** เก็บล็อกไฟล์ทั้งหมดและการจับภาพหน้าจอจากระบบที่ถูกโจมตี
    2. **จัดเก็บอุปกรณ์สำคัญ:** จัดเก็บอุปกรณ์ที่เกี่ยวข้อง เช่น เซิร์ฟเวอร์ที่มีการโจมตีในตู้เซฟที่มีการควบคุมการเข้าถึง
    3. **ทำรายการหลักฐาน:** ทำรายการหลักฐานที่ถูกเก็บไว้ และลงบันทึกวันเวลาที่ได้รับและจัดเก็บหลักฐาน

4. **ส่งมอบหลักฐานให้บุคคลภายนอก:** หากมีความจำเป็นในการดำเนินคดี ให้ประสานงานกับหน่วยงานบังคับใช้กฎหมายและส่งมอบหลักฐานให้กับผู้ที่เกี่ยวข้อง

7. ข้อสรุปและการดำเนินการเพิ่มเติม

- **การทบทวนและปรับปรุง**
  1. ทีม CIRT ได้จัดประชุมเพื่อทบทวนเหตุการณ์ ภายใน 7 วันหลังเหตุการณ์สิ้นสุด
  2. ผลการทบทวนระบุข้อบกพร่องในการตอบสนอง เช่น การตรวจจับที่ล่าช้าและการแจ้งเตือนผู้ใช้งานที่ไม่เพียงพอ
  3. เสนอการปรับปรุงแผนการตอบสนองต่อเหตุการณ์เพื่อป้องกันการโจมตีที่คล้ายคลึงในอนาคต

8. รายละเอียดเพิ่มเติม (Appendices)

- รายชื่อผู้ที่เกี่ยวข้องในเหตุการณ์
  - นาย A , หน่วยงาน …. , ติดต่อ ….
  - นาย B , หน่วยงาน …. , ติดต่อ ….
  - นาย C , หน่วยงาน …. , ติดต่อ ….
- ล็อกไฟล์และหลักฐานทางดิจิทัลที่เกี่ยวข้อง
  - Audit Logging of Firewall

2. กระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)

Logo	ระเบียบกระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)	รหัสเอกสาร	CSMS-Respond -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	คุณ xxx	คุณ xxx
ตำแหน่ง	เจ้าหน้าที่ xxx	ผอ.ฝ่ายบริหาร	ผอ.ฝ่ายบริหาร
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	2 ต.ค. 2567	จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา
01	12 ต.ค. 2567	แก้ไขเนื้อหา บริบทองค์กร
02	24 ต.ค. 2567	เพิ่มเติมหัวข้อ 11

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)	รหัสเอกสาร	CSMS-Respond -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 24.2.1, ข้อ 24.2.2, ข้อ 24.2.3, ข้อ 24.2.4]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าองค์กรมีแผนการสื่อสารที่มีประสิทธิภาพในภาวะวิกฤตที่เกิดจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การสื่อสารและการเผยแพร่ข้อมูลเป็นไปอย่างทันท่วงที ประสานกัน และสอดคล้องกับทุกฝ่ายที่เกี่ยวข้อง

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการจัดทำ การทบทวน และการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตที่เกิดจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ รวมถึงการกำหนดบทบาทหน้าที่และช่องทางการสื่อสารที่เหมาะสม

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติแผนการสื่อสารในภาวะวิกฤตและกำกับดูแลการดำเนินการในช่วงวิกฤต
- **ทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team)**: รับผิดชอบในการดำเนินการตามแผนการสื่อสารในภาวะวิกฤต รวมถึงการจัดการการสื่อสารและการประสานงานกับทุกฝ่ายที่เกี่ยวข้อง

4. การจัดทำแผนการสื่อสารในภาวะวิกฤต (Development of Crisis Communication Plan)

- **4.1 การจัดตั้งทีมสื่อสารในภาวะวิกฤต**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)	รหัสเอกสาร	CSMS-Respond -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

- **ขั้นตอน**: จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต โดยประกอบด้วยบุคลากรที่มีบทบาทสำคัญในการสื่อสารและการตัดสินใจ โดยการแต่งตั้งผู้บริหารระดับสูงเป็นหัวหน้าทีมสื่อสารในภาวะวิกฤต และแต่งตั้งตัวแทนจากฝ่าย IT และฝ่ายอื่นๆ เป็นสมาชิกทีม

การจัดตั้งทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team)

	ตำแหน่ง	หน้าที่รับผิดชอบ	ชื่อบุคคลที่รับผิดชอบ	ข้อมูลการติดต่อ
1	**หัวหน้าทีมสื่อสารในภาวะวิกฤต** (Crisis Communication Leader)	รับผิดชอบการตัดสินใจหลักในการสื่อสารและประสานงานกับผู้บริหารระดับสูง และควบคุมแผนการสื่อสารทั้งหมด	นาย A	โทร: 081-xxx-xxxx อีเมล: A@company.com
2	**โฆษกหลัก** (Primary Spokesperson)	เป็นตัวแทนองค์กรในการแถลงข่าวและตอบคำถามต่อสื่อมวลชน	นาย B	โทร: 083-xxx-xxxx อีเมล: B@company.com
3	**ผู้เชี่ยวชาญด้านเทคนิค** (Technical Expert)	ให้ข้อมูลด้านเทคนิคที่เกี่ยวข้องกับเหตุการณ์และให้คำแนะนำทางเทคนิคในการแก้ไขปัญหา	นาย C	โทร: 086-xxx-xxxx อีเมล: C@company.com
4	**ผู้จัดการการสื่อสารกับสื่อมวลชน** (Media Relations Manager)	จัดการสื่อมวลชนและประสานงานการเผยแพร่	นาย D	โทร: 089-xxx-xxxx อีเมล: D@company.com

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

		ข้อมูลผ่านช่องทางสื่อดั้งเดิมและโซเชียลมีเดีย		
5	**ผู้จัดการด้านการสื่อสารภายใน** (Internal Communications Manager)	รับผิดชอบการสื่อสารภายในองค์กรและประสานงานกับพนักงาน	นาย E	โทร: 087-xxx-xxxx อีเมล: E@company.com
6	**ผู้จัดการการประสานงานกับหน่วยงานภายนอก** (External Coordination Manager)	ประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง เช่น หน่วยงานรัฐและผู้มีส่วนได้ส่วนเสีย	นาย F	โทร: 082-xxx-xxxx อีเมล: F@company.com
7	**ผู้ประสานงานฉุกเฉิน** (Emergency Response Coordinator)	ดูแลการจัดการแผนฉุกเฉินและการติดต่อประสานงานกับหน่วยงานด้านความปลอดภัย	นาย G	โทร: 085-xxx-xxxx อีเมล: G@company.com

- **4.2 การระบุสถานการณ์จำลองและแผนการดำเนินการ**
  - **ขั้นตอน**: ระบุสถานการณ์จำลองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น เช่น กรณีที่มีการรั่วไหลของข้อมูลสำคัญ และกำหนดแผนการดำเนินการที่เกี่ยวข้องสำหรับแต่ละสถานการณ์ ซึ่งต้องมีการกำหนดขั้นตอนการสื่อสารกับสาธารณชนและผู้มีส่วนได้ส่วนเสีย
- **4.3 การระบุกลุ่มเป้าหมายและผู้มีส่วนได้ส่วนเสีย**
  - **ขั้นตอน**: ระบุกลุ่มเป้าหมายและผู้มีส่วนได้ส่วนเสีย พร้อมจัดทำรายชื่อผู้ใช้บริการหลัก ผู้รับเหมา และหน่วยงานรัฐบาลที่ต้องได้รับการแจ้งเตือนและข้อมูลในกรณีที่เกิดการโจมตีทางไซเบอร์ ในแต่ละสถานการณ์จำลอง เพื่อให้แน่ใจว่าการสื่อสารครอบคลุมทุกฝ่ายที่ได้รับผลกระทบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **4.4 การระบุช่องทางการเผยแพร่ที่เหมาะสม**
  - **ขั้นตอน**: ระบุแพลตฟอร์มและช่องทางการเผยแพร่ข้อมูลที่เหมาะสม สำหรับการสื่อสารในช่วงวิกฤต โดยการใช้โซเชียลมีเดีย หรือเว็บไซต์ขององค์กร

5. การประสานงานและการฝึกซ้อม (Coordination and Drills)

- **5.1 การประสานงานระหว่างทุกฝ่ายที่เกี่ยวข้อง**
  - **ขั้นตอน**: ตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้มีการตอบสนองที่สอดคล้องและมีประสิทธิภาพ โดยการจัดประชุมระหว่างทีมสื่อสารในภาวะวิกฤตกับทีม IT และฝ่ายอื่นๆ ที่เกี่ยวข้อง รวมถึงหน่วยงานที่รับผิดชอบ ตาม พรบ ไซเบอร์ กำหนด
- **5.2 การฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต**
  - **ขั้นตอน**: ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อทดสอบความพร้อมและความสามารถในการสื่อสารในช่วงวิกฤต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan Procedure)	รหัสเอกสาร	CSMS-Respond -02
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

การทบทวนระเบียบกระบวนการดำเนินการ **Procedure Review**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. ทีมสื่อสารในภาวะวิกฤต
2. แผนการสื่อสารในภาวะวิกฤต
3. หลักฐานหรือเอกสารแสดงการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : นาย A , หัวหน้าหน่วยงานการสื่อสารในภาวะวิกฤต

จัดทำเมื่อ : 1 ธันวาคม 2567

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

1. การจัดตั้งทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team Establishment)

	ตำแหน่ง	หน้าที่รับผิดชอบ	ชื่อบุคคลที่รับผิดชอบ	ข้อมูลการติดต่อ
1	**หัวหน้าทีมสื่อสารในภาวะวิกฤต** (Crisis Communication Leader)	รับผิดชอบการตัดสินใจหลักในการสื่อสารและประสานงานกับผู้บริหารระดับสูง และควบคุมแผนการสื่อสารทั้งหมด	นาย A	โทร: 081-xxx-xxxx อีเมล: A@company.com
2	**โฆษกหลัก** (Primary Spokesperson)	เป็นตัวแทนองค์กรในการแถลงข่าวและตอบคำถามต่อสื่อมวลชน	นาย B	โทร: 083-xxx-xxxx อีเมล: B@company.com
3	**ผู้เชี่ยวชาญด้านเทคนิค** (Technical Expert)	ให้ข้อมูลด้านเทคนิคที่เกี่ยวข้องกับเหตุการณ์และให้คำแนะนำทางเทคนิคในการแก้ไขปัญหา	นาย C	โทร: 086-xxx-xxxx อีเมล: C@company.com
4	**ผู้จัดการการสื่อสารกับสื่อมวลชน** (Media Relations Manager)	จัดการสื่อมวลชนและประสานงานการเผยแพร่ข้อมูลผ่านช่องทางสื่อดั้งเดิมและโซเชียลมีเดีย	นาย D	โทร: 089-xxx-xxxx อีเมล: D@company.com
5	**ผู้จัดการด้านการสื่อสารภายใน** (Internal Communications Manager)	รับผิดชอบการสื่อสารภายในองค์กรและประสานงานกับพนักงาน	นาย E	โทร: 087-xxx-xxxx อีเมล: E@company.com
6	**ผู้จัดการการประสานงานกับหน่วยงานภายนอก** (External Coordination Manager)	ประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง เช่น หน่วยงานรัฐและผู้มีส่วนได้ส่วนเสีย	นาย F	โทร: 082-xxx-xxxx อีเมล: F@company.com
7	**ผู้ประสานงานฉุกเฉิน** (Emergency Response Coordinator)	ดูแลการจัดการแผนฉุกเฉินและการติดต่อประสานงานกับหน่วยงานด้านความปลอดภัย	นาย G	โทร: 085-xxx-xxxx อีเมล: G@company.com

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

2. สถานการณ์จำลองด้านความมั่นคงปลอดภัยไซเบอร์

	สถานการณ์จำลอง	แผนการดำเนินการ	กลุ่มเป้าหมาย	ผู้มีส่วนได้ส่วนเสีย	โฆษกหลัก	ช่องทางการเผยแพร่ข้อมูล
1	**การโจมตีแบบ DDoS** (DDoS Attack)	- แจ้งทีม IT ทำการปิดกั้นทราฟฟิกที่น่าสงสัย - เพิ่มการตรวจสอบความปลอดภัยเพิ่มเติม - แจ้งผู้บริหารถึงสถานการณ์และการตอบสนอง	ลูกค้า, ผู้ใช้งานทั่วไป, ทีมพัฒนา IT	ผู้ให้บริการอินเทอร์เน็ต, ผู้บริหารระดับสูง	โฆษกฝ่าย IT	สื่อดั้งเดิม: การแถลงข่าวผ่านโทรทัศน์ โซเชียลมีเดีย: Twitter, Facebook
2	**มัลแวร์แพร่กระจาย** (Malware Outbreak)	- กักกันเครื่องที่ติดมัลแวร์ทันที - เริ่มการสแกนระบบทั้งหมดเพื่อหามัลแวร์ที่แพร่กระจาย - แจ้งเตือนพนักงานเกี่ยวกับการระวังอีเมล Phishing - ติดต่อหน่วยงานความปลอดภัยทางไซเบอร์	พนักงาน, ลูกค้าองค์กร, ผู้บริหาร	หน่วยงานความปลอดภัยไซเบอร์, ทีม IT	ผู้จัดการฝ่ายความปลอดภัย	โซเชียลมีเดีย: Facebook, LinkedIn, Blog บนเว็บไซต์องค์กร
3	**ข้อมูลรั่วไหล** (Data Breach)	- แจ้งผู้มีส่วนเกี่ยวข้องทันทีว่ามีการรั่วไหลของข้อมูล - ประสานงานกับทีมกฎหมายและผู้เชี่ยวชาญด้านข้อมูล - ส่งประกาศแจ้งลูกค้าเกี่ยวกับสถานการณ์และแนวทางแก้ไข	ลูกค้า, หน่วยงานกฎหมาย, ผู้ถือหุ้น	ทีมกฎหมาย, ผู้เชี่ยวชาญด้านข้อมูล, ลูกค้า	CEO หรือผู้จัดการฝ่ายกฎหมาย	สื่อดั้งเดิม: การประกาศผ่านสื่อมวลชน โซเชียลมีเดีย: LinkedIn, Website
4	**การเข้าถึงโดยไม่ได้รับอนุญาต** (Unauthorized Access)	- บล็อกการเข้าถึงที่ไม่ได้รับอนุญาตทันที - แจ้งให้ทีมรักษาความปลอดภัยตรวจสอบความเสียหายที่เกิดขึ้น - ส่งประกาศแจ้งหน่วยงานรัฐและหน่วยงานที่เกี่ยวข้อง	ผู้บริหาร, หน่วยงานที่เกี่ยวข้อง, พนักงาน	หน่วยงานรัฐ, ผู้ดูแลระบบ IT, ผู้จัดการความปลอดภัย	โฆษกฝ่ายกฎหมาย	โซเชียลมีเดีย: Twitter, Facebook, Blog บนเว็บไซต์องค์กร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

คำอธิบาย

1. **สถานการณ์จำลอง:** เป็นเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่คาดว่าจะเกิดขึ้น เช่น การโจมตีแบบ DDoS, การแพร่กระจายของมัลแวร์, ข้อมูลรั่วไหล, หรือการเข้าถึงที่ไม่ได้รับอนุญาต
2. **แผนการดำเนินการ:** การจัดการเหตุการณ์และการตอบสนองที่จำเป็น เช่น การกักกันระบบ, การแจ้งเตือนผู้ใช้งาน, หรือการปิดกั้นการเข้าถึง
3. **กลุ่มเป้าหมาย:** บุคคลหรือกลุ่มที่ต้องรับรู้หรือได้รับผลกระทบจากเหตุการณ์
4. **ผู้มีส่วนได้ส่วนเสีย:** องค์กรหรือบุคคลที่มีบทบาทสำคัญในการจัดการหรือมีผลกระทบต่อเหตุการณ์นั้น ๆ
5. **โฆษกหลัก:** บุคคลที่มีหน้าที่แถลงการณ์หรือให้ข้อมูลแก่สาธารณชนหรือสื่อมวลชน
6. **ช่องทางการเผยแพร่ข้อมูล:** ช่องทางที่ใช้ในการสื่อสาร เช่น สื่อดั้งเดิม (โทรทัศน์ วิทยุ) หรือโซเชียลมีเดีย (Facebook, Twitter)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

3.กระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Exercise Procedure)

Logo	**ระเบียบกระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Procedure)**	**รหัสเอกสาร**	**CSMS-Respond -06**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Procedure)	รหัสเอกสาร	CSMS-Respond -06
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58) , ประมวลและกรอบ [ข้อ 24.3.1, ข้อ 24.3.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้องค์กรมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติและระดับภาคส่วน เพื่อเพิ่มความพร้อมและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการวางแผน การดำเนินการ และการประเมินผลการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ รวมถึงการปฏิบัติตามคำขอของหน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจตาม พรบ ไซเบอร์ กำหนด

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและสนับสนุนการมีส่วนร่วมในกระบวนการฝึกซ้อม รวมถึงการจัดสรรทรัพยากรที่จำเป็น
- **ทีมร่วมการฝึกซ้อม (Exercise Security Team)**: รับผิดชอบในการวางแผนและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ รวมถึงการประสานงานกับหน่วยงานภายนอก
- **บุคลากรที่เกี่ยวข้อง (Relevant Personnel)**: มีหน้าที่เข้าร่วมในการฝึกซ้อมตามที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

4. การวางแผนและการเตรียมการฝึกซ้อม (Planning and Preparation for Cybersecurity Exercise)

- **4.1 การมีส่วนร่วมในการฝึกซ้อม**
  - **ขั้นตอน**: องค์กร, หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งจากหน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจตาม พรบ ไซเบอร์ กำหนด
- **4.2 การระบุตัวบุคคลที่ต้องเข้าร่วมฝึกซ้อม**
  - **ขั้นตอน**: ระบุบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อให้เข้าร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

5. การให้ข้อมูลและการประสานงาน (Providing Information and Coordination)

- **5.1 การให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ**
  - **ขั้นตอน**: ปฏิบัติตามคำขอใด ๆ ของหน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่มีอำนาจตาม พรบ ไซเบอร์ กำหนด โดยให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญขององค์กรหรือหน่วยงาน สำหรับการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์
- **5.2 การประสานงานระหว่างฝ่ายที่เกี่ยวข้อง**
  - **ขั้นตอน**: ประสานงานระหว่างทีมรักษาความปลอดภัยสารสนเทศกับหน่วยงานภายนอกและผู้มีส่วนได้ส่วนเสีย เพื่อให้แน่ใจว่าการฝึกซ้อมเป็นไปอย่างมีประสิทธิภาพและครอบคลุมทุกฝ่ายที่เกี่ยวข้อง หรือมีการจัดการประชุมระหว่างหน่วยงานรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญ และหน่วยงานระดับชาติ เพื่อประสานการฝึกซ้อมร่วมกัน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Procedure)	รหัสเอกสาร	CSMS-Respond -06
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

6. การดำเนินการฝึกซ้อมและการประเมินผล (Execution and Evaluation of Cybersecurity Exercise)

- **6.1 การดำเนินการฝึกซ้อม**
  - **ขั้นตอน**: ดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ตามแผนที่กำหนด และติดตามการดำเนินงานของบุคลากรที่เกี่ยวข้อง รวมทั้งการดำเนินการฝึกซ้อมการตอบสนองต่อการโจมตีทางไซเบอร์ที่จำลองขึ้น พร้อมสังเกตการณ์การตอบสนองของทีมรักษาความปลอดภัยสารสนเทศ
- **6.2 การประเมินผลการฝึกซ้อม**
  - **ขั้นตอน**: ประเมินผลการฝึกซ้อมเพื่อวิเคราะห์ประสิทธิภาพในการตอบสนองต่อภัยคุกคาม และระบุจุดที่ต้องปรับปรุงในการฝึกซ้อมครั้งถัดไป หรืออาจจัดทำรายงานผลการฝึกซ้อมที่สรุปจุดแข็งและจุดอ่อนที่ต้องปรับปรุง และนำเสนอให้กับผู้บริหารเพื่อวางแผนการปรับปรุงในอนาคต

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนการฝึกซ้อม
2. ทีมร่วมการฝึกซ้อมและบทบาท รวมถึงหน้าที่ของทีมร่วมการฝึกซ้อม
3. รายงานผลการฝึกซ้อม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

จัดทำโดย : ทีมเฝ้าระวังภัยคุกคามทางไซเบอร์

จัดทำเมื่อ : 1 ธันวาคม 2567

แผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Plan)

1. จัดทีมร่วมการฝึกซ้อม (Exercise Security Team)

