กองโรคติดต่อทั่วไป

แผนรับมือสถานการณ์ฉุกเฉิน จากภัยพิบัติระบบเทคโนโลยีสารสนเทศ กองโรคติดต่อทั่วไป

ฉบับปรับปรุง ณ วันที่ 14 กุมภาพันธ์ 2568

จัดทำโดย คณะทำงานความมั่นคงปลอดภัยทางไซเบอร์

กองโรคติดต่อทั่วไป กรมควบคุมโรค

Software Development

Cyber Security

IT Infrastructure Management

02 590 3168

develdcd2024@gmail.com

คำนำ

ระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของกองโรคติดต่อทั่วไป จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ กองโรคติดต่อทั่วไปได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศของหน่วยงาน ซึ่งอาจมีความเสี่ยงต่างๆ ที่ทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้นจึงได้จัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยพิบัติระบบเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น และเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศก็สามารถประสบกับเหตุการณ์ฉุกเฉินที่ไม่สามารถคาดการณ์ล่วงหน้าได้ เช่น ความล้มเหลวของระบบฮาร์ดแวร์ ซอฟต์แวร์ การโจมตีจากภัยคุกคามทางไซเบอร์ หรือภัยธรรมชาติต่างๆ ที่อาจส่งผลกระทบต่อการดำเนินงานของหน่วยงานและการให้บริการประชาชน

เพื่อให้กองโรคติดต่อทั่วไป สามารถดำเนินการได้อย่างต่อเนื่องในกรณีเกิดเหตุการณ์ฉุกเฉิน และลดผลกระทบที่อาจเกิดขึ้นจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ หน่วยงานจึงได้จัดทำ **แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ** ขึ้น โดยมีวัตถุประสงค์ เพื่อเตรียมความพร้อมในการป้องกันและตอบสนองต่อภัยพิบัติทางเทคโนโลยีสารสนเทศ รักษาความต่อเนื่องของภารกิจของกองโรคติดต่อทั่วไป และกำหนดแนวทางการฟื้นฟูระบบสารสนเทศที่เสียหายให้กลับมาใช้งานได้อย่างมีประสิทธิภาพในเวลาที่เหมาะสม ด้วยความมุ่งมั่นในการพัฒนาระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงและปลอดภัยสูงสุด จึงขอให้บุคลากร กองโรคติดต่อทั่วไป ได้ตระหนักถึงความสำคัญของแผนนี้ และร่วมมือกันเพื่อให้แผนนี้ได้รับการปฏิบัติอย่างมีประสิทธิภาพ

คณะทำงานความมั่นคงปลอดภัยทางไซเบอร์ กองโรคติดต่อทั่วไป กรมควบคุมโรค

๒๕ เมษายน ๒๕๖๘

สารบัญ

บทที่ 1 บทนำ

1.1 ความเป็นมาและความสำคัญของแผน

ในยุคปัจจุบัน หน่วยงานราชการได้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการให้บริการประชาชนอย่างกว้างขวาง ไม่ว่าจะเป็นระบบงานสารบรรณอิเล็กทรอนิกส์ ระบบฐานข้อมูลประชาชน ระบบสารสนเทศเพื่อการตัดสินใจ หรือบริการภาครัฐผ่านระบบดิจิทัล (Digital Government) อย่างไรก็ตาม การพึ่งพาระบบเทคโนโลยีสารสนเทศในระดับสูงย่อมนำมาซึ่งความเสี่ยงต่อการดำเนินงานของหน่วยงาน เช่น ความล้มเหลวของระบบ การถูกโจมตีทางไซเบอร์ ไวรัสคอมพิวเตอร์ หรือภัยธรรมชาติที่อาจส่งผลให้ระบบให้บริการหยุดชะงัก ซึ่งอาจกระทบต่อประชาชนและภาพลักษณ์ของภาครัฐโดยรวม ด้วยเหตุนี้ หน่วยงานราชการจึงมีความจำเป็นต้องจัดทำแผนรับมือสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น และสามารถฟื้นฟูระบบให้กลับมาดำเนินงานได้อย่างรวดเร็วและต่อเนื่อง

1.2 วัตถุประสงค์ของแผน

1) เพื่อเตรียมความพร้อมในการป้องกันและตอบสนองต่อภัยคุกคามทางเทคโนโลยีสารสนเทศ

2) เพื่อรักษาความต่อเนื่องของภารกิจหลักของกองโรคติดต่อทั่วไป

3) เพื่อกำหนดแนวทางการฟื้นฟูระบบสารสนเทศที่เสียหายให้กลับมาใช้งานได้อย่างมีประสิทธิภาพในเวลาที่เหมาะสม

1.3 ขอบเขตของแผน

แผนฉบับนี้ครอบคลุมการบริหารจัดการสถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติหรือเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป ทั้งในด้านโครงสร้างพื้นฐาน ระบบงานแอปพลิเคชั่น ฐานข้อมูล และการให้บริการที่เกี่ยวข้องกับการดำเนินภารกิจของกองโรคติดต่อทั่วไป โดยมีขอบเขตดังนี้

- **ประเภทความเสี่ยงที่ครอบคลุม**
  - ความเสี่ยงด้านข้อมูล
  - ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ
  - ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์
  - ความเสี่ยงด้านบุคลากร
  - ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม
  - ความเสี่ยงด้านเครือข่ายสื่อสาร
  - ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก
  - ความเสี่ยงด้านกระบวนการทำงาน

1.4 คำนิยามที่สำคัญ

1) **แผนรับมือสถานการณ์ฉุกเฉิน (Emergency Response Plan หรือ ERP)** คือ แนวทางหรือชุดของขั้นตอนที่หน่วยงานกำหนดไว้ล่วงหน้า เพื่อเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ที่ไม่คาดคิดหรือภาวะวิกฤตที่อาจเกิดขึ้น ส่งผลกระทบต่อการดำเนินงาน ความปลอดภัยของบุคลากร ระบบงาน หรือทรัพย์สินขององค์กร

2) **สถานการณ์ฉุกเฉิน (Emergency Situation)** คือ เหตุการณ์หรือภาวะที่เกิดขึ้นโดยไม่คาดคิดและต้องการการตอบสนองอย่างเร่งด่วน เนื่องจากส่งผลกระทบอย่างรุนแรงต่อบุคลากร ระบบงาน ทรัพย์สินหรือกระบวนการดำเนินงานของหน่วยงาน หากไม่มีการจัดการที่เหมาะสมและทันท่วงที อาจนำไปสู่ความเสียหายขนาดใหญ่และส่งผลกระทบต่อประชาชนหรือประเทศชาติ

3) **ภัยพิบัติจากเทคโนโลยีสารสนเทศ (Information Technology Disasters)** คือเหตุการณ์หรือสถานการณ์ที่เกิดขึ้นโดยไม่คาดคิดซึ่งส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นระบบฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย หรือข้อมูล ที่สำคัญต่อการดำเนินงานขององค์กร หรือหน่วยงาน ทำให้ระบบเกิดความเสียหาย หยุดชะงัก หรือสูญเสียข้อมูลสำคัญ

บทที่ 2 การวิเคราะห์สถานการณ์

2.1 ภาพรวมระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป

ระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป เป็นระบบที่สนับสนุนการทำงานของหน่วยงานในด้านต่าง ๆ เช่น การบริหารจัดการภายใน การจัดการข้อมูล การให้บริการประชาชน โดยใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือหลักในการเพิ่มประสิทธิภาพ ลดขั้นตอนการทำงาน ซึ่งประกอบไปด้วยระบบสารสนเทศ เว็บไซต์ และอุปกรณ์ ครุภัณฑ์คอมพิวเตอร์ ต่าง ๆ ดังนี้

2.1.1 ระบบสารสนเทศ จำนวน 14 ระบบ ได้แก่

1. ระบบออกใบเสร็จรับเงินบริการตรวจห้องปฏิบัติการโรคติดเชื้อไวรัสโคโรนา 2019
2. ระบบออกหนังสือรับรองแหล่งผลิตแหล่งกำเนิดอาหารปลอดโรค
3. ระบบออกหนังสือรับรองแหล่งผลิตแหล่งกำเนิดอาหารปลอดโรค ผ่านระบบ national single window กรมศุลกากร
4. ระบบทดสอบออกหนังสือรับรองแหล่งผลิตแหล่งกำเนิดอาหารปลอดโรค ผ่านระบบ national single window กรมศุลกากร
5. ระบบฐานข้อมูลเอกสารรับรองการฉีดวัคซีนเพื่อการเดินทางระหว่างประเทศ
6. ระบบสำหรับแสดงผลการออกเอกสารรับรองวัคซีนแบบอิเล็กทรอนิกส์เพื่อการเดินทางระหว่างประเทศ
7. ระบบบริหารจัดการคลังวัคซีนและเวชภัณฑ์
8. ระบบรายงานการให้บริการวัคซีนป้องกันโรคไข้หวัดใหญ่ (DDC FLU)
9. ระบบ e-learning หลักสูตรการป้องกันควบคุมโรคติดต่อและภัยสุขภาพในเด็ก
10. ระบบฐานข้อมูลครุภัณฑ์คอมพิวเตอร์
11. ระบบฐานข้อมูลการเฝ้าระวังโรคหนอนพยาธิในนักเรียนและเยาวชนในพื้นที่ถิ่นทุรกันดาร ตามพระราชดำริฯ (Helminth) (ระบบเก่า)
12. ระบบฐานข้อมูลการเฝ้าระวังโรคหนอนพยาธิในนักเรียนและเยาวชนในพื้นที่ถิ่นทุรกันดาร ตามพระราชดำริฯ (Helminth) (ระบบใหม่)
13. ระบบ AI-OVMIF Migrating to AI-Helminths
14. ระบบการประเมินตนเองเพื่อการสร้างพื้นที่ปลอดโรคพิษสุนัขบ้า (Rabies Free Zone Self-assessment Application)

