การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management)

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Practice Guidelines)

เอกสารโดย
ส่วนสารสนเทศและพัฒนาระบบ
โรงงานไพ่ กรมสรรพสามิต

รหัสเอกสาร IT-DOC-NCSA-002
ปรับปรุงล่าสุด 30 กรกฎาคม 2567

บทนำ

บทนำ

ตามที่โรงงานไพ่ กรมสรรพสามิต ได้ออกประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนั้น กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ปีละ 1 ครั้ง โดยฝ่ายตรวจสอบภายใน เพื่อตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ของโรงงานไพ่ กรมสรรพสามิต และทำให้หน่วยงานได้ทราบถึงระดับความมั่นคงปลอดภัยไซเบอร์

ส่วนสารสนเทศและพัฒนาระบบ ในฐานะหน่วยงานที่มีหน้าที่ดูแลความมั่นคงปลอดภัยไซเบอร์ ของโรงงานไพ่ กรมสรรพสามิต จึงได้จัดทำแนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โรงงานไพ่ กรมสรรพสามิต เพื่อให้องค์กรมีกรอบแนวทางปฏิบัติด้านการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

เพื่อกำหนดแนวทางการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ตรวจสอบ

สารบัญ

บทที่ 1
แผนการตรวจสอบความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

1. ผู้เกี่ยวข้องกับกระบวนการตรวจสอบ

1) เจ้าหน้าที่ตรวจสอบภายใน คณะกรรมการตรวจสอบ หรือผู้ที่ได้รับมอบหมาย ในฐานะผู้ตรวจสอบ
2) ส่วนสารสนเทศและพัฒนาระบบ ในฐานะผู้ถูกตรวจสอบ
3) ผู้มีส่วนได้ส่วนเสีย ผู้ใช้งานระบบเครือข่าย ผู้ใช้งานระบบสารสนเทศ

2. การอ้างอิงการตรวจสอบตามกฎหมาย

เอกสารนี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3. การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยผู้มีอำนาจ เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่ฯ ทั้งนี้ มีเกณฑ์การพิจารณามี 2 ประการ ได้แก่ ความเป็นอิสระและความสามารถที่หน่วยตรวจสอบภายในหรือทีมงาน (Audit Firm/Team) และผู้ตรวจสอบ (Auditors) ต้องปฏิบัติตาม ดังนี้

1) ไม่อยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้มหรือได้รับรู้ผลประโยชน์ทับซ้อน

2) มีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่

4. ความคาดหวังในการตรวจสอบ

โรงงานไพ่ฯ ได้ระบุความคาดหวังในการตรวจสอบไว้ 7 ประการ ดังนี้

4.1 หลักการตรวจสอบ (Principles of Auditing)

การตรวจสอบควรยึดหลักการต่อไปนี้

1) ความซื่อสัตย์ (Integrity)
   - ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
   - ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
   - ดำเนินการตรวจสอบอย่างเป็นกลาง
   - ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ
2) การนำเสนออย่างยุติธรรม (Fair Presentation): การรายงานตามความเป็นจริงและถูกต้อง
   - ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
   - รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่าง
   - ทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ

- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

3) การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

4) การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์
- ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

5) ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบ

- และความเที่ยงธรรมของข้อสรุปการตรวจสอบ
- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
- ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
- รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (Audit Evidence) เท่านั้น

4.2 วัตถุประสงค์ในการตรวจสอบ

1) เพื่อตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

2) เพื่อประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

4.3 ขอบเขตการตรวจสอบ

ขอบเขต	คำอธิบาย
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

4.4 แนวทางการตรวจสอบ

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (Compliance Approach) และตามความเสี่ยง (Risk-based Approach)

1) การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

2) ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่โรงงานไพ่ฯ เผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

4.5 ข้อค้นพบการตรวจสอบ

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้

1) ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

2) เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

3) เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (Corrective Action) แล้วก็ตาม

4) เน้นแนวปฏิบัติที่ดี (Good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

องค์ประกอบ	คำอธิบาย
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (Root Cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ(ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

4.6 สรุปผลการตรวจสอบ

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

1) ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

2) ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

4.7 รูปแบบรายงานการตรวจสอบ

รายงานการตรวจสอบควรมีอย่างน้อยดังต่อไปนี้ :

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ 4.2 ของเอกสารนี้
ขอบเขตการตรวจสอบ	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน 4.3 ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และวิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน 4.6 ของเอกสารนี้
สรุปการตรวจสอบ	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน 4.6 ของเอกสารนี้

5. ขั้นตอนการปฏิบัติในการตรวจสอบ

1) ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

2) ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ

- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

3) ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4) ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ
- ข้อเสนอแนะในการปรับปรุง
- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

5) ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

6) คณะทำงานรับทราบผลการตรวจสอบ

7) ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับในการตรวจสอบ

8) คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

9) คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

10) ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

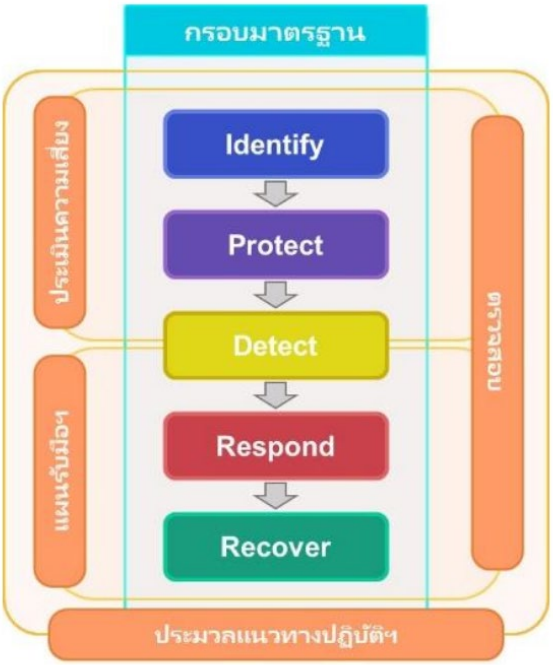
บทที่ 2
แนวปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับ ภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคง ปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบ ดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



เอกสารฉบับนี้ เป็นการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการความเสี่ยงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงานและยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน

หน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสม และได้มาตรฐานเพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงและเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงของโรงงานไพ่ฯ โดยการประเมินความเสี่ยงทำให้สามารถ

- ระบุเหตุการณ์ความเสี่ยงที่เป็นภัยคุกคาม และอาจนำไปสู่กระทบต่อโรงงานไพ่ฯในด้านต่างๆ
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมองค์กรเพื่อให้บุคลากรมีส่วนร่วมในการจัดการเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2. วัตถุประสงค์

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีกรอบการดำเนินงานเกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

3. กลุ่มเป้าหมาย

กลุ่มเป้าหมายของเอกสารนี้:

ก. ผู้ประเมินความเสี่ยง

ข. หน่วยงานทางโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ค. ผู้มีส่วนได้ส่วนเสีย ผู้ใช้งานระบบเครือข่าย ระบบสารสนเทศของโรงงานไพ่ กรมสรรพสามิต พนักงานของโรงงานไพ่ กรมสรรพสามิต นักเรียน นักศึกษา

4. ขอบเขต

เอกสารฉบับนี้เป็นกรอบแนวทางการดำเนินงาน เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่ กรมสรรพสามิต

5. สร้างบริบทความเสี่ยง

เป็นการสร้างข้อกำหนดที่สำคัญสำหรับการประเมินความเสี่ยง เพื่อให้กลุ่มเป้าหมาย ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

นิยามความเสี่ยง

5.1 ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายของหน่วยงาน ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน งบประมาณ และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

5.2 ภัยคุกคามไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบ

คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

5.3 การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หมายถึง การดำเนินการในการป้องกันภัยคุกคามไซเบอร์โดยใช้มาตรการ และกระบวนการบริหารความเสี่ยง เพื่อวิเคราะห์ภัยคุกคามไซเบอร์ ประเมินความเสี่ยงที่อาจจะเกิดขึ้น โดยการจัดหา จัดทำมาตรการ จัดหาวัสดุอุปกรณ์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์ ความมั่นคงปลอดภัยไซเบอร์หมายถึง วิธีการ มาตรการ หรือการดำเนินการใดๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งาน ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศของโรงงานไพ่ฯ