	ตำแหน่ง	หน้าที่รับผิดชอบ	ชื่อและติดต่อ
1	หัวหน้าทีมฝึกซ้อม	กำหนดทิศทางและเป้าหมายของการฝึกซ้อม รวมถึงประสานงานกับคณะกรรมการที่เกี่ยวข้อง	นาย A , 081-XXX
2	ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์	จัดทำและออกแบบสถานการณ์จำลองภัยคุกคาม รวมถึงให้คำแนะนำด้านเทคนิค	นาย B , 081-XXX
3	ผู้จัดการการสื่อสาร	จัดการการสื่อสารกับพนักงานและทีมงานทั้งหมดที่มีส่วนเกี่ยวข้องในการฝึกซ้อม	นาย C , 081-XXX
4	ผู้จัดการด้าน IT	รับผิดชอบในการจัดการและตรวจสอบระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องในสถานการณ์จำลอง	นาย D , 081-XXX

2. การวางแผนการฝึกซ้อม (Exercise Planning)

	ขั้นตอน	รายละเอียด
1	การรับคำสั่งและเริ่มต้นการวางแผน	รับคำสั่งเป็นลายลักษณ์อักษรจากคณะกรรมการเพื่อเริ่มต้นการวางแผน
2	การระบุเป้าหมายการฝึกซ้อม	ระบุเป้าหมาย เช่น การทดสอบการตอบสนองต่อ Ransomware การตรวจสอบแผนการสื่อสารในภาวะวิกฤต
3	การรวบรวมข้อมูลและการวิเคราะห์	รวบรวมข้อมูลจากหน่วยงาน เช่น แผนรับมือภัยคุกคามไซเบอร์ แผนการสื่อสารในภาวะวิกฤต ข้อมูลเกี่ยวกับบริการสำคัญ
4	การออกแบบสถานการณ์จำลอง	ออกแบบสถานการณ์ที่เหมาะสมกับเป้าหมาย โดยคำนึงถึงความเป็นไปได้และระดับความซับซ้อนของภัยคุกคาม
5	การกำหนดบทบาทและความรับผิดชอบ	กำหนดบทบาทของบุคลากรที่ร่วมการฝึกซ้อม รวมถึงการกำหนดความรับผิดชอบ เช่น หัวหน้าฝ่าย IT เป็นผู้นำทีมตอบสนอง หัวหน้าฝ่ายประชาสัมพันธ์เป็นโฆษกหลักในการฝึกซ้อม

3. การดำเนินการฝึกซ้อม (Exercise Execution)

	ขั้นตอน	รายละเอียด
1	**การเตรียมพร้อมก่อนการฝึกซ้อม**	เตรียมความพร้อม เช่น การแจ้งเตือนทีมงานที่เกี่ยวข้องและจัดเตรียมเครื่องมือ
2	**การเริ่มต้นฝึกซ้อม**	แจ้งให้ทีมงานทราบถึงสถานการณ์จำลองและเริ่มต้นการฝึกซ้อม เช่น ส่งแจ้งเตือนการโจมตีแบบ Ransomware ให้ทีม IT เพื่อตอบสนองทันที
3	**การตรวจสอบและบันทึกการดำเนินการ**	ตรวจสอบการดำเนินงานของทีมงานและบันทึกเพื่อใช้ในการประเมินผลหลังการฝึกซ้อม
4	**การดำเนินการปรับปรุงทันที**	หากพบปัญหาในการฝึกซ้อม ต้องดำเนินการแก้ไขทันทีและแจ้งให้ทีมงานที่เกี่ยวข้องทราบ
5	**การสรุปการฝึกซ้อม**	ประเมินผลการดำเนินงานของทีมต่าง ๆ และจัดทำรายงานสรุปผลเพื่อวิเคราะห์ข้อดีและข้อผิดพลาดที่เกิดขึ้นในการฝึกซ้อม

4. การประเมินผลและการปรับปรุง (Post-exercise Evaluation and Improvement)

	ขั้นตอน	รายละเอียด
1	**การประเมินผลการตอบสนอง**	ประเมินความพร้อมและความเร็วในการตอบสนองของบุคลากร เช่น การรับมือกับการโจมตีแบบ Ransomware
2	**การวิเคราะห์ข้อผิดพลาดและจุดที่ต้องปรับปรุง**	วิเคราะห์ข้อผิดพลาดและปัญหาที่เกิดขึ้นในระหว่างการฝึกซ้อม เช่น การประสานงานที่ล่าช้าระหว่างทีม IT และฝ่ายกฎหมาย
3	**การจัดทำรายงานสรุปและข้อเสนอแนะ**	จัดทำรายงานสรุปและข้อเสนอแนะในการปรับปรุงแผนการรับมือภัยคุกคาม
4	**การปรับปรุงแผนการรับมือภัยคุกคาม**	ปรับปรุงแผนรับมือภัยคุกคามตามข้อเสนอแนะที่ได้จากการฝึกซ้อม เช่น การปรับปรุงแผนการสื่อสารในภาวะวิกฤต
5	**การติดตามผลการปรับปรุง**	ติดตามผลการปรับปรุงที่ดำเนินการและประเมินผลในการฝึกซ้อมครั้งถัดไป

รายงานผลการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Report)

วันที่ฝึกซ้อม: 9 ธันวาคม 2567

หน่วยงานที่จัด: ทีมเฝ้าระวังภัยคุกคามทางไซเบอร์

ผู้จัดการฝึกซ้อม: นาย A

1. วัตถุประสงค์ของการฝึกซ้อม

การฝึกซ้อมครั้งนี้มีวัตถุประสงค์เพื่อ

- ประเมินความพร้อมของบุคลากรในการตอบสนองต่อภัยคุกคามทางไซเบอร์
- ทดสอบขั้นตอนการรับมือกับการโจมตีแบบ **Ransomware**
- ทดสอบแผนการสื่อสารในภาวะวิกฤตขององค์กร

2. สถานการณ์จำลอง (Exercise Scenarios)

สถานการณ์จำลองที่ 1: การโจมตีแบบ Ransomware

- **สถานการณ์:** จำลองการโจมตีโดยมัลแวร์ประเภท Ransomware ที่เข้ารหัสข้อมูลในเซิร์ฟเวอร์หลักขององค์กร และส่งผลให้ข้อมูลสำคัญของลูกค้าไม่สามารถเข้าถึงได้
- **วัตถุประสงค์:** ทดสอบความพร้อมของทีม IT และการสื่อสารกับกลุ่มลูกค้าและสื่อมวลชน

สถานการณ์จำลองที่ 2: การโจมตีแบบ DDoS

- **สถานการณ์:** จำลองการโจมตีแบบ Distributed Denial of Service (DDoS) ที่ทำให้บริการออนไลน์ขององค์กรไม่สามารถใช้งานได้
- **วัตถุประสงค์:** ทดสอบความสามารถของระบบตรวจจับและการตอบสนองของทีมเครือข่าย

3. ผลการดำเนินการฝึกซ้อม (Exercise Execution Results)

ลำดับ	สถานการณ์จำลอง	การดำเนินการที่เกิดขึ้น	ผลการประเมิน	ข้อเสนอแนะในการปรับปรุง
1	การโจมตีแบบ Ransomware	ทีม IT ทำการกักกันเซิร์ฟเวอร์ที่ได้รับผลกระทบทันที และเริ่มกระบวนการกู้คืนข้อมูลจากการสำรองข้อมูล	ความรวดเร็วในการตอบสนองอยู่ในระดับที่ดี แต่การประสานงานยังขาดความคล่องตัว	เพิ่มการฝึกอบรมการประสานงานระหว่างทีม IT และฝ่ายกฎหมายเพื่อให้การตอบสนองรวดเร็วยิ่งขึ้น
2	การโจมตีแบบ DDoS	ทีมเครือข่ายทำการปิดกั้นทราฟฟิกที่ไม่ปกติ และปรับการตั้งค่าไฟร์วอลล์เพื่อป้องกันการโจมตีซ้ำ	ทีมเครือข่ายทำงานได้อย่างมีประสิทธิภาพ แต่การสื่อสารกับผู้บริหารช้าเกินไป	ปรับปรุงขั้นตอนการแจ้งเตือนผู้บริหารและผู้มีส่วนเกี่ยวข้องอย่างรวดเร็วเมื่อมีการโจมตีเกิดขึ้น
3	การสื่อสารในภาวะวิกฤต	ทีมประชาสัมพันธ์ออกแถลงการณ์ผ่านโซเชียลมีเดียและการแถลงข่าวให้สื่อมวลชนทราบเกี่ยวกับสถานการณ์	การสื่อสารกับสื่อมวลชนมีความชัดเจนและมีความรวดเร็วพอสมควร	เพิ่มช่องทางการสื่อสารอื่น ๆ เช่น การแจ้งเตือนลูกค้าผ่าน SMS

4. การประเมินผลและข้อเสนอแนะ (Evaluation and Recommendations)

1. **ประเมินการตอบสนอง**
   - **ทีม IT**: สามารถตอบสนองต่อสถานการณ์ Ransomware ได้อย่างรวดเร็ว และการกู้คืนข้อมูลจากการสำรองทำได้อย่างสมบูรณ์
   - **ทีม Network** : มีประสิทธิภาพในการป้องกันการโจมตี DDoS โดยทำการปิดกั้นทราฟฟิกที่ไม่ปกติได้ทันที
   - **ทีมประชาสัมพันธ์**: สามารถสื่อสารกับสื่อมวลชนได้ชัดเจน และยังสามารถปรับปรุงการตอบสนองได้รวดเร็วขึ้น
2. **ข้อผิดพลาดและจุดที่ต้องปรับปรุง**
   - การประสานงานระหว่าง **ทีม IT** และ **ฝ่ายกฎหมาย** ยังไม่คล่องตัวพอ ทำให้การตอบสนองต่อเหตุการณ์ช้าไปบ้าง
   - **การแจ้งเตือนผู้บริหาร** ในช่วงเหตุการณ์ DDoS ยังล่าช้า ควรมีการปรับปรุงขั้นตอนการสื่อสารภายในองค์กรให้รวดเร็วขึ้น

3. **ข้อเสนอแนะในการปรับปรุง**
    - เพิ่มการฝึกอบรมด้านการสื่อสารระหว่างทีมต่าง ๆ และการประสานงานระหว่างทีม IT และฝ่ายกฎหมาย
    - ปรับปรุงขั้นตอนการแจ้งเตือนผู้บริหารในภาวะวิกฤตเพื่อให้การตอบสนองรวดเร็วและมีประสิทธิภาพยิ่งขึ้น
    - เพิ่มการใช้ **ระบบแจ้งเตือนอัตโนมัติ** ผ่านแพลตฟอร์มต่าง ๆ เช่น SMS และอีเมล เพื่อให้สามารถติดต่อสื่อสารได้ทันท่วงที

5. การปรับปรุงแผนการรับมือภัยคุกคาม (Update Incident Response Plan)

- ปรับปรุงแผนการรับมือ **Ransomware** โดยเพิ่มเติมการสื่อสารระหว่างทีม IT และฝ่ายกฎหมาย
- เพิ่มขั้นตอนการแจ้งเตือนผู้บริหารทันทีเมื่อเกิดการโจมตีแบบ **DDoS** เพื่อให้สามารถตัดสินใจได้อย่างรวดเร็ว
- อัปเดตแผนการสื่อสารในภาวะวิกฤตเพื่อให้ครอบคลุมช่องทางการสื่อสารมากขึ้น เช่น การแจ้งเตือนลูกค้าผ่าน **SMS**

6. สรุปผลการฝึกซ้อม (Exercise Summary)

- การฝึกซ้อมในครั้งนี้สามารถบรรลุวัตถุประสงค์หลักได้สำเร็จ โดยมีการตอบสนองต่อภัยคุกคามได้รวดเร็วและมีประสิทธิภาพ
- มีข้อเสนอแนะในการปรับปรุงบางประการที่เกี่ยวข้องกับการสื่อสารระหว่างทีมงานและการเพิ่มช่องทางการแจ้งเตือนที่หลากหลายขึ้น เพื่อให้สามารถตอบสนองได้ดียิ่งขึ้นในภาวะวิกฤต

RECOVER

1. กระบวนการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)

Logo	**ระเบียบกระบวนการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)**	**รหัสเอกสาร**	**CSMS-Recover -01**
		แก้ไขครั้งที่	**0**
		วันที่บังคับใช้	**1 ม.ค. 2568**
		ชั้นความลับของเอกสาร	**Internal Use Only**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย xxx xxx	**คุณ xxx**	**คุณ xxx**
ตำแหน่ง	เจ้าหน้าที่ xxx	**ผอ.ฝ่ายบริหาร**	**ผอ.ฝ่ายบริหาร**
วันเดือนปี	1 ตุลาคม 2567	21 ตุลาคม 2567	21 ตุลาคม 2567

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**2 ต.ค. 2567**	**จัดทำเอกสารครั้งแรก เรียบเรียงเนื้อหา**
01	**12 ต.ค. 2567**	**แก้ไขเนื้อหา บริบทองค์กร**
02	**24 ต.ค. 2567**	**เพิ่มเติมหัวข้อ 11**

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

Logo	ระเบียบกระบวนการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)	รหัสเอกสาร	CSMS-Recover -01
		แก้ไขครั้งที่	0
		วันที่บังคับใช้	1 ม.ค. 2568
		ชั้นความลับของเอกสาร	Internal Use Only

ระเบียบกระบวนการการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(Cybersecurity Resilience and Recovery Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 25.1.1, ข้อ 25.1.2]

1. วัตถุประสงค์ (Objective)

ระเบียบกระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าบริการที่สำคัญขององค์กร สามารถให้บริการต่อไปได้อย่างต่อเนื่องในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้กระบวนการฟื้นฟูความเสียหายเป็นไปอย่างมีประสิทธิภาพและใช้เวลาสั้นในการฟื้นฟู

2. ขอบเขต (Scope)

ระเบียบกระบวนการนี้ครอบคลุมถึงการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) การทบทวนแผน BCP ของผู้ให้บริการภายนอก และการฝึกซ้อมแผน BCP เพื่อประเมินความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

3. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ผู้บริหาร (Top Management)**: รับผิดชอบในการอนุมัติและสนับสนุนการจัดทำและการทบทวนแผน BCP รวมถึงการจัดสรรทรัพยากรที่จำเป็นสำหรับการฟื้นฟูความเสียหาย
- **ทีมรักษาความต่อเนื่องทางธุรกิจ (Business Continuity Team)**: รับผิดชอบในการพัฒนาแผน BCP และการประสานงานกับผู้ให้บริการภายนอกเพื่อให้แน่ใจว่าแผน BCP ของผู้ให้บริการภายนอกสอดคล้องกับแผนขององค์กร

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **บุคลากรที่เกี่ยวข้อง (Relevant Personnel)**: มีหน้าที่เข้าร่วมในการฝึกซ้อมแผน BCP และปฏิบัติตามขั้นตอนที่กำหนดไว้ในแผนเมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

4. การจัดทำและทบทวนแผนความต่อเนื่องทางธุรกิจ (Development and Review of Business Continuity Plan)

- **4.1 การจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP)**
  - **ขั้นตอน**: จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อให้บริการที่สำคัญขององค์กรหรือหน่วยงานสามารถดำเนินการต่อไปได้ในกรณีที่เกิดการหยุดชะงักจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีการกำหนดขอบเขตของแผน BCP ที่ครอบคลุมทุกส่วนที่เกี่ยวข้องกับบริการที่สำคัญ และการกำหนดระยะเวลาในการฟื้นฟู (RTO, RPO)
- **4.2 การทบทวนแผนของผู้ให้บริการภายนอก**
  - **ขั้นตอน**: ทบทวนแผน BCP ของผู้ให้บริการภายนอกเพื่อให้แน่ใจว่ามีความสอดคล้องกับแผนความต่อเนื่องทางธุรกิจ ขององค์กรหรือหน่วยงาน อีกทั้ง เพื่อให้แน่ใจว่าการฟื้นฟูระบบสามารถดำเนินการได้ภายในระยะเวลาที่กำหนดในแผนความต่อเนื่องทางธุรกิจ ขององค์กรหรือหน่วยงาน

5. การฝึกซ้อมและการประเมินผล (Exercise and Evaluation)

- **5.1 การฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP)**
  - **ขั้นตอน**: ดำเนินการฝึกซ้อมแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนในการรับมือกับภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยการการจำลองสถานการณ์การโจมตีทางไซเบอร์และการทดสอบความสามารถของบุคลากรในการดำเนินการตามแผน BCP

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

- **5.2 การประเมินผลการฝึกซ้อม**
  - **ขั้นตอน**: ประเมินผลการฝึกซ้อมแผน BCP เพื่อวิเคราะห์จุดแข็งและจุดอ่อนที่ต้องปรับปรุงในการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดทำรายงานผลการฝึกซ้อมที่สรุปผลการดำเนินงานพร้อมข้อเสนอแนะการปรับปรุงแผน BCP เพื่อเพิ่มประสิทธิภาพในการฟื้นฟูความเสียหายในอนาคต

การทบทวนระเบียบกระบวนการดำเนินการ (**Procedure Review)**

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนความต่อเนื่องทางธุรกิจ
2. แผนการสอบทานแผนของผู้ให้บริการภายนอก
3. ผลการฝึกซ้อมแผนตามแผนความต่อเนื่องทางธุรกิจ
4. คู่มือแผนความต่อเนื่องทางธุรกิจ
5. ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของบริษัท aaa จำกัด ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตจากบริษัทฯ เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

แผนงานและผลการสอบทานแผนความต่อเนื่องทางธุรกิจของผู้ให้บริการภายนอก (Vendor BCP Review Report)

ส่วนที่ 1: ข้อมูลทั่วไป (General Information)

- **ชื่อองค์กร (Organization Name):** XYZ Corporation
- **ชื่อผู้ให้บริการภายนอก (Vendor Name):** ABC Cloud Services
- **วันที่ทำการสอบทาน (Review Date):** 15 มกราคม 2567
- **ผู้ทำการสอบทาน (Review Conducted by):** นาย aaa (หัวหน้าฝ่ายความเสี่ยง)

ส่วนที่ 2: วัตถุประสงค์และขอบเขต (Objective and Scope)

- **วัตถุประสงค์ (Objective)**
  - เพื่อประเมินและตรวจสอบแผนความต่อเนื่องทางธุรกิจ (BCP) ของบริษัท ABC Cloud Services ว่ามีความสอดคล้องกับ พรบ ไซเบอร์ และความต้องการของ XYZ Corporation
  - เพื่อระบุความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการของผู้ให้บริการภายนอกและเสนอแนวทางในการปรับปรุง
- **ขอบเขต (Scope)**
  - การสอบทานนี้ครอบคลุมการตรวจสอบเอกสารแผน BCP ของ ABC Cloud Services, การประเมินรายงานการทดสอบ BCP, และการตรวจสอบการสอดคล้องของข้อตกลงด้านการบริการ (SLA) กับความต้องการขององค์กรและสอดคล้องกับ พรบ ไซเบอร์

ส่วนที่ 3: สรุปผลการสอบทาน (Summary of Review Findings)

3.1 การตรวจสอบเอกสารแผน BCP (BCP Document Review)

- **การตรวจสอบความสอดคล้อง (Compliance Check)**
  - ผลการตรวจสอบพบว่าแผน BCP ของ ABC Cloud Services มีการกำหนด RTO และ RPO สอดคล้องกับความต้องการของ XYZ Corporation โดย RTO ถูกกำหนดไว้ที่ 2 ชั่วโมง และ RPO อยู่ที่ 15 นาที

- **การตรวจสอบความครบถ้วนของแผน (Completeness Check)**
    - แผน BCP ครอบคลุมทุกด้านที่จำเป็น เช่น การจัดการข้อมูลสำรอง, การกู้คืนระบบ, และการสื่อสารในภาวะวิกฤต อย่างไรก็ตาม พบว่าแผนการสื่อสารยังขาดการระบุรายละเอียดเกี่ยวกับการแจ้งเตือนลูกค้าในกรณีเกิดเหตุการณ์ฉุกเฉินและไม่ได้มีการจัดทำเอกสารใดๆ ที่เกี่ยวข้องกับ พรบ ไซเบอร์เลย

3.2 การประเมินการทดสอบแผน BCP (BCP Testing Assessment)

- **การทดสอบและผลการทดสอบ (Testing and Results)**
    - รายงานการทดสอบแผน BCP ของ ABC Cloud Services แสดงให้เห็นว่าการทดสอบการกู้คืนระบบจากข้อมูลสำรองสำเร็จภายใน 1.5 ชั่วโมง ซึ่งอยู่ในเกณฑ์ที่กำหนด อย่างไรก็ตาม การทดสอบการสื่อสารกับลูกค้ายังไม่ครอบคลุมทุกสถานการณ์ที่อาจเกิดขึ้น และยังไม่มีการทดสอบเกี่ยวกับการถูกโจมตีทางไซเบอร์