2.1.2 เว็บไซต์ จำนวน 5 เว็บไซต์ ได้แก่

1. เว็บไซต์ศูนย์เด็กเล็กปลอดภัย เด็กไทยปลอดโรค
2. เว็บไซต์วัคซีนโควิด 19 ประเทศไทย
3. เว็บไซต์ thaionehealth
4. เว็บไซต์ฐานข้อมูลโรคติดต่อและโรคติดต่ออุบัติใหม่
5. เว็บไซต์ E-book เที่ยวอย่างไรให้ปลอดภัยต่อสุขภาพ

2.1.3 อุปกรณ์ ครุภัณฑ์คอมพิวเตอร์ ได้แก่

1. เครื่องคอมพิวเตอร์แม่ข่าย	จำนวน	5	เครื่อง
2. เครื่องคอมพิวเตอร์ประมวลผล	จำนวน	170	เครื่อง
3. เครื่องคอมพิวเตอร์โน้ตบุ๊ค	จำนวน	75	เครื่อง
4. เครื่องคอมพิวเตอร์เท็ปเลต	จำนวน	24	เครื่อง
5. เครื่องสำรองไฟฟ้า	จำนวน	149	เครื่อง
6. เครื่องสแกนเนอร์	จำนวน	13	เครื่อง
7. เครื่องปริ้นเตอร์	จำนวน	70	เครื่อง
8. กล้องวีดีโอคอนเฟอร์เร้น และกล้องวงจรปิด	จำนวน	8	ชุด

2.2 การประเมินความเสี่ยงและภัยคุกคาม (Risk Assessment)

2.2.1 ความเสี่ยงด้านเทคโนโลยีสารสน เทศ (Information Technology Risk)

ความเสี่ยงด้านเทคโนโลยีสารสน เทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน (Disruptive Technology / Disruptive Innovation) เช่น Internet of Things (IoT), Blockchain, Big Data เป็นต้น ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ 3 ประการ ได้แก่ แผนงานการใช้เทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงานของกองโรคติดต่อทั่วไป

2.2.2 ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Type of Risk) แบ่งออกได้เป็น 8 ประเภทดังนี้

1) ความเสี่ยงด้านข้อมูล (Information Risk)

ความเสี่ยงด้านข้อมูล (Information Risk) คือ ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้

หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญ คือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information Back-Up) การกู้คืนข้อมูล (Information Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่อง (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

2) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) คือ ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน และขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

3) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) คือ ความเสี่ยงที่เกิดจากการเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการ Reversion software ไม่เพียงพอ การที่ซอฟต์แวร์ที่ใช้อยู่ล้าสมัย ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากควบคุมการเปลี่ยนแปลง (Change control) ไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งาน Software การไม่ได้จัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

4) ความเสี่ยงด้านบุคลากร (People Risk)

ความเสี่ยงด้านบุคลากร (People Risk) คือ ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในส่วนการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศและสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่อย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

5) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) คือ ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ แผ่นดินไหวการไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

6) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk)

ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) คือ ความเสี่ยงที่เกิดจากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากการที่ไม่ได้กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหารเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารไม่สม่ำเสมอ การไม่มีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานอื่น กรณีมีความจำเป็น เช่น บมจ. ทศท คอร์เปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัย สำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย เป็นต้น

7) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing)

ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) คือ ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

8) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk)

ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) คือ ความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดีมาใช้งาน โดยกำหนดกระบวนการที่เป็นมาตรฐานที่ดีไว้ และกำหนดBest Practice ของกระบวนการต่าง ๆ ไว้ให้การขาดการนำ Best Practice เหล่านั้นมาใช้งานอาจทำให้องค์กร ไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่มาตรฐานดังกล่าวได้กำหนดไว้ ได้กำหนดเป้าหมาย ทางธุรกิจสำหรับการนำเทคโนโลยีสารสนเทศมาใช้งาน

2.2.3 ผลกระทบที่อาจเกิดขึ้นจากเหตุฉุกเฉิน

เหตุฉุกเฉินที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศของหน่วยงานราชการ อาจส่งผลกระทบในหลายด้าน ทั้งต่อกระบวนการดำเนินงาน ภารกิจหลักของหน่วยงาน การให้บริการแก่ประชาชน รวมถึงความมั่นคงปลอดภัยของข้อมูลสำคัญ โดยสามารถสรุปผลกระทบที่อาจเกิดขึ้นได้ ดังนี้

- **ผลกระทบต่อภาพลักษณ์ชื่อเสียงขององค์กร**

หากหน่วยงานไม่สามารถจัดการกับสถานการณ์ฉุกเฉินได้อย่างเหมาะสมและทันเวลา อาจส่งผลกระทบต่อภาพลักษณ์ของหน่วยงาน ทั้งในสายตาของประชาชน หน่วยงานภาครัฐอื่น หรือสื่อมวลชน ซึ่งอาจทำให้เกิดความไม่ไว้วางใจต่อความสามารถในการบริหารจัดการระบบสารสนเทศของหน่วยงาน

- **ผลกระทบต่อองค์กรด้านการเงิน**

การกู้คืนระบบหรือแก้ไขปัญหาที่เกิดจากเหตุฉุกเฉิน มักต้องใช้งบประมาณเพิ่มเติมเพื่อจัดซื้ออุปกรณ์หรือว่าจ้างผู้เชี่ยวชาญ อีกทั้งยังส่งผลให้ต้องใช้กำลังคนเพิ่มขึ้น หรือทำงานนอกเวลาปกติ ซึ่งเป็นภาระต่อทรัพยากรของหน่วยงานทั้งในระยะสั้นและระยะยาว

- **ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน**

การหยุดชะงักของระบบเทคโนโลยีสารสนเทศที่สนับสนุนการปฏิบัติงาน อาจทำให้ไม่สามารถดำเนินงานตามภารกิจหลักของหน่วยงานได้ ส่งผลให้เกิดความล่าช้าในการปฏิบัติงาน การให้บริการประชาชนขาดความต่อเนื่อง และอาจทำให้กระทบต่อความเชื่อมั่นของผู้รับบริการในภาพรวม

- **ผลกระทบด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม**

ผลกระทบด้านกฎหมายและระเบียบข้อบังคับจากการเกิดภัยพิบัติทางเทคโนโลยีสารสนเทศต่อหน่วยงานราชการมีความร้ายแรงและครอบคลุมในหลายมิติ ทั้งด้านการคุ้มครองข้อมูล ความรับผิดชอบต่อประชาชน และพันธกรณีทางกฎหมาย ดังนั้น หน่วยงานราชการควรมีมาตรการเชิงรุกและแผนรับมือสถานการณ์ฉุกเฉินอย่างชัดเจน เพื่อหลีกเลี่ยงความเสียหายและการฝ่าฝืนกฎหมาย

การประเมินความเสี่ยงโดยทั่วไป เกณฑ์การประเมินความเสี่ยงจะประกอบด้วยองค์ประกอบ ๒ ส่วน คือ

- โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood) ซึ่งหมายถึง ความเป็นไปได้ที่ความเสี่ยงที่ผู้ประเมินสนใจจะเกิดขึ้น
- ระดับความรุนแรงของผลกระทบ (Impact) ซึ่งหมายถึง ความเสี่ยงนั้นหากเกิดขึ้นจะมีความรุนแรงในระดับใด

โดยมีการกำหนดเกณฑ์การประเมินทั้ง 2 ส่วน ตามตารางที่ 2.1 และ 2.2 ดังนี้

ตารางที่ 2.1 โอกาสการเกิดขึ้นของความเสี่ยง (Likelihood)

ระดับ	โอกาสที่จะเกิด
1	แทบจะไม่เกิดหรืออย่างมากปีละ 1 ครั้ง
2	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง
3	ปานกลาง ปีละ 3 - 5 ครั้ง
4	ค่อนข้างบ่อย ปีละ 6 - 10 ครั้ง
5	เกิดเป็นประจำ อย่างน้อยเดือนละ 1 ครั้ง