5.4 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด ทำไม และเกิดขึ้นได้อย่างไร ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

5.5 การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 5 ระดับ คือ สูงมาก สูง ปานกลางต่ำ และต่ำมาก

5.6 การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้ ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง ดังนี้

- **การยอมรับความเสี่ยง (Risk Acceptance)** เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง
- **การลด/การควบคุมความเสี่ยง (Risk Reduction)** เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
- **การกระจายความเสี่ยงหรือการโอนความเสี่ยง (Risk Sharing)** เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้อื่นช่วยแบ่งความรับผิดชอบไป
- **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงและหน่วยงานไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมนั้นไป

5.7 การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ

- การควบคุมเพื่อการป้องกัน
- การควบคุมเพื่อให้ตรวจสอบ
- การควบคุมโดยการชี้แนะ
- การควบคุมเพื่อการแก้ไข

6. หลักการบริหารความเสี่ยง

หลักการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Treadway Commission) และ ISO 27001 มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุปัจจัยเสี่ยง (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. การระบุวิธีการจัดการความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

6.1 การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เพื่อให้โรงงานไพ่ฯมีระบบในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่ฯโดยสามารถดำเนินการอย่างมีประสิทธิภาพ และบรรลุเป้าหมายตามแผนยุทธศาสตร์ของโรงงานไพ่ฯ จึงได้ตั้งเป้าหมายในการดำเนินการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังตารางที่ 6.1

ตารางเป้าหมายในการดำเนินการบริหารความเสี่ยงตัวชี้วัดความสำเร็จ

เป้าหมายในการดำเนินการบริหารความเสี่ยง	ตัวชี้วัดความสำเร็จ
1. เพื่อให้โรงงานไพ่ฯมีแผนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และดำเนินการตามแผนอย่างครบถ้วน	มีแผนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการรายงานผล การดำเนินการตามแผนการบริหารความเสี่ยงใน ทุก ๆ ปีงบประมาณ
2.เพื่อให้ผู้บริหารและบุคลากรทุกระดับใน โรงงานไพ่ฯ มีความรู้ ความเข้าใจกระบวนการ บริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	- ผู้บริหารและบุคลากรมีความรู้ความเข้าใจในหลักการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มีหลักสูตร e-courseware เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างความรู้ความเข้าใจให้บุคลากร นักเรียน นักศึกษาของโรงงานไพ่ฯ
3. เพื่อให้โรงงานไพ่ฯสามารถบริหารจัดการความ เสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ทันเวลาจนป้องกันและลดความเสี่ยงให้ อยู่ในระดับที่ยอมรับได้	มีการประเมินผลความสำเร็จในการดำเนินการตามแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยระดับความเสี่ยงที่ เหลืออยู่ต้องอยู่ในระดับที่ยอมรับได้

6.2 การระบุปัจจัยเสี่ยง (Event Identification)

ปัจจัยเสี่ยง (Risk Factor) คือ สาเหตุที่มาของความเสี่ยง ที่ทำให้ไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่วางไว้ การระบุปัจจัยเสี่ยงควรมีความเชื่อมโยงกับผลความสำเร็จตามเป้าหมายของโรงงานไพ่ฯ โดยคำนึงถึงวัตถุประสงค์ตามแผนงานของหน่วยงาน และโอกาสของเหตุการณ์ที่อาจจะเกิดขึ้น อันจะส่งผลกระทบต่อหน่วยงาน ทำให้ไม่สามารถบรรลุวัตถุประสงค์นั้นได้ โรงงานไพ่ฯ ได้จัดประเภทของความเสี่ยงในการระบุความเสี่ยง ออกเป็น 9 ประเภทด้วยกัน และได้กำหนดเกณฑ์ดังกล่าว เพื่อใช้ในการระบุปัจจัยเสี่ยงแยกตามประเภท ความเสี่ยงของหน่วยงานทุกระดับในโรงงานไพ่ฯ ดังนี้

ประเภทของความเสี่ยง

1) ความเสี่ยงด้านกลยุทธ์(Strategic Risk) ตัวย่อ S ความเสี่ยงที่เกี่ยวกับการบรรลุเป้าหมาย และพันธกิจในภาพรวม โดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยงเนื่องจากการ เปลี่ยนแปลงของสถานการณ์และเหตุการณ์ภายนอก ส่งผลต่อกลยุทธ์ที่กำหนดไว้ ไม่สอดคล้องกับประเด็นยุทธศาสตร์/วิสัยทัศน์ หรือเกิดจากการกำหนดกลยุทธ์ที่ขาดการ มีส่วนร่วม ทำให้โครงการขาดการยอมรับและโครงการไม่ได้นำไปสู่การแก้ไขปัญหาหรือการตอบสนองต่อความต้องการของผู้รับบริการหรือผู้มีส่วนได้ส่วนเสียอย่างแท้จริง หรือเป็น ความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาด หรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

2) ความเสี่ยงด้านการเงินและทรัพย์สิน (Financial and Asset Risk) ตัวย่อ F ความเสี่ยงที่ เกี่ยวกับการเงินและทรัพย์สิน ซึ่งมีผลทำให้โรงงานไพ่ฯต้องมีรายได้ลดน้อยลง หรือ ค่าใช้จ่ายเพิ่มขึ้น หรือความเสียหายต่อทรัพย์สินของโรงงานไพ่ฯ การจัดการความเสี่ยงจึงมีลักษณะของการปกป้องทรัพย์สิน การเงิน และมาตรการประหยัดค่าใช้จ่าย

3) ความเสี่ยงด้านปฏิบัติงาน (Operational Risk) ตัวย่อ O ความเสี่ยงที่เกิดขึ้นใน กระบวนการทำงานตามปกติทุกขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับ กระบวนการ เทคโนโลยีสารสนเทศ วัสดุ/อุปกรณ์ บุคลากรที่ปฏิบัติงาน ฯลฯ ซึ่งจะส่งผลกระทบต่อ ความสำเร็จของการดำเนินงานตามแผนปฏิบัติการหรือแผนกลยุทธ์ของโรงงานไพ่ฯ

4) ความเสี่ยงด้านกฎระเบียบ (Compliance Risk) ตัวย่อ C ความเสี่ยงที่เกี่ยวข้องกับ การปฏิบัติตามกฎ ระเบียบต่าง ๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจาก ความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับ ต่าง ๆ รวมถึงการทำนิติกรรมสัญญา การร่างสัญญาที่ไม่ครอบคลุมการดำเนินงานจากเหตุการณ์ภายนอก

5) ความเสี่ยงด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk) ตัวย่อ IM ภาพพจน์ของโรงงานไพ่ฯอาจเกิดความเสียหาย เนื่องจากมีการเผยแพร่ข่าวสื่อเชิงลบ ในระดับจังหวัด ระดับชาติ และระดับนานาชาติ

6) ความเสี่ยงด้านสุขภาพและความปลอดภัย (Health and Safety Risk) ตัวย่อ HS ความเสี่ยงเกี่ยวกับการเกิดอุบัติเหตุ การบาดเจ็บ ความเจ็บป่วยที่เกิดขึ้นกับนักศึกษาและบุคลากร ของโรงงานไพ่ฯ

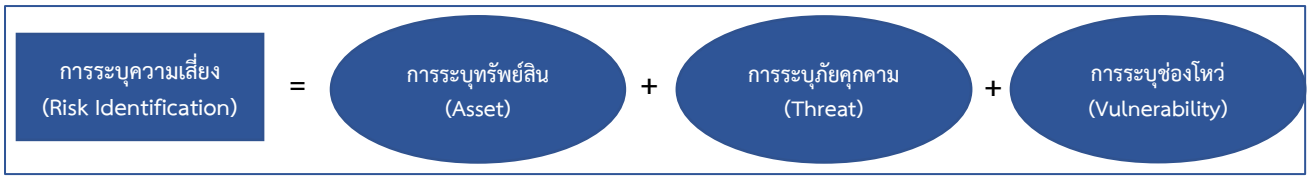
7) ความเสี่ยงด้านบุคลากร (Personnel Risk) ตัวย่อ P ความเสี่ยงที่เกี่ยวข้องกับพนักงาน ของโรงงานไพ่ฯ เป็นความเสี่ยงจากบุคลากรสายวิชาการ และบุคลากรสายปฏิบัติการ ความเสี่ยงนี้ครอบคลุมถึงการบริหารงานบุคคล เช่น อัตราการลาออกของพนักงานโรงงานไพ่ฯ

8) ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk) ตัวย่อ D เป็นความเสี่ยง เกี่ยวกับการจัดการเทคโนโลยีดิจิทัลของแต่ละหน่วยงานในการกำหนดให้มีการจัดการ ความเสี่ยงตามพื้นฐานความจำเป็นของงานแต่ละงาน เช่น การรักษาความปลอดภัยของ ข้อมูล การเรียกข้อมูลกลับคืน เป็นต้น

9) ความเสี่ยงด้านธรรมาภิบาลและอัตตาภิบาล (Good Governance and Self Governance Risk) ตัวย่อ G เป็นความเสี่ยงที่อาจเกิดขึ้นในกระบวนงานหลักขององค์กร เพื่อให้มั่นใจได้ว่าการดำาเนินการเป็นไปตามหลักธรรมาภิบาลและอัตตาภิบาล เช่น ความมี ประสิทธิภาพ ความคุ้มค่า โปร่งใส ตรวจสอบได้ เป็นต้น รวมถึงความเสี่ยงในการกำกับดูแลตนเองที่ดีด้วย

การบ่งชี้ความเสี่ยง (Risk identification)

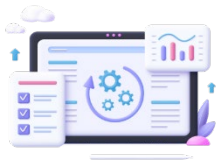
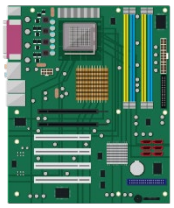
เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อเป้าหมายขององค์กรหรือการปฏิบัติงานทั้งในระดับองค์กรและกิจกรรม เช่น ทรัพย์สิน ภัยคุกคาม ห่องโหว่ด้านความปลอดภัย



ภาพการบ่งชี้ความเสี่ยงตามแนวทางของมาตรฐานสากล ISO/IEC 27005

สินทรัพย์สารสนเทศ

ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น มีวัตถุประสงค์เพื่อบริหารกิจกรรมของโรงงานไพ่ กรมสรรพสามิต ให้บรรลุพันธกิจของโรงงานไพ่ กรมสรรพสามิต

ระบุประเภททรัพย์สินสารสนเทศ (Identification of Asset Types)			
กลุ่มทรัพย์สินหลัก (Primary Asset)	กลุ่มทรัพย์สินสนับสนุน (Supporting Asset)		
			
กระบวนการทำงาน	**ฮาร์ดแวร์**	**ซอฟต์แวร์**	**สถานที่ (Site)**
			
ข้อมูลและสารสนเทศ	**เครื่องแม่ข่ายเสมือน (Virtual Machine)**	**บุคลากร (Personnel)**	**องค์กร (Organization)**

อาคารสถานที่

1) พื้นที่ตั้งสำนักงาน โรงงานไพ่ กรมสรรพสามิต ณ อาคารโรงงานไพ่ กรมสรรพสามิต ชั้น 2

2) ห้องเครือข่ายหลัก (Internet Data Center) ณ อาคารโรงงานไพ่ กรมสรรพสามิต ชั้น 3 เป็นห้องสำหรับจัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์จัดเก็บข้อมูล ประกอบไปด้วยสิ่งที่สำคัญดังนี้ สำรองไฟฟ้า (UPS) ระบบปรับอากาศ ระบบตรวจจับควันไฟ ระบบดับเพลิง และระบบรักษาความปลอดภัยของการเข้า-ออก

3) DR-Site ณ อาคารเทคโนโลยีสารสนเทศ ชั้น 3 เป็นห้อง Internet Data Center สำรองแห่งที่ 2 สำหรับการจัดทำ Backup & Recovery ข้อมูลจัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์จัดเก็บข้อมูล และระบบที่สำคัญดังนี้ สำรองไฟฟ้า (UPS) ระบบเครื่องกำเนิดไฟฟ้า (Generator) ระบบปรับอากาศ ระบบตรวจจับควันไฟ ระบบดับเพลิง และระบบรักษาความปลอดภัยของการเข้า-ออก

3) ห้องสำนักงานอำนวยการจำนวน 17 ห้องห้องฝ่ายผลิตไพ่ 3 ห้อง ห้องฝ่ายโรงพิมพ์ 3 ห้อง

รายการอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

ลำดับที่	รายละเอียด	จำนวน
1	อุปกรณ์ให้บริการระบบเครือข่าย	
	- อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Access Point)	16 ชุด
	- อุปกรณ์กระจายสัญญาณเครือข่าย (Switch Hub)	17 ชุด
	- อุปกรณ์แปลงสัญญาณด้วยการเชื่อมต่อแบบใยแก้วนำแสง (Fiber Converter)	1 ชุด
	- อุปกรณ์กำหนดเส้นทางเครือข่ายและเชื่อมต่ออินเทอรเน็ต (Internet Gateway Router)	2 ชุด
	- ผู้ให้บริการอินเทอร์เน็ต (nt CAT และ ntTOT)	2 ISP
	- อุปกรณ์กระจายการทำงานสำหรับเครือข่าย (Link Load Balancer)	1 ชุด
	- อุปกรณ์ป้องกันเครือข่าย (Firewall)	
	- อุปกรณ์ป้องกันเครือข่าย (IPS)	2 ชุด
	- อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	1 ชุด
2	อุปกรณ์ให้บริการจัดเก็บระบบสารสนเทศ	
	- เครื่องคอมพิวเตอร์แม่ข่ายแบบกายภาพ (Physical Machine)	10 ชุด
	- เครื่องคอมพิวเตอร์แม่ข่ายแบบจำลองกายภาพ (Virtual Machine)	3 ชุด
	- ระบบสำรองและกู้คืนข้อมูลระบบแบบออฟไลน์	1 ชุด
	- ระบบสำรองและกู้คืนข้อมูลระบบแบบออนไลน์	1 ชุด
	- ระบบกล้องวงจรปิด	2 ชุด
	- กล้องวงจรปิด	42+8 ชุด
3	อุปกรณ์ให้บริการระบบโทรศัพท์	
	- โทรศัพท์ระบบ Analog	42 คู่สาย
	- เครื่องโทรสาร	2 เครื่อง
4	Hardware ให้บริการที่สำคัญ	
	- เครื่องคอมพิวเตอร์แบบ Desktop	1 ชุด
	- เครื่องคอมพิวเตอร์แบบ Notebook	78 เครื่อง
	- เครื่องถ่ายเอกสาร	X ชุด
	- เครื่องพิมพ์	6 ชุด
	- เครื่องสแกนเอกสาร	6 ชุด
	- เครื่องฉายภาพ	3 ชุด
	- ชุดอุปกรณ์สำหรับการประชุมออนไลน์ (ไมโครโฟน, ลำโพง, กล้อง Webcam)	2 ชุด
5	Software ให้บริการที่สำคัญ	
	- ระบบการสื่อสารแบบรวมศูนย์ (workD)	90 ผู้ใช้งาน
	- ระบบการประชุมอิเล็กทรอนิกส์	1 ชุด
	- ระบบบริหารทรัพยากรองค์การ	29 ผู้ใช้งาน
6		