3.3 การตรวจสอบในสถานที่ (On-site Review)

- **สภาพแวดล้อมทางกายภาพและโครงสร้างพื้นฐาน (Physical Environment and Infrastructure)**
    - จากการเยี่ยมชมศูนย์ข้อมูลของ ABC Cloud Services พบว่าโครงสร้างพื้นฐานมีความปลอดภัยและได้รับการดูแลอย่างดี มาตรการป้องกันภัยทางกายภาพและระบบสำรองพลังงานมีประสิทธิภาพ
- **การสัมภาษณ์ผู้รับผิดชอบ (Interviews with Key Personnel)**
    - จากการสัมภาษณ์หัวหน้าทีม BCP ของ ABC Cloud Services พบว่าทีมงานมีความเข้าใจในขั้นตอนการกู้คืนระบบและการสื่อสารในกรณีฉุกเฉิน แต่ยังต้องปรับปรุงการฝึกอบรมพนักงานใหม่เกี่ยวกับแผน BCP อีกทั้งพนักงานยังไม่มีความรู้เกี่ยวกับ พรบ ไซเบอร์

ส่วนที่ 4: ข้อเสนอแนะในการปรับปรุง (Recommendations for Improvement)

1. **ควรมีการทดสอบการโจมตีทางไซเบอร์ (Cybersecurity Hacker Testing)**
    - แนะนำให้ ABC Cloud Services ทำแผนการทดสอบการโจมตีทางไซเบอร์ พร้อมทำการทดสอบ เพื่อให้สอดคล้องตาม พรบ ไซเบอร์

- **การดำเนินการ:** จัดทำแผนพร้อมทดสอบ ภายใน 30 วัน

2. **ควรมีการสร้างความตระหนักรู้และอบรมทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness and Training)**
    - แนะนำให้ ABC Cloud Services ทำแผนการอบรมและสร้างความตระหนักรู้ให้แก่พนักงาน พร้อมปฏิบัติ เพื่อให้สอดคล้องตาม พรบ ไซเบอร์
    - **การดำเนินการ:** จัดทำแผนการอบรมและสร้างความตระหนักรู้ให้แก่พนักงาน พร้อมปฏิบัติ ภายใน 30 วัน
3. **ควรปรับปรุงแผนการสื่อสาร (Enhance Communication Plan)**
    - แนะนำให้ ABC Cloud Services ปรับปรุงแผนการสื่อสารโดยเพิ่มรายละเอียดเกี่ยวกับการแจ้งเตือนลูกค้าในกรณีที่เกิดเหตุการณ์ฉุกเฉิน เพื่อให้ครอบคลุมทุกสถานการณ์ที่อาจเกิดขึ้น
    - **การดำเนินการ:** อัปเดตแผนการสื่อสารภายใน 30 วัน
4. **ควรฝึกอบรมพนักงานใหม่ (Training for New Employees)**
    - แนะนำให้ ABC Cloud Services เพิ่มการฝึกอบรมเกี่ยวกับแผน BCP สำหรับพนักงานใหม่ เพื่อให้มั่นใจว่าทุกคนมีความเข้าใจในขั้นตอนการกู้คืนระบบและการสื่อสารในกรณีฉุกเฉิน
    - **การดำเนินการ:** จัดฝึกอบรมเพิ่มเติมภายใน 90 วัน

ส่วนที่ 5: การติดตามผลและการสอบทานอย่างต่อเนื่อง (Follow-up and Ongoing Review)

- **การติดตามผลการปรับปรุง (Follow-up on Recommendations)**
    - XYZ Corporation จะติดตามการดำเนินการแก้ไขตามข้อเสนอแนะภายใน 30, 60, และ 90 วัน เพื่อให้แน่ใจว่า ABC Cloud Services ได้ดำเนินการปรับปรุงตามที่แนะนำ
- **การสอบทานประจำปี (Annual Review)**
    - จะมีการสอบทานแผน BCP ของ ABC Cloud Services อีกครั้งในเดือนมกราคม 2568 เพื่อให้มั่นใจว่ามีการอัปเดตและปรับปรุงแผนอย่างต่อเนื่อง

รายงานแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP Report)

ส่วนที่ 1: ข้อมูลทั่วไป (General Information)

- **ชื่อองค์กร (Organization Name):** XYZ Corporation
- **ชื่อผู้ทำรายงาน (Report Prepared by):** นาย aaa (หัวหน้าฝ่ายความเสี่ยง)
- **วันที่จัดทำรายงาน (Report Date):** 15 มกราคม 2567
- **เวอร์ชันของแผน (Plan Version):** 2.0
- **วันที่ทบทวนแผนล่าสุด (Last Review Date):** 1 มกราคม 2567

ส่วนที่ 2: วัตถุประสงค์และขอบเขตของแผน (Objective and Scope)

- **วัตถุประสงค์ (Objective)**
    - เพื่อเป็นการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร
    - เพื่อสอดคล้องตามแนวทางปฏิบัติ ตาม พรบ ไซเบอร์
    - เพื่อเตรียมความพร้อมและกำหนดแนวทางในการดำเนินธุรกิจอย่างต่อเนื่องในกรณีที่เกิดภัยพิบัติหรือเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก เช่น ภัยคุกคามทางไซเบอร์, ภัยธรรมชาติ หรือเหตุการณ์ทางสังคมและเศรษฐกิจ
    - เพื่อปกป้องทรัพยากรที่สำคัญขององค์กร เช่น ข้อมูลลูกค้า, ระบบการเงิน, และทรัพย์สินทางปัญญา
    - เพื่อรักษาความเชื่อมั่นของลูกค้า, ผู้ถือหุ้น, และพนักงานในความสามารถขององค์กรในการดำเนินงานต่อไป

- **ขอบเขต (Scope)**
    - แผนนี้ครอบคลุมทุกแผนกและระบบที่สำคัญของ XYZ Corporation รวมถึงการประสานงานกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการคลาวด์, คู่ค้าทางธุรกิจ
    - ระบบและกระบวนการที่ครอบคลุมในแผนนี้ ได้แก่ ระบบคอมพิวเตอร์, ระบบการเงิน, ระบบจัดการข้อมูลลูกค้า (CRM), ระบบการผลิต และระบบ ITอื่นๆ ที่สนับสนุนการดำเนินงาน

ส่วนที่ 3: การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

วัตถุประสงค์: เพื่อระบุและประเมินผลกระทบที่อาจเกิดขึ้นหากบริการหรือกระบวนการสำคัญหยุดชะงัก และกำหนดมาตรการที่เหมาะสมในการฟื้นฟูการดำเนินงาน

3.1 การระบุบริการและกระบวนการที่สำคัญ (Identify Critical Services and Processes)

- **บริการ/กระบวนการที่สำคัญ**
    - **ระบบคอมพิวเตอร์:** Network security, Host Security, Architecture security
    - **ระบบการเงิน:** จัดการบัญชี, การชำระเงิน, การจัดทำรายงานทางการเงิน
    - **ระบบจัดการลูกค้า (CRM):** จัดการข้อมูลลูกค้า, การสนับสนุนลูกค้า, การติดตามการขาย
    - **ระบบการผลิต:** การวางแผนการผลิต, การจัดการวัสดุ, การตรวจสอบคุณภาพ

3.2 การประเมินผลกระทบ (Impact Assessment)

- **ระบบคอมพิวเตอร์**
    - **ผลกระทบทางด้านระบบคอมพิวเตอร์:** ทุกๆ ระบบในเครือข่ายคอมพิวเตอร์ภายในองค์กร ไม่สามารถใช้งานได้
    - **ผลกระทบต่อภาพลักษณ์:** ส่งผลกระทบต่อภาพลักษณ์ขององค์กรในทางลบ
- **ระบบการเงิน**
    - **ผลกระทบทางการเงิน:** การชำระเงินที่ล่าช้า, การสูญเสียความเชื่อมั่นจากลูกค้าและผู้ถือหุ้น
    - **ผลกระทบต่อภาพลักษณ์:** หากไม่สามารถจัดทำรายงานทางการเงินได้ตรงเวลา อาจส่งผลกระทบต่อภาพลักษณ์ขององค์กร

- **ระบบ CRM**
  - **ผลกระทบต่อการขาย:** การสูญเสียข้อมูลลูกค้าหรือการเข้าถึงข้อมูลที่ล่าช้าอาจทำให้พลาดโอกาสทางการขาย
  - **ผลกระทบต่อการสนับสนุนลูกค้า:** ความสามารถในการตอบสนองคำถามและแก้ไขปัญหาของลูกค้าจะถูกจำกัด

3.3 การกำหนด Maximum Tolerable Period of Disruption (MTPD) และ Recovery Time Objective (RTO)

- **ระบบคอมพิวเตอร์**
  - **MTPD:** 30 นาที
  - **RTO:** 15 นาที ต้องฟื้นฟูระบบคอมพิวเตอร์ให้กลับมาใช้งานได้ภายใน 15 นาทีหลังเกิดเหตุการณ์
- **ระบบการเงิน**
  - **MTPD:** 4 ชั่วโมง
  - **RTO:** 2 ชั่วโมง ต้องฟื้นฟูระบบการเงินให้กลับมาใช้งานได้ภายใน 2 ชั่วโมงหลังเกิดเหตุการณ์
- **ระบบ CRM**
  - **MTPD:** 3 ชั่วโมง
  - **RTO:** 3 ชั่วโมง ระบบ CRM ต้องกลับมาใช้งานได้ภายใน 3 ชั่วโมงเพื่อให้ทีมขายสามารถทำงานต่อได้

3.4 การกำหนด Recovery Point Objective (RPO)

- **ระบบคอมพิวเตอร์**
  - **RPO:** 15 นาที ที่ระบบหยุดชะงัก เวลาที่ยอมรับได้คือไม่เกิน 15 นาที
- **ระบบการเงิน**
  - **RPO:** 15 นาที ข้อมูลที่สูญเสียไปในช่วงก่อนการหยุดชะงักที่ยอมรับได้คือไม่เกิน 15 นาที
- **ระบบ CRM**
  - **RPO:** 30 นาที ข้อมูลการติดตามลูกค้าที่สูญเสียไปต้องไม่เกิน 30 นาที

ส่วนที่ 4: กลยุทธ์การกู้คืน (Recovery Strategies)

วัตถุประสงค์: เพื่อกำหนดกลยุทธ์ในการฟื้นฟูการดำเนินงานและลดผลกระทบจากเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก

4.1 การระบุทรัพยากรที่จำเป็น (Identify Required Resources)

- **ทรัพยากรที่จำเป็นสำหรับการกู้คืนระบบ**
  - เซิร์ฟเวอร์สำรอง
  - ซอฟต์แวร์การกู้คืนข้อมูล (Backup Software)
  - ทีม IT, ผู้จัดการการเงิน, ทีมสนับสนุนลูกค้า

4.2 การพัฒนากลยุทธ์การกู้คืนข้อมูล (Develop Data Recovery Strategies)

- **กลยุทธ์ที่ใช้**
  - การสำรองข้อมูลแบบอัตโนมัติรายวันไปยังศูนย์ข้อมูลสำรอง (Off-site Data Backup)
  - การใช้ระบบคลาวด์ในการเก็บสำรองข้อมูลที่สามารถเข้าถึงได้จากทุกที่

4.3 การกำหนดแผนการสื่อสารในภาวะวิกฤต (Develop Crisis Communication Plan)

- **เนื้อหาของแผนการสื่อสาร**
  - การแจ้งเตือนผู้บริหารและพนักงานผ่านอีเมลและโทรศัพท์ทันทีที่เกิดเหตุการณ์
  - การออกประกาศอย่างเป็นทางการแก่ลูกค้าและผู้ถือหุ้นผ่านทางเว็บไซต์ขององค์กรและโซเชียลมีเดียและแจ้งหน่วยงานที่รับผิดชอบ ตาม พรบ ไซเบอร์ กำหนด

4.4 การพัฒนาขั้นตอนการกู้คืนระบบ (Develop System Recovery Procedures)

- **ขั้นตอนการกู้คืนระบบที่ระบุ**
  - การรีบูตเซิร์ฟเวอร์และเชื่อมต่อกับระบบสำรองข้อมูล
  - การกู้คืนฐานข้อมูลจาก Backup ล่าสุดและทดสอบการใช้งานก่อนเปิดให้ผู้ใช้เข้าถึง

4.5 การทดสอบและปรับปรุงกลยุทธ์ (Test and Refine Recovery Strategies)

- **การทดสอบที่ทำ**
  - การจำลองสถานการณ์การโจมตีทางไซเบอร์และทดสอบการกู้คืนระบบ
  - การทบทวนผลการทดสอบและปรับปรุงขั้นตอนการกู้คืนให้มีประสิทธิภาพมากขึ้น

ส่วนที่ 5: การดำเนินงานฉุกเฉิน (Emergency Operations)

วัตถุประสงค์: เพื่อเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินธุรกิจ

5.1 การระบุสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น (Identify Potential Emergency Scenarios)

- **สถานการณ์ฉุกเฉิน**
  - การโจมตีทางไซเบอร์ เช่น Ransomware, DDoS
  - ภัยธรรมชาติ เช่น แผ่นดินไหว, น้ำท่วม
  - เหตุการณ์ทางสังคม เช่น การประท้วง, การหยุดงาน

5.2 การกำหนดบทบาทและความรับผิดชอบในสถานการณ์ฉุกเฉิน (Assign Roles and Responsibilities)

- **บทบาทในสถานการณ์ฉุกเฉิน**
  - **หัวหน้าทีมฉุกเฉิน (Emergency Team Leader):** นาย bbb (CIO)
  - **ผู้ประสานงานด้านการสื่อสาร (Communication Coordinator):** นาง ccc (หัวหน้าฝ่ายความเสี่ยง)
  - **ผู้รับผิดชอบการกู้คืนระบบ (System Recovery Lead):** นาย ggg (หัวหน้าฝ่าย IT)

5.3 การพัฒนาขั้นตอนการตอบสนองฉุกเฉิน (Develop Emergency Response Procedures)

- **ขั้นตอนการตอบสนองที่ระบุ**
  - การปิดระบบทันทีที่ตรวจพบการโจมตีทางไซเบอร์เพื่อลดความเสียหาย
  - การอพยพพนักงานในกรณีเกิดเหตุไฟไหม้และการให้ความช่วยเหลือเบื้องต้น
- หากมีการโจมตีแบบ DDoS ระบบจะถูกปิดทันทีและเปลี่ยนเส้นทางทราฟฟิกไปยังระบบสำรอง

5.4 การทดสอบและฝึกซ้อมการตอบสนอง (Test and Drill Emergency Response)

- **การฝึกซ้อมที่ทำ**
  - การจำลองสถานการณ์การโจมตีทางไซเบอร์และการอพยพพนักงานจากอาคารสำนักงาน
  - การทดสอบความพร้อมของทีม IT ในการกู้คืนระบบจากศูนย์ข้อมูลสำรอง

5.5 การปรับปรุงขั้นตอนตามผลการทดสอบ (Refine Procedures Based on Testing)

- **การปรับปรุงที่ทำ**
  - ปรับปรุงขั้นตอนการอพยพพนักงานหลังพบปัญหาในการฝึกซ้อม
  - แก้ไขขั้นตอนการกู้คืนระบบให้มีประสิทธิภาพมากขึ้นตามผลการทดสอบ
- หลังจากฝึกซ้อมการโจมตีทางไซเบอร์ XYZ Corporation ได้ปรับปรุงขั้นตอนการกู้คืนข้อมูลให้รวดเร็วยิ่งขึ้นโดยลดจำนวนขั้นตอนที่ไม่จำเป็น

ส่วนที่ 6: การฝึกอบรมและการสื่อสาร (Training and Communication)

วัตถุประสงค์: เพื่อให้บุคลากรในองค์กรมีความเข้าใจและสามารถปฏิบัติตามแผน BCP ได้อย่างมีประสิทธิภาพ

6.1 การสื่อสารแผน BCP ให้กับบุคลากร (Communicate BCP to Staff)

- **การสื่อสาร**
  - ส่งเอกสารแผน BCP ให้กับพนักงานทุกคนผ่านทางอีเมลและระบบอินทราเน็ต
  - จัดการประชุมและเวิร์กช็อปเพื่ออธิบายรายละเอียดของแผน BCP และบทบาทของพนักงานแต่ละคน

6.2 การฝึกอบรมเกี่ยวกับแผน BCP (BCP Training Sessions)

- **การฝึกอบรม**
  - จัดอบรมให้กับทีม IT เกี่ยวกับขั้นตอนการกู้คืนระบบจากศูนย์ข้อมูลสำรอง
  - อบรมทีมบริหารเกี่ยวกับการตัดสินใจในภาวะวิกฤตและการสื่อสารกับลูกค้าและผู้ถือหุ้น

6.3 การพัฒนาสื่อการฝึกอบรม (Develop Training Materials)

- **สื่อการฝึกอบรม**
  - คู่มือการตอบสนองต่อการโจมตีทางไซเบอร์
  - วิดีโอการฝึกอบรมเกี่ยวกับการกู้คืนระบบและการสื่อสารในภาวะวิกฤต

6.4 การทบทวนและปรับปรุงสื่อการฝึกอบรม (Review and Update Training Materials)

- **การปรับปรุง**
  - ทบทวนสื่อการฝึกอบรมทุกปีเพื่อให้แน่ใจว่าเนื้อหายังคงสอดคล้องกับภัยคุกคามและเทคโนโลยีล่าสุด
  - อัปเดตคู่มือการตอบสนองต่อภัยคุกคามตามข้อเสนอแนะจากการฝึกอบรมและการทดสอบ

6.5 การติดตามผลการฝึกอบรม (Monitor and Evaluate Training Outcomes)

- **การประเมิน**
  - ใช้แบบสอบถามหลังการฝึกอบรมเพื่อประเมินความเข้าใจของพนักงานเกี่ยวกับแผน BCP
  - ติดตามผลการฝึกซ้อมเพื่อประเมินความพร้อมของพนักงานและทีมงานในสถานการณ์จริง
- หลังการฝึกอบรม XYZ Corporation ส่งแบบสอบถามให้พนักงานทุกคนเพื่อประเมินความเข้าใจและรวบรวมข้อเสนอแนะในการปรับปรุง

ส่วนที่ 7: การฝึกซ้อมและการทดสอบแผน BCP (BCP Drills and Testing)

วัตถุประสงค์: เพื่อทดสอบและประเมินประสิทธิภาพของแผน BCP ในการรับมือกับเหตุการณ์ที่ทำให้ธุรกิจหยุดชะงัก

7.1 การวางแผนการฝึกซ้อม (Drill Planning)

- **การวางแผน**
  - กำหนดสถานการณ์จำลองการโจมตีทางไซเบอร์หรือภัยพิบัติธรรมชาติที่เหมาะสมกับองค์กร
  - จัดเตรียมทรัพยากรและบุคลากรที่จำเป็นสำหรับการฝึกซ้อม

7.2 การกำหนดบทบาทและความรับผิดชอบ (Role Assignment for Drills)

- **บทบาทในการฝึกซ้อม**
  - **ผู้นำการฝึกซ้อม:** นาย a (CIO)
  - **ผู้รับผิดชอบการกู้คืนระบบ:** นาย b (หัวหน้าฝ่าย IT)
  - **ผู้ประสานงานการสื่อสาร:** นางสาว c (หัวหน้าฝ่ายความเสี่ยง)
- ในการฝึกซ้อม XYZ Corporation มอบหมายให้หัวหน้าฝ่าย IT ดูแลการกู้คืนระบบจากศูนย์ข้อมูลสำรอง และหัวหน้าฝ่ายความเสี่ยงดูแลการสื่อสารกับพนักงานและลูกค้า

7.3 การดำเนินการฝึกซ้อม (Drill Execution)

- **การดำเนินการ**
  - เริ่มต้นสถานการณ์จำลองตามแผนที่วางไว้ และติดตามการตอบสนองของทีมงาน
  - บันทึกเวลาที่ใช้ในการกู้คืนระบบและความถูกต้องของขั้นตอนการดำเนินงาน
- ในการฝึกซ้อมการโจมตีแบบ Ransomware ทีม IT ของ XYZ Corporation ดำเนินการกู้คืนระบบจาก Backup ในศูนย์ข้อมูลสำรองภายใน 2 ชั่วโมง

7.4 การประเมินผลการฝึกซ้อม (Drill Evaluation)