ตารางที่ 2.2 ระดับความรุนแรงของผลกระทบ (Impact) แต่ละด้าน

เกณฑ์	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
1.ผลกระทบต่อภาพลักษณ์/ชื่อเสียงขององค์กร (Reputation)	- คำวิจารณ์ที่ไม่ส่งผลกระทบต่อการดำเนินขององค์กร หรือ - สามารถจัดการได้โดยง่าย หรือ - ผู้บริหารต้องยอมรับ รับฟัง แต่ยังไม่จำเป็นต้องดำเนินการใด ๆ ต่อคำวิจารณ์นั้น หรือ - ไม่มีการฟ้องร้องต่อศาล หรือ - กระทบชื่อเสียงขององค์กรน้อยมากหรือไม่กระทบ	- คำวิจารณ์ที่ส่งผลกระทบเล็กน้อยต่อการดำเนินงานขององค์กร หรือ - สามารถจัดการได้โดยง่าย หรือ - ผู้บริหารต้องยอมรับ รับฟัง แต่ยังไม่จำเป็นต้องดำเนินการใดๆ ต่อคำวิจารณ์นั้น หรือ - ไม่มีการฟ้องร้องต่อศาล หรือ - กระทบชื่อเสียงขององค์กรภายในกลุ่มงาน	- คำวิจารณ์ที่ส่งผลกระทบต่อการดำเนินงานขององค์กร หรือ - ยากต่อการจัดการ หรือ - เสื่อมเสียชื่อเสียงขององค์กร หรือ - ผู้บริหารต้องยอมรับและแสดงความรับผิดชอบต่อคำวิจารณ์นั้น หรือ - ไม่มีการฟ้องร้องต่อศาล หรือ - กระทบชื่อเสียงขององค์กร ทำให้เกิดการรายงานต่อผู้บริหารระดับสูง	- คำวิจารณ์ที่ส่งผลกระทบต่อการดำเนินงานตามพันธกิจขององค์กร หรือ - เสื่อมเสียชื่อเสียงขององค์กรในวงกว้าง หรือ - ยากมากในการจัดการ หรือ - ผู้บริหารต้องยอมรับและแสดงความรับผิดชอบต่อคำวิจารณ์นั้น หรือ - มีโอกาสที่จะผิดกฎหมายร้ายแรงส่งผลกระทบต่อความน่าเชื่อถือในสายตาของผู้ใช้บริการและสาธารณชน หรือ - กระทบชื่อเสียงขององค์กร ทำให้เกิดความไม่พอใจจากผู้มีส่วนได้ส่วนเสีย (Stakeholder)	- คำวิจารณ์ที่ส่งผลกระทบร้ายแรงต่อการดำเนินงานหลักขององค์กร หรือ - มีโอกาสที่จะผิดกฎหมายร้ายแรงส่งผลกระทบต่อความน่าเชื่อถือในสายตาของผู้ใช้บริการและสาธารณชน หรือ - เสื่อมเสียชื่อเสียงขององค์กรในวงกว้าง หรือ - ไม่สามารถจัดการได้ หรือ - ศาลรับฟ้องจากคำวิจารณ์นั้น หรือ - กระทบชื่อเสียงขององค์กรมาก ทำให้เกิดการวิพากษ์วิจารณ์จากสื่อสาธารณะ

เกณฑ์	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
2.ผลกระทบต่อองค์กรด้านการเงิน (Finance)	เกิดเหตุร้ายที่ไม่มีความสำคัญอาจประเมินมูลค่าความเสียหายทางการเงินน้อยกว่า 500,000 บาท	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้อาจประเมินมูลค่าความเสียหายทางการเงินตั้งแต่ 500,000 - 1,000,000 บาท	ระบบมีปัญหาและมีความสูญเสียไม่มากอาจประเมินมูลค่าความเสียหายทางการเงินเกินตั้งแต่ 1,000,000 - 50,000,000 บาท	เกิดปัญหากับระบบที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วนอาจประเมินมูลค่าความเสียหายทางการเงินตั้งแต่ 50,000,000 - 100,000,000 บาท	เกิดความสูญเสียต่อระบบที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ อาจประเมินมูลค่าความเสียหายทางการเงินมากกว่า 100,000,000 บาทขึ้นไป
3.ผลกระทบต่อองค์กรด้านผู้ใช้บริการและด้านการดำเนินงาน (User and Operation)	- การดำเนินงานมีปัญหาแต่ไม่เป็นนัยสำคัญหรือ - บริการเกิดเหตุขัดข้องแต่สามารถให้บริการได้ หรือใช้งานได้ไม่สมบูรณ์เป็นระยะเวลาน้อยกว่า 1 ชั่วโมง หรือ - กระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียน้อยกว่า 10,000 คน หรือ - ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	- การดำเนินงานมีปัญหาและส่งผลกระทบระดับส่วนงาน หรือ - บริการประเภท Information ไม่สามารถให้บริการได้เป็นระยะเวลาน้อยกว่า 1 ชั่วโมง หรือ - กระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียตั้งแต่ 10,000 – 20,000 คน หรือ - มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 1 - 200 คน	- การดำเนินงานมีปัญหาและส่งผลกระทบให้การดำเนินงานภายในหยุดชะงัก หรือ - บริการประเภท Transaction หรือ Portal ไม่สามารถให้บริการได้ เป็นระยะเวลาน้อยกว่า 1 ชั่วโมง หรือ - กระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียตั้งแต่ 200 - 500 คน หรือ - มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 20,000 - 50,000 คน	-การดำเนินงานมีปัญหาและส่งผลกระทบต่อระบบที่สำคัญหยุดชะงักและบางระบบอาจส่งผลต่อผู้รับบริการในวงกว้าง - บริการประเภท Communication ไม่สามารถให้บริการได้เป็นระยะเวลาน้อยกว่า 1 ชั่วโมง หรือ - กระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียตั้งแต่ 50,000 - 100,000 คน หรือ - มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 500 - 1,000 คน	- การดำเนินงานมีปัญหาและส่งผลกระทบต่อระบบที่สำคัญทั้งหมดส่งผลต่อผู้รับบริการในวงกว้าง หรือ - กระทบผู้ใช้บริการรายสำคัญ ๑ หน่วยงาน/ราย ไม่สามารถใช้งานได้ หรือ - บริการประเภท Infrastructure หรือบางประเภทบริการไม่สามารถให้บริการได้เป็นระยะเวลามากกว่า 1 ชั่วโมง หรือ - กระทบกับจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียมากกว่า 100,000 คน หรือ - มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยมากกว่า 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คนขึ้นไป

เกณฑ์	ระดับค่าคะแนนของความรุนแรงของผลกระทบ (Impact)				
	1=น้อยมาก	2=น้อย	3=ปานกลาง	4=สูง	5=สูงมาก
4.ด้านกฎหมายหรือระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม (Compliance)	- ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร โดยไม่เกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญและไม่เกิดความเสียหายต่อองค์กรหรือบุคคลอื่น	- ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร และเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญ แต่ไม่เกิดความเสียหายต่อองค์กรหรือบุคคลอื่น	- ปฏิบัติหรือละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญ และเกิดความเสียหายเพียงเล็กน้อยต่อองค์กรหรือบุคคลอื่น	- ปฏิบัติหรือละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญ ไม่เป็นไปตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อองค์กรหรือบุคคลอื่น	- ปฏิบัติหรือละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบต่อการดำเนินงานขององค์กรที่มีนัยสำคัญ ไม่เป็นไปตามเป้าของ ก.พ.ร. และเกิดความเสียหายอย่างร้ายแรงต่อองค์กรหรือบุคคลอื่นโดยปรากฏเป็นข่าวในสื่อสาธารณะที่ก่อให้เกิดความเสียหายต่อชื่อเสียงหรือภาพลักษณ์ขององค์กร

จากตารางโอกาสที่จะเกิดขึ้นของความเสี่ยง และความรุนแรงของเหตุการณ์ ได้กำหนดค่าระดับความเสี่ยงไว้ ดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ความรุนแรงของเหตุการณ์

ตารางที่ 2.3 ค่าระดับความรุนแรงของเหตุการณ์

โอกาสที่จะเกิด						
	ระดับ 5	5	10	15	20	25
	ระดับ 4	4	8	12	16	20
	ระดับ 3	3	6	9	12	15
	ระดับ 2	2	4	6	8	10
	ระดับ 1	1	2	3	4	5
		ระดับ 1	ระดับ 2	ระดับ 3	ระดับ 4	ระดับ 5
		ผลกระทบ				

โดยแบ่งค่าระดับความเสี่ยงออกเป็น 4 ระดับ ตามที่แสดงในตารางที่ 2.4

ตารางที่ 2.4 ระดับความเสี่ยง

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1 - 4	**ต่ำ**	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
5 - 12	**ปานกลาง**	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
15 - 16	**สูง**	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
20 - 25	**สูงมาก**	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

คณะทำงานการเตรียมความพร้อมรัฐบาลดิจิทัลของหน่วยงาน ประจำปีงบประมาณ 2568 (คณะทำงานที่ 4 คณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์) ได้ร่วมกันวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ เว็ปไซต์ อุปกรณ์ คอมพิวเตอร์ ของกองโรคติดต่อทั่วไป โดยจำแนกตามประเภทความเสี่ยง ได้ดังนี้

ตารางที่ 2.5 ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ประเภทความเสี่ยง	**ลักษณะความเสี่ยง**	**ช่องโหว่**
1. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูล จากภายนอกที่มีการละเมิดข้อมูลในระบบ - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย
2. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่ไม่เหมาะสมกับลักษณะงาน และองค์กรที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์	- Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย - Software ล้าสมัย - ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง
3. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ	- โปรแกรม/ระบบการทำงานผิดพลาดของโปรแกรม - โปรแกรม/ระบบไม่มีการอัพเดตระบบอย่างสม่ำเสมอ - โปรแกรม/ระบบประยุกต์ติดต่อฐานข้อมูล ไม่ได้ - การใช้โปรแกรม/ระบบไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัส มัลแวร์ หรือเกิดช่อง โหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ช่องโหว่
4. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบ ไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคคลากร มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศ เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้ - การโยกย้ายของบุคลากรด้านคอมพิวเตอร์ - การพัฒนาอย่างรวดเร็วของเทคโนโลยี
5. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่อง คอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหาย ทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้ งานได้โดยอัตโนมัติ	- ไฟฟ้าดับ - ไฟไหม้ - น้ำท่วม
6. ความเสี่ยงด้านเครือข่ายสื่อสาร	การเกิดระบบเครือข่ายสื่อสารขัดข้อง ไม่ได้กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย	- ระบบปฏิบัติการไม่อัพเดตข้อมูล ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย
7. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	ผู้ว่าจ้างไม่สามารถดำเนินงาน ตามรายละเอียดของสัญญาที่กำหนดไว้	- ผู้ให้บริการไม่สามารถดำเนินงานตาม รายละเอียดของสัญญาที่กำหนดไว้ - หากเกิดปัญหา ต้องใช้เวลานานในการ แก้ปัญหา
8. ความเสี่ยงด้านกระบวนการทำงาน	การที่เกิดกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล	- ไม่มีกระบวนการทำงานตามมาตรฐานสากล

จากช่องโหว่ที่วิเคราะห์ได้ตามประเภทความเสี่ยงทั้ง 8 ด้าน ตามตารางที่ 2.5 กองโรคติดต่อทั่วไปได้นำมาประเมินความเสี่ยง แสดงผลตามตารางที่ 2.6

ตารางที่ 2.6 การประเมินของค่าระดับความเสี่ยงของประเภทความเสี่ยงทั้ง 8 ด้าน

ช่องโหว่	โอกาส	ความรุนแรงของเหตุการณ์ต่อองค์กร			
		ด้านภาพลักษณ์/ชื่อเสียง	ด้านการเงิน	ด้านผู้ใช้บริการและด้านการดำเนินงาน	ด้านกฎหมายหรือระเบียบ
1. ความเสี่ยงด้านข้อมูล					
1.1 ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอกที่มีการละเมิดข้อมูลในระบบ	3	5	1	2	2
ระดับความเสี่ยง		15	3	6	6
1.2 ข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์	3	2	1	3	1
ระดับความเสี่ยง		6	3	9	3
1.3 ไม่มีระบบสำรองข้อมูลเมื่อระบบหลักเสียหาย	1	1	1	3	1
ระดับความเสี่ยง		1	1	3	1
2. ความเสี่ยงด้านอุปกรณ์เทคโนโลโลยีสารสนเทศ					
2.1 Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย	4	1	1	2	1
ระดับความเสี่ยง		5	5	8	4
2.2 Software ล้าสมัย	2	1	2	3	1
ระดับความเสี่ยง		2	4	6	2
2.3 ผู้ใช้งานไม่มีความรู้ในการใช้งานที่ถูกต้อง	2	1	1	2	1
ระดับความเสี่ยง		2	2	4	2
3. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์					
3.1 โปรแกรม/ระบบการทำงานผิดพลาดของโปรแกรม	2	1	1	2	1
ระดับความเสี่ยง		2	2	4	2
3.2 โปรแกรม/ระบบไม่มีการอัพเดตระบบอย่างสม่ำเสมอ	4	1	1	3	1
ระดับความเสี่ยง		4	4	12	4
3.3 โปรแกรม/ระบบประยุกต์ติดต่อฐานข้อมูลไม่ได้	1	1	1	2	1
ระดับความเสี่ยง		1	1	2	1

ช่องโหว่	โอกาส	ความรุนแรงของเหตุการณ์ต่อองค์กร			
		ด้านภาพลักษณ์/ชื่อเสียง	ด้านการเงิน	ด้านผู้ใช้บริการและด้านการดำเนินงาน	ด้านกฎหมายหรือระเบียบ
3.4 การใช้โปรแกรม/ระบบไม่ถูกลิขสิทธิ์ อาจเกิดการติดไวรัสมัลแวร์ หรือเกิดช่องโหว่ที่นำไปสู่ความไม่ปลอดภัยทางไซเบอร์	4	1	1	2	1
ระดับความเสี่ยง		4	4	8	1
4. ความเสี่ยงด้านบุคลากร					
4.1 ไม่มีขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้บุคคลอื่นสามารถทำงานทดแทนได้	1	-	-	2	-
ระดับความเสี่ยง		-	-	2	-
4.2 การโยกย้ายของบุคลากรด้านคอมพิวเตอร์	1	-	-	1	-
ระดับความเสี่ยง		-	-	1	-
4.3 การพัฒนาอย่างรวดเร็วของเทคโนโลยี	3	-	1	2	-
ระดับความเสี่ยง		-	3	6	
5. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม					
5.1 ไฟฟ้าดับ	5	1	1	2	1
ระดับความเสี่ยง		5	5	10	5
5.2 ไฟไหม้	1	1	4	5	3
ระดับความเสี่ยง		1	4	5	3
5.3 น้ำท่วม	1	1	4	5	3
ระดับความเสี่ยง		1	4	5	3
6. ความเสี่ยงด้านเครือข่ายสื่อสาร					
6.1 ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต	2	1	1	2	1
ระดับความเสี่ยง		2	2	4	1
6.2 ความเสี่ยงจากการโจมตีของผู้ไม่วังดี เช่น Hacker	2	2	1	2	1
ระดับความเสี่ยง		4	1	4	1
6.3 สาย Lan ชำรุดเสียหาย	3	1	2	3	1
ระดับความเสี่ยง		3	6	9	1

7. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก					
7.1 ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้	1	1	2	2	1
ระดับความเสี่ยง		1	2	2	1
7.2 หากเกิดปัญหา ต้องใช้เวลานานในการแก้ปัญหา	2	1	2	3	1
ระดับความเสี่ยง		1	4	6	2
8. ความเสี่ยงด้านกระบวนการทำงาน					
8.1 ไม่มีกระบวนการทำงานตามมาตรฐานสากล	1	1	-	1	-
ระดับความเสี่ยง		1	-	1	-

และจากการประเมินความเสี่ยงแต่ละด้าน ได้นำความเสี่ยงที่มีระดับความเสี่ยงสูงสุด 3 ลำดับแรกมาจัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ เพื่อรองรับความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป ได้แก่

ลำดับที่ 1 ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอกที่มีการละเมิดข้อมูลในระบบ (ระดับความเสี่ยง 15) ซึ่งเป็นความเสี่ยงด้านข้อมูล

ลำดับที่ 2 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ /ระบบไม่มีการอัพเดทระบบอย่างสม่ำเสมอ (ระดับความเสี่ยง 12) ซึ่งเป็นความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

ลำดับที่ 3 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (ระดับความเสี่ยง 10) ซึ่งเป็นความเสี่ยงจากไฟฟ้าดับ

ตาราง 2.7 ค่าคะแนนความเสี่ยงจากการวิเคราะห์ช่องโหว่ ของกองโรคติดต่อทั่วไป

ลำดับที่	ค่าคะแนน	ประเภทความเสี่ยง	ช่องโหว่
1	15	ความเสี่ยงด้านข้อมูล	ความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอกที่มีการละเมิดข้อมูลในระบบ
2	12	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	โปรแกรม/ระบบไม่มีการอัพเดตระบบอย่างสม่ำเสมอ
3	10	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ไฟฟ้าดับ
4	9	ความเสี่ยงด้านเครือข่ายสื่อสาร	สาย Lan ชำรุดเสียหาย
5	8	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	Hard disk ชำรุดเสียหาย เช่น Main board, Memory, Power Supply ชำรุดเสียหาย
6	6	ความเสี่ยงด้านบุคลากร	การพัฒนาอย่างรวดเร็วของเทคโนโลยี
7	6	ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากเกิดปัญหา ต้องใช้เวลานานในการแก้ปัญหา
8	1	ความเสี่ยงด้านกระบวนการทำงาน	ไม่มีกระบวนการทำงานตามมาตรฐานสากล

บทที่ 3 กลไกและโครงสร้างการบริหารจัดการเหตุฉุกเฉิน

การบริหารจัดการเหตุฉุกเฉินที่เกิดจากภัยพิบัติทางเทคโนโลยีสารสนเทศจำเป็นต้องมีโครงสร้างที่ชัดเจน มีความพร้อมในการตอบสนองต่อสถานการณ์ และสามารถฟื้นฟูระบบให้กลับมาใช้งานได้ภายในระยะเวลาที่เหมาะสม ทั้งนี้เพื่อให้หน่วยงานสามารถปฏิบัติงานได้อย่างต่อเนื่อง (Business Continuity) และลดผลกระทบต่อประชาชนและภารกิจของรัฐ โดยมีโครงสร้างทีมจัดการเหตุฉุกเฉิน (Emergency Response Team) ดังนี้

3.1 โครงสร้างทีมจัดการเหตุฉุกเฉิน (Emergency Response Team) ประกอบไปด้วย 5 ทีม ดังนี้

1. ทีมบริหารจัดการเหตุฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Emergency Management Committee)

ตารางที่ 3.1 ทีมบริหารจัดการเหตุฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Emergency Management Committee)

ลำดับที่	ชื่อ - นามสกุล	ตำแหน่ง	ช่องทางสื่อสาร	
			โทรศัพท์	มือถือ
1.	นายยงเจือ เหล่าศิริถาวร	ผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3160	081-81113615
2.	นางเกษรา ญาณเวทย์กุล	นักวิชาการสาธารณสุขเชี่ยวชาญ รองผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3160	097-9949891
3.	นางสุพินดา ตีระรัตน์	นักวิชาการสาธารณสุขชำนาญการพิเศษ รองผู้อำนวยการกองโรคติดต่อทั่วไป	0-2951-1361	081-6138323
4.	นายธีรศักดิ์ ชักนำ	นายสัตวแพทย์ชำนาญการพิเศษ รองผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3176	089-5361585
5.	นายอภิชัย พจน์เลิศอรุณ	เภสัชกรชำนาญการพิเศษ รองผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3222	081-5537774
6.	นางรณิดา เตชะสุวรรณา	นายแพทย์ชำนาญการพิเศษ ผู้ช่วยผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3185	094-4144653
7.	นางปิยดา อังศุวัชรากร	นายแพทย์ชำนาญการ ผู้ช่วยผู้อำนวยการกองโรคติดต่อทั่วไป	0-2590-3196-7	086-8946633

บทบาทหน้าที่ทีมบริหารจัดการเหตุฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Emergency Management Committee) : กำหนดนโยบาย กำกับ ติดตาม และตัดสินใจเชิงยุทธศาสตร์ในการบริหารจัดการเหตุฉุกเฉิน รวมทั้งเป็นผู้อนุมัติแนวทางการตอบสนองและการฟื้นฟูระบบ