ระบบสารสนเทศ-ระบบฐานข้อมูล

ลำดับที่	ระบบ	หน่วยงาน	หมายเหตุ
1	ระบบสารบรรณอิเล็กทรอนิกส์	ส่วนบริหารงานกลาง	
2	ระบบทรัพยากรบุคคล	ส่วนทรัพยากรบุคคล	
3	ระบบบริหารทรัพยากรองค์การ	ฝ่ายตรวจสอบภายใน ฝ่ายโรงพิมพ์ ฝ่ายผลิตไพ่ ส่วนสารสนเทศและพัฒนาระบบ ส่วนทรัพยากรบุคคล ส่วนแผนงานและกลยุทธ์ ส่วนบัญชีและการเงิน ส่วนพัสดุและอาคารสถานที่ ส่วนผลิตสิ่งพิมพ์ ส่วนเตรียมการพิมพ์ ส่วนผลิตไพ่ป๊อก ส่วนผลิตไพ่ตัวเล็ก	
4	ระบบอินทราเน็ต	โรงงานไพ่ฯ	
5	ระบบเว็บไซต์หน่วยงาน	โรงงานไพ่ฯ	
6	ระบบการสื่อสารแบบรวมศูนย์ (workD)	โรงงานไพ่ฯ	
7	ระบบกรมบัญชีกลาง	ส่วนพัสดุและอาคารสถานที่	
8	ระบบประชุมอิเล็กทรอนิกส์	โรงงานไพ่ฯ	
9	ระบบ Microsoft 365	โรงงานไพ่ฯ	
10	ระบบแจ้งปัญหาการใช้งานผ่านระบบอินเทอร์เน็ต	โรงงานไพ่ฯ	

จำนวนบุคลากรผู้ปฏิบัติงานด้านสารสนเทศ

ลำดับที่	หน่วยงาน	ตำแหน่ง	จำนวน (คน)
1	ส่วนสารสนเทศและพัฒนาระบบ	เจ้าหน้าที่สารสนเทศ	4

เหตุการณ์ภัยคุกคาม (Threat Event)

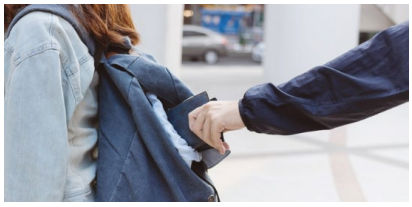
เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์การโจมตี (Threat Vector)) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

- Ransomware (แรนซัมแวร์) ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถ

ล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware

- Phishing (ฟิชชิง) คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่น การส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล
- Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น
- Virus (ไวรัส) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างซึ่งโดยมุ่งเน้นในการโจมตี ขัดขวาง เพื่อไม่ให้ระบบสามารถใช้งานได้
- Worms (เวิร์ม) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้
- Trojan (โทรจัน) เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้
- Spyware (สปายแวร์) ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล
- Adware (แอดแวร์) คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้
- Data leaks (ข้อมูลรั่วไหล) ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

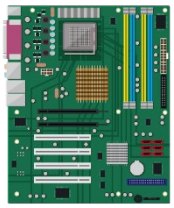
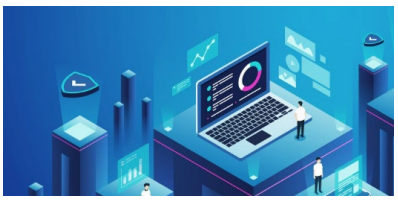
การระบุภัยคุกคาม (Threat)

		
อัคคีภัย	Hacker	Malware
		
การโจรกรรมอุปกรณ์	**ข้อมูลรั่วไหล**	**อุทกภัย**

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ

การระบุช่องโหว่ (Vulnerability)

		
Access Control	**บุคลากร**	**ขั้นตอน**
		
Software	Hardware	**สภาพแวดล้อมทางกายภาพ**

6.3 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้ การใช้มาตรการรักษาความปลอดภัยทางไซเบอร์ โดยระบุค่าโอกาสของความเสี่ยง และค่าผลกระทบ

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน

- ผลกระทบที่เกิดขึ้น (Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

เกณฑ์การให้คะแนนค่าโอกาสของความเสี่ยง

คำอธิบาย ขั้นตอนนี้เป็นการระบุค่าโอกาสการเกิดเหตุการณ์ว่าจะอยู่ในระดับเป็นไปได้ มากหรือน้อยเพียงใด โดยจัดค่าโอกาสการเกิดเหตุการณ์ ออกเป็น 5 ระดับ

ตารางเกณฑ์การให้คะแนนค่าโอกาสของความเสี่ยง

ระดับ	เชิงปริมาณ	เชิงคุณภาพ
1	0–1 ครั้งต่อปี	อาจเกิดขึ้นเฉพาะในสถานการณ์ที่ไม่ปกติบางกรณี
2	2–3 ครั้งต่อปี	อาจจะเกิดขึ้นน้อยมาก
3	4–5 ครั้งต่อปี	เป็นไปได้ ที่เกิดขึ้นในบางครั้ง
4	6 ครั้งต่อปี	เป็นไปได้มาก คาดหมายว่าจะเกิดขึ้นค่อนข้างบ่อย
5	ตลอดทั้งปี (มากกว่า 6 ครั้งต่อปี)	ค่อนข้างแน่นอน คาดหมายว่าจะเกิดขึ้นในสถานการณ์ส่วนใหญ่

เกณฑ์การให้คะแนนค่าผลกระทบ

คำอธิบาย คณะกรรมการบริหารความเสี่ยงและการควบคุมภายในโรงงานไพ่ฯ ได้กำหนด เกณฑ์การหาค่าผลกระทบ ออกเป็น 5 ระดับ ตามประเภทของความเสี่ยง ไว้ทั้งหมด 9 ประเภท (ตามหัวข้อที 6.2.1) โดยเกณฑ์ การหาค่าผลกระทบที่ปรากฏในแต่ละประเภทนี้ เป็นกรอบหลักในการพิจารณา

1) เกณฑ์การให้คะแนนค่าผลกระทบด้านกลยุทธ์ (S: Strategic Risk)

ระดับ	ด้านกลยุทธ์	ความหมาย
1	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป
2	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับ ร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานน้อยกว่าหรือเท่ากับร้อยละ 60

2) เกณฑ์การให้คะแนนค่าผลกระทบด้านการเงินและทรัพย์สิน (F: Financial)

ระดับ	ด้านกลยุทธ์	ความหมาย
1	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป

ระดับ	ด้านกลยุทธ์	ความหมาย
2	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับ ร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานน้อยกว่าหรือเท่ากับร้อยละ 60

3) เกณฑ์การให้คะแนนค่าผลกระทบด้านปฏิบัติงาน (O: Operational Risk)

ระดับ	ด้านกลยุทธ์	ความหมาย
1	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป
2	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับ ร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานน้อยกว่าหรือเท่ากับร้อยละ 60

4) เกณฑ์การให้คะแนนค่าผลกระทบด้านกฎระเบียบ (C: Compliance Risk)

ระดับ	ด้านกลยุทธ์	ความหมาย
1	ได้ผลงานตามเป้าหมาย มากกว่าร้อยละ 90 ขึ้นไป	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานมากกว่าร้อยละ 90 ขึ้นไป
2	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 81 – 90	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 81 – 90
3	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 71 – 80	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 71 – 80
4	ได้ผลงานตามเป้าหมาย ตั้งแต่ร้อยละ 61 – 70	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานตั้งแต่ร้อยละ 61 – 70
5	ได้ผลงานตามเป้าหมายน้อยกว่าหรือเท่ากับ ร้อยละ 60	หน่วยงานสามารถปฏิบัติให้เป็นไปตามแผนกลยุทธ์ได้ผลงานน้อยกว่าหรือเท่ากับร้อยละ 60

5).เกณฑ์การให้คะแนนค่าผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์ (CS: Cyber security risk)

ระดับ	ด้านกลยุทธ์	ความหมาย
5	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงงานไพ่ฯ	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน ทั้งนี้ไม่ส่งผลต่อความเสียหายแก่โรงงานไพ่ฯ
4	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) ทั้งนี้ส่งผลต่อความเสียหายแก่โรงงานไพ่ฯ	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน ทั้งนี้ส่งผลต่อความเสียหายแก่โรงงานไพ่ฯ
3	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited)ทั้งนี้ส่งผลต่อความเสียหายแก่โรงงานไพ่ฯ และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)
2	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)
1	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)

6.4 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication) การสื่อสารทำความเข้าใจเกี่ยวกับแผนความเสี่ยงด้านสารสนเทศให้บุคลากรที่เกี่ยวข้องทราบสามารถนำไป ปฏิบัติได้ และรายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยงด้านสารสนเทศตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 : 2013) ใน 3 ด้าน คือ

ด้านบุคคล (People)

1) การสร้างความตระหนักของการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศ โดยการพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (People)