- **การประเมิน**
  - ประเมินประสิทธิภาพของแผน BCP โดยตรวจสอบความเร็วในการกู้คืนระบบ ความชัดเจนในการสื่อสาร และความสามารถของทีมในการจัดการกับเหตุการณ์
  - จัดทำรายงานสรุปผลการฝึกซ้อมและข้อเสนอแนะในการปรับปรุง
- หลังการฝึกซ้อม XYZ Corporation ประเมินว่าการกู้คืนระบบ CRM ทำได้ช้ากว่าเป้าหมาย RTO ที่กำหนด และได้จัดทำรายงานเสนอแนะแนวทางในการปรับปรุงขั้นตอน

7.5 การปรับปรุงแผน BCP ตามผลการฝึกซ้อม (BCP Refinement Based on Drills)

- **การปรับปรุง**
  - ปรับปรุงแผน BCP ตามผลการประเมินจากการฝึกซ้อม เพื่อให้มั่นใจว่าแผนยังคงมีประสิทธิภาพและทันสมัย
  - แก้ไขขั้นตอนการกู้คืนระบบและการสื่อสารตามข้อเสนอแนะที่ได้รับจากทีมงาน
- **ทาง** XYZ Corporation ปรับปรุงแผน BCP โดยลดขั้นตอนการกู้คืนระบบ CRM เพื่อให้สามารถตอบสนองได้เร็วขึ้นในกรณีเกิดวิกฤต

ส่วนที่ 8: การตรวจสอบและทบทวนแผน BCP (BCP Review and Maintenance)

วัตถุประสงค์: เพื่อให้แน่ใจว่าแผน BCP ยังคงทันสมัยและสอดคล้องกับภัยคุกคามและการเปลี่ยนแปลงในธุรกิจ

8.1 การทบทวนแผน BCP ประจำปี (Annual BCP Review)

- **การทบทวน**
  - ตรวจสอบและทบทวนแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อปรับปรุงให้สอดคล้องกับสถานการณ์และภัยคุกคามที่เปลี่ยนแปลงไป
  - ประเมินความสอดคล้องของแผนกับกฎหมายและข้อบังคับใหม่ ๆ
- **ทาง** XYZ Corporation ทบทวนแผน BCP ทุกปีในเดือนธันวาคม โดยพิจารณาจากการเปลี่ยนแปลงของเทคโนโลยีและการอัปเดตข้อบังคับด้านความปลอดภัย

8.2 การปรับปรุงแผนตามการเปลี่ยนแปลงในธุรกิจ (Update BCP Based on Business Changes)

- **การปรับปรุง**
  - ปรับปรุงแผน BCP ให้สอดคล้องกับการเปลี่ยนแปลงในองค์กร เช่น การขยายธุรกิจ, การเปลี่ยนแปลงโครงสร้างองค์กร, หรือการเปิดตัวผลิตภัณฑ์ใหม่
- หลังจากการรวมกิจการ XYZ Corporation ปรับปรุงแผน BCP เพื่อครอบคลุมกระบวนการใหม่ที่เกิดจากการรวมธุรกิจ

8.3 การตรวจสอบความสอดคล้องกับกฎหมายและข้อบังคับ (Compliance Check)

- **การตรวจสอบ**
  - ตรวจสอบให้แน่ใจว่าแผน BCP สอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง เช่น ข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูล
- ทาง XYZ Corporation ปรับปรุงแผน BCP ให้สอดคล้องกับกฎหมายใหม่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

8.4 การตรวจสอบความสอดคล้องของแผนกับผู้ให้บริการภายนอก (Vendor BCP Alignment)

- **การตรวจสอบ**
  - ตรวจสอบและปรับปรุงแผน BCP ของผู้ให้บริการภายนอก เพื่อให้แน่ใจว่ามีความสอดคล้องกับแผนขององค์กร เช่น การกำหนด RTO และ RPO ที่สอดคล้องกัน
- **ทาง** XYZ Corporation ตรวจสอบแผน BCP ของผู้ให้บริการคลาวด์และปรับปรุงข้อตกลงการบริการเพื่อให้แน่ใจว่ามีความสอดคล้องกับ RTO และ RPO ที่องค์กรกำหนด

8.5 การรายงานผลการทบทวนแผน (BCP Review Reporting)

- **การรายงาน**
  - จัดทำรายงานผลการทบทวนแผน BCP และการปรับปรุงให้กับผู้บริหารและคณะกรรมการบริหารเพื่อการอนุมัติ
- **ทาง** XYZ Corporation จัดทำรายงานการทบทวนแผน BCP และนำเสนอให้คณะกรรมการบริหารเพื่ออนุมัติการปรับปรุงในเดือนมกราคมของทุกปี

ลงชื่อ :

นาง bbb

หัวหน้าฝ่ายความเสี่ยง

XYZ Corporation

วันที่: 20 มกราคม 2567

รายงานการวิเคราะห์ผลกระทบทางธุรกิจ

(Business Impact Analysis: BIA)

วันที่: 10 มกราคม 2568

หน่วยงาน: แผนก IT และความมั่นคงปลอดภัยทางไซเบอร์

ผู้จัดทำ: นาย A , หัวหน้าแผนก IT

1. บทนำ

รายงานนี้จัดทำขึ้นเพื่อประเมินผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักในการดำเนินธุรกิจในกระบวนการที่สำคัญ รวมถึงการกำหนดเกณฑ์ในการฟื้นฟูกระบวนการต่าง ๆ หลังจากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ เช่น การโจมตีแบบ Ransomware, DDoS, หรือการรั่วไหลของข้อมูล

2. การระบุและประเมินกระบวนการทางธุรกิจที่สำคัญ

ลำดับ	กระบวนการทางธุรกิจที่สำคัญ	รายละเอียดของกระบวนการ	ความสำคัญ
1	ระบบธนาคารออนไลน์ (Internet Banking)	บริการออนไลน์สำหรับลูกค้าของธนาคารในการทำธุรกรรมทางการเงินตลอด 24 ชั่วโมง	สูงสุด (ต้องพร้อมใช้งานตลอดเวลา)
2	ฐานข้อมูลลูกค้า (Customer Database)	ฐานข้อมูลที่เก็บข้อมูลส่วนบุคคลและประวัติการทำธุรกรรมของลูกค้า	สูงสุด (ข้อมูลสำคัญในการให้บริการ)
3	ระบบสนับสนุนการขาย (Sales Support System)	ระบบที่ใช้ในการจัดการและสนับสนุนการขาย รวมถึงการติดตามการทำธุรกรรม	ปานกลาง

3. การกำหนดเกณฑ์ระยะเวลาที่สำคัญ (Critical Time Criteria)

ลำดับ	กระบวนการ	MTPD (ระยะเวลาสูงสุดที่หยุดทำงานได้)	RTO (ระยะเวลาที่ต้องฟื้นฟูระบบ)	RPO (ข้อมูลที่กู้คืนได้)
1	ระบบธนาคารออนไลน์ (Internet Banking)	4 ชั่วโมง	2 ชั่วโมง	15 นาที
2	ฐานข้อมูลลูกค้า (Customer Database)	6 ชั่วโมง	3 ชั่วโมง	30 นาที
3	ระบบสนับสนุนการขาย (Sales Support)	8 ชั่วโมง	4 ชั่วโมง	1 ชั่วโมง

4. การประเมินผลกระทบทางธุรกิจจากเหตุการณ์ที่เป็นไปได้

4.1 เหตุการณ์ที่ 1: การโจมตีแบบ Ransomware

- **กระบวนการที่ได้รับผลกระทบ**: ระบบธนาคารออนไลน์และฐานข้อมูลลูกค้า
- **ผลกระทบ**: หากระบบธนาคารออนไลน์ถูกโจมตีด้วย Ransomware จะทำให้ลูกค้าไม่สามารถเข้าถึงบริการทางการเงินได้ ส่งผลกระทบโดยตรงต่อรายได้ของธนาคารและความเชื่อมั่นของลูกค้า
- **เกณฑ์การฟื้นฟู**: ระบบต้องฟื้นฟูภายใน 2 ชั่วโมง (RTO) และข้อมูลจะต้องกู้คืนได้จาก 15 นาทีสุดท้าย (RPO)

4.2 เหตุการณ์ที่ 2: การโจมตีแบบ DDoS

- **กระบวนการที่ได้รับผลกระทบ**: ระบบสนับสนุนการขาย
- **ผลกระทบ**: หากระบบสนับสนุนการขายถูกโจมตีด้วย DDoS จะทำให้ทีมขายไม่สามารถเข้าถึงข้อมูลการทำธุรกรรมและติดตามลูกค้าได้ ส่งผลให้การขายเกิดความล่าช้า
- **เกณฑ์การฟื้นฟู**: ระบบต้องฟื้นฟูภายใน 4 ชั่วโมง (RTO) และข้อมูลจะต้องกู้คืนได้ภายใน 1 ชั่วโมงสุดท้าย (RPO)

5. ข้อเสนอแนะในการปรับปรุง

1. **เพิ่มความมั่นคงของระบบธนาคารออนไลน์**:
    - แนะนำให้เพิ่มมาตรการป้องกัน Ransomware เช่น การติดตั้งระบบสแกนมัลแวร์และการสำรองข้อมูลแบบอัตโนมัติที่บ่อยขึ้น
2. **พัฒนาความสามารถในการตรวจจับการโจมตี DDoS**:
    - ควรพัฒนาระบบตรวจจับและตอบสนองต่อการโจมตี DDoS เพื่อให้ทีม IT สามารถดำเนินการแก้ไขได้อย่างรวดเร็ว

6. สรุปผลการวิเคราะห์

การวิเคราะห์ผลกระทบทางธุรกิจในครั้งนี้ได้ระบุกระบวนการที่สำคัญของธนาคารที่มีความจำเป็นต้องฟื้นฟูอย่างรวดเร็วหลังจากเกิดเหตุการณ์ที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ โดยได้กำหนดเกณฑ์ MTPD, RTO, และ RPO สำหรับแต่ละกระบวนการเพื่อให้สามารถฟื้นฟูและกลับมาใช้งานได้โดยเร็วที่สุด

Business Continuity Plan

For

AAA Company

Confidential

Business Continuity Plan

Created by: aaa
Creation/Issue date: 14/09/2567
Last modified date: 21/11/2567
Last modified by: aaa
Last reviewed by: 15/12/2567
Review date
Review schedule:
Approved by: bbb

Version Number: 1.0

TABLE OF CONTENTS

I. Introduction 3
I.1 Title of Plan 3
I.2 Purpose 3
I.3 Executive Summary 3
I.4 Documentation and References (Appendices) 3
I.5 Document Location 4
I.6 Document Security 4

II.Scope of The Disaster Recovery Plan 4
II.1 Users of this Procedure 4
II.2 Participating Systems 4

III.Communications Plan 5
III.1 Who Can Declare a Business Continuity 5
III.2 Emergency Funding 5
III.3 Key IT Staff & Alternates 5
III.4 Key Business Staff Contacts and 3rd Party Service 7
III.5 Customers/Authorities/Media/Press Communications 8

IV.Risk Assessment 9
IV.1.0 Risk Definitions 9
IV.1.1 Vulnerabilities, Threats and Exposure Identification for Business/Location 9
IV.1.2 Conclusions on Vulnerabilities, Threats and Exposure Identification 12
IV.2. Business Impact Analysis 13
IV.3. Recovery Assumptions 14

V. Business Continuity Recovery Process Overview 15
V.1 Business Continuity Recovery Architecture Overview 15
V.2 Core Services Recovery Overview 16
V.3 Application Recovery Overview 17

VI. Business Continuity Recovery Procedures 18

VII. Business Continuity Plan Testing Requirements 19

VIII. Business Continuity Plan Business Approval 20

IX. Appendix 21

I. INTRODUCTION

I.1 Title of Plan

AAA COMPANY, BUSINESS CONTINUITY PLAN

I.2 Purpose

1. วัตถุประสงค์

เพื่อกำหนดขั้นตอนและแนวทางในการจัดการความต่อเนื่องทางธุรกิจตามมาตรฐาน พรบ ไซเบอร์ เพื่อให้มั่นใจว่าองค์กรสามารถดำเนินงานได้ต่อเนื่องและกู้คืนจากเหตุการณ์วิกฤติได้อย่างมีประสิทธิภาพ

2. ขอบเขต

ขั้นตอนนี้ครอบคลุมทุกกระบวนการและระบบสารสนเทศภายในองค์กรที่เกี่ยวข้องกับการจัดการความต่อเนื่องทางธุรกิจ

3. ความรับผิดชอบ

- **ผู้จัดการความต่อเนื่องทางธุรกิจ (BCM Manager / ISMS Manager) :** รับผิดชอบในการกำกับดูแลและตรวจสอบการดำเนินงานตามแผน BCM
- **ทีม BCM :** รับผิดชอบในการดำเนินการตามแผน BCM และประสานงานกับหน่วยงานต่างๆ
- **ผู้ใช้ :** ปฏิบัติตามแนวทางและขั้นตอนที่กำหนดในแผน BCM

BCM Organization Chart

แสดงโครงสร้างของทีม พร้อมเบอร์ติดต่อ

I.3 Executive Summary

ขั้นตอนการทำงานนี้ ถูกใช้ในกรณีที่เกิดภัยพิบัติที่ศูนย์ข้อมูลหรือเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่ทำให้ธุรกิจหยุดชะงัก ซึ่งขั้นตอนการทำงานนี้มีเป้าหมายเพื่ออธิบายโครงสร้างการกู้คืนจากภัยพิบัติ/ความปลอดภัยทางไซเบอร์ วิธีการที่ใช้ในการกู้คืน และขั้นตอนสำหรับการนำบริการเทคโนโลยีสารสนเทศหลักและแอปพลิเคชันระบบธุรกิจที่สำคัญกลับมาใช้งาน โดยได้มาจากการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ณ สถานที่กู้คืนจากภัยพิบัติ/ความปลอดภัยทางไซเบอร์ และ แผนนี้ยังกล่าวถึงทรัพยากรที่จำเป็นและลำดับการกู้คืนที่ต้องปฏิบัติตามเพื่อให้แผนประสบความสำเร็จ

I.4 Documentation and References (Appendices)

i. WAN disaster / Cybersecurity recovery plan
ii. All server installation guide
iii. Application and vendor contact List
iv. Hardware and software inventory
v. Backup and Restore Manual / Scheduling
vi. Backup system and Offsite Backup

I.5 Document Location

แผนนี้ถูกจัดเก็บไว้และจะถูกนำมาใช้จากเวอร์ชันที่อยู่ในโฟลเดอร์ "แผนการกู้คืนจากภัยพิบัติ/ความปลอดภัยทางไซเบอร์" ที่อยู่ใน GOOGLE DRIVE

Show link of google drive

I.6 Document Security

แผนนี้เป็นข้อมูลธุรกิจที่เป็นความลับ ออกแบบมาสำหรับกลุ่มงาน IT และกลุ่มงานตรวจสอบที่เหมาะสม

II. SCOPE OF THE DISASTER / CYBERSECURITY RECOVERY PLAN

II.1 Users of this Procedure

กลุ่มงาน ITS และกลุ่มสนับสนุนที่มีสิทธิ์เข้าถึงแผนนี้ ได้แก่:

ITS Infrastructure
ITS Data Center Recovery Team
ITS Risk Management
ITS Audit

II.2 Participating Systems

เอกสารนี้อธิบายการออกแบบที่เหมาะสมต่อการเกิดภัยพิบัติและกิจกรรมการสำรองเพื่อรับมือกับภัยพิบัติ/ความปลอดภัยทางไซเบอร์สำหรับเซิร์ฟเวอร์ที่ทาง AAA Company ได้ใช้พร้อมกับบริการ IT หลักและแอปพลิเคชันหลักสำหรับระบบธุรกิจตามที่ระบุด้านล่าง และขั้นตอนระดับสูงที่จำเป็นในการดำเนินการ fail over ในกรณีที่เกิดภัยพิบัติ/เหตุการณ์ความปลอดภัยทางไซเบอร์จริง

บริการ IT หลัก ที่รวมอยู่ในแผนนี้ ได้แก่:

- Windows Authentication
- DNS/DHCP
- E-mail
- All application / Data that established on AAA Company's system

III. COMMUNICATIONS PLAN

III.1 Who Can Declare a Disaster/Cybersecurity

การประกาศภัยพิบัติ/เหตุการณ์ความปลอดภัยทางไซเบอร์ ดำเนินการโดย AAA Company, หัวหน้า ITS หากไม่มีบุคคลเหล่านี้อยู่ สามารถรายงานตรงไปยังหัวหน้าแอปพลิเคชันหลักระบบธุรกิจหรือหัวหน้าโครงสร้างพื้นฐาน IT เพื่อทำการตัดสินใจ โดยบุคลากรดังต่อไปนี้ จะเป็นผู้ตัดสินใจหลักอย่างต่อเนื่อง:

- IT Infrastructure Head
- Business System Applications Head
- Representative, Telecomm
- Representative, LAN Engineering
- Representative, Data Center
- Representative, Help Desk

III.2 Emergency Funding

อาจจำเป็นต้องใช้เงินทุนก่อนที่ระบบการเงินจะกลับมาออนไลน์ ดังนั้นจึงจำเป็นต้องนำเสนองบประมาณที่จำเป็นต้องใช้ต่อคณะผู้บริหารต่อไป

III.3 Key IT Staff & Alternates

โครงสร้างของบุคลากร IT ที่มีบทบาทสำคัญในการดำเนินการตามแผนความต่อเนื่องทางธุรกิจ จะถูกเปิดใช้งานทันทีหลังจากที่มีการประกาศเหตุภัยพิบัติ

- BCM Coordinator - จุดศูนย์กลางสำหรับการสื่อสารและแผนปฏิบัติการ จัดตารางเวลาและบันทึกเหตุการณ์
- Senior Management - ตัดสินใจเกี่ยวกับการจัดลำดับความสำคัญและวิธีการกู้คืน สื่อสารกับผู้นำธุรกิจระดับสูง
- Server Coordinator - รักษาความปลอดภัยและดำเนินการสร้างฐานของเซิร์ฟเวอร์ เตรียมอุปกรณ์สำหรับการติดตั้งแอปพลิเคชัน
- Server Application Coordinator - ติดตั้งและกำหนดค่าแอปพลิเคชัน
- Workstation Application Coordinator – ติดตั้งและกำหนดค่าแอปพลิเคชันบนเวิร์กสเตชัน
- Backup Coordinator - รักษาความปลอดภัยของข้อมูลที่จำเป็นสำหรับการกู้คืน
- Network Coordinator - จัดเตรียมเครือข่ายที่เหมาะสม เป็นจุดติดต่อกับผู้ให้บริการเครือข่าย
- Telecomm Coordinator – รับผิดชอบด้านการสื่อสารโทรคมนาคมในสถานที่สำรอง
- Operations Leader – รับผิดชอบการดำเนินงานในสถานที่สำรอง
- Facilities Coordinator – รับผิดชอบด้านสิ่งอำนวยความสะดวกในสถานที่สำรอง

บุคลากรที่มีบทบาทตามที่อธิบายไว้ข้างต้นได้ถูกคัดเลือกและฝึกอบรมล่วงหน้าเพื่อรับมือกับเหตุการณ์ ข้อมูลการติดต่อแนบไว้ดังต่อไปนี้:

Business Continuity Plan Execution Key IT Staff

Role	Personnel Assigned	Contact Information
IT BCM Coordinator	A	Home Address: Mobile No.
BCM Coordinator (Member)	B	Home Address: Mobile No.
BCM Coordinator (Member)	C	Home Address: Mobile No.
Top Management	F	Home Address: Mobile No.
Top Management (Alt)	G	Home Address: Mobile No.
Application Server Coordinator	H	Home Address: Mobile No.
International Link / Firewall / Network Management	I	Home Address: Mobile No.
E-Mail Management	K	Home Address: Mobile No.
AD/Windows Server	L	Home Address: Mobile No.
Server Coordinator	M	Home Address: Mobile No.
Server Coordinator (Alt)	N	Home Address: Mobile No.
Server Application Coordinator	O	Home Address: Mobile No.
Server Application Coordinator (Alt)	P	Home Address: Mobile No.
Workstation Application Coordinator	R	Home Address: Mobile No.
Workstation Application Coordinator (Alt)	S	Home Address: Mobile No.
Backup Coordinator	T	Home Address: Mobile No.
Backup Coordinator (Alt)	U	Home Address: Mobile No.
Network Coordinator	V	Home Address: Mobile No.
Network Coordinator (Alt)	W	Home Address: Mobile No.
Telecomm Coordinator	X	Home Address: Mobile No.
Telecomm Coordinator (Alt)	Y	Home Address: Mobile No.
Operation Leader	Z	Home Address: Mobile No.
Facility Leader	AA	Home Address: Mobile No.

