กรมชลประทาน

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

IT CONTINGENCY PLAN

ประจำปีงบประมาณ พ.ศ. 2568

คณะทำงานจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ภายใน 2625

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมชลประทาน กระทรวงเกษตรและสหกรณ์

สารบัญ

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(IT Contingency Plan)

๑. ความเป็นมา

กรมชลประทาน ได้พัฒนาระบบเทคโนโลยีสารสนเทศช่วยบริหารจัดการงานด้านพัฒนาแหล่งน้ำด้านบริหารจัดการน้ำ และการป้องกันและบรรเทาภัยอันเกิดจากน้ำ รวมถึงการมีส่วนร่วมของประชาชนในภารกิจต่าง ๆ ของงานชลประทาน และเพื่อรักษาระดับประสิทธิภาพในการดำเนินงานให้บริการแก่ประชาชนให้ได้รับความสะดวก ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศที่กำกับดูแลนั้น อาจได้รับความเสียหายจากการถูกโจมตีจากโลกไซเบอร์ ไม่ว่าจะเป็น ไวรัสคอมพิวเตอร์ แฮกเกอร์ หรือจากสภาพแวดล้อมพื้นฐาน ปัญหาไฟฟ้า จากอัคคีภัย แม้กระทั่งการชุมนุมทางการเมืองหรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของกรมชลประทาน เพื่อป้องกันและแก้ไขปัญหาดังกล่าว ศูนย์เทคโนโลยีสารสารสนเทศและการสื่อสาร กรมชลประทาน ได้เล็งเห็นความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒. หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการจำเป็นต้องได้รับการดูแล รักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสารสนเทศและการสื่อสาร กรมชลประทาน ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศของกรมชลประทาน ซึ่งอาจมีปัจจัยภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลสารสนเทศ ที่ใช้ในการบริหารจัดการ

ดังนั้น ศูนย์เทคโนโลยีสารสารสนเทศและการสื่อสาร กรมชลประทาน จึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนสู่ความปกติ ตลอดจนการดูแลรักษาฐานข้อมูลและสารสนเทศของกรมชลประทาน ให้มีเสถียรภาพพร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

๓. วัตถุประสงค์

๓.๑ เพื่อให้ระบบเทคโนโลยีสารสนเทศ สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพในการแก้ไขสถานการณ์ฉุกเฉินได้อย่างทันท่วงที

๓.๒ เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓.๓ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๓.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมชลประทาน

๓.๕ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกรมชลประทาน

๔. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๔.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกรมชลประทาน สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องคอมพิวเตอร์แม่ข่าย เช่น อัคคีภัย อุทกภัย วาตภัย ความชื้น อุณหภูมิ แผ่นดินไหว ภัยแล้ง คลื่นความร้อน ฯลฯ

๒) การชุมนุมประท้วงทางการเมือง เพื่อปิดกั้นการเข้าถึงกรมชลประทานและศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดประสงค์ไม่ให้เจ้าหน้าที่สามารถปฏิบัติงานได้

๓) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๔) ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

๕) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๖) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๗) ไวรัสคอมพิวเตอร์ และโปรแกรมเรียกค่าไถ่ (Ransomware)

๘) โรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง

ภัยพิบัติจากภายใน

๑) เครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) เครื่องมืออุปกรณ์ด้านสื่อสารโทรคมนาคม เสียหายหรือถูกทำลาย

๓) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

๔) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์ด้านสื่อสารโทรคมนาคมอันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

๔.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้วจะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อนำมาจัดทำกระบวนการและผังงานการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ รวมทั้งแผนกู้คืนระบบกลับสู่สภาพเดิมต่อไป

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (๑ รุนแรงต่ำสุด, ๕ รุนแรงสูงสุด)				คะแนนรวม	จัดลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อเจ้าหน้าที่ภายในกรม	ต่อประชาชน		
ไฟไหม้	๕	๕	๕	๕	๒๐	๑
โดนเจาะระบบ และภัยคุกคามทางไซเบอร์	๕	๓	๕	๕	๑๘	๒
ไฟฟ้าดับ / หม้อไฟระเบิด	๕	๑	๕	๕	๑๖	๓
น้ำท่วม	๔	๒	๕	๔	๑๕	๔
แผ่นดินไหว	๔	๑	๕	๔	๑๔	๕
โรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง	๓	๑	๕	๔	๑๓	๖
ชุมนุมประท้วง และก่อจลาจล	๓	๑	๔	๔	๑๒	๗