2). สร้างความตระหนักและการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Awareness) สำหรับผู้ใช้งาน (User) และวิธีการตรวจสอบช่องโหว่ Vulnerability Assessment

(Web Application Hacking) และการเจาะระบบ (Penetration Testing) สำหรับผู้ดูแลระบบ (System Administrator)

3).การพัฒนากำลังคนผู้ปฏิบัติงานด้านการรักษาความปลอดภัยไซเบอร์

4) การพัฒนากำลังคนผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)

5) การฝึกซ้อมรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber drill) เพื่อให้บุคลากร และผู้บริหาร มีการเตรียมความพร้อมรับสถานการณ์การโจมตี (Cyber Drill) มีความเข้าใจและตระหนักถึงภัยจากการโจมตีทางอิเล็กทรอนิกส์ที่อยู่ใกล้ตัว เพราะเมื่อการโจมตีเกิดขึ้นจะได้ไม่ตกเป็นเหยื่อ โดยรู้เท่าไม่ถึงการณ์ที่การบริหารความมั่นคงปลอดภัยขององค์การในอนาคตต้องมีรูปแบบเป็น “Cyber Resilience” ซึ่งหมายถึง ระบบต้องมีความสามารถในการรองรับการโจมตีและจะต้องสามารถทำงานหรือให้บริการได้อย่างต่อเนื่อง ไม่ทำให้เกิดความเสียหายต่อภารกิจและภาพลักษณ์ขององค์การ ภาพลักษณ์ของผู้บริหาร ดังนั้นแนวคิดของ Information Security Management ในรูปแบบเดิมๆ จึงไม่ครอบคลุม เพียงพอ จำเป็นต้องนำแนวคิด Cyber Security Resilience Framework (Cyber Security Centric and Cyber Resilience in Action) มาปรับใช้ในองค์กรด้วย

ด้านกระบวนการ (Process)

ขั้นตอน นโยบาย ระเบียบ ข้อบังคับและแนวปฏิบัติสำคัญต่าง ๆ ที่เป็นแนวทางในการปฏิบัติตนทั้งในสิ่งที่ต้องทำ ควรทำ และไม่ควรทำ รวมถึงการระบุบทบาทหน้าที่ความรับผิดชอบ เป็นส่วนสนับสนุนให้องค์กรสามารถทำงานได้อย่างราบรื่นและแก้ไขสถานการณ์หรือเหตุการณ์ที่ไม่ปกติที่เกิดขึ้นได้ เช่น ระบบหยุดทำงาน หรือเครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ หรือเหตุการณ์การโจมตีของผู้ไม่ประสงค์ดี รวมถึงมัลแวร์และไวรัสเรียกค่าไถ่ที่สามารถเกิดขึ้นได้หลากหลายช่องทาง หากองค์กรไม่มีการนโยบายในการใช้งาน และแนวทางการรับมือเหตุการณ์ต่าง ๆ ที่ดีเพียงพอ ก็จะส่งผลให้เกิดปัญหาเดิมซ้ำ ๆ และอาจจะยิ่งรุนแรงมากขึ้นเรื่อย ๆ

สำหรับโรงงานไพ่ฯ ได้มีการจัดทำเรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและหน่วยงาน ผู้ปฏิบัติงาน และผู้ใช้งานได้ยึดถือและปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ด้านเทคโนโลยี (Technology)

เทคโนโลยี ซอฟต์แวร์ ลิขสิทธิ์และการอัปเดต สิ่งจำเป็นในขั้นตอนนำมาปฏิบัติงานและช่วยในการทำงาน รวมถึงการปฏิบัติหน้าที่ ยังช่วยบริหารจัดการต่าง ๆ เพื่อให้บุคคลที่เกี่ยวข้องในการทำงาน สามารถติดตามและตรวจสอบเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้ นอกจากมีเทคโนโลยีที่ดี องค์กรต้องมีกระบวนการในการเฝ้าระวังและปรับปรุงแก้ไขช่องโหว่ และตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

6.7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

หลังจากจัดทำแผนบริหารความเสี่ยง และมีการดำเนินงานตามแผนแล้ว จะต้องมีการรายงานและติดตามผลเป็น ระยะๆ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสม โดยมีเป้าหมายในการติดตามผล คือ เป็น การประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการ ดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่

การติดตามผล

ตามที่โรงงานไพ่ กรมสรรพสามิต ได้ประกาศเรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ ส่วนสารสนเทศและพัฒนาระบบ หน่วยตรวจสอบภายใน และผู้ดูแลระบบที่ได้รับมอบหมาย ตรวจสอบและประเมินความเสี่ยงด้านสารสารเทศ โดยมีแนวปฏิบัติดังนี้

- ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ1 ครั้ง

- ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้โรงงานไพ่ฯได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ
- มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ 1 ครั้ง
- มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศปีละ 1 ครั้ง
- มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
- มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง ต่อคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร และแจ้งคณะกรรมการบริหารความเสี่ยงของโรงงานไพ่ฯ
- มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ภาพกระบวนการดำเนินการประเมินความเสี่ยง

ขั้นตอนที่ 1: การระบุความเสี่ยง (Risk Identification)

- ระบุทรัพย์สิน (Identify Assets)
- การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)
  การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

1. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) - ข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคาม

2. การระบุภัยคุกคาม (Threat Identification) –เพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

3. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

- สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก 4 ประการ ต่อไปนี้:

- ทรัพย์สิน (Asset) - สิ่งที่มีค่าที่ได้รับการระบุในงาน A
- เหตุการณ์ภัยคุกคาม (Threat event) - เหตุการณ์การโจมตีที่ระบุในงาน B
- ช่องโหว่ (Vulnerability) - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง
- ผลที่ตามมา (Consequence) – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

ขั้นตอนที่ 2: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(1) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น

(2) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

- กำหนดโอกาส (Determine Likelihood)

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าว เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่
- ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี
- ความสามารถในการทำซ้ำ (Reproducibility) – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น 3 ระดับ (เช่น 1 – 3)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ 3 คือ “มีแนวโน้มสูง” และ 1 คือ “เป็นไปได้ยาก”

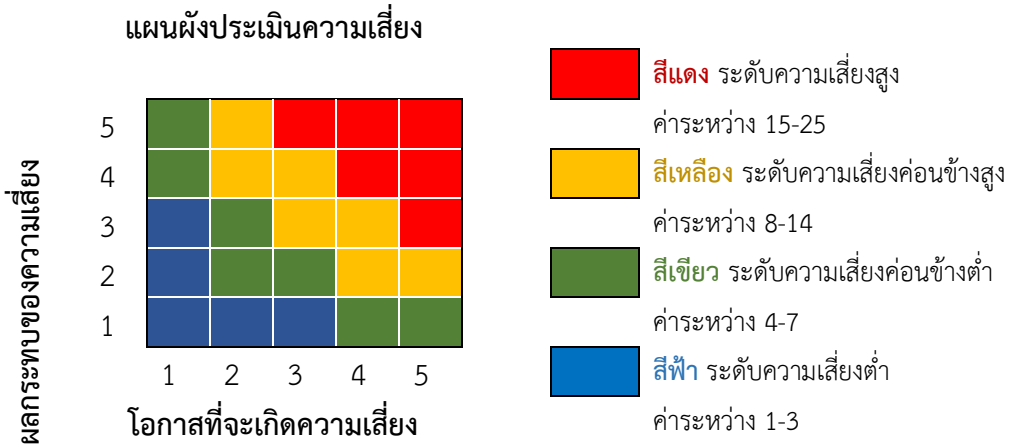
ขั้นตอนที่ 3: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับ ความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

ดังที่กล่าวไว้ในหัวข้อที่ 3 ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง 3 ต่อ 3 สำหรับกำหนดระดับความเสี่ยงสำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง



เมทริกซ์ความเสี่ยง 5 คูณ 5 สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนด โดยหน่วยงานสถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของ

หน่วยงานมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- สถานการณ์ความเสี่ยง (Risk Scenario) – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร

- วันที่ระบุความเสี่ยง (Identification Date) – วันที่ที่ระบุสถานการณ์ความเสี่ยง

- มาตรการที่มีอยู่ (Existing Measures) – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง

- ความเสี่ยงในปัจจุบัน (Current Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)