VI. BUSINESS CONTINUITY RECOVERY PROCEDURES

ตามลำดับความสำคัญและลำดับการดำเนินการที่กำหนดไว้ในตารางสรุปผลกระทบทางธุรกิจสำหรับโครงสร้างพื้นฐานและแอปพลิเคชันหลัก ขั้นตอนต่อไปนี้ควรดำเนินการตามลำดับที่แสดงในตารางต่อไปนี้เพื่อให้สามารถใช้งานสภาพแวดล้อมสำรองได้ในกรณีที่มีการประกาศเหตุการณ์ระดับความต่อเนื่องทางธุรกิจ

Seq #	Application/ IT Service Name	Recovery Procedure	Document Name	Version
1	WAN Services	Core Services Recovery and Operational Validation	WAN Disaster recovery plan	1.0
2	Server Installation	Server Installation Procedure	Disaster Procedure for Restoring VMWare and Operating System	1.0
3	Cyber HRM System	VMware Configuration	VMware Configuration	1.0
4	Crisis Communication	Crisis Communication Document	Crisis Comm. Guidelines	1.0
5	DR Test	Step on how to do a DR Testing	DR testing procedure	1.0
6	VMware Configuration	VMware Configuration	VMware Configuration	1.0
7	VMware Restoration Procedure	VM Ware Restoration Procedure	Disaster Procedure for Restoring VMWare and Operating System	1.0
8	Cyber HRM System	VM Ware Restoration Procedure	Disaster Procedure for Restoring VMWare and Operating System	1.0

VII. BUSINESS CONTINUITY PLAN TESTING REQUIREMENTS

มีการทดสอบการกู้คืนความต่อเนื่องทางธุรกิจเป็นประจำทุกปีเพื่อให้แน่ใจว่าขั้นตอนนี้ได้รับการเข้าใจอย่างดีและกระบวนการมีความถูกต้อง แอปพลิเคชันอาศัยบริการ IT จำนวนหนึ่งในการทำงาน เครือข่ายพื้นฐานให้การเชื่อมต่อและการกำหนดเส้นทางระหว่างส่วนประกอบของแอปพลิเคชันและผู้ใช้ปลายทาง จำเป็นต้องมีเซิร์ฟเวอร์ทางกายภาพสำหรับเซิร์ฟเวอร์ที่ใช้ฮาร์ดแวร์สำหรับความต้องการเฉพาะ เช่น ฐานข้อมูลและ EMAIL

รายงาน BIA ให้ข้อกำหนดพื้นฐานสำหรับการวางแผนความต่อเนื่องทางธุรกิจ ในระหว่างขั้นตอนการวางแผนการทดสอบ แอปพลิเคชันที่จะทดสอบจะถูกวิเคราะห์เพื่อทำความเข้าใจว่ามีการใช้ส่วนประกอบใดในการทำงานปกติ ทรัพยากรเหล่านี้จะถูกวิจัยเพื่อระบุว่าแอปพลิเคชันอื่น ๆ ใดจะได้รับผลกระทบในระหว่างการทดสอบ และสิ่งนี้จะถูกนำมาพิจารณาในการวางแผนการทดสอบ ขั้นตอนการทดสอบความต่อเนื่องทางธุรกิจมีอยู่ใน 'ภาคผนวก'

ด้านล่างนี้คือตารางการทดสอบโดยรวมที่จำเป็นสำหรับแอปพลิเคชันหลักที่อยู่ในขอบเขตเป็นส่วนหนึ่งของแผนการกู้คืนจากภัยพิบัตินี้:

AAA COMPANY, Business Continuity Recovery Testing Calendar

Application DR Plan	Year Test Schedule											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
WAN Disaster Recovery												✔
Core Services												✔
AD Server												✔
Internet												✔
HIS Access												✔
ERP Access												✔
HRM System												✔

VIII. BUSINESS CONTINUITY PLAN BUSINESS APPROVAL

แผนการกู้คืนความต่อเนื่องทางธุรกิจที่บันทึกไว้ในขั้นตอนนี้และเอกสารสนับสนุนที่เกี่ยวข้อง ได้รับการตรวจสอบและอนุมัติโดยทีมผู้บริหารระดับสูงของ AAA Company โดยสมาชิกในทีมได้ลงนามและอนุมัติเอกสารดังนี้:

_____
Aaa bbb
Financial Control / IT Manager
Date_____/_____/_____

_____
Ddd eee
Managing Director
Date_____/_____/_____

IX. APPENDIX

สามารถศึกษาขั้นตอนต่อไปนี้เพื่อสนับสนุนแผนการกู้คืนจากภัยพิบัตินี้:

Insurance Evident
Hardware and Software Inventory List
BCM Testing
BCM Approve from Top Management

แบบประเมินสถานภาพการดำเนินการ

CII
(98 Controls)

	แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for CII)			
	D1 : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562			
ลำดับที่	**รายการ (Objective)**	**ที่มา (Requirement)**		**หลักฐาน (Evident)**
1	มีการดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 43	1	นโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์
			2	ผังโครงสร้างองค์กรผังโครงสร้างองค์กร (Organizational Chart) ที่มีการระบุตำแหน่งผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และ ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)
			3	เอกสารที่แสดงถึงบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)
			4	เอกสารความร่วมมือหรือหลักฐานการเข้าร่วมในโครงการต่าง ๆ ตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
			5	กรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
2	มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 44	1	แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
			2	การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
			3	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
			4	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอาจเป็น เอกสาร เช่น ระเบียบ นโยบาย แนวปฏิบัติ ตามมาตรการทางด้าน Identity, Protect, Detect, Respond, Recovery

			5	หลักฐานที่แสดงว่าหน่วยงานใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ
3	มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 45	1	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
			2	หลักฐานการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ
			3	หลักฐานการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานไปยังบุคลากรที่เกี่ยวข้องทั้งหมด
4	มีการแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช . รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง	ม. 46	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ
5	มีการแจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ไปยัง สกมช หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา 50 (Sectoral CERT) ภายใน 30 วัน นับแต่วันที่คณะกรรมการประกาศ	ม. 52	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือEmail หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ
6	มีการเปลี่ยนแปลงรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ หน่วยงานได้แจ้งปรับปรุงข้อมูลไปยัง สกมช .	ม. 52	1	หลักฐานการแจ้งการเปลี่ยนแปลงข้อมูล เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ
7	มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดย ผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง	ม. 54	1	หลักฐานการตรวจประเมิน เช่น รายงานผลการประเมินความเสี่ยงประจำปี
			2	หลักฐานการตรวจสอบ เช่น รายงานผลการตรวจสอบประจำปี
8	มีการจัดส่งผลสรุปรายงานการดำเนินการ (การ ประเมินความเสี่ยงฯ และการตรวจสอบ) ต่อ สกมช . ภายใน 30 วัน นับแต่วันที่ดำเนินการแล้วเสร็จ	ม. 54	1	หลักฐานการจัดส่งผลสรุปรายงานการประเมินความเสี่ยงฯ ต่อ สกมช. ภายใน30 วัน นับแต่วันที่ดำเนินการแล้วเสร็จ เช่น สำเนาหนังสือแจ้งหรือ Email ที่ได้แจ้งผลสรุปรายงานการประเมินความเสี่ยงฯ ดังกล่าวให้ สกมช. ทราบ

9	มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ เกี่ยวข้องกับโครงสร้างพื้นฐานสาคัญทางสารสนเทศของตนตาม มาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับ ดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบ มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัย ไซเบอร์ที่คณะกรรมการหรือ กกม . กำหนด	ม. 56	1	คู่มือ ขั้นตอนปฏิบัติในการเฝ้าระวังภัยคุกคามทางไซเบอร์
10	มีการเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับ ภัยคุกคามทางไซเบอร์ที่ สกมช . จัดขึ้น เพื่อให้มั่นใจว่า หน่วยงานสามารถตอบสนองต่อภัยคุกคามทางไซเบอร์หรือ เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ได้	ม. 56	1	หลักฐานการเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือ กับภัยคุกคามทางไซเบอร์ที่ สกมช. จัดขึ้น (National Cyber Exercise) เช่น คำสั่งมอบหมายให้บุคลากรเข้าร่วม หลักฐานการลงทะเบียนเข้าร่วม ประกาศนียบัตรการเข้าร่วม กิจกรรม ภาพถ่ายกิจกรรม ฯลฯ
11	มีกระบวนงานหรือขั้นตอนปฏิบัติ ในการรายงานต่อ สกมช และหน่วยงานควบคุมหรือกำกับดูแล เมื่อมีเหตุภัยคุกคาม ทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงาน และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์	ม. 57	1	หลักฐานการรายงาน ต่อ สกมช. เช่น รายละเอียด การรายงาน สำเนาหนังสือแจ้ง Email หรือช่องทางการ แจ้ง อื่น ๆที่ได้ รายงาน เรื่องดังกล่าวให้ สกมช. ทราบ
			2	หลักฐานขั้นตอนปฏิบัติ ในการรายงานต่อ สกมช. และหน่วยงาน ควบคุมหรือกำกับดูแล เมื่อมีเหตุภัยคุกคาม ทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานและ ปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์

12	หากเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์หน่วยงานของท่านได้ปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในมาตรา 58 ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้แก่ (1) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงาน หน่วยงานของท่านได้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมของตนเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (2) หน่วยงานของท่านได้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (3) หน่วยงานของท่านได้แจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว	ม. 58	1	หลักฐานการดำเนินการ หรือ รายงานการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
			2	หลักฐานการแจ้งเหตุภัยคุกคามทางไซเบอร์ เช่น หนังสือแจ้ง Email หรือช่องทางการแจ้งอื่นๆ ที่หน่วยงานได้แจ้งการเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตน
			3	รายงานผลการตรวจสอบข้อมูลที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่
			4	แนวทางการปฏิบัติในการแจ้งเหตุภัยคุกคามทางไซเบอร์ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล

แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for CII)

D2 : นโยบายบริหารจัดการ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2560 - 2570)

ลำดับที่	รายการ (Objective)	ที่มา (Requirement)		หลักฐาน (Evident)
13	มีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กรพร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.1	1	เอกสารผังโครงสร้างขององค์กร และ การกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ ที่แสดงการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ Three Lines of Defense)
14	หน่วยงานมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.3	1	เอกสารคำสั่งแต่งตั้ง ผู้บริหารระดับสูง ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่า
15	ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และ งานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.3	1	เอกสารแสดงอำนาจหน้าที่หรือความรับผิดชอบของผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่า
16	มีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
17	มีเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และระดับความเสี่ยงที่ยอมรับได้ Risk Appetite)	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
18	มีวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
19	มีการเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

20	มีการเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.2	1	เอกสารรายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register)
21	มีการติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.3	1	เอกสารรายงานผลการติดตาม/ประเมินผลการดำเนินงานเกี่ยวกับการบริหารความเสี่ยง
22	มีการกำหนดและอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงาน จากภัยคุกคามทางไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐานและแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ (ต้องเป็นเอกสารที่มีการอนุมัติหรือประกาศใช้งานในหน่วยงาน)
23	มีนโยบายมาตรฐาน และแนวปฏิบัติในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงาน ที่มีความสอดคล้องกับหลักประมวลแนวทางปฏิบัติที่คณะกรรมการกำหนด ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ (ต้องเป็นเอกสารที่มีการอนุมัติหรือประกาศใช้งานในหน่วยงาน)
24	มีนโยบาย มาตรฐาน และแนวปฏิบัติที่มีการเผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ
25	มีการทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงาน และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละ 1 ครั้ง	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.2	1	เอกสารรายงานผลการทบทวนประจำปี เกี่ยวกับนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ

แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for CII)

D3 : ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับที่	รายการ (Objective)	ชื่อองค์ประกอบ	ที่มา (Requirement)		ตัวอย่างเอกสารหลักฐาน (Evident)
26	มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1	1	รายงานหรือผลการตรวจสอบ
27	มีการตรวจสอบในเรื่องกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ก)	1	แผนการดำเนินการตรวจสอบ (Audit Program/Plan) ที่ระบุถึงขอบเขตการตรวจสอบกระบวนการจัดทำ และผลการวิเคราะห์ผลกระทบทางธุรกิจ
				2	รายงานการตรวจสอบ (Audit Report) กระบวนการการจัดทำการวิเคราะห์ผลกระทบทางธุรกิจและผลการวิเคราะห์ผลกระทบทางธุรกิจ
				3	รายงานหรือเอกสารแสดงการจัดทำ BIA (วันที่ หรือ version ของเอกสาร) ที่ครอบคลุมธุรกิจหรือบริการของหน่วยงาน
28	มีการตรวจสอบในเรื่องบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ข)	1	รายงานผลการตรวจสอบ (Audit Report) ที่ระบุขอบเขตหรือรายการบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ
				2	รายงานหรือเอกสารแสดงการจัดทำ BIA
				3	หลักฐานที่แสดงให้เห็นว่า BIA ได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ที่รับมอบหมายหรือคณะกรรมการที่ได้รับมอบหมาย
				4	แนวทางการตรวจสอบ (Audit Program) ที่ครอบคลุมบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ
				5	เอกสารหรือวาระการประชุมที่เป็นลายลักษณ์อักษร แสดงถึงตัวแทนอาวุโสอย่างน้อยหนึ่งคนจากแต่ละหน่วยธุรกิจ
29	มีการตรวจสอบในเรื่องการปฏิบัติตามประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่ กมช. กำหนด	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ค)	1	รายงานผลการตรวจสอบ (Audit Report) ด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ
				2	แนวทางการตรวจสอบ (Audit Program) ที่ครอบคลุมบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ
				3	แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมันคงปลอดภัยไซเบอร์ของหน่วยงาน
				4	มาตรฐานการปฏิบัติงานของหน่วยงาน
30	หน่วยงานของท่านได้จัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อ สกมช . ภายในกำหนด 30 วัน นับแต่วันที่ดำเนินการแล้วเสร็จ	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.2	1	หลักฐานการจัดส่ง เช่น สำเนาหนังสือจัดส่งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ

31	มีการจัดส่งสำเนาผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ตามข้อ 30 ต่อหน่วยงานควบคุมหรือกำกับดูแล	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.2	1	รายงานผลการตรวจสอบ (Audit Report) ด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ
				2	หนังสือการส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ไปยังหน่วยงานควบคุมหรือกำกับดูแล
32	ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ระบุการไม่ปฏิบัติตามข้อ 17.1 เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานส่งแผนการดำเนินการแก้ไขไปยัง สกมช. ภายในกำหนด 30 (สามสิบ) วัน นับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ประกอบด้วยรายละเอียดการดำเนินการแก้ไขที่หน่วยงานจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และกำหนด ระยะเวลาสำหรับการดำเนินการแก้ไข	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.3	1	แผนการดำเนินการแก้ไขและระยะเวลาที่ใช้ดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม
				2	หนังสือการจัดส่งแผนการดำเนินการแก้ไขไปยัง สกมช.
33	ในกรณีที่ กกม เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยัง สกมช ภายในระยะเวลาที่ กกม . กำหนด พร้อมทั้ง ส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแล ด้วย	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.4	1	แผนการดำนเนินการแก้ไขและระยะเวลาที่ใช้ดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม [ฉบับปรับปรุง]
				2	หนังสือการจัดส่งแผนการดำเนินการแก้ไข [ฉบับปรับปรุง] ไปยัง สกมช.
				3	หนังสือการจัดส่งแผนการดำเนินการแก้ไข [ฉบับปรับปรุง] ไปยังหน่วยงานควบคุมหรือกำกับดูแล
34	เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม หน่วยงาน CII จะ ดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม .	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.5	1	แผนการดำเนินการแก้ไขที่ได้รับความเห็นชอบจาก กกม.
				2	รายงาน ผลการดำเนินการแก้ไขตามแผนการดำเนินการแก้ไขที่ได้รับความเห็นชอบจาก กกม.
35	หน่วยงานของท่านได้กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
36	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีเนื้อหาที่ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
37	มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	เอกสารที่เกี่ยวข้องต่าง ๆ ที่จัดทำต้องมีการอนุมัติ ประกาศใช้

38	มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
39	มีการระบุถึงความเสี่ยง (Risk Identification) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ และพิจารณาสาเหตุความเสี่ยงจากกกระบวนการปฏิบัติงานระบบงาน บุคลากร หรือปัจจัยภายนอก	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ก)	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
40	มีการวิเคราะห์ความเสี่ยง (Risk Analysis) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ข)	1	เกณฑ์การวิเคราะห์ความเสี่ยง และแนวปฏิบัติการจัดการความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	ผลการวิเคราะห์ความเสี่ยง ที่แสดงถึงแนวทางการจัดการความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
41	มีการประเมิน ถึงโอกาสที่ ความเสี่ยง (Risk Evaluation) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ค)	1	รายงานผลประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	เอกสารที่แสดงถึง ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ ของหน่วยงาน
				3	แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงาน
42	มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.2 (ข)	1	ผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงาน
				2	เอกสารแนวทางจัดการ ควบคุม และป้องกันความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	เอกสารที่แสดงถึงระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ของหน่วยงาน
43	มีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.2	1	เอกสารที่แสดงถึง กระบวนการ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือเอกสารอื่นใดที่กำหนดดัชนีชี้วัดความเสี่ยง ที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	รายงาน ผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
44	มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.3	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	ทะเบียนความเสี่ยง (Risk Register) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	รายงานการตอบสนองและจัดการเปลี่ยนแปลงที่สำคัญที่มีผลต่อความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

				4	รายงานผลการวิเคราะห์ประสิทธิภาพ และการปรับปรุงแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				5	ผลประเมินตาม ดัชนี ชี้วัดความเสี่ยงที่สำคัญ
45	มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.4	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	หลักฐานการรายงาน เช่น รายงานการประชุม ที่เกี่ยวข้อง
46	มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.4	1	รายงานผลการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	Minute of Meeting ที่ได้มีการรีวิวและรับรองรายงานโดยผู้บริหาร
				3	ระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
47	มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.1	1	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของหน่วยงาน
48	มีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด อย่างมีประสิทธิผล	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.2	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ ที่หน่วยงานใช้ ในการสื่อสารในองค์กร
49	มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.3	1	หลักฐานหรือรายงานผลการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง
50	มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.4	1	บันทึกเหตุการณ์การเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สคัญของหน่วยงานหรือการเปลี่ยนข้อกำหนดในการตอบสนองต่อเหตุการณ์
				2	หลักฐานหรือ รายงาน ผลการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
51	หน่วยงานของท่านมีทะเบียนทรัพย์สิน ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน ทั้งนี้ทะเบียนทรัพย์สินของบริการที่สำคัญต้องมี	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.1	1	เอกสารนโยบาย กระบวนการและขั้นตอนการกำหนดและดูแลรักษาทะเบียนทรัพย์สินที่อยู่ระหว่างการจัดทำ
				2	เอกสารนโยบาย กระบวนการ และขั้นตอนการกำหนดและดูแลรักษาทะเบียนทรัพย์สินที่ประกาศใช้ในหน่วยงานแล้ว
				3	ทะเบียนทรัพย์สินที่ครอบคลุมทรัพย์สินของบริการสำคัญทั้งหมดของหน่วยงานและเป็นปัจจุบัน
				4	รายการทรัพยากรฮาร์ดแวร์และซอฟแวร์ของระบบปรับปรุงทะเบียนทรัพย์สินอัตโนมัติ

				5	รายงานหรือภาพหน้าจอที่สามารถแสดงให้เห็นถึงการดำเนินการตรวจสอบการเปลี่ยนแปลงของรายการบริการที่อยู่ในทะเบียนทรัพย์สินที่ระบุบริการที่สำคัญ ตามกระบวนการการตรวจสอบของหน่วยงาน
52	มีการระบุขอบเขตเครือข่ายของบริการที่สำคัญและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ Direct and Significant Interface)	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.2	1	แผนผังเครือข่ายที่แสดงถึงขอบเขตเครือข่ายของบริการที่สำคัญ แผนผังเครือข่ายที่แสดงถึงขอบเขตเครือข่ายของบริการที่สำคัญและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ
53	มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.3	1	รายงานการตรวจสอบทะเบียนทรัพย์สินประจำปี
54	มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ตามรายการที่ระบุไว้ในทะเบียนทรัพย์สิน ที่ระบุบริการสาคัญ อย่างน้อยปีละ 1 ครั้ง	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.4	1	รายงานการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ
55	มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้สำหรับการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด	Identify | Risk Assessment and Risk MGT Strategy	กรอบมาตรฐาน ข้อ 21.2.1	1	หลักฐานการกำหนดเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ที่กำหนดไว้สำหรับการบริหารความเสี่ยง (Risk Management) และสอดคล้องตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ภายใต้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)
				2	รายงานการประเมินความเสี่ยง
56	มีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	Identify | Risk Assessment and Risk MGT Strategy	กรอบมาตรฐาน ข้อ 21.2.2	1	ทะเบียนความเสี่ยง (Risk Register) ที่มีบันทึกการปรับปรุงทะเบียนดังกล่าว
57	มีการประเมินช่องโหว่โดยครอบคลุมบริการที่สำคัญซึ่งเป็นระบบเทคโนโลยีสารสนเทศ Information Technology System) หรือระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม Industrial Control System: ICS)	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.1	1	รายงานการประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน
				2	บันทึกการใช้ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ประเมินช่องโหว่อัตโนมัติ
				3	คู่มือการบริหารความเสี่ยงของหน่วยงาน
58	หน่วยงานของท่านได้ระบุขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญหรือไม่ (โดยขอบเขตดังกล่าวต้องครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม)	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.2	1	รายงานการประเมินช่องโหว่ของบริการที่สำคัญที่ได้ระบุขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญ

59	หน่วยงานของท่านได้ประเมินช่องโหว่ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ที่จะเชื่อมต่อ หรือ ดำเนินการเปลี่ยนแปลงระบบที่สำคัญกับบริการที่สำคัญ หรือไม่ หมายเหตุ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี ทั้งนี้รวมถึงการเปลี่ยนไปใช้ระบบใหม่แทนที่ ระบบเดิมด้วย	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.3	1	รายงานการทดสอบระบบใหม่ที่เชื่อมต่อกับบริการที่สำคัญ ที่ระบุวันเวลาในการทดสอบ หรือ รายงานการเปลี่ยนแปลง ระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ที่ระบุวันเวลาของการเปลี่ยนแปลง
				2	รายงานการประเมินช่องโหว่ของบริการที่สำคัญ ที่ระบุวันเวลาในการประเมิน
60	มีการพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.4	1	รายงานการทดสอบเจาะระบบ ที่แสดงให้เห็นถึงการดำเนินการที่สอดคล้องกับระดับของความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากการทดสอบเจาะระบบ
				2	รายงานการพิจารณาดำเนินการทดสอบเจาะระบบ ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือ รายงานการพิจารณาดำเนินการทดสอบเจาะระบบ ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบ
61	มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ Scope of a Penetration Test) ได้รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.5	1	รายงานการเจาะระบบ ตามขอบเขตของการทดสอบเจาะระบบที่ได้ถูกกำหนด
				2	เอกสารแสดงขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test)
62	มีการดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.6	1	รายงานการทดสอบเจาะระบบ
63	มีการตรวจสอบเพื่อให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศมีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.7	1	สัญญาจ้างบริการการทดสอบเจาะระบบ สัญญาจ้างบริการการทดสอบเจาะระบบ ที่กำหนดเงื่อนไขของระบบที่ใช้ทดสอบและผู้ทดสอบเจาะระบบ
				2	รายงานผลการประเมินบริการการทดสอบเจาะระบบ
64	มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.8	1	รายงานผลการทดสอบเจาะระบบที่แสดงถึงผลการกำกับดูแลการทดสอบเจาะระบบของบุคลากรของหน่วยงาน
				2	สัญญาจ้างบริการการทดสอบเจาะระบบ ที่ระบุเงื่อนไขการดำเนินงานที่เกี่ยวข้อง

				3	เอกสารนโยบาย กระบวนการ และขั้นตอนการกำกับดูแลการทดสอบเจาะระบบของหน่วยงาน
65	มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ (ทั้งนี้หมายรวมถึง ช่องโหว่ของซอฟต์แวร์ ฮาร์ดแวร์ และระบบต่าง ๆ ที่ควบคุมการเข้าถึงทางกายภาพ)	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.9	1	เอกสารนโยบาย กระบวนการ และขั้นตอนการติดตามและจัดการช่องโหว่ที่อยู่ระหว่างการจัดทำ
				2	เอกสารนโยบาย กระบวนการ และขั้นตอนการติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์ที่ประกาศใช้ในหน่วยงาน
				3	รายงานการจัดการช่องโหว่ซอฟต์แวร์และฮาร์ดแวร์
				4	รายงานการสแกนช่องโหว่ของซอฟต์แวร์และฮาร์ดแวร์ทั้งก่อนและหลังการอัปเดตซอฟต์แวร์
				5	ภาพหน้าจอของระบบสแกนช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์
				6	เอกสารที่แสดงการจัดลำดับความสำคัญของช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์ และการทดสอบการติดตั้งแพตช์ ซึ่งสอดคล้องกับระดับความเสี่ยง
				7	รายงานการจัดการแพตช์ หรือ เฟิร์มแวร์
				8	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ติดตามและจัดการช่องโหว่อัตโนมัติ
				9	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้จัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์อัตโนมัติ
				10	รายงานการติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์
				11	รายงานการจัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์
				12	รายงานการจัดการแพตช์ (Patch) เฟริม์แวร์ และอัปเดตซอฟต์แวร์อัตโนมัติสำหรับแอปพลิเคชันและอุปกรณ์เครือข่าย รายงานการจัดการแพตช์ (Patch) เฟริม์แวร์ และอัปเดตซอฟต์แวร์อัตโนมัติสำหรับแอปพลิเคชันและอุปกรณ์เครือข่ายทั้งหมด
				13	รายงานการวัดประสิทธิภาพของระบบติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์อัตโนมัติ
				14	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้จัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์อัตโนมัติ
				15	รายงานผลการวิเคราะห์โค้ดของซอฟต์แวร์ในเชิงลึก

66	มีการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ ให้ กกม หรือ สกมช . ทราบภายใน 30 วัน นับจากที่ได้รับหนังสือร้องขอ	Identify | Vul. Assessment and Penetration Testing	กรอบมาตรฐาน ข้อ 21.3.10	1	หนังสือนำส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ
				2	สำเนารายงานสรุปผลการทดสอบเจาะระบบ
67	หน่วยงานของท่านได้ระบุเกี่ยวกับความรับผิดชอบและภาระรับผิดชอบ (Responsible, Accountable) ของผู้ให้บริการภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ หรือด้านเทคโนโลยีด้านการปฏิบัติการ (Operational Technology) ในสัญญาการจัดซื้อจัดจ้าง	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.1	1	สัญญาจ้างผู้ให้บริการภายนอกหน่วยงาน
				2	ขอบเขตของงาน (TOR)
68	หน่วยงานของท่านมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก หรือไม่	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.2	1	ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement)
				2	เงื่อนไขด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญากับผู้ให้บริการภายนอก
69	มีกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.3	1	รายงานสรุปการให้บริการของผู้ให้บริการภายนอก ที่จัดทำโดยหรือที่ได้รับการตรวจสอบจากบุคลากรของหน่วยงาน
				2	เอกสารที่แสดงถึงกระบวนการตรวจสอบความสอดคล้องของผู้ให้บริการภายนอกกับข้อกำหนดหรือเงื่อนไขของสัญญา
70	หน่วยงานของท่านได้ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.4	1	สัญญาจ้างผู้ให้บริการภายนอกหน่วยงานที่ได้รับการแก้ไขหลังจากการเจรจาต่อรองเงื่อนไขของสัญญาจ้าง เพื่อให้สอดคล้องข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่
71	มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากรกิจกรรม อุปกรณ์ และอินเทอร์เฟซ ที่ได้รับอนุญาตเท่านั้น	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.1	1	นโยบายความมั่นคงปลอดภัยไซเบอร์ของสารสนเทศในหน่วยงาน
				2	กลยุทธ์ นโยบาย และกระบวนการด้านการจัดการตัวตนและการเข้าถึง (Identity and Access Management)
				3	รายการฮาร์ดแวร์หรือซอฟต์แวร์ของระบบการจัดการตัวตนและการเข้าถึง (รวมถึง ระบบควบคุมการเข้าถึงทางกายภาพ)
				4	เอกสารที่ระบุบทบาทหน้าที่ และแสดงถึงการดำเนินงานของเจ้าหน้าที่ได้รับมอบหมายหน้าที่ในการพัฒนา จัดการและตรวจสอบตัวชี้วัดเกี่ยวกับประสิทธิภาพของการจัดการตัวตนและการเข้าถึง
				5	ข้อกำหนดการตั้งรหัส และการกำหนดวันหมดอายุของรหัสผ่าน
				6	แผนการปรับปรุงรายการผู้ใช้ และการปรับปรุงการให้สิทธิ์การเข้าถึง
				7	ผลการทบทวนการตั้งค่าใน Active Directory (แสดงถึง การเปิดใช้งาน Multi-factor Authentication)

				8	หลักฐานการตั้งค่าสำหรับการจัดการตัวตน และจำกัดการเข้าถึง
				9	หนังสือเวียนถึงบุคลากรเพื่อแจ้งให้ตรวจสอบสิทธิ์การเข้าถึงบริการที่สำคัญ
72	มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.2	1	รายการเทคนิคการตรวจสอบสิทธิ์ เช่น การใช้รหัสผ่าน รายการควบคุมการเข้าถึง (Access Control List) ไฟร์วอลล์ (Firewall) ระบบการจัดการเข้าถึงพิเศษ (Privileged Access Management: PAM)
				2	รายงานการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยง (Risk Profile) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	โปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
73	มีการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด Logs of All Accesses) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.3	1	หลักฐานที่มีการบันทึกการเข้าถึงและความพยายามเข้าถึงบริการที่สำคัญ (รวมถึงการบันทึกการเข้าถึงและความพยายามเข้าถึงเครือข่าย และเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับบริการที่สำคัญดังกล่าว)
				2	หลักฐานที่มีการบันทึกวิธีที่ผู้ใช้ที่ไม่มีสิทธิ์แต่พยายามเข้าถึงบริการที่สำคัญ (รวมถึงการบันทึกการเข้าถึงและความพยายามเข้าถึงเครือข่าย และเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับบริการที่สำคัญดังกล่าว)
74	มีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ และการเข้าถึงทางลอจิคอล Logical) มีการกำกับดูแลโดยหน่วยงาน	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.4	1	นโยบายความมั่นคงปลอดภัยไซเบอร์ของสารสนเทศในหน่วยงาน
				2	รายการฮาร์ดแวร์หรือซอฟต์แวร์ของระบบการจัดการตัวตนและการเข้าถึง (รวมถึง ระบบควบคุมการเข้าถึงทางกายภาพ)
				3	กลยุทธ์ นโยบาย และกระบวนการด้านการจัดการตัวตนและการเข้าถึง (Identity and Access Management)
				4	เอกสารที่ระบุบทบาทหน้าที่ และแสดงถึงการดำเนินงานของเจ้าหน้าที่ที่ได้รับมอบหมายหน้าที่ในการพัฒนา จัดการและตรวจสอบตัวชี้วัดเกี่ยวกับประสิทธิภาพของการจัดการตัวตนและการเข้าถึง
				5	รายงานการกำกับดูแลของบุคลากรในหน่วยงาน เมื่อมีการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB และพอร์ตอนุกรม) หรือมีการเข้าถึงทางลอจิคอล Logical)
75	มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ Cybersecurity Risk Profile)	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.1	1	มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ

				2	โปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
				3	กระบวนการตรวจสอบความสอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				4	รายการบริการที่สำคัญของหน่วยงาน
76	มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ต่อไปนี้ (ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด Least Access Privilege) (ข) การแบ่งแยกหน้าที่ Separation of Duties) (ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน (ง) การลบบัญชีที่ไม่ได้ใช้ (จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก Vendor Support Application) (ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน (ช) การป้องกันมัลแวร์ Malware) และ (ซ) การปรับปรุงซอฟต์แวร์และแพตช์ Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.2	1	เอกสารที่แสดงมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของหน่วยงาน พร้อมระบุความสอดคล้องตามข้อ (ก)--(ซ)
77	มีการตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.3	1	หลักฐานบันทึกการใช้มาตรฐานการกำหนดค่าขั้นต่ำฯ ตามข้อ (ก)--(ซ) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย
78	มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.4	1	บันทึกหรือผลการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำฯ ประจำปี
				2	คู่มือปฏิบัติการในการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
79	มีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.5	1	กระบวนการหรือคู่มือปฏิบัติการจัดการเปลี่ยนแปลงของหน่วยงาน
				2	แบบฟอร์มที่เกี่ยวข้องกับการขออนุมัติการเปลี่ยนแปลงของหน่วยงาน
80	มีการตรวจสอบว่าระบบเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.3.1	1	นโยบาย แนวปฏิบัติในการเชื่อมต่อระยะไกลที่มายังบริการที่สำคัญ

				2	กระบวนการตรวจสอบการเชื่อมต่อระยะไกลทั้งหมดที่มายังบริการที่สำคัญ
				3	บันทึกหรือรายงานการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ
				4	กลไกการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ
81	หน่วยงานของท่านปฏิบัติตามแนวปฏิบัติในการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานท่าน มีองค์ประกอบข้อใดต่อไปนี้ (ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น (ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง Transmission Security) และความสมบูรณ์ของข้อความ Message Integrity) ที่แข็งแกร่ง (ค ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น (ง ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงาน เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ (จ จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.3.2	1	หลักเกณฑ์การพิจารณาอนุมัติให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล การพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) การเข้ารหัสสำหรับการเชื่อมต่อเครือข่าย การใช้คำสั่งระบบ (Issuing System Commands) และการจำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำ
				2	หนังสือขออนุมัติ/แบบฟอร์มร้องขอการเชื่อมต่อระยะไกล
82	มีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพากับบริการที่สำคัญ (ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ (ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น (ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.4.1	1	นโยบาย แนวปฏิบัติในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพากับบริการที่สำคัญของหน่วยงาน
				2	บันทึกการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB Storage) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา
				3	บันทึกการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ
				4	บันทึกการใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาต

83	มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.4.2	1	นโยบาย แนวปฏิบัติ (1) นโยบาย แนวปฏิบัติ หรือมาตรฐานการเข้ารหัสข้อมูลของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้
				2	บันทึกการเข้ารหัสข้อมูลที่ละเอียดอ่อนของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้
84	มีแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของหน่วยงานท่าน	Protect | Cybersecurity Awareness	กรอบมาตรฐาน ข้อ 22.5.1	1	แผนงานในการสร้างตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
				3	รายการกิจกรรมและกำหนดการจัดกิจกรรมที่เกี่ยวข้องในแผนงาน
				4	คู่มือปฏิบัติงานของบุคลากรทุกประเภท
85	มีการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม	Protect | Cybersecurity Awareness	กรอบมาตรฐาน ข้อ 22.5.2	1	ผลการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี
86	กำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับบริการที่สำคัญ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว	Protect | Information Sharing	กรอบมาตรฐาน ข้อ 22.6.1	1	นโยบาย แนวปฏิบัติ คู่มือปฏิบัติการแสดงรายละเอียดขั้นตอนการแบ่งปันข้อมูลของหน่วยงาน
				2	แนวทางและรูปแบบในการแบ่งปันข้อมูล เช่น รายการซอฟต์แวร์หรือฮาร์ดแวร์ ที่ใช้งาน หรือ Community ที่เข้าร่วมเพื่อแบ่งปันข้อมูล เป็นต้น
				3	รายการหลักฐานการเข้าร่วมแบ่งปันข้อมูล เช่น การเข้าร่วมและแบ่งปันข้อมูลใน Community เป็นต้น
				4	มาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				5	รายการ MOAs, MOUs กับหน่วยงานที่มีการแบ่งปันข้อมูล
87	มีการสร้างกลไกและกระบวนการเพื่อ ตรวจจับ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ	Detect | Cyber Threat Detection and Monitoring	กรอบมาตรฐาน ข้อ 23.1.1	1	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				2	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการ เพื่อจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

				3	รายการซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ในการตรวจจับเหตุการณ์ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				4	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการเพื่อระบุว่ายังมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				5	รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
88	หน่วยงานมีการทบทวนกลไกและกระบวนการ ดังนี้ (1) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน (2) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ (3) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานหรือไม่ เพื่อตรวจจับ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้ องกับบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง	Detect | Cyber Threat Detection and Monitoring	กรอบมาตรฐาน ข้อ 23.1.2	1	ผลการทบทวนกลไกและกระบวนการประจำปี
				2	คู่มือปฏิบัติการในการทบทวนกลไกและกระบวนการ
				3	ผลการทบทวน รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (outsourcing)
				4	ผลการทบทวน ปรับปรุง ระดับการให้บริการในสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
89	มีการจัดทำสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง	Respond | Cybersecurity Incident Response Plan	กรอบมาตรฐาน ข้อ 24.1.1	1	ผลการ ทบทวน แผนการรับมือภัยคุกคามทางไซเบอร์ประจำปี
				2	คู่มือปฏิบัติการในการทบทวน แผนการรับมือภัยคุกคามทางไซเบอร์ ประจำปี
				3	แผนการรับมือภัยคุกคามทางไซเบอร์ ที่ปรับปรุงจากการทบทวน
				4	ผลการทบทวน รายละเอีย ดขอบเขตของงาน (TOR) หรือสัญญาจ้างที่เกี่ยวข้อง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก Outsourcing)
				5	ผลการเปลี่ยนแปลงรายละเอีย ดขอบเขตของงาน (TOR) หรือสัญญาจ้างที่เกี่ยวข้อง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก Outsourcing)

90	มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.1	1	นโยบาย แนวปฏิบัติในการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	แผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
91	มีแผนการสื่อสารในภาวะวิกฤตของหน่วยงานท่าน มีองค์ประกอบ ดังต่อไปนี้ (ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต (ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง (ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท (ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน (จ) ระบุแพลตฟอร์ม ช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.2	1	แผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
92	มีการตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.3	1	ผลการตรวจสอบแผนการสื่อสารในภาวะวิกฤตของหน่วยงาน
				2	กลไก คู่มือปฏิบัติงานในการตรวจสอบแผนการสื่อสารในภาวะวิกฤตของหน่วยงาน
93	มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการทดสอบแผนและความเข้าใจของทีมงาน	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.4	1	ผลการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี
				2	แผนการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี
94	มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ทั้งในระดับชาติหรือระดับภาคส่วน	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.1	1	รายการกิจกรรมฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ที่หน่วยงานเข้าร่วม
				2	หนังสือตอบรับการเข้าร่วมการฝึก
				3	ประกาศนียบัตรการเข้าร่วมกิจกรรม
95	มีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.1	1	รายงานการเข้าร่วมกิจกรรมฝึกซ้อมแผนรับมือภัยคุกคาม
				2	ประกาศนียบัตรการเข้าร่วมกิจกรรม
				3	รายชื่อผู้เข้าร่วมกิจกรรมการฝึกซ้อมแผนรับมือภัยคุกคาม
96	มีการปฏิบัติตามคำขอใดของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.2	1	หนังสือตอบรับคำขอจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

				2	รายการกิจกรรมที่หน่วยงานปฏิบัติตามคำขอจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
				3	รายการคำขอจากคณะกรรมการ
97	มีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) เพื่อให้หน่วยงานสามารถกลับมาดำเนินการได้อย่างต่อเนื่อง	Recover | Cybersecurity Resilience and Recovery	กรอบมาตรฐาน ข้อ 25.1.1	1	แผนความต่อเนื่องทางธุรกิจของหน่วยงาน
				2	แนวทางการจัดทำแผนความต่อเนื่องทางธุรกิจของหน่วยงาน
98	มีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อทดสอบแผนเตรียมความพร้อมต่อสภาวะวิกฤตและพัฒนาปรับปรุงแผนให้มีประสิทธิภาพ	Recover | Cybersecurity Resilience and Recovery	กรอบมาตรฐาน ข้อ 25.1.2	1	แผนการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจของหน่วยงาน
				2	ผลการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจประจำปี

Gov
(89 Controls)

	แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Gov)			
	D1 : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562			
ลำดับที่	**รายการ (Objective)**	**ที่มา (Requirement)**		**หลักฐาน (Evident)**
1	มีการดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 43	1	นโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์
			2	ผังโครงสร้างองค์กรผังโครงสร้างองค์กร (Organizational Chart) ที่มีการระบุตำแหน่งผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และ ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)
			3	เอกสารที่แสดงถึงบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)
			4	เอกสารความร่วมมือหรือหลักฐานการเข้าร่วมในโครงการต่าง ๆ ตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
			5	กรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
2	มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 44	1	เอกสารประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอาจเป็น เอกสารเช่น ระเบียบ นโยบาย แนวปฏิบัติ ตามมาตรการทางด้าน Identity, Protect, Detect, Respond, Recovery
			2	หลักฐานที่แสดงว่าหน่วยงานมีการใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ
	มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน		1	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