๕. แนวทางการป้องกันและเตรียมการเบื้องต้น

๕.๑ การประกาศแผน (Activation)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการประกาศใช้แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัดเมื่อเกิดเหตุการณ์ฉุกเฉิน

๕.๒ กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในกรมชลประทาน โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้องระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๕.๓ การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอกเพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๕.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC/เครื่องคอมพิวเตอร์ Notebook

- อุปกรณ์สำรองข้อมูลของระบบงานที่สำคัญ เช่น External Hard Disk/SAN Storage/NAS Storage/Cloud
- โปรแกรม Antivirus/Spyware
- Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน/ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๕.๕ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยกรมชลประทานมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy) ดังนี้

๑) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้โดยสำรองในเวลาตามที่ระบบกำหนดไว้รวมถึงการสำรองไปยัง Backup site ตามแนวทางที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนดแต่ละประเภทตามแผนการสำรองข้อมูล

๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำสัปดาห์ โดยจะทำการสำรองข้อมูล Source Code และบันทึกข้อมูลในหน่วยจัดเก็บข้อมูลสำรอง (Secondary Storage)

๕.๖ การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยกรมชลประทานมีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

๕.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) มีระบบสำรองไฟฉุกเฉินและแยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายเมนหลักของอาคารศูนย์วิศวกรรมการชลประทาน (อาคารที่ตั้งของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ของกรมชลประทาน)

๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องแม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้ประมาณ ๑๕-๓๐ นาที

๓) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๕) ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ ปริมาณน้ำมัน แบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติ สัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้า

ถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้ อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

๕.๘ การป้องกันการบุกรุก และภัยคุกคามทางไซเบอร์

เพื่อเป็นการป้องกัน และเสริมสร้างความมั่นคงความปลอดภัยทางไซเบอร์ให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทาง ดังนี้

๑) มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน

๒) มีมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) หรือรหัสเพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้งระบบ SSL VPN ควบคุมการเข้าถึงและใช้บริการระบบเครือข่ายจากภายนอก

๕) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)

๖) มีการติดตั้ง SSL (Secure Socket Layer) ใบรับรองความปลอดภัยบนเครื่องคอมพิวเตอร์แม่ข่าย

๗) มีการติดตั้งระบบ Anti-Spam mail ป้องกันอีเมล์ขยะ

๘) มีการติดตั้งระบบป้องกันมัลแวร์

๙) มีการสำรองข้อมูล

๑๐) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๑๑) มีการตรวจสอบด้านความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย

๑๒) มีระบบรักษาความมั่นคงปลอดภัยของเว็บไซต์ตามมาตรฐานการรักษาความมั่นคงปลอดภัย สำหรับเว็บไซต์ (Website Security Standard : WSS)

๑๓) มีการพัฒนาเว็บไซต์ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บไซต์ (Web Application security Standard : WAS)

๑๔) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางไซเบอร์ได้เป็นอย่างดี

๑๕) มีการกำหนดแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน

๑๖) เข้าร่วมโครงการกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) เพื่อติดตามตรวจสอบ เครือข่าย ป้องกันการบุกรุก ช่วยวิเคราะห์รูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นกับระบบเครือข่ายกรมชลประทาน (Government Threat Monitoring System : GTM) และเพื่อตรวจสอบช่องโหวเว็บไซต์ (Vulnerability Assessment) และป้องกันการโจมตีเว็บไซต์กรมชลประทาน (Government Website Protection System : GWP)

๕.๙ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็นกรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ ดังนี้

๑) เตรียมไฟฉายอุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้นเพื่อปฏิบัติในยามฉุกเฉิน

๓) ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และตู้ควบคุมระบบไฟฟ้าในอาคาร

๔) ไม่วางของหนักไว้บนชั้น หลังตู้หรือที่สูง

๕) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๖) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๖. การเตรียมความพร้อม

๖.๑ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อไฟฟ้าดับและปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๖.๑.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อแปลงไฟฟ้าระเบิด

๖.๑.๒ ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ ปริมาณน้ำมัน แบตเตอรี่และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้ อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

๖.๑.๓ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๑๕-๓๐ นาที

๖.๑.๔ ตรวจสอบระบบไฟฟ้าและอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ

๖.๑.๕ จัดทำ Checklist ระยะเวลาในการปิด/เปิดระบบสารสนเทศกรมชลประทาน ที่มีเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย กรณีที่ระบบไฟฟ้าดับหรือถูกตัด

๖.๑.๖ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๖.๑.๗ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ

๖.๑.๘ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๖.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๖.๒.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

๖.๒.๒ ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น สำหรับห้องปฏิบัติงานคอมพิวเตอร์ควรติดตั้งถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ได้เป็นอย่างน้อย (อุปกรณ์ ไฟฟ้า อิเล็กทรอนิกส์คอมพิวเตอร์)

๖.๒.๓ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๖.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุน้ำท่วม

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๖.๓.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม

๖.๓.๒ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๖.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัสคอมพิวเตอร์

๖.๔.๑ ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๖.๔.๒ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๖.๔.๓ อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย (Update Patch)

๖.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางไซเบอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการป้องกัน และเสริมสร้างความปลอดภัยทางไซเบอร์ให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๖.๕.๑ กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๖.๕.๒ หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้อง ให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออกและคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card และรหัสผ่านพร้อมทั้งติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๖.๕.๓ มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยเปิดใช้งาน Firewall ตลอดเวลา

๖.๕.๔ มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ ผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๖.๕.๕ มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๖.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่แผนกต่าง ๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๖.๖.๑ สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กรเพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๖.๖.๒ วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติเพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๖.๗ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูลประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๖.๗.๑ ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลกมาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

๑) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศข้อมูลอุณหภูมิข่าวเตือนภัย (www.tmd.go.th)

๒) ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (https://ndwc.disaster.go.th/)

๓) กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม/แผ่นดินไหว (www.dmr.go.th)

๔) หน่วยงานสำรวจเชิงภูมิศาสตร์ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)

๕) กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัยมาตรการและแนวทางปฏิบัติ (www.disaster.go.th)

๖.๗.๒ การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้เช่น

๑) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

๒) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน

๓) หนู งู ออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

๔) ปลากระโดดขึ้นมาจากผิวน้ำ

๖.๗.๓ การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

๑) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

๒) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคนวัสดุอุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

๓) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่มสำหรับบุคลากรขององค์กร

๔) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

๕) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๖.๗.๔ การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๑) สำรวจอาคารสูงอาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบ ของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบ กฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

๒) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๖.๗.๕ การปฏิบัติขั้นเตรียมการ

๑) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

๒) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัยโดยแยกประเภทเป้าหมายตามความสำคัญและกำหนดมาตรการในการเผชิญภัย

๓) อบรมให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่มแก่เจ้าหน้าที่ในองค์กร

๔) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๖.๘ การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๖.๘.๑ จัดทำแผนเตรียมความพร้อมรับสถานการณ์การชุมนุมทางการเมืองด้านเทคโนโลยีสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน

๖.๘.๒ จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ กรมชลประทาน (Business Continuity Planning) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่สำนักงานกรมชลประทานได้ ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์วิทยุและหน่วยงานที่เกี่ยวข้อง

๖.๘.๓ จัดเตรียมกำลังเจ้าหน้าที่ วัสดุอุปกรณ์เครื่องมือเครื่องใช้ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๖.๘.๔ ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมระบบเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน

๖.๘.๕ ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๖.๘.๖ สำรองข้อมูล

๖.๘.๗ จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันทีโดยไม่ต้องเดินทางมาปฏิบัติงานที่กรมชลประทาน

๖.๘.๘ จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๖.๙ การเตรียมความพร้อมรับสถานการณ์ภัยจากโรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง

๖.๙.๑ จัดทำแนวทางการใช้เทคโนโลยีสนับสนุนการปฏิบัติงานนอกสถานที่ตั้งราชการ

๖.๙.๒ เพื่อเป็นการเฝ้าระวัง และตรวจสอบให้ระบบสารสนเทศของกรมชลประทานพร้อมใช้งานอย่างต่อเนื่อง จึงต้องมีการจัดเวรยามรักษาการณ์เฝ้าระวัง ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตรวจสอบความพร้อมใช้งานของห้องควบคุมเครือข่ายคอมพิวเตอร์ ได้แก่

- ห้องควบคุมเครือข่ายคอมพิวเตอร์
- เครื่องสำรองไฟฟ้าอัตโนมัติ (UPS)
- ระบบเครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น (Precision Air Conditioning System)
- เครื่องกำเนิดไฟฟ้า

๖.๙.๓ จัดเตรียมช่องทาง SSL VPN เพื่อให้ดูแลระบบสามารถเข้าถึงระบบ ฯ หรือเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างปลอดภัย

๖.๙.๔ จัดเตรียมระบบอินเทอร์เน็ตความเร็วสูง (Fiber Optic) หรือ เทคโนโลยี MPLS (Multiprotocol Label Switching) หรือ Leased Line

๖.๙.๕ จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่พร้อมกล้องวีดีโอ หูฟัง และลำโพง หรือ Device อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายภายในสำนักงานได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติราชการนอกสถานที่

๖.๙.๖ จัดเตรียมแอปพลิเคชัน และเทคโนโลยีที่สนับสนุนการทำงานต่าง ๆ สำหรับการปฏิบัติงานร่วมกันระหว่างผู้ที่ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

๖.๙.๗ จัดเตรียมระบบสนับสนุนการทำงานร่วมกันจากทางไกล จัดเก็บเอกสาร ไฟล์เข้าถึงไฟล์งานได้จากภายนอก รองรับการจัดเก็บข้อมูลต่าง ๆ แบบรวมศูนย์

๖.๙.๘ จัดเตรียมระบบประชุม Conference สนับสนุนการประชุมทางไกลออนไลน์นอกสถานที่

๖.๙.๙ จัดเตรียมบัญชีรายชื่อติดต่อ ของหน่วยงาน บุคลากร สำหรับการติดต่อประสานระหว่างผู้ที่ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

๖.๙.๑๐ จัดเตรียมเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) ที่มีการป้องกันและความเป็นส่วนตัวที่สูงเมื่อใช้งานผ่านอินเทอร์เน็ต สำหรับการเข้าใช้งานแอปพลิเคชันระบบงานภายในหน่วยงานของผู้ปฏิบัติงานจากนอกสถานที่

๖.๙.๑๑ ผู้ปฏิบัติงานจัดเตรียมอินเทอร์เน็ตความเร็วสูง (Fiber Optic) หรืออินเทอร์เน็ตไร้สาย (Mobile broadband) หรือ 4G/5G Mobile

๖.๙.๑๒ ผู้ปฏิบัติงานจัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่พร้อมกล้องวีดีโอ หูฟัง และลำโพง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายความเร็วสูงได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติงาน ณ สำนักงาน

๖.๙.๑๓ จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้

๖.๙.๑๔ ผู้ปฏิบัติงานจัดเตรียมโปรแกรมประยุกต์ และเทคโนโลยีที่สนับสนุนการทำงานต่าง ๆ

๗. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จัดเตรียมคณะทำงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๗.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติผู้รับผิดชอบ ได้แก่

- อธิบดีกรมชลประทาน
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๒ ระดับปฏิบัติ

๗.๒.๑ คณะบริหารจัดการการกู้คืนระบบ

มีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ให้สามารถกลับมาใช้งานได้ตามปกติ ผู้รับผิดชอบ ได้แก่

นายวรพจน์ เพชรนรชาติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๙๔๒-๗๖๔๓
นายราชพล หิรัญรักษ์	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๓
นายเกรียงไกร ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๖๒๔-๙๑๙๑

๗.๒.๒ คณะกู้คืนเครือข่าย

มีหน้าที่ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๓ คณะกู้คืนระบบสารสนเทศและแอพพลิเคชั่น

มีหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

ว่าที่ร้อยตรีหญิงณฐมน อยู่เล่ห์	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๓๖๕-๔๙๔๙
นางสาวณัชชา ศรีทองสุข	เบอร์โทรศัพท์ติดต่อ	๐๘-๖๘๑๗-๖๕๒๖
นายสมพล สุนัยรัตนาภรณ์	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๐๘๙-๘๕๘๕

๗.๒.๔ คณะประเมินความเสียหาย

มีหน้าที่ตรวจสอบและประเมินความความเสียหายทั้งด้าน Hardware และ Software พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบ ได้แก่

นายราชพล หิรัญรักษ์	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๓
นายเกรียงไกร ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๖๒๔-๙๑๙๑
นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางอัจฉรา ดาวัน	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๐
นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
ว่าที่ร้อยตรีหญิงณฐมน อยู่เล่ห์	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๓๖๕-๔๙๔๙
นายภาคภูมิ อิงคปรัชญากุล	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๑๔๕-๔๖๖๔

๗.๒.๕ คณะอาคารสถานที่

มีหน้าที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร ระบบปรับอากาศให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางสันธณา ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๑๗๖๕-๙๐๙๐

๗.๒.๖ คณะการจัดการทั่วไป

มีหน้าที่ประสานงานช่วยเหลือคณะอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน ผู้รับผิดชอบ ได้แก่

นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางสันธณา ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๑๗๖๕-๙๐๙๐

๗.๒.๗ คณะแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบเครือข่าย และห้องปฏิบัติงานคอมพิวเตอร์

มีหน้าที่แก้ไขปัญหาเบื้องต้นควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๘ คณะแก้ไขปัญหาเบื้องต้น กรณีไฟดับ/หม้อแปลงไฟฟ้าระเบิด

มีหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๙ คณะแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบเครือข่าย

มีหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบสูบน้ำออกจากห้องควบคุมระบบฯผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๑๐ คณะแก้ไขปัญหาเนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางไซเบอร์

มีหน้าที่กู้คืนระบบให้ทำงานได้ปกติรวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๑๑ คณะสำรองและกู้คืนข้อมูล (Backup & Recovery)

มีหน้าที่สำรองและกู้คืนข้อมลู เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์ผู้รับผิดชอบ ได้แก่

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๗.๒.๑๒ คณะแก้ไขปัญหาเนื่องจากแผ่นดินไหว

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากแผ่นดินไหว แจ้งเหตุต่อผู้บังคับบัญชาเพื่อผู้บังคับบัญชา ดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้า เพื่อป้องกัน เหตุเพลิงไหม้และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัยอาคารที่เสียหายแจ้งความ เสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางสันธณา ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๑๗๖๕-๙๐๙๐

๗.๒.๑๓ คณะแก้ไขปัญหาเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางสันธณา ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๑๗๖๕-๙๐๙๐

๘. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติ ดังนี้

๘.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อแก้ไขปัญหาต่อไป

๘.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ ประสิทธิภาพของเครื่องสำรองไฟฟ้าและเครื่องกำเนิดไฟฟ้า

๓) ตัดระบบจ่ายไฟ

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๘) ผู้ดูแลระบบต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยเร็ว

๙. ผังกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

๙.๑ กรณีจากไฟไหม้ห้องปฏิบัติงานคอมพิวเตอร์และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๑. เมื่อพบเหตุไฟไหม้ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบ ประกอบด้วย

นายราชพล หิรัญรักษ์	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๓
นายเกรียงไกร ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๖๒๔-๙๑๙๑
นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางอัจฉรา ดาวัน	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๐
นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
ว่าที่ร้อยตรีหญิงณฐมน อยู่เล่ห์	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๓๖๕-๔๙๔๙
นายภาคภูมิ อิงคปรัชญากุล	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๑๔๕-๔๖๖๔

๒. เจ้าหน้าที่รับผิดชอบแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องปฏิบัติงานฯ เสียหายน้อยที่สุด

๓. เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ดำเนินการดับเพลิงโดยเฉพาะ ซึ่งมีติดตั้งอยู่ภายในห้องปฏิบัติงานคอมพิวเตอร์โดยการใช้ถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟ ประเภท C เป็นอย่างน้อย ได้แก่ อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์คอมพิวเตอร์โดยไม่ทำลายหรือทำให้เกิดความเสียหายแก่อุปกรณ์ดังกล่าว ไม่ทิ้งคราบรอยสกปรกไม่หลงเหลือน้ำยาตกค้างเมื่อฉีดใช้งาน