- แผนจัดการความเสี่ยง (Treatment Plan) – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของหน่วยงาน)

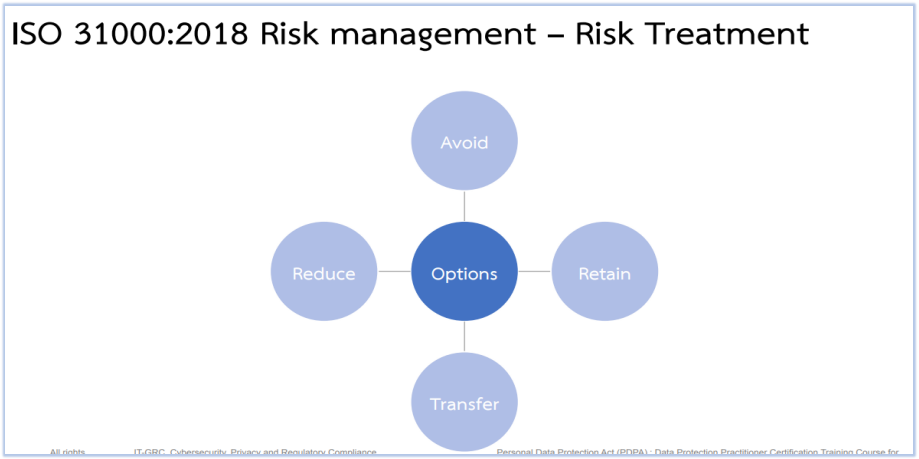
- สถานะความคืบหน้า (Progress Status) – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง
(เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

- เจ้าของความเสี่ยง (Risk Owner) – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

<u>ตอบสนองต่อความเสี่ยง</u>

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน



การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม หน่วยงาน

ควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่าตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคาแพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบ ให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยง
หรือการลดผลกระทบจากความเสี่ยง

ประเภทความเสี่ยง	ชื่อความเสี่ยง	คำอธิบาย/สาเหตุความเสี่ยง	ประเมินความเสี่ยง		ระดับความเสี่ยง	คำอธิบายการควบคุม /วิธีปฏิบัติงานในปัจจุบัน	ประเมินความเสี่ยง		ระดับความเสี่ยงที่เหลืออยู่	วิธีการจัดการความเสี่ยง
			โอกาส	ผลกระทบ			โอกาส	ผลกระทบ		
O CS	ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดต **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	1. เสียงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ 2. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	3	5	15	1. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำ อย่างสม่ำเสมอ 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	2	4	8	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากข้อมูลรั่วไหลจากสื่อบันทึกภายนอก **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	ผู้ใช้งานมีการนำข้อมูลอุปกรณ์ภายนอกไปใช้บนเครื่องที่ไม่ใช่เครื่องสำนักงาน เช่น External HDD, CD/DVD, USB Drive, SD Card	2	3	6	มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Harddisk, CD/DVD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวรหรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้ว หากทำได้	1	3	3	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O C CS	ความเสี่ยงจากการโจรกรรมฐานข้อมูล **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	1	5	5	1. มีการบริหารจัดการด้านการป้องกันข้อมูล 2. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) 3. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Harddisk 4. Disk ม้วนเทป (Cartridge Tape) แผ่น CD/DVD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวรหรือได้ทำลายอุปกรณ์หรือสื่อเก็บข้อมูลนั้น ๆ ทิ้งแล้ว หากทำได้	1	4	4	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O F CS	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. ไม่สามารถใช้งานระบบงานได้เต็มประสิทธิภาพ 2. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	3	5	15	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 2. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	2	4	8	การลด/การควบคุมความเสี่ยง (Risk Reduction)

ประเภทความเสี่ยง	ชื่อความเสี่ยง	คำอธิบาย/สาเหตุความเสี่ยง	ประเมินความเสี่ยง		ระดับความเสี่ยง	คำอธิบายการควบคุม /วิธีปฏิบัติงานในปัจจุบัน	ประเมินความเสี่ยง		ระดับความเสี่ยงที่เหลืออยู่	วิธีการจัดการความเสี่ยง
			โอกาส	ผลกระทบ			โอกาส	ผลกระทบ		
	ผู้รับผิดชอบ ส่วนสารสนเทศและพัฒนาระบบ									
O F CS	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์ **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	2	4	8	1. ตรวจสอบผู้เข้ามาติดต่อ 2. ติดตั้งกล้องวงจรปิดให้ครอบคลุม	1	4	4	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินเทอร์เน็ตและอินทราเน็ตขัดข้อง **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	1. ไม่สามารถใช้งานระบบงานภายในขององค์กรได้ 2. ไม่สามารถเชื่อมต่อเครือข่ายภายนอกผ่านอินเทอร์เน็ตได้	3	3	9	1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก	2	3	6	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	3	4	12	1. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ 3. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	2	4	8	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	1. อุปกรณ์เครื่องแม่ข่ายและเครือข่ายอาจเสียหายได้ 2. ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ 3. ความเสี่ยงต่อความเสียหายของระบบปฏิบัติการและระบบฐานข้อมูลระหว่างทำงานอัน	3	4	12	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS)	2	4	8	การลด/การควบคุมความเสี่ยง (Risk Reduction)

ประเภทความเสี่ยง	ชื่อความเสี่ยง	คำอธิบาย/สาเหตุความเสี่ยง	ประเมินความเสี่ยง		ระดับความเสี่ยง	คำอธิบายการควบคุม /วิธีปฏิบัติงานในปัจจุบัน	ประเมินความเสี่ยง		ระดับความเสี่ยงที่เหลืออยู่	วิธีการจัดการความเสี่ยง
			โอกาส	ผลกระทบ			โอกาส	ผลกระทบ		
		เนื่องมาจากการปิดเครื่องที่ไม่ถูกต้อง								
O CS	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์ **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูล	2	5	10	1. ติดตั้งโปรแกรมป้องกันไวรัสกับเครื่องแม่ข่ายและเครื่องลูกข่าย 2. อัพเดตข้อมูลไวรัสอย่างสม่ำเสมอ	1	5	5	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O C CS	ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์ **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	1. เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การดู Live Streaming, Video Content ขนาดใหญ่, เว็บไซต์ดูหนังผิดกฎหมาย, เล่นเกม เป็นต้น 2. การดาวน์โหลดไฟล์ผิดกฎหมาย เช่น วิดีโอ, ภาพยนตร์, เพลงที่มีลิขสิทธิ์ เป็นต้น	2	3	6	1. การกำหนด Policy ของอุปกรณ์ความมั่นคงปลอดภัย เปิด Port เท่าที่จำเป็น 2. การมีข้อตกลงระหว่างผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ไปใช้ในทางที่ผิด รวมถึงบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้งานที่ฝ่าฝืนต่อผู้บังคับบัญชา	1	3	3	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากการนำอุปกรณ์ภายนอกเข้ามาใช้งานภายในเครือข่ายองค์กร **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	เสี่ยงต่อการนำไวรัสคอมพิวเตอร์เข้ามาแพร่กระจายภายในองค์กร	2	3	6	1. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายภายใน	1	3	3	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O CS	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก **ผู้รับผิดชอบ**	เสี่ยงต่อการถูกโจมตีจากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและเครือข่ายในทุกรูปแบบ	3	5	15	1. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2. ตรวจสอบ Policy และ Log ของ Firewall และ IPS อย่างสม่ำเสมอ	2	5	10	การลด/การควบคุมความเสี่ยง (Risk Reduction)