3	ไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	ม. 45	2	หลักฐานการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานไปยังบุคลากรที่เกี่ยวข้องทั้งหมด
			3	หลักฐานการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ
4	มีการแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช . รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง	ม. 46	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ
5	หากเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์หน่วยงานของท่านได้ปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในมาตรา 58 ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้แก่ (1) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงาน หน่วยงานของท่านได้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมของตนเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (2) หน่วยงานของท่านได้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (3) หน่วยงานของท่านได้แจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว	ม. 58	1	หลักฐานการดำเนินการ หรือ รายงานการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
			2	หลักฐานการแจ้งเหตุภัยคุกคามทางไซเบอร์ เช่น หนังสือแจ้ง Email หรือช่องทางการแจ้งอื่นๆ ที่หน่วยงานได้แจ้งการเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตน
			3	รายงานผลการตรวจสอบข้อมูลที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่
			4	แนวทางการปฏิบัติในการแจ้งเหตุภัยคุกคามทางไซเบอร์ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล

แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Gov)

D2 : นโยบายบริหารจัดการ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2560 - 2570)

ลำดับที่	รายการ (Objective)	ที่มา (Requirement)		หลักฐาน (Evident)
6	มีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กรพร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.1	1	เอกสารผังโครงสร้างขององค์กร และ การกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ ที่แสดงการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)
7	หน่วยงานมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.2	1	เอกสารคำสั่งแต่งตั้งผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า
8	ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) หรือเทียบเท่า ของหน่วยงานท่าน เป็นผู้ที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.2	1	เอกสารแสดงความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ ของผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า
9	ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) หรือเทียบเท่าของหน่วยงานท่าน มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ IT Development) ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) หรือเทียบเท่าของหน่วยงานท่าน มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ IT Development) หรือไม่	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.2	1	เอกสารแสดงอำนาจหน้าที่หรือความรับผิดชอบของผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า

10	ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) หรือเทียบเท่า ของหน่วยงานท่าน มีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานด เนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือไม่	นโยบายบริหารจัดการ ภาคผนวก ข้อ 1.2	1	เอกสารแสดงอำนาจหน้าที่หรือความรับผิดชอบของผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) เอกสารแสดงอำนาจหน้าที่หรือความรับผิดชอบของผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Head of Information Security) หรือเทียบเท่า
11	มีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
12	มีเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และระดับความเสี่ยงที่ยอมรับได้ Risk Appetite)	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
13	มีวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
14	มีการเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.1	1	เอกสารกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
15	มีการเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.2	1	เอกสารรายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register)
16	มีการติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้	นโยบายบริหารจัดการ ภาคผนวก ข้อ 2.3	1	เอกสารรายงานผลการติดตาม/ประเมินผลการดำเนินงานเกี่ยวกับการบริหารความเสี่ยง
17	มีการกำหนดและอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงาน จากภัยคุกคามทางไซเบอร์	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐานและแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ (ต้องเป็นเอกสารที่มีการอนุมัติหรือประกาศใช้งานในหน่วยงาน)
18	มีนโยบายมาตรฐาน และแนวปฏิบัติในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงาน ที่มีความสอดคล้องกับหลักประมวลแนวทางปฏิบัติที่คณะกรรมการกำหนด ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนและนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ (ต้องเป็นเอกสารที่มีการอนุมัติหรือประกาศใช้งานในหน่วยงาน)

19	มีนโยบาย มาตรฐาน และแนวปฏิบัติที่มีการเผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงาน	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.1	1	เอกสารนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ
20	มีการทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงาน และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละ 1 ครั้ง	นโยบายบริหารจัดการ ภาคผนวก ข้อ 3.2	1	เอกสารรายงานผลการทบทวนประจำปี เกี่ยวกับนโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญ

แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Gov)

D3 : ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับที่	รายการ (Objective)	ชื่อองค์ประกอบ	ที่มา (Requirement)		หลักฐาน (Evident)
21	มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1	1	รายงานหรือผลการตรวจสอบประจำปี
22	มีการตรวจสอบในเรื่องกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ก)	1	แผนการดำเนินการตรวจสอบ (Audit Program/Plan) ที่ระบุถึงขอบเขตการตรวจสอบกระบวนการจัดทำ และผลการวิเคราะห์ผลกระทบทางธุรกิจ
				2	รายงานการตรวจสอบ (Audit Report) กระบวนการการจัดทำการวิเคราะห์ผลกระทบทางธุรกิจและผลการวิเคราะห์ผลกระทบทางธุรกิจ
				3	รายงานหรือเอกสารแสดงการจัดทำ BIA (วันที่ หรือ version ของเอกสาร) ที่ครอบคลุมธุรกิจหรือบริการของหน่วยงาน
23	มีการตรวจสอบในเรื่องบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ข)	1	รายงานผลการตรวจสอบ (Audit Report) ที่ระบุขอบเขตหรือรายการบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ
				2	รายงานหรือเอกสารแสดงการจัดทำ BIA
				3	หลักฐานที่แสดงให้เห็นว่า BIA ได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ที่รับมอบหมายหรือคณะกรรมการที่ได้รับมอบหมาย
				4	แนวทางการตรวจสอบ (Audit Program) ที่ครอบคลุมบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ
				5	เอกสารหรือวาระการประชุมที่เป็นลายลักษณ์อักษร แสดงถึงตัวแทนอาวุโสอย่างน้อยหนึ่งคนจากแต่ละหน่วยธุรกิจ
24	มีการตรวจสอบในเรื่องการปฏิบัติตามประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่ กมช. กำหนด	แผนการตรวจสอบ	ประมวลแนวปฏิบัติ ข้อ 17.1 (ค)	1	รายงานผลการตรวจสอบ (Audit Report) ด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ
				2	แนวทางการตรวจสอบ (Audit Program) ที่ครอบคลุมบริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ
				3	แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				4	มาตรฐานการปฏิบัติงานของหน่วยงาน

25	หน่วยงานของท่านได้กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
26	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีเนื้อหาที่ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
27	มีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	เอกสารที่เกี่ยวข้องต่าง ๆ ที่จัดทำต้องมีการอนุมัติ ประกาศใช้
28	มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
29	มีการระบุถึงความเสี่ยง (Risk Identification) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ และพิจารณาสาเหตุความเสี่ยงจากกกระบวนการปฏิบัติงานระบบงาน บุคลากร หรือปัจจัยภายนอก	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ก)	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
30	มีการวิเคราะห์ความเสี่ยง (Risk Analysis) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ข)	1	เกณฑ์การวิเคราะห์ความเสี่ยง และแนวปฏิบัติการจัดการความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	ผลการวิเคราะห์ความเสี่ยง ที่แสดงถึงแนวทางการจัดการความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
31	มีการประเมิน ถึงโอกาสที่ ความเสี่ยง (Risk Evaluation) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.1 (ค)	1	รายงานผลประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	เอกสารที่แสดงถึง ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ ของหน่วยงาน
				3	แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงาน
32	มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.2 (ข)	1	ผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงาน
				2	เอกสารแนวทางจัดการ ควบคุม และป้องกันความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	เอกสารที่แสดงถึงระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ของหน่วยงาน

33	มีการกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.2	1	เอกสารที่แสดงถึง กระบวนการ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือเอกสารอื่นใด ที่กำหนดดัชนีชี้วัดความเสี่ยง ที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตัวอย่าง
				2	รายงาน ผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
34	มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.3	1	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	ทะเบียนความเสี่ยง (Risk Register) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	รายงานการตอบสนองและจัดการเปลี่ยนแปลงที่สำคัญที่มีผลต่อความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				4	รายงานผลการวิเคราะห์ประสิทธิภาพ และการปรับปรุงแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				5	ผลประเมินตาม ดัชนี ชี้วัดความเสี่ยงที่สำคัญ
35	มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.4	1	รายงานผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	หลักฐานการรายงาน เช่น รายงานการประชุม ที่เกี่ยวข้อง
36	มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.4	1	รายงานผลการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				2	ระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
37	มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ)	การประเมินความเสี่ยง	ประมวลแนวปฏิบัติ ข้อ 18.4	1	ระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	รายงานผลการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
38	มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.1	1	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของหน่วยงาน
39	มีการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด อย่างมีประสิทธิผล	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.2	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ ที่หน่วยงานใช้ ในการสื่อสารในองค์กร
				2	แผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงาน
				3	กำหนดการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์
				4	แนวทางการจัดทำและสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์

40	มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.3	1	หลักฐานหรือรายงานผลการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง
41	มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	แผนการรับมือภัยคุกคาม	ประมวลแนวปฏิบัติ ข้อ 19.4	1	บันทึกเหตุการณ์การเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สคัญของหน่วยงานหรือการเปลี่ยนข้อกำหนดในการตอบสนองต่อเหตุการณ์
				2	หลักฐานหรือ รายงาน ผลการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
42	หน่วยงานของท่านมีทะเบียนทรัพย์สิน ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน ทั้งนี้ทะเบียนทรัพย์สินของบริการที่สำคัญต้องมี	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.1	1	เอกสารนโยบาย กระบวนการและขั้นตอนการกำหนดและดูแลรักษาทะเบียนทรัพย์สินที่อยู่ระหว่างการจัดทำ
				2	เอกสารนโยบาย กระบวนการ และขั้นตอนการกำหนดและดูแลรักษาทะเบียนทรัพย์สินที่ประกาศใช้ในหน่วยงานแล้ว
				3	ทะเบียนทรัพย์สินที่ครอบคลุมทรัพย์สินของบริการสำคัญทั้งหมดของหน่วยงานและเป็นปัจจุบัน
				4	รายการทรัพยากรฮาร์ดแวร์และซอฟแวร์ของระบบปรับปรุงทะเบียนทรัพย์สินอัตโนมัติ
				5	รายงานหรือภาพหน้าจอที่สามารถแสดงให้เห็นถึงการดำเนินการตรวจสอบการเปลี่ยนแปลงของรายการบริการที่อยู่ในทะเบียนทรัพย์สินที่ระบุบริการที่สำคัญ ตามกระบวนการการตรวจสอบของหน่วยงาน
43	มีการระบุขอบเขตเครือข่ายของบริการที่สำคัญและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ Direct and Significant Interface)	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.2	1	แผนผังเครือข่ายที่แสดงถึงขอบเขตเครือข่ายของบริการที่สำคัญ แผนผังเครือข่ายที่แสดงถึงขอบเขตเครือข่ายของบริการที่สำคัญและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ
44	มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.3	1	รายงานการตรวจสอบทะเบียนทรัพย์สินประจำปี
45	มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ตามรายการที่ระบุไว้ในทะเบียนทรัพย์สิน ที่ระบุบริการสำคัญ อย่างน้อยปีละ 1 ครั้ง	Identify | Asset MGT	กรอบมาตรฐาน ข้อ 21.1.4	1	รายงานการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ
46	มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้สำหรับการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด	Identify | Risk Assessment and Risk MGT Strategy	กรอบมาตรฐาน ข้อ 21.2.1	1	หลักฐานการกำหนดเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ที่กำหนดไว้สำหรับการบริหารความเสี่ยง (Risk Management) และสอดคล้องตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ภายใต้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)
				2	รายงานการประเมินความเสี่ยง

47	มีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	Identify | Risk Assessment and Risk MGT Strategy	กรอบมาตรฐาน ข้อ 21.2.2	1	ทะเบียนความเสี่ยง (Risk Register) ที่มีบันทึกการปรับปรุงทะเบียนดังกล่าว
48	มีการประเมินช่องโหว่โดยครอบคลุมบริการที่สำคัญซึ่งเป็นระบบเทคโนโลยีสารสนเทศ Information Technology System) หรือระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม Industrial Control System: ICS)	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.1	1	รายงานการประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน
				2	บันทึกการใช้ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ประเมินช่องโหว่อัตโนมัติ
				3	คู่มือการบริหารความเสี่ยงของหน่วยงาน
49	หน่วยงานของท่านได้ระบุขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญหรือไม่ (โดยขอบเขตดังกล่าวต้องครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม)	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.2	1	รายงานการประเมินช่องโหว่ของบริการที่สำคัญที่ได้ระบุขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญ
50	หน่วยงานของท่านได้ประเมินช่องโหว่ของบริการที่สำคัญก่อนที่จะทำการทดสอบระบบใหม่ที่จะเชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญกับบริการที่สำคัญหรือไม่ หมายเหตุ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี ทั้งนี้รวมถึงการเปลี่ยนไปใช้ระบบใหม่แทนที่ระบบเดิมด้วย	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.3	1	รายงานการทดสอบระบบใหม่ที่เชื่อมต่อกับบริการที่สำคัญ ที่ระบุวันเวลาในการทดสอบ หรือ รายงานการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ที่ระบุวันเวลาของการเปลี่ยนแปลง
				2	รายงานการประเมินช่องโหว่ของบริการที่สำคัญ ที่ระบุวันเวลาในการประเมิน
51	มีการพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.4	1	รายงานการทดสอบเจาะระบบ ที่แสดงให้เห็นถึงการดำเนินการที่สอดคล้องกับระดับของความเสี่ยง และผลกระทบที่อาจเกิดขึ้นจากการทดสอบเจาะระบบ
				2	รายงานการพิจารณาดำเนินการทดสอบเจาะระบบ ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือ รายงานการพิจารณาดำเนินการทดสอบเจาะระบบ ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบ
52	มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ Scope of a Penetration Test) ได้รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.5	1	รายงานการเจาะระบบ ตามขอบเขตของการทดสอบเจาะระบบที่ได้ถูกกำหนด
				2	เอกสารแสดงขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test)

53	มีการดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.6	1	รายงานการทดสอบเจาะระบบ
54	มีการตรวจสอบเพื่อให้แน่ใจว่าการทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระ	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.7	1	สัญญาจ้างบริการการทดสอบเจาะระบบ สัญญาจ้างบริการการทดสอบเจาะระบบ ที่กำหนดเงื่อนไขของระบบที่ใช้ทดสอบและผู้ทดสอบเจาะระบบ
				2	รายงานผลการประเมินบริการการทดสอบเจาะระบบ
55	มีการตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.8	1	รายงานผลการทดสอบเจาะระบบที่แสดงถึงผลการกำกับดูแลการทดสอบเจาะระบบของบุคลากรของหน่วยงาน
				2	สัญญาจ้างบริการการทดสอบเจาะระบบ ที่ระบุเงื่อนไขการดำเนินงานที่เกี่ยวข้อง
				3	เอกสารนโยบาย กระบวนการ และขั้นตอนการกำกับดูแลการทดสอบเจาะระบบของหน่วยงาน
56	มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ (ทั้งนี้หมายรวมถึง ช่องโหว่ของซอฟต์แวร์ ฮาร์ดแวร์ และระบบต่าง ๆ ที่ควบคุมการเข้าถึงทางกายภาพ)	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.9	1	เอกสารนโยบาย กระบวนการ และขั้นตอนการติดตามและจัดการช่องโหว่ที่อยู่ระหว่างการจัดทำ
				2	เอกสารนโยบาย กระบวนการ และขั้นตอนการติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์ที่ประกาศใช้ในหน่วยงาน
				3	รายงานการจัดการช่องโหว่ซอฟต์แวร์และฮาร์ดแวร์
				4	รายงานการสแกนช่องโหว่ของซอฟต์แวร์และฮาร์ดแวร์ทั้งก่อนและหลังการอัปเดตซอฟต์แวร์
				5	ภาพหน้าจอของระบบสแกนช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์
				6	เอกสารที่แสดงการจัดลำดับความสำคัญของช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์ และการทดสอบการติดตั้งแพตช์ ซึ่งสอดคล้องกับระดับความเสี่ยง
				7	รายงานการจัดการแพตช์ หรือ เฟิร์มแวร์
				8	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ติดตามและจัดการช่องโหว่อัตโนมัติ
				9	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้จัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์อัตโนมัติ
				10	รายงานการติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์
				11	รายงานการจัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์

				12	รายงานการจัดการแพตช์ (Patch) เฟริม์แวร์ และอัปเดตซอฟต์แวร์อัตโนมัติสำหรับแอปพลิเคชันและอุปกรณ์เครือข่าย รายงานการจัดการแพตช์ (Patch) เฟริม์แวร์ และอัปเดตซอฟต์แวร์อัตโนมัติสำหรับแอปพลิเคชันและอุปกรณ์เครือข่าย ทั้งหมด
				13	รายงานการวัดประสิทธิภาพของระบบติดตามและจัดการช่องโหว่ในซอฟต์แวร์และฮาร์ดแวร์อัตโนมัติ
				14	รายการฮาร์ดแวร์และซอฟต์แวร์ที่ใช้จัดการแพตช์ (Patch) เฟิร์มแวร์ และอัปเดตซอฟต์แวร์อัตโนมัติ
				15	รายงานผลการวิเคราะห์โค้ดของซอฟต์แวร์ในเชิงลึก
57	มีการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ ให้ กกม หรือ สกมช . ทราบภายใน 30 วัน นับจากที่ได้รับหนังสือร้องขอ	Identify | Vul. Assessment and Pentetration Testing	กรอบมาตรฐาน ข้อ 21.3.10	1	หนังสือนำส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ
				2	สำเนารายงานสรุปผลการทดสอบเจาะระบบ
58	หน่วยงานของท่านได้ระบุเกี่ยวกับความรับผิดชอบและภาระรับผิดชอบ (Responsible, Accountable) ของผู้ให้บริการภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ หรือด้านเทคโนโลยีด้านการปฏิบัติการ (Operational Technology) ในสัญญาการจัดซื้อจัดจ้าง	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.1	1	สัญญาจ้างผู้ให้บริการภายนอกหน่วยงาน
				2	ขอบเขตของงาน (TOR)
59	หน่วยงานของท่านมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก หรือไม่	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.2	1	ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement)
				2	เงื่อนไขด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญากับผู้ให้บริการภายนอก
60	มีกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.3	1	รายงานสรุปการให้บริการของผู้ให้บริการภายนอก ที่จัดทำโดยหรือที่ได้รับการตรวจสอบจากบุคลากรของหน่วยงาน
				2	เอกสารที่แสดงถึงกระบวนการตรวจสอบความสอดคล้องของผู้ให้บริการภายนอกกับข้อกำหนดหรือเงื่อนไขของสัญญา
61	หน่วยงานของท่านได้ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่	Identify | Third Party MGT	กรอบมาตรฐาน ข้อ 21.4.4	1	สัญญาจ้างผู้ให้บริการภายนอกหน่วยงานที่ได้รับการแก้ไขหลังจากการเจรจาต่อรองเงื่อนไขของสัญญาจ้าง เพื่อให้สอดคล้องข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่
62	มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากรกิจกรรม อุปกรณ์ และอินเทอร์เฟซ ที่ได้รับอนุญาตเท่านั้น	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.1	1	นโยบายความมั่นคงปลอดภัยไซเบอร์ของสารสนเทศในหน่วยงาน
				2	กลยุทธ์ นโยบาย และกระบวนการด้านการจัดการตัวตนและการเข้าถึง (Identity and Access Management)

				3	รายการฮาร์ดแวร์หรือซอฟต์แวร์ของระบบการจัดการตัวตนและการเข้าถึง (รวมถึง ระบบควบคุมการเข้าถึงทางกายภาพ)
				4	เอกสารที่ระบุบทบาทหน้าที่ และแสดงถึงการดำเนินงานของเจ้าหน้าที่ได้รับมอบหมายหน้าที่ในการพัฒนา จัดการและตรวจสอบตัวชี้วัดเกี่ยวกับประสิทธิภาพของการจัดการตัวตนและการเข้าถึง
				5	ข้อกำหนดการตั้งรหัส และการกำหนดวันหมดอายุของรหัสผ่าน
				6	แผนการปรับปรุงรายการผู้ใช้ และการปรับปรุงการให้สิทธิ์การเข้าถึง
				7	ผลการทบทวนการตั้งค่าใน Active Directory (แสดงถึง การเปิดใช้งาน Multi-factor Authentication)
				8	หลักฐานการตั้งค่าสำหรับการจัดการตัวตน และจำกัดการเข้าถึง
				9	หนังสือเวียนถึงบุคลากรเพื่อแจ้งให้ตรวจสอบสิทธิ์การเข้าถึงบริการที่สำคัญ
63	มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.2	1	รายการเทคนิคการตรวจสอบสิทธิ์ เช่น การใช้รหัสผ่าน รายการควบคุมการเข้าถึง (Access Control List) ไฟร์วอลล์ (Firewall) ระบบการจัดการเข้าถึงพิเศษ (Privileged Access Management: PAM)
				2	รายงานการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				3	โปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
64	มีการเก็บรักษาบันทึกของการเข้าถึงทั้งหมด Logs of All Accesses) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.3	1	หลักฐานที่มีการบันทึกการเข้าถึงและความพยายามเข้าถึงบริการที่สำคัญ (รวมถึงการบันทึกการเข้าถึงและความพยายามเข้าถึงเครือข่าย และเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับบริการที่สำคัญดังกล่าว)
				2	หลักฐานที่มีการบันทึกวิธีที่ผู้ใช้ที่ไม่มีสิทธิ์แต่พยายามเข้าถึงบริการที่สำคัญ (รวมถึงการบันทึกการเข้าถึงและความพยายามเข้าถึงเครือข่าย และเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับบริการที่สำคัญดังกล่าว)
65	มีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ และการเข้าถึงทางลอจิคอล Logical) มีการกำกับดูแลโดยหน่วยงาน	Protect | Access Control	กรอบมาตรฐาน ข้อ 22.1.4	1	นโยบายความมั่นคงปลอดภัยไซเบอร์ของสารสนเทศในหน่วยงาน
				2	รายการฮาร์ดแวร์หรือซอฟต์แวร์ของระบบการจัดการตัวตนและการเข้าถึง (รวมถึง ระบบควบคุมการเข้าถึงทางกายภาพ)
				3	กลยุทธ์ นโยบาย และกระบวนการด้านการจัดการตัวตนและการเข้าถึง (Identity and Access Management)