2. ทีมด้านการตอบสนองเหตุการณ์ (Incident Response Team – IRT)

ตารางที่ 3.2 ทีมด้านการตอบสนองเหตุการณ์ (Incident Response Team – IRT)

ลำดับที่	ชื่อ - นามสกุล	ตำแหน่ง	ช่องทางสื่อสาร	
			โทรศัพท์	มือถือ
1.	น.ส.ภิญญาดา ดอนนนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	081-81113615
2.	นายเทพาทิป เชาวนิวิจิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	097-9949891
3.	นางอำภาพร รอดรัตน์	นักวิชาการคอมพิวเตอร์	0-2590-3168	091-9861282
4.	น.ส.กัลยาณี ดวงตา	เจ้าพนักงานคอมพิวเตอร์	0-2590-3168	081-7716061

บทบาทหน้าที่ทีมด้านการตอบสนองเหตุการณ์ (Incident Response Team-IRT) : รับผิดชอบในการเฝ้าระวัง ตรวจจับ แจ้งเตือน และตอบสนองเมื่อเกิดเหตุฉุกเฉิน โดยเฉพาะกรณีที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ หรือความเสียหายของระบบ

3. ทีมกู้คืนระบบ (System Recovery Team)

ตารางที่ 3.3 ทีมกู้คืนระบบ (System Recovery Team)

ลำดับที่	ชื่อ - นามสกุล	ตำแหน่ง	ช่องทางสื่อสาร	
			โทรศัพท์	มือถือ
1.	น.ส.ภิญญาดา ดอนนนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	081-81113615
2.	นายเทพาทิป เชาวนิวิจิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	097-9949891
3.	นางอำภาพร รอดรัตน์	นักวิชาการคอมพิวเตอร์	0-2590-3168	091-9861282
4.	น.ส.กัลยาณี ดวงตา	เจ้าพนักงานคอมพิวเตอร์	0-2590-3168	081-7716061

บทบาทหน้าที่ทีมด้านการกู้คืนระบบ (System Recovery Team) : รับผิดชอบในการวางแผนและดำเนินการกู้คืนระบบและข้อมูล เพื่อให้สามารถกลับมาใช้งานได้ตามปกติภายในระยะเวลาที่กำหนด

4. ทีมสื่อสารและประชาสัมพันธ์ (Communication and PR Team)

ตารางที่ 3.4 ทีมสื่อสารและประชาสัมพันธ์ (Communication and PR Team)

ลำดับที่	ชื่อ - นามสกุล	ตำแหน่ง	ช่องทางสื่อสาร	
			โทรศัพท์	มือถือ
1.	นางรณิดา เตชะสุวรรณา	นายแพทย์ชำนาญการพิเศษ	0-2590-3185	094-4144653
2.	น.ส.ชนัดดา ตั้งวงศ์จุลเนียม	นักวิชาการสาธารณสุขชำนาญการพิเศษ	0-2590-3185	088-4287331
3.	นายศิโรรัช ทองทิพย์	นักประชาสัมพันธ์	0-2590-3185	089-2346904
4.	น.ส.ขนิษฐา ทับทิม	นักวิชาการเผยแพร่	0-2590-3185	098-2933537

บทบาทหน้าที่ทีมด้านสื่อสารและประชาสัมพันธ์ (Communication and PR Team) : ดูแลการสื่อสารภายในและภายนอกในสถานการณ์ฉุกเฉิน รวมถึงการแถลงข่าว การแจ้งเตือนผู้ใช้งาน และการประสานกับหน่วยงานรัฐอื่น ๆ

5. ทีมประเมินและปรับปรุงแผน (Post-Incident Evaluation Team)

ตารางที่ 3.5 ทีมประเมินและปรับปรุงแผน (Post-Incident Evaluation Team)

ลำดับที่	ชื่อ - นามสกุล	ตำแหน่ง	ช่องทางสื่อสาร	
			โทรศัพท์	มือถือ
1.	นางสาวสุดธิดา แสงยนต์	นักวิชาการสาธารณสุขชำนาญการ	0-2590-3168	086-1045584
2.	น.ส.ภิญญาดา ดอนนนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	081-81113615
3.	นายเทพาทิป เชาวนิวิจิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	0-2590-3168	097-9949891
4.	นางอำภาพร รอดรัตน์	นักวิชาการคอมพิวเตอร์	0-2590-3168	091-9861282
5.	น.ส.กัลยาณี ดวงตา	เจ้าพนักงานคอมพิวเตอร์	0-2590-3168	081-7716061

บทบาทหน้าที่ทีมประเมินและปรับปรุงแผน (Post-Incident Evaluation Team) : ภายหลังการเกิดเหตุฉุกเฉิน คณะทำงานนี้จะรับผิดชอบการวิเคราะห์เหตุการณ์ ประเมินประสิทธิภาพของการตอบสนอง และจัดทำข้อเสนอแนะเพื่อปรับปรุงแผนในอนาคต

3.2 ช่องทางการสื่อสารในภาวะเกิดเหตุการณ์วิกฤต

1. ช่องทางการสื่อสารภายใน (Internal Communication Channels)
   ใช้สำหรับการประสานงานภายในหน่วยงานระหว่างผู้บริหาร เจ้าหน้าที่ IT คณะทำงานฉุกเฉิน และบุคลากรที่เกี่ยวข้อง ตามตารางที่ 1.7

ตารางที่ 3.6 ช่องทางการสื่อสารภายใน (Internal Communication Channels)

ลำดับ	ช่องทาง	รายละเอียดการใช้งาน
1	โทรศัพท์สายตรง / Hotline	ใช้ติดต่อด่วนระหว่างผู้มีอำนาจตัดสินใจและเจ้าหน้าที่ผู้รับผิดชอบ
2	ระบบวิทยุสื่อสาร (หากมี)	ใช้ในกรณีเครือข่ายโทรศัพท์ล่ม
3	กลุ่มไลน์ / Zoom Conference	สำหรับส่งข้อความแจ้งเตือนและติดตามสถานการณ์แบบ Real-time
4	อีเมลภายในหน่วยงาน	ใช้สำหรับการส่งรายงานสรุปสถานการณ์และคำสั่งต่าง ๆ
5	ป้ายประชาสัมพันธ์ / ระบบ Intranet	สำหรับแจ้งเตือนบุคลากรทั้งหน่วยงาน

2. ช่องทางการสื่อสารภายนอก (External Communication Channels)

ใช้ในการประสานงานกับหน่วยงานภายนอก และประชาชนผู้ใช้งาน

ตารางที่ 3.7 ช่องทางการสื่อสารภายนอก (External Communication Channels)

ลำดับ	ช่องทาง	รายละเอียดการใช้งาน
1	โทรศัพท์สายตรงผู้ให้บริการ (ISP, Cloud, Data Center)	แจ้งเหตุขัดข้องและขอความช่วยเหลือทันที
2	ติดต่อสำนักงานพัฒนารัฐบาลดิจิทัล (DGA) หรือ ThaiCERT	แจ้งเหตุภัยคุกคามไซเบอร์หรือเหตุความไม่มั่นคง
3	เว็บไซต์หน่วยงาน	แจ้งสถานการณ์และแนวทางแก้ไขให้ประชาชนทราบ
4	ช่องทางโซเชียลมีเดีย (Facebook, Line , TikTok ฯลฯ)	กระจายข้อมูลข่าวสารอย่างรวดเร็วและกว้างขวาง
5	สื่อมวลชน / แถลงข่าว	กรณีเกิดเหตุการณ์ขนาดใหญ่ที่กระทบต่อสาธารณะภาพรวม

บทที่ 4 แนวทางการรับมือเหตุฉุกเฉิน

ด้วยสถานการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศมีแนวโน้มทวีความรุนแรงและซับซ้อนมากยิ่งขึ้น หน่วยงานภาครัฐจึงจำเป็นต้องมีมาตรการ และแนวทาง เพื่อรองรับเหตุการณ์ฉุกเฉิน เพื่อให้สามารถฟื้นฟูระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้กลับมาทำงานได้โดยเร็ว ลดความเสียหาย และรักษาความมั่นคงปลอดภัยของข้อมูลภาครัฐ

4.1 เหตุการณ์ความเสี่ยงด้านข้อมูลช่องโหว่จากความเสี่ยงจากผู้บุกรุกระบบฐานข้อมูลจากภายนอกที่มีการละเมิดข้อมูลในระบบ

4.1.1 มาตรการเตรียมความพร้อม (Preparedness)

1) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 โดยได้จัดหาระบบบริหาร จัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของหน่วยงานให้ดียิ่งขึ้น

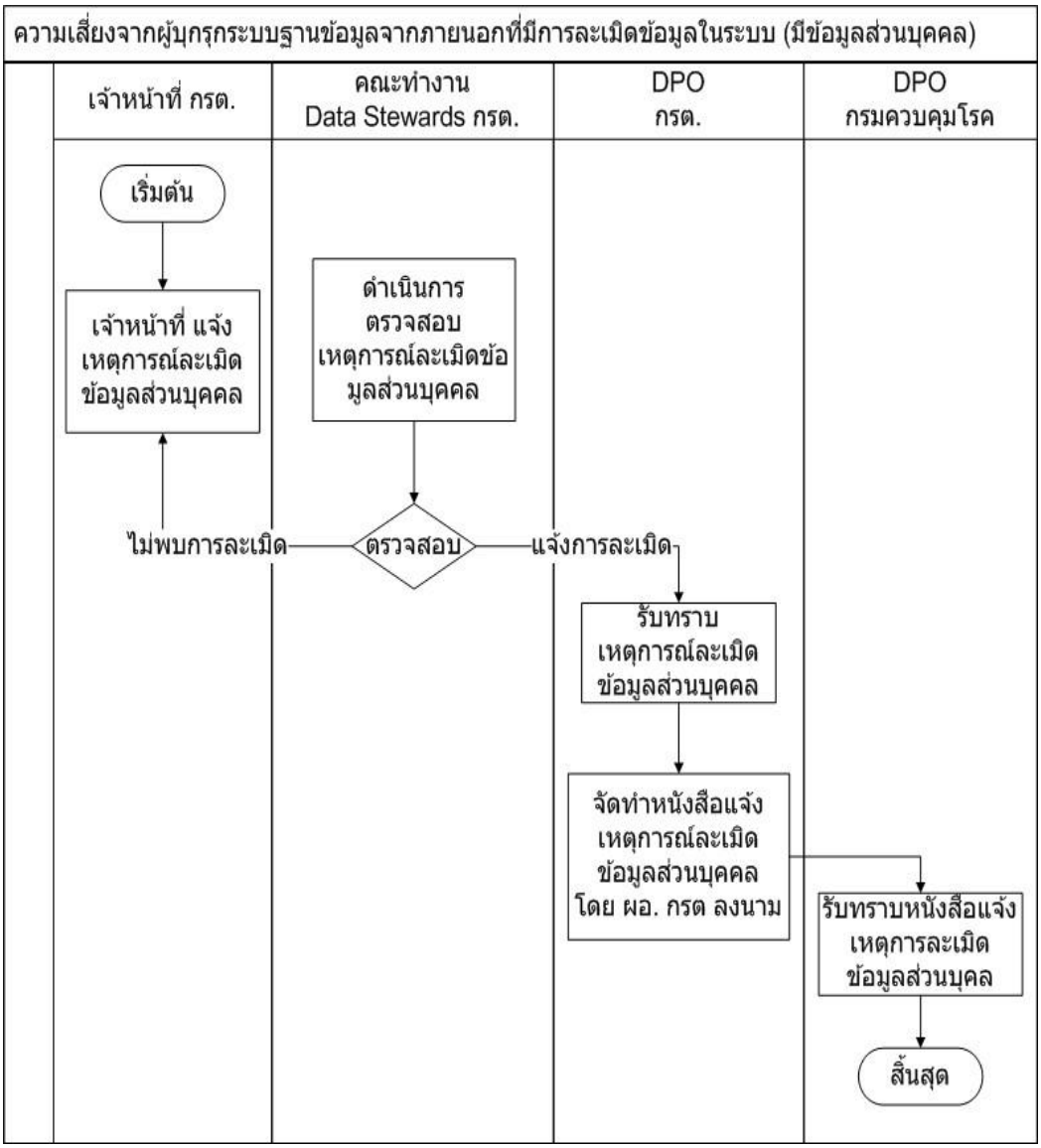
2) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

3) อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอวันละ 1 ครั้ง เป็นอย่างน้อย สั่งสแกนไวรัสสัปดาห์ละ 1 ครั้ง

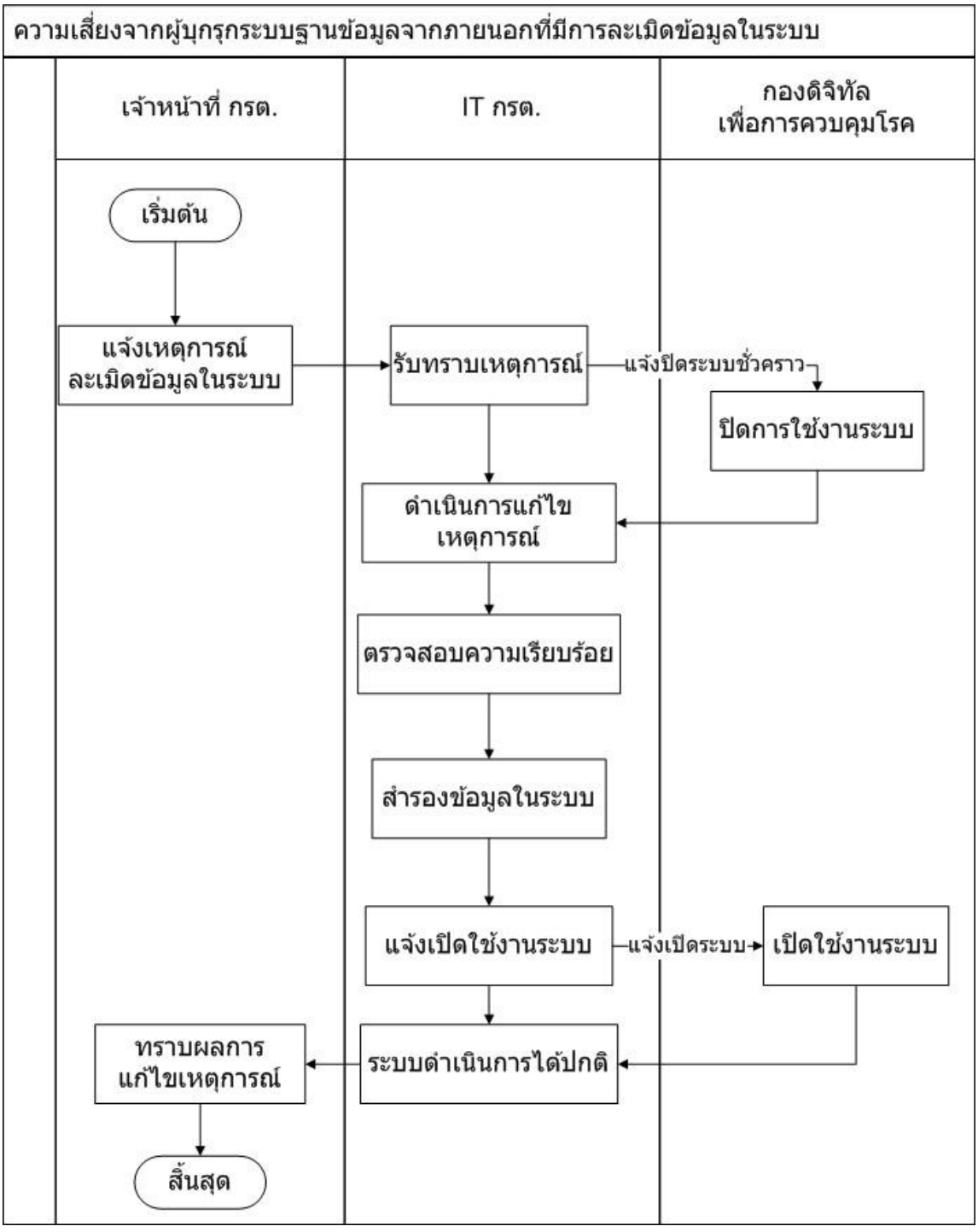
4) ผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ตหรือการใช้งานอีเมล์ เพื่อไม่ให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

4.1.2 มาตรการตอบสนองเมื่อเกิดเหตุ (Response)

กรณีบุกรุกฐานข้อมูลจากบุคคลภายนอก (มีข้อมูลส่วนบุคคล)



กรณีบุกรุกฐานข้อมูลจากบุคคลภายนอก (ไม่มีข้อมูลส่วนบุคคล)



5 มาตรการฟื้นฟูระบบให้กลับมาใช้งาน (Recovery)

กรณีบุกรุกฐานข้อมูลจากบุคคลภายนอก

1. ระงับเหตุและแยกระบบที่ได้รับผลกระทบ
2. ประเมินความเสียหายและค้นหาสาเหตุ
3. กู้คืนข้อมูลจากระบบสำรอง (Backup Recovery)
4. ปิดช่องโหว่ก่อนนำระบบกลับมาใช้งาน
5. ทดสอบระบบก่อนเปิดใช้งาน
6. แจ้งเหตุและรายงานตามขั้นตอนราชการ
7. สรุปบทเรียนและปรับปรุงระบบ

6 การสื่อสารความเสี่ยงและรายงานเหตุการณ์

1. ตรวจพบการละเมิดข้อมูล (Data Breach Detection)
   - ตรวจพบจากระบบเฝ้าระวัง (SIEM, Firewall, IDS/IPS) หรือการแจ้งจากบุคคลภายนอก
   - ทำการบันทึกเวลาที่ตรวจพบ และรายละเอียดเบื้องต้น

2. แจ้งเตือนทีมความมั่นคงสารสนเทศ (IT Security Team) และเริ่มต้นกระบวนการตอบสนองเหตุการณ์ (Incident Response)

3. ประเมินความรุนแรงของเหตุการณ์ ตรวจสอบข้อมูลที่ถูกเข้าถึง เช่น ข้อมูลบุคลากร ข้อมูลทางการเงิน ประเมินผลกระทบต่อหน่วยงานและข้อกฎหมาย

4. แจ้งผู้บริหารและผู้มีส่วนเกี่ยวข้องพร้อมทั้งรายงานเหตุการณ์เบื้องต้นต่อผู้บริหารระดับสูงหรือคณะกรรมการความปลอดภัยสารสนเทศ

5. แจ้งหน่วยงานกำกับดูแล (ถ้ามี)
   - หากเหตุการณ์เข้าข่ายการละเมิดข้อมูลส่วนบุคคล ให้แจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล (PDPA) ภายใน 72 ชั่วโมง
   - จัดเตรียมข้อมูลหลักฐานและแนวทางการแก้ไขเบื้องต้น

6. สื่อสารต่อผู้มีข้อมูลได้รับผลกระทบ
   - แจ้งผู้ใช้หรือเจ้าของข้อมูลที่ได้รับผลกระทบโดยสุภาพและโปร่งใส
   - แนะนำวิธีป้องกันตัว เช่น การเปลี่ยนรหัสผ่าน หรือระวังอีเมลหลอกลวง

7. ดำเนินการตอบสนองและแก้ไขช่องโหว่ เช่น ปรับสิทธิ์ผู้ใช้, ปรับ Firewall ตรวจสอบ log และติดตามร่องรอยผู้บุกรุกเพิ่มเติม

8. จัดทำรายงานสรุปเหตุการณ์ (Incident Report) สรุปเหตุการณ์ สาเหตุ ผลกระทบ การตอบสนองและแนวทางป้องกัน เสนอต่อฝ่ายบริหารและเก็บเป็นเอกสารอ้างอิง

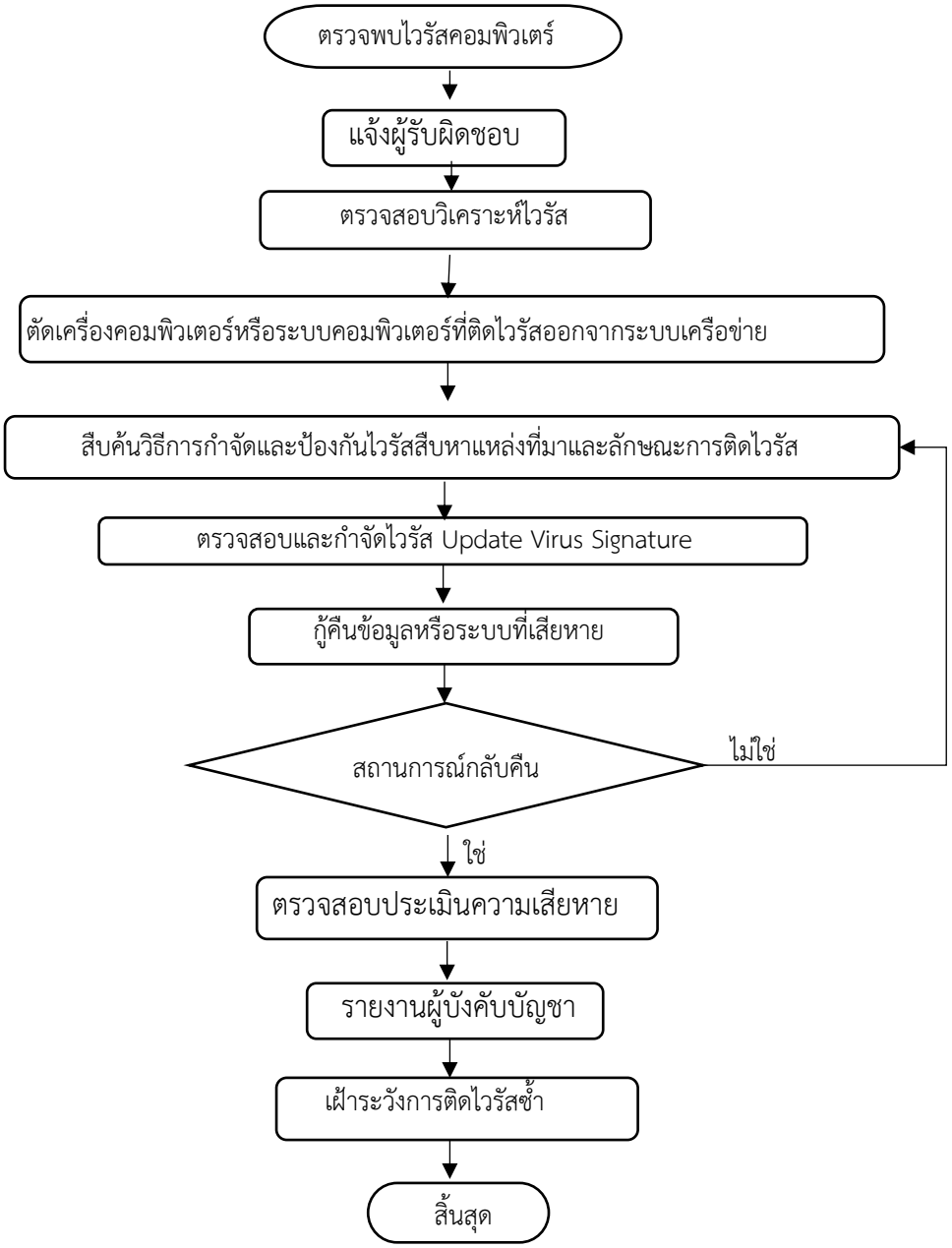
9. อบรมและให้ความรู้แก่บุคลากรเพิ่มเติม จัดกิจกรรมฝึกอบรมเพื่อให้พนักงานตระหนักรู้เกี่ยวกับภัยไซเบอร์และข้อมูลส่วนบุคคล ส่งเสริมการใช้ระบบอย่างปลอดภัย

4.2 เหตุการณ์ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ ช่องโหว่จากโปรแกรม/ระบบไม่มีการอัพเดทอย่างสม่ำเสมอ

7 มาตรการเตรียมความพร้อม (Preparedness)

- ระบบป้องกันเชิงเทคนิค (Technical Measures)
- ติดตั้งโปรแกรม Antivirus/Anti-Malware ที่มีลิขสิทธิ์และทันสมัยทุกเครื่อง
- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ อย่างสม่ำเสมอ (Windows Update, Security Patch
- ปิดฟีเจอร์ Autorun และการรันไฟล์จาก USB โดยอัตโนมัติ
- การตรวจสอบและทดสอบ (Monitoring & Testing)
- สแกนไวรัสตามรอบเวลา อย่างน้อยรายสัปดาห์ในทุกเครื่อง

8 มาตรการตอบสนองเมื่อเกิดเหตุ (Response)



9 มาตรการฟื้นฟูระบบให้กลับมาใช้งาน (Recovery)

1.แยกและควบคุมระบบหรือเครื่องคอมพิวเตอร์ที่ติดไวรัส ปิดเครื่องหรือแยกออกจากเครือข่ายทันที (Network Isolation)

2. ตรวจสอบและวิเคราะห์ความเสียหาย สแกนด้วยโปรแกรม Antivirus / Anti-malware ที่เชื่อถือได้

3. ดำเนินการฟื้นฟูระบบ ล้างเครื่อง (Format) และติดตั้ง OS ใหม่ หากจำเป็นกู้คืนข้อมูลจาก Backup ที่ปลอดภัยและไม่ปนเปื้อนไวรัสตรวจสอบความสมบูรณ์ของข้อมูล ก่อนกลับเข้าสู่ระบบ

4. อัปเดตระบบและเสริมความปลอดภัยติดตั้ง Security Patch และอัปเดตโปรแกรม Antivirus ทบทวนนโยบายการใช้ USB, การดาวน์โหลด, การเข้าถึงระบบ

10 **การสื่อสารความเสี่ยงและรายงานเหตุการณ์**

1. เจ้าหน้าที่หรือผู้ใช้งานแจ้งเหตุ หรือระบบตรวจพบว่ามีช่องโหว่ที่ยังไม่ได้รับการอัปเดต

2. ทีมความมั่นคงสารสนเทศทำการประเมินระดับความเสี่ยงของช่องโหว่

3. แจ้งเตือนฝ่ายที่เกี่ยวข้องทันทีส่งข้อมูลเหตุการณ์ไปยังผู้มีหน้าที่รับผิดชอบ (IT Security, IT Support, ผู้บริหารระดับที่เกี่ยวข้อง)

4. บันทึกเหตุการณ์ลงในระบบรายงานเหตุการณ์ (Incident Log) ระบุวันเวลา, ผู้แจ้งเหตุ, รายละเอียดช่องโหว่, โปรแกรมที่ได้รับผลกระทบ, ระดับความรุนแรง

5. สื่อสารภายในองค์กร แจ้งผู้ใช้งานระบบเกี่ยวกับช่องโหว่ พร้อมคำแนะนำเบื้องต้น เช่น หลีกเลี่ยงการใช้งานบางฟีเจอร์, ปิดการใช้งานชั่วคราว

6. แจ้งแผนการดำเนินการแก้ไข สื่อสารกำหนดการอัปเดตระบบหรือการแก้ไขช่องโหว่ให้ผู้เกี่ยวข้องรับทราบ

7. ติดตามและรายงานสถานะการแก้ไข แจ้งความคืบหน้าอย่างสม่ำเสมอจนกว่าจะดำเนินการอัปเดตหรือแก้ไขเรียบร้อย

8. จัดทำรายงานสรุปเหตุการณ์ จัดทำรายงานฉบับสมบูรณ์ (Incident Report) สำหรับผู้บริหารและหน่วยงานกำกับดูแล (ถ้ามี)

9. ทบทวนและสื่อสารบทเรียนจากเหตุการณ์ ประชุมสรุปบทเรียน (Lessons Learned) และสื่อสารแนวทางป้องกันไม่ให้เกิดซ้ำ

10. ปรับปรุงแผนรับมือเหตุการณ์ (Incident Response Plan) อัปเดตขั้นตอนหรือคู่มือให้สอดคล้องกับเหตุการณ์ที่เกิดขึ้น

4.3 เหตุการณ์ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม ช่องโหว่จากไฟฟ้าดับ

11 มาตรการเตรียมความพร้อม (Preparedness)

1.ติดตั้งระบบสำรองไฟ (UPS/Generator)

2. จัดทำแผนความต่อเนื่อง (Business Continuity Plan: BCP)

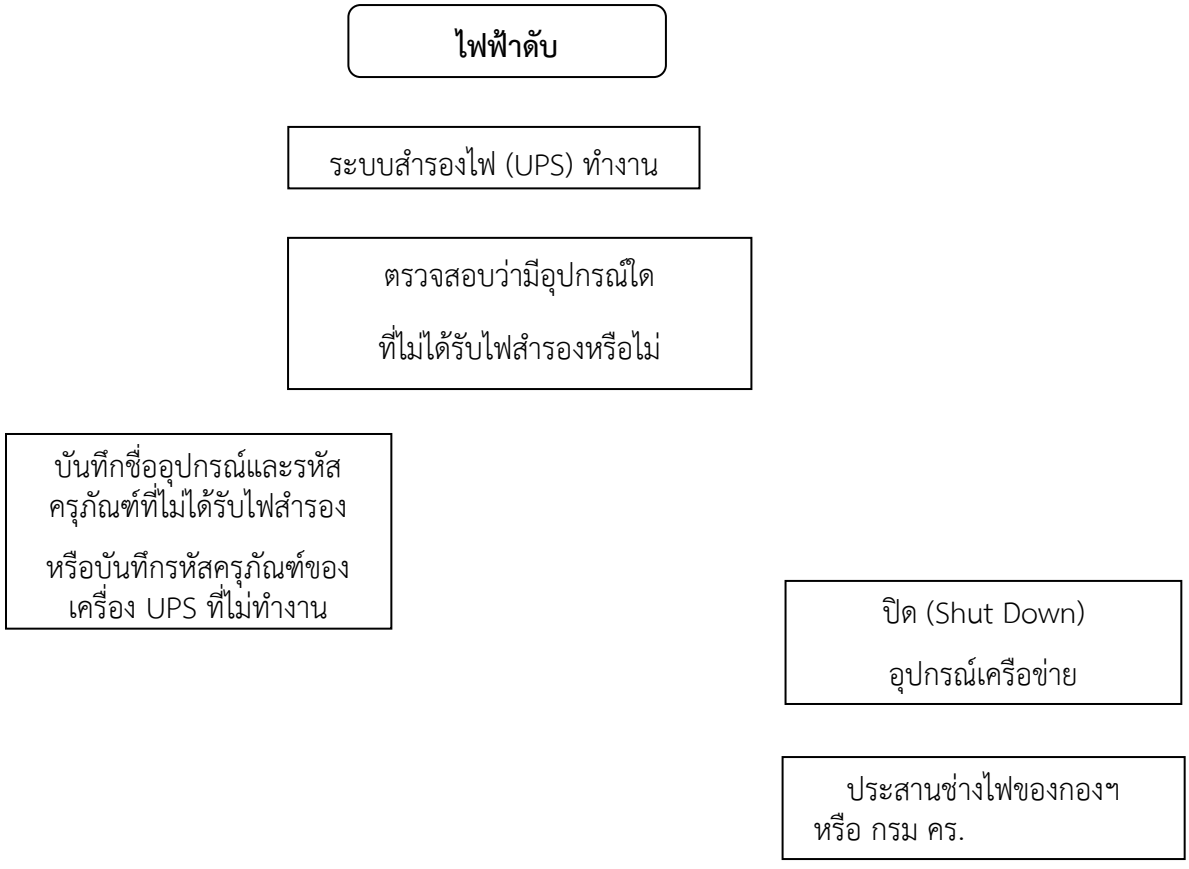
3. ระบบแจ้งเตือนและเฝ้าระวัง

4. อบรมบุคลากรเกี่ยวกับการรับมือเหตุไฟฟ้าดับ

5. สำรองข้อมูลอย่างต่อเนื่อง

6. ปฏิบัติตามแนวทางการจัดการพลังงานภาครัฐ

12 มาตรการตอบสนองเมื่อเกิดเหตุ (Response)



13 มาตรการฟื้นฟูระบบให้กลับมาใช้งาน (Recovery)

1. ประเมินสถานการณ์ทันทีหลังไฟฟ้ากลับมาตรวจสอบว่าไฟฟ้า และระบบสำรองไฟ (UPS/Generator) ว่ายังทำงานหรือมีปัญหากลับมาใช้งานได้คงที่หรือไม่

2. ตรวจสอบระบบและอุปกรณ์ IT ว่าเปิดทำงานตามปกติหรือไม่ หากระบบไม่สามารถบูตได้ ให้บันทึก Error และแจ้งเจ้าหน้าที่ที่เกี่ยวข้อง

3. ดำเนินการเปิดระบบตามขั้นตอนอย่างปลอดภัย เช่นระบบฐานข้อมูล ระบบ Application หลีกเลี่ยงการเปิดระบบพร้อมกันทุกเครื่องเพื่อลดโหลดไฟฟ้า

4. ทดสอบระบบและการให้บริการ ตรวจสอบว่า Services ต่าง ๆ สามารถใช้งานได้ เช่นระบบฐานข้อมูล ระบบสารบรรณ ระบบเว็บไซต์ บริการประชาชน

5.ตรวจสอบความสมบูรณ์ของข้อมูล ตรวจสอบว่าไม่มีข้อมูลสูญหายหรือเสียหายจากการดับกะทันหัน หากพบปัญหา ให้ดำเนินการกู้คืนจาก Backup

6. แจ้งผู้บริหารและหน่วยงานต้นสังกัดถึงสถานการณ์และการกู้ระบบ หากมีผลกระทบต่อประชาชน ให้แจ้งผ่านช่องทางทางการของหน่วยงาน เช่น เว็บไซต์/เพจ

14 การสื่อสารความเสี่ยงและรายงานเหตุการณ์

1.ตรวจพบเหตุการณ์ไฟดับ

- เจ้าหน้าที่ตรวจพบการไฟฟ้าขัดข้อง
- แจ้งเจ้าหน้าที่ไอทีหรือทีมวิศวกรรมทันที

2. ประเมินผลกระทบเบื้องต้น
3. ตรวจสอบว่าพื้นที่ใดได้รับผลกระทบ (เฉพาะส่วน, ทั้งอาคาร, เฉพาะระบบไอที)
4. ตรวจสอบอุปกรณ์สำคัญ เช่น Server, ระบบเน็ตเวิร์ก, ระบบสำรองไฟ
5. แจ้งเตือนฝ่ายที่เกี่ยวข้อง
    - ฝ่ายบริหาร
    - เจ้าหน้าที่อาคารหรือทีมซ่อมบำรุง
    - ทีมเจ้าหน้าที่ไอที
    - พนักงานในพื้นที่ที่ได้รับผลกระทบ
6. บันทึกรายละเอียด: วันเวลาเกิดเหตุ, สาเหตุ (หากทราบ), ระยะเวลาที่ไฟดับ, อุปกรณ์ได้รับผลกระทบ
7. สื่อสารแนวทางการดำเนินการให้แก่ผู้ใช้งานเกี่ยวกับ
    - การปิดระบบอย่างปลอดภัย (หากจำเป็น)
    - การใช้งานเครื่องสำรองไฟ
    - การย้ายไปทำงานในพื้นที่ปลอดภัย (ถ้ามี)

8. ติดตามสถานการณ์
    - สื่อสารความคืบหน้าการฟื้นฟูไฟฟ้า หรือการเปลี่ยนไปใช้พลังงานสำรอง
    - ประเมินเวลาที่ระบบจะกลับมาใช้งานได้ตามปกติ
9. แจ้งผลการฟื้นฟูเมื่อไฟฟ้ากลับมาเป็นปกติ พร้อมแจ้งขั้นตอนการเปิดใช้งานระบบใหม่อย่างปลอดภัย
10. จัดทำรายงานสรุปเหตุการณ์ (Post-Incident Report)
11. รายงานผลกระทบ, การตอบสนอง, ระยะเวลา downtime, แนวทางป้องกันในอนาคต
12. สื่อสารบทเรียนและแนวทางป้องกัน
    - ประชุมสรุปเหตุการณ์ พร้อมแนะนำการปรับปรุง เช่น การเพิ่มระบบสำรองไฟ, การฝึกซ้อมแผนรับมือไฟดับ

หมายเหตุ: รายงานควรถูกส่งให้กับ

- ผู้บริหารหน่วยงาน
- หน่วยงานแม่ข่ายด้าน ICT (เช่น สำนักงานปลัดกระทรวงสาธารณสุข/กองดิจิทัลเพื่อการควบคุมโรค)
- หน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ เช่น สกมช. หรือ ThaiCERT ในกรณีไซเบอร์

ภาคผนวก

เบอร์โทรศัพท์หน่วยงานที่เกี่ยวข้อง หากเกิดเหตุฉุกเฉิน

หน่วยงาน	หมายเลขโทรศัพท์
กลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์ กองดิจิทัลเพื่อการควบคุมโรค	0 2590 3260
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข	0 2590 1000
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ(NECTEC)	0 2564 6900
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	0 2114 3531
สำนักเลขานุการกรมควบคุมโรค	0 2590 3820
สายด่วนแจ้งเหตุเพลิงไหม้และดับเพลิง	199
กรมป้องกันและบรรเทาสาธารณภัย (ปภ.)	1784
กรมอุตุนิยมวิทยา (ข้อมูลพยากรณ์อากาศและแจ้งเตือนพายุ)	1182
กรมทางหลวงชนบท (แจ้งถนนเสียหายหรือสะพานชำรุด)	1182
กรมทางหลวง (สอบถามเส้นทางและแจ้งถนนอันตราย)	1586
ศูนย์เตือนภัยพิบัติแห่งชาติ (แจ้งเตือนแผ่นดินไหวและภัยธรรมชาติอื่น ๆ)	1586
แจ้งเหตุด่วนเหตุร้าย (ตำรวจ)	191
สายด่วนแพทย์ฉุกเฉิน / รถพยาบาล	1669
สภากาชาดไทย (บรรเทาทุกข์ผู้ประสบภัย)	02 251 7853-6
กรมควบคุมโรค	1422