ประเภทความเสี่ยง	ชื่อความเสี่ยง	คำอธิบาย/สาเหตุความเสี่ยง	ประเมินความเสี่ยง		ระดับความเสี่ยง	คำอธิบายการควบคุม /วิธีปฏิบัติงานในปัจจุบัน	ประเมินความเสี่ยง		ระดับความเสี่ยงที่เหลืออยู่	วิธีการจัดการความเสี่ยง
			โอกาส	ผลกระทบ			โอกาส	ผลกระทบ		
	ส่วนสารสนเทศและพัฒนาระบบ									
O CS	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	เสี่ยงจากเครื่องลูกข่ายโดยผู้ใช้งานอาจตั้งใจและไม่ได้ตั้งใจผ่านทางโปรแกรมต่างๆ ที่ได้ติดตั้งบนเครื่องลูกข่าย	3	5	15	1. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายภายใน	1	5	5	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O F CS	ความเสี่ยงจากการถูกโจมตีเว็บไซต์ **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	เสี่ยงต่อการถูกโจมตีอาจเกิดจาก ภาษาที่ใช้เขียน (Source code) ไม่มีการอัพเดท , ใช้ username password ง่ายต่อการถูกเจาะเว็บไซต์	3	4	12	1. ดำเนินการ backup ข้อมูลเพื่อเตรียมพร้อมในการกู้ระบบกลับคืน	2	4	8	การลด/การควบคุมความเสี่ยง (Risk Reduction)
O F CS	ความเสี่ยงจากวินาศภัย/การก่อการร้าย **ผู้รับผิดชอบ** ส่วนสารสนเทศและพัฒนาระบบ	การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	2	5	10	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน 3. จัดทำศูนย์สำรอง (Backup Site)	1	4	4	การลด/การควบคุมความเสี่ยง (Risk Reduction)

ประเภทความเสี่ยงแบ่งออกเป็น 4 ส่วน คือ

1. S = Strategic Risk
2. O = Operational Risk
3. F = Financial Risk และ
4. C = Compliance Risk
5. CS = Cyber Security Risk

บทที่ 3
แผนการรับมือภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ หน่วยงานโรงงานไพ่ กรมสรรพสามิต

1. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของ โรงงานไพ่ กรมสรรพสามิต ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไป ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ที่กำหนดให้หน่วยงาน ของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้งและ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่ กรมสรรพสามิต) ด้วย

2. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใน โรงงานไพ่ กรมสรรพสามิต โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้ โรงงานไพ่ กรมสรรพสามิต การกำหนดประเภทของเหตุภัยคุกคามทาง ไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ โรงงานไพ่ กรมสรรพสามิต

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของโรงงานไพ่ กรมสรรพสามิต รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

ส่วนสารสนเทศและพัฒนาระบบ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจหน่วยงานของท่าน

5. หน้าที่ในการดำเนินการตามแผน

ส่วนสารสนเทศและพัฒนาระบบ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย ส่วนทรัพยากรบุคคล ส่วนเตรียมการพิมพ์

6. รายละเอียดการบังคับใช้เอกสาร

หน่วยงานจะต้องระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

6.1. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	นายวสุพล วงษ์วิโรจน์
ผู้ดำเนินการตามเอกสาร (Owner)	ส่วนสารสนเทศและพัฒนาระบบ
วันที่จัดทำเอกสาร (Date created)	30 กรกฎาคม 2567
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	นางสาวปชาดา บุตรครุธ
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	5 สิงหาคม 2567
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	พันโทนราวิทย์ เปาอินทร์
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

6.2. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
1.0		พันโทนราวิทย์ เปาอินทร์	ฉบับสมบูรณ์

7. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

7.1 (ชื่อนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน)

7.2 (ชื่อนโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลของหน่วยงาน)

7.3 ชื่อกฎ ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้อง (ถ้ามี)

8. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการ กระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงๆ ประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมี ชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะ ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

9. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

9.1. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

หน่วยงานควรระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรจะกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง/ 7 วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นางสาวปชาดา บุตรครุธ	8 ชั่วโมง	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 063-271-8886 Email : pachada@playingcard.mail.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
2	นายวสุพล วงษ์วิโรจน์	8 ชั่วโมง	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 083-555-4005 Email : vasupon-w@playingcard.mail.go.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้

9.2. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

โปรดระบุว่าหน่วยงานใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบใด เช่น แบบรวมศูนย์ (Centralize), แบบกระจาย (Distributed), แบบให้คำปรึกษา (Coordinating) หรือ แบบอื่นๆ ตามบริบทของหน่วยงาน โดยหน่วยงานจะต้องระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นางสาวปชาดา บุตรครุธ	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 063-271-8886 Email : pachada@playingcard.mail.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
2	นายวสุพล วงษ์วิโรจน์	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 083-555-4005 Email : vasupon-w@playingcard.mail.go.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
3	นายกวีศิลป์ นันทิพัฒน์สถิต	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 083-555-4005 Email : vasupon-w@playingcard.mail.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ (ชื่อหน่วยงานเจ้าของระบบภายใต้หน่วยงานของท่าน) ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
4	นายทวีวัฒน์ จันทร์แดง	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 083-555-4005 Email : vasupon-w@playingcard.mail.go.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นางสาวปชาดา บุตรครุธ	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 063-271-8886 Email : pachada@playingcard.mail.go.th	(ชื่อหน่วยงานเจ้าของระบบภายใต้หน่วยงานหลัก)	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
2	นางสาวปชาดา บุตรครุธ	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 063-271-8886 Email : pachada@playingcard.mail.go.th	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงานของท่าน]
3	นายวสุพล วงษ์วิโรจน์	เบอร์โทรศัพท์ภายใน : 16 เบอร์โทรศัพท์มือถือ : 083-555-4005 Email : vasupon-w@playingcard.mail.go.th	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตาม [นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของท่าน]
4	ว่าที่ ร.ต. ฐานพงษ์ ราชเดิม	เบอร์โทรศัพท์ภายใน : 59 เบอร์โทรศัพท์มือถือ : 086-406-7787 Email : @playingcard.mail.go.th	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงานของท่าน]
5	นายสมภพ สุขประสงค์	เบอร์โทรศัพท์ภายใน : 34 เบอร์โทรศัพท์มือถือ : 086-560-5757 Email : sompop@playingcard.mail.go.th	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงานของท่าน]

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
6	นายธาวิต มะพล	เบอร์โทรศัพท์ภายใน : 14 เบอร์โทรศัพท์มือถือ : 086-876-6222 Email : tawit@playingcard.mail.go.th	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงานของท่าน]

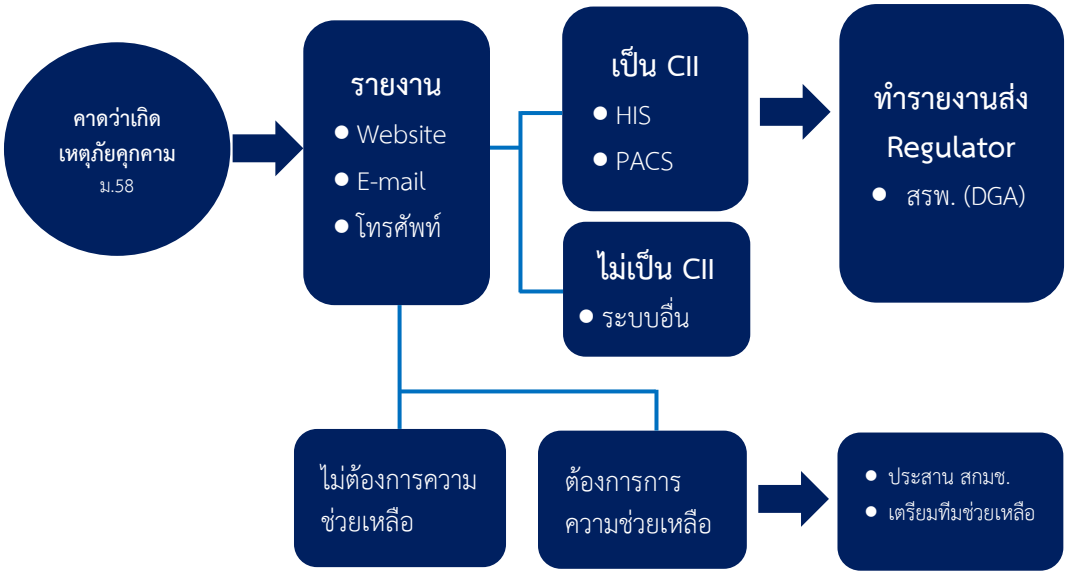
9.3. หน่วยงานภายนอกที่เกี่ยวข้อง

หน่วยงานจะต้องจัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1		เบอร์โทรศัพท์ : 0-2283-4681-83 , 0-2283-4688-90 Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม, 2550 ถนน แจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	
2		เบอร์โทรศัพท์ : 02-142-6888 Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 1 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ThaiCERT	

9.4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

หน่วยงานควรจัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



แผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

10. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ 19.1 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงงานไพ่ฯ ดังนี้

10.1 ขั้นการเตรียมการ (Preparation)

หน่วยงานจะต้องดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 9.2

กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 9.4

กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปรกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก 1)

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

หน่วยงานจะต้องดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(1) หน่วยงานจะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

ประเภท	อธิบาย	วิธีการรับมือ
อุปกรณ์แบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงาน และตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด
ระบบอินเทอร์เน็ต	การโจมตีที่ดำเนินการจากภายนอกและอยู่นอกช่วงเวลาทำการ เช่น การ	จำกัดการเข้าถึงเป็นช่วงเวลาตามแนวโยบายและแนวปฏิบัติ

(2) หน่วยงานจะต้องดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(3) หน่วยงานจะต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

(4) หน่วยงานจะต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

(5) หน่วยงานจะต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 3)

(6) กรณีหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 4 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก1 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 5 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก2 รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา 24 ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ 31 มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก3 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.2 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.3 ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

หน่วยงานจะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่ง การดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(2) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(3) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(4) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.4 ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

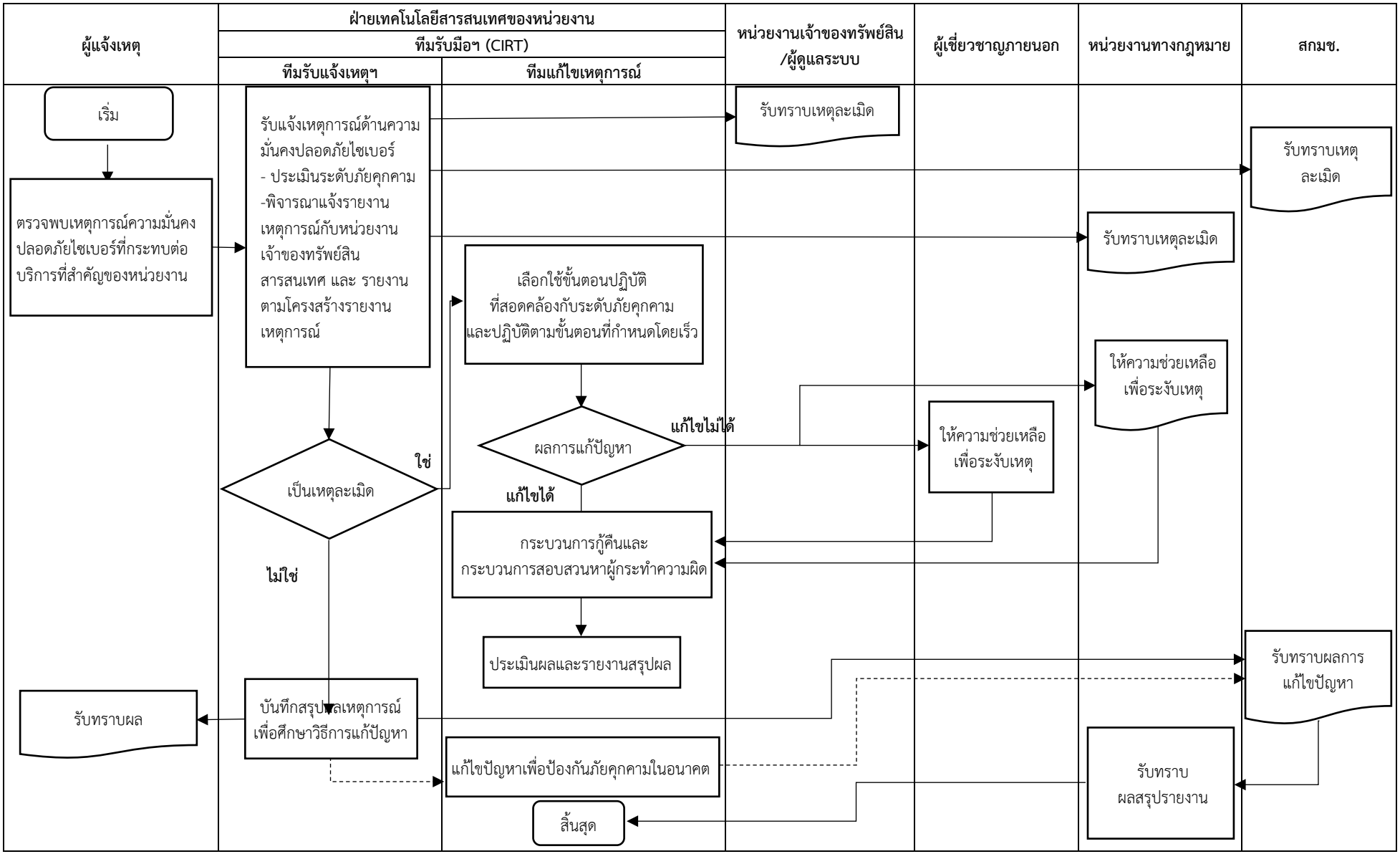
หน่วยงานควรกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(1) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.4 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.5 การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก 5)


ผู้แจ้งเหตุ
ฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน
ทีมรับมือฯ (CIRT)
ทีมรับแจ้งเหตุฯ
ทีมแก้ไขเหตุการณ์
หน่วยงานเจ้าของทรัพย์สิน /ผู้ดูแลระบบ
ผู้เชี่ยวชาญภายนอก
หน่วยงานทางกฎหมาย
สกมช.
เริ่ม
ตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่กระทบต่อบริการที่สำคัญของหน่วยงาน
รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- ประเมินระดับภัยคุกคาม
-พิจารณาแจ้งรายงานเหตุการณ์กับหน่วยงานเจ้าของทรัพย์สิน สารสนเทศ และ รายงานตามโครงสร้างรายงานเหตุการณ์
รับทราบเหตุละเมิด
รับทราบเหตุละเมิด
รับทราบเหตุละเมิด
เลือกใช้ขั้นตอนปฏิบัติที่สอดคล้องกับระดับภัยคุกคามและปฏิบัติตามขั้นตอนที่กำหนดโดยเร็ว
ผลการแก้ปัญหา
แก้ไขไม่ได้
ให้ความช่วยเหลือเพื่อระงับเหตุ
ให้ความช่วยเหลือเพื่อระงับเหตุ
เป็นเหตุละเมิด
ใช่
แก้ไขได้
ไม่ใช่
กระบวนการกู้คืนและกระบวนการสอบสวนหาผู้กระทำความผิด
ประเมินผลและรายงานสรุปผล
รับทราบผลการแก้ไขปัญหา
รับทราบผล
บันทึกสรุปผลเหตุการณ์เพื่อศึกษาวิธีการแก้ปัญหา
แก้ไขปัญหาเพื่อป้องกันภัยคุกคามในอนาคต
รับทราบผลสรุปรายงาน
สิ้นสุด

บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง 12/1/66 – 09.00 น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

เอกสาร ก1 ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

1. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

2. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

3. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

4. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

5. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา 60)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

6. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ 0 หมวดหมู่ที่ 1 และหมวดหมู่ที่ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก2 แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ 1

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ
วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก1. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม
ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก2. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม
ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ

ก3. ความต่อเนื่องของเหตุภัยคุกคาม
☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก4. ลักษณะภัยคุกคามทางไซเบอร์
ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน
☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา 60)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)
☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข4. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม
ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง1. ข้อมูลการตรวจจับและการวิเคราะห์

ง1.1 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง1.2 ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง1.3 รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

- ☐ ข้อมูลไบโอเมตริกซ์
- ☐ ข้อมูลการติดต่อ
- ☐ ข้อมูลการเงิน
- ☐ ข้อมูลบุคลากรของรัฐ
- ☐ หมายเลขบัตรประชาชน
- ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ
- ☐ ข้อมูลทางการแพทย์
- ☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

ง1.4 <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)
โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง2.2 การคาดการณ์ความสามารถฟื้นฟู
โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

	รายการตรวจสอบการจัดการเหตุการณ์	Complete
	ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
1	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
1.1	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
1.2	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
1.3	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
1.4	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
3	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
	ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)	
4	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
	การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)	
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	