				4	เอกสารที่ระบุบทบาทหน้าที่ และแสดงถึงการดำเนินงานของเจ้าหน้าที่ที่ได้รับมอบหมายหน้าที่ในการพัฒนา จัดการและตรวจสอบตัวชี้วัดเกี่ยวกับประสิทธิภาพของการจัดการตัวตนและการเข้าถึง
				5	รายงานการกำกับดูแลของบุคลากรในหน่วยงาน เมื่อมีการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB และพอร์ตอนุกรม) หรือมีการเข้าถึงทางลอจิคอล Logical)
66	มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ Cybersecurity Risk Profile)	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.1	1	มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ
				2	โปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
				3	กระบวนการตรวจสอบความสอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
				4	รายการบริการที่สำคัญของหน่วยงาน
67	มีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ต่อไปนี้ (ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด Least Access Privilege) (ข) การแบ่งแยกหน้าที่ Separation of Duties) (ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน (ง) การลบบัญชีที่ไม่ได้ใช้ (จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก Vendor Support Application) (ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน (ช) การป้องกันมัลแวร์ Malware) และ (ซ) การปรับปรุงซอฟต์แวร์และแพตช Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.2	1	เอกสารที่แสดงมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของหน่วยงาน พร้อมระบุความสอดคล้องตามข้อ (ก)--(ซ)
68	มีการตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.3	1	หลักฐานบันทึกการใช้มาตรฐานการกำหนดค่าขั้นต่ำฯ ตามข้อ (ก)--(ซ) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย

69	มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.4	1	บันทึกหรือผลการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำฯ ประจำปี
				2	คู่มือปฏิบัติการในการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
70	มีกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ	Protect | System Hardening	กรอบมาตรฐาน ข้อ 22.2.5	1	กระบวนการหรือคู่มือปฏิบัติการจัดการเปลี่ยนแปลงของหน่วยงาน
				2	แบบฟอร์มที่เกี่ยวข้องกับการขออนุมัติการเปลี่ยนแปลงของหน่วยงาน
71	มีการตรวจสอบว่าระบบเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.3.1	1	นโยบาย แนวปฏิบัติในการเชื่อมต่อระยะไกลที่มายังบริการที่สำคัญ
				2	กระบวนการตรวจสอบการเชื่อมต่อระยะไกลทั้งหมดที่มายังบริการที่สำคัญ
				3	บันทึกหรือรายงานการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ
				4	กลไกการตรวจสอบการเชื่อมต่อที่มายังบริการที่สำคัญ
72	หน่วยงานของท่านปฏิบัติตามแนวปฏิบัติในการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานท่านมีองค์ประกอบข้อใดต่อไปนี้ (ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น (ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง Transmission Security) และความสมบูรณ์ของข้อความ Message Integrity) ที่แข็งแกร่ง (ค ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น (ง ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงาน เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ (จ จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ	Protect | Remote Connection	กรอบมาตรฐาน ข้อ 22.3.2	1	หลักเกณฑ์การพิจารณาอนุมัติให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล การพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) การเข้ารหัสสำหรับการเชื่อมต่อเครือข่าย การใช้คำสั่งระบบ (Issuing System Commands) และการจำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำ
				2	หนังสือขออนุมัติ/แบบฟอร์มร้องขอการเชื่อมต่อระยะไกล

73	มีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพากับบริการที่สำคัญ (ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ (ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น (ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน	Protect | Removable Storage Media	กรอบมาตรฐาน ข้อ 22.4.1	1	นโยบาย แนวปฏิบัติในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพากับบริการที่สำคัญของหน่วยงาน
				2	บันทึกการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB Storage) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา
				3	บันทึกการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ
				4	บันทึกการใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาต
74	มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้	Protect | Removable Storage Media	กรอบมาตรฐาน ข้อ 22.4.2	1	นโยบาย แนวปฏิบัติ (1) นโยบาย แนวปฏิบัติ หรือมาตรฐานการเข้ารหัสข้อมูลของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้
				2	บันทึกการเข้ารหัสข้อมูลที่ละเอียดอ่อนของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้
75	มีแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของหน่วยงานท่าน	Protect | Cybersecurity Awareness	กรอบมาตรฐาน ข้อ 22.5.1	1	แผนงานในการสร้างตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
				3	รายการกิจกรรมและกำหนดการจัดกิจกรรมที่เกี่ยวข้องในแผนงาน
				4	คู่มือปฏิบัติงานของบุคลากรทุกประเภท
76	มีการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม	Protect | Cybersecurity Awareness	กรอบมาตรฐาน ข้อ 22.5.2	1	ผลการทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี
77	กำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับบริการที่สำคัญ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว	Protect | Information Sharing	กรอบมาตรฐาน ข้อ 22.6.1	1	นโยบาย แนวปฏิบัติ คู่มือปฏิบัติการแสดงรายละเอียดขั้นตอนการแบ่งปันข้อมูลของหน่วยงาน

				2	แนวทางและรูปแบบในการแบ่งปันข้อมูล เช่น รายการซอฟต์แวร์หรือฮาร์ดแวร์ ที่ใช้งาน หรือ Community ที่เข้าร่วมเพื่อแบ่งปันข้อมูล เป็นต้น
				3	รายการหลักฐานการเข้าร่วมแบ่งปันข้อมูล เช่น การเข้าร่วมและแบ่งปันข้อมูลใน Community เป็นต้น
				4	มาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				5	รายการ MOAs, MOUs กับหน่วยงานที่มีการแบ่งปันข้อมูล
78	มีการสร้างกลไกและกระบวนการเพื่อ ตรวจจับ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ	Detect | Cyber Threat Detection and Monitoring	กรอบมาตรฐาน ข้อ 23.1.1	1	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				2	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการ เพื่อจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				3	รายการซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ในการตรวจจับเหตุการณ์ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				4	เอกสารที่มีรายละเอียดของกลไกหรือกระบวนการเพื่อระบุว่ายังมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
				5	รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
79	หน่วยงานมีการทบทวนกลไกและกระบวนการ ดังนี้ (1) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน (2) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ (3) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานหรือไม่ เพื่อตรวจจับ จัดประเภท วิเคราะห์และระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้ องกับบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง	Detect | Cyber Threat Detection and Monitoring	กรอบมาตรฐาน ข้อ 23.1.2	1	ผลการทบทวนกลไกและกระบวนการประจำปี
				2	คู่มือปฏิบัติการในการทบทวนกลไกและกระบวนการ
				3	ผลการทบทวน รายละเอียดขอบเขตของงาน (TOR) หรือสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (outsourcing)

				4	ผลการทบทวน ปรับปรุง ระดับการให้บริการในสัญญาจ้าง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก (Outsourcing)
80	มีการจัดทำสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง	Respond | Cybersecurity Incident Response Plan	กรอบมาตรฐาน ข้อ 24.1.1	1	ผลการ ทบทวน แผนการรับมือภัยคุกคามทางไซเบอร์ประจำปี
				2	คู่มือปฏิบัติการในการทบทวน แผนการรับมือภัยคุกคามทางไซเบอร์ ประจำปี
				3	แผนการรับมือภัยคุกคามทางไซเบอร์ ที่ปรับปรุงจากการทบทวน
				4	ผลการทบทวน รายละเอีย ดขอบเขตของงาน (TOR) หรือสัญญาจ้างที่เกี่ยวข้อง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก Outsourcing)
				5	ผลการเปลี่ยนแปลงรายละเอีย ดขอบเขตของงาน (TOR) หรือสัญญาจ้างที่เกี่ยวข้อง หากใช้บริการการดูแลจากการจัดจ้างบุคคลหรือหน่วยงานภายนอก Outsourcing)
81	มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.1	1	นโยบาย แนวปฏิบัติในการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
				2	แผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
82	มีแผนการสื่อสารในภาวะวิกฤตของหน่วยงานท่าน มีองค์ประกอบ ดังต่อไปนี้ (ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต (ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง (ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท (ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน (จ) ระบุแพลตฟอร์ม ช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.2	1	แผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
83	มีการตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.3	1	ผลการตรวจสอบแผนการสื่อสารในภาวะวิกฤตของหน่วยงาน
				2	กลไก คู่มือปฏิบัติงานในการตรวจสอบแผนการสื่อสารในภาวะวิกฤตของหน่วยงาน

84	มีการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการทดสอบแผนและความเข้าใจของทีมงาน	Respond | Crisis Communication Plan	กรอบมาตรฐาน ข้อ 24.2.4	1	ผลการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี
				2	แผนการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตประจำปี
85	มีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.1	1	รายการกิจกรรมฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ที่หน่วยงานเข้าร่วม
				2	หนังสือตอบรับการเข้าร่วมการฝึก
				3	ประกาศนียบัตรการเข้าร่วมกิจกรรม
86	มีการตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.1	1	รายงานการเข้าร่วมกิจกรรมฝึกซ้อมแผนรับมือภัยคุกคาม
				2	ประกาศนียบัตรการเข้าร่วมกิจกรรม
				3	รายชื่อผู้เข้าร่วมกิจกรรมการฝึกซ้อมแผนรับมือภัยคุกคาม
87	มีการปฏิบัติตามคำขอใดของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์	Respond | Cybersecurity Exercise	กรอบมาตรฐาน ข้อ 24.3.2	1	รายการคำขอจากคณะกรรมการ
				2	รายการกิจกรรมที่หน่วยงานปฏิบัติตามคำขอจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
				3	หนังสือตอบรับคำขอจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
88	มีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) เพื่อให้หน่วยงานสามารถกลับมาดำเนินการได้อย่างต่อเนื่อง	Recover | Cybersecurity Resilience and Recovery	กรอบมาตรฐาน ข้อ 25.1.1	1	แผนความต่อเนื่องทางธุรกิจของหน่วยงาน
				2	แนวทางการจัดทำแผนความต่อเนื่องทางธุรกิจของหน่วยงาน
89	มีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อทดสอบแผนเตรียมความพร้อมต่อสภาวะวิกฤตและพัฒนาปรับปรุงแผนให้มีประสิทธิภาพ	Recover | Cybersecurity Resilience and Recovery	กรอบมาตรฐาน ข้อ 25.1.2	1	แผนการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจของหน่วยงาน
				2	ผลการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจประจำปี

Regulator
(19 Controls)

	แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Reg)			
	D1 : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562			
ลำดับที่	**รายการ (Objective)**	**ที่มา (Requirement)**		**หลักฐาน (Evident)**
1	มีการกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศและหน่วยงานของรัฐ	พ.ร.บ. ไซเบอร์ ม.13(5)	1	เอกสารการกำหนดมาตรฐานการรับมือกับภัยคุกคามทางไซเบอร์ให้กับหน่วยงาน
2	มีการดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ. ไซเบอร์ ม.43	1	ผังโครงสร้างองค์กร (Organizational Chart) ที่มีการระบุตำแหน่งผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ เช่น มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) และ มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)
			2	เอกสารที่แสดงถึงบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)
			3	นโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์
			4	เอกสารความร่วมมือหรือหลักฐานการเข้าร่วมในโครงการต่าง ๆ ตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
			5	กรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
			1	เอกสารประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

3	มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ. ไซเบอร์ ม.44	2	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอาจเป็น เอกสาร เช่น ระเบียบ นโยบาย แนวปฏิบัติ ประกาศ แต่เอกสารดังกล่าวต้องมีรายละเอียดครบถ้วนประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
			3	หลักฐานที่แสดงว่าหน่วยงานใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ตามวรรคท้ายของมาตรา 44 ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4	มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ. ไซเบอร์ ม.45	1	เอกสารประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
			2	หลักฐานการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
5	มีการแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง	พ.ร.บ. ไซเบอร์ ม.46	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email หรือช่องทางอิเล็กทรอนิกส์อื่น ๆ ที่ได้แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวให้ สกมช. ทราบ

6	ในรอบปีนี้ หน่วยงานของท่าน ได้ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับหรือควบคุมดูแลแล้ว	พ.ร.บ. ไซเบอร์ ม.53	1	รายงานผลการตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน CII ที่อยู่ภายใต้การกำกับควบคุมดูแลของตน
7	มีการแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศปรับปรุงแก้ไข กรณีมีการดำเนินการที่ไม่สอดคล้องมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ. ไซเบอร์ ม.53	1	หลักฐานการดำเนินการตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแล และหลักฐานการแจ้งหน่วยงานที่มีการดำเนินการ ไม่สอดคล้องมาตรฐานขั้นต่ำให้ปรับปรุงแก้ไข
8	มีการดำเนินการส่งเรื่องให้ กกม. กรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพิกเฉยต่อการแก้ไขเพื่อการปฏิบัติให้สอดคล้องมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ. ไซเบอร์ ม.53	1	หลักฐานการแจ้งหน่วยงานที่มีการดำเนินการไม่สอดคล้องมาตรฐานขั้นต่ำให้ปรับปรุงแก้ไข และเอกสารที่ได้มีการส่งเรื่องให้ กกม.
9	เมื่อปรากฏแก่หน่วยงานของท่านหรือเมื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับหรือควบคุมดูแลได้แจ้งตามมาตรา 58 หน่วยงานของท่านร่วมกับ Sectoral CERT (หน่วยงานตามมาตรา 50) ได้มีการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ หรือไม่	พ.ร.บ. ไซเบอร์ ม.59	1	รายงานผลการตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์
10	เมื่อปรากฏแก่หน่วยงานของท่านหรือเมื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับหรือควบคุมดูแล ได้แจ้งเหตุตามมาตรา 58 หน่วยงานของท่านได้สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังกล่าว และให้ความร่วมมือและประสานงานกับ สกมช. ในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์	พ.ร.บ. ไซเบอร์ ม.59	1	หลักฐานการให้ความช่วยเหลือหรือการประสานงาน เช่น หนังสือขอความร่วมมือในการจัดการเหตุ การส่งบุคลากรเข้าร่วมประสานงานหรือเข้าร่วมแก้ไขเหตุการณ์
11	เมื่อปรากฏแก่หน่วยงานของท่าน หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้การกำกับหรือควบคุมดูแลได้แจ้งเหตุตามมาตรา 58 หน่วยงานของท่านได้แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลรวมทั้งหน่วยงานควบคุมหรือกำกับดูแลอื่นหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้อง	พ.ร.บ. ไซเบอร์ ม.59	1	หลักฐานการแจ้งเตือนหน่วยงานที่เกี่ยวข้อง เช่น หนังสือแจ้งเตือน Email หรือช่องทางการสื่อสารอื่น ๆ

แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Reg)

D2 : ประกาศ กมช เรื่องการกำหนดหลักการณ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงาน CII และการมอบหมายการควบคุมและกำกับดูแล

ลำดับที่	รายการ (Objective)	ที่มา (Requirement)		หลักฐาน (Evident)
12	มีการกำหนดแนวทางพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลของตนเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ประกาศ ม.49 หลักเกณฑ์ข้อ 2	1	เอกสารที่ระบุเกณฑ์ในการพิจารณาหน่วยงานที่อยู่ภายใต้การดูแลของตนว่าหน่วยงานใดเข้าข่ายที่จะเป็นหน่วยงาน CII เช่นเกณฑ์ที่ระบุ Threshold ของผลกระทบในด้านจำนวนผู้ใช้งาน
13	มีการแจ้งแนวทางพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลของตนเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต่อ สกมช. เพื่อทราบ	ประกาศ ม.49 หลักเกณฑ์ข้อ 2	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email ที่ได้แจ้งแนวทางการพิจารณาดังกล่าวให้ สกมช. ทราบ

	แบบประเมินการตรวจสอบว่าทำตามกฎหมาย พรบ ไซเบอร์ (Compliance Audit CheckList for Reg)				
	D3 : ประกาศ กมช เรื่องลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ สำหรับหน่วยงาน CII และภารกิจหรือบริการที่เกี่ยวข้อง				
ลำดับที่	**รายการ (Objective)**	**ชื่อองค์ประกอบ**	**ที่มา (Requirement)**		**หลักฐาน (Evident)**
14	ใน Sector ของท่านมีการจัดตั้งหรือดำเนินการให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Sectoral CERT) แล้ว		ประกาศหน้าที่ Sectoral CERT ข้อ 3	1	หลักฐานการจัดตั้งหรือการมีศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับ Sector เช่น เอกสารความร่วมมือในการจัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์
15	หน่วยงานของท่านได้จัดให้มีหลักเกณฑ์ เงื่อนไขและแนวทางในการพิจารณาคุณสมบัติและความเหมาะสมของการเป็น Sectoral CERT แล้ว		ประกาศหน้าที่ Sectoral CERT ข้อ 3	1	เอกสารหลักเกณฑ์ เงื่อนไขและแนวทางในการพิจารณาคุณสมบัติและความเหมาะสมของการเป็นศูนย์ประสาน
16	ในกรณีที่ Sector ของทา่ นได้มีการจัดตั้ง Sectoral CERT แล้ว ท่านได้มีการแจ้งการจัดตั้งดังกล่าว ให้ สกมช. ทราบแล้ว		ประกาศหน้าที่ Sectoral CERT ข้อ 4	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email ที่ได้แจ้งการจัดตั้งศูนย์ประสานฯ ให้ สกมช. ทราบ
17	ในรอบปีนี้ ท่านได้แจ้งรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้ สกมช. ทราบภายในเวลาที่ สกมช. กำหนด		ประกาศหน้าที่ Sectoral CERT ข้อ 4	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email ที่ได้แจ้งการจัดตั้งศูนย์ประสานฯ ให้ สกมช. ทราบ
18	กรณีที่ใน sector ของท่านมีการจัดตั้งเพิ่มเติม หรือมีการเปลี่ยนแปลงใด ๆ เกี่ยวกับ Sectoral CERT ให้แจ้งการจัดตั้งเพิ่มเติมหรือการเปลี่ยนแปลงดังกล่าวพร้อมข้อมูลที่เกี่ยวข้อง ต่อ สกมช. ทราบภายใน 30 วันนับแต่วันที่จัดตั้งเพิ่มเติมหรือเปลี่ยนแปลงแล้วเสร็จ		ประกาศหน้าที่ Sectoral CERT ข้อ 4	1	หลักฐานการแจ้ง เช่น สำเนาหนังสือแจ้งหรือ Email ที่ได้แจ้งการเปลี่ยนแปลงเกี่ยวกับศูนย์ประสานฯ ดังกล่าว
19	หาก sector ของท่าน อยู่ในระยะเริ่มต้นของการจัดตั้ง Sectoral CERT และยังไม่สามารถดำเนินภารกิจหรือให้บริการได้ครบถ้วนตามที่กำหนดในแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 หน่วยงานของท่านได้มีการกำหนดแนวทางการเริ่มต้นภารกิจหรือบริการร่วมกับ Sectoral CERT กรณีที่ศูนย์ประสานฯ ยังไม่สามารถดำเนินภารกิจหรือให้บริการได้ครบถ้วนตามที่กำหนด โดยอาจจัดทำแผนการปฏิบัติงานโดยแบ่งเป็นระยะต่าง ๆ ตามระดับความสำคัญและความพร้อมของหน่วยงาน และนำเสนอต่อ สกมช.		ประกาศหน้าที่ Sectoral CERT ข้อ 6	1	เอกสารแนวทางการเริ่มต้นภารกิจหรือบริการ ในระยะเริ่มต้นของการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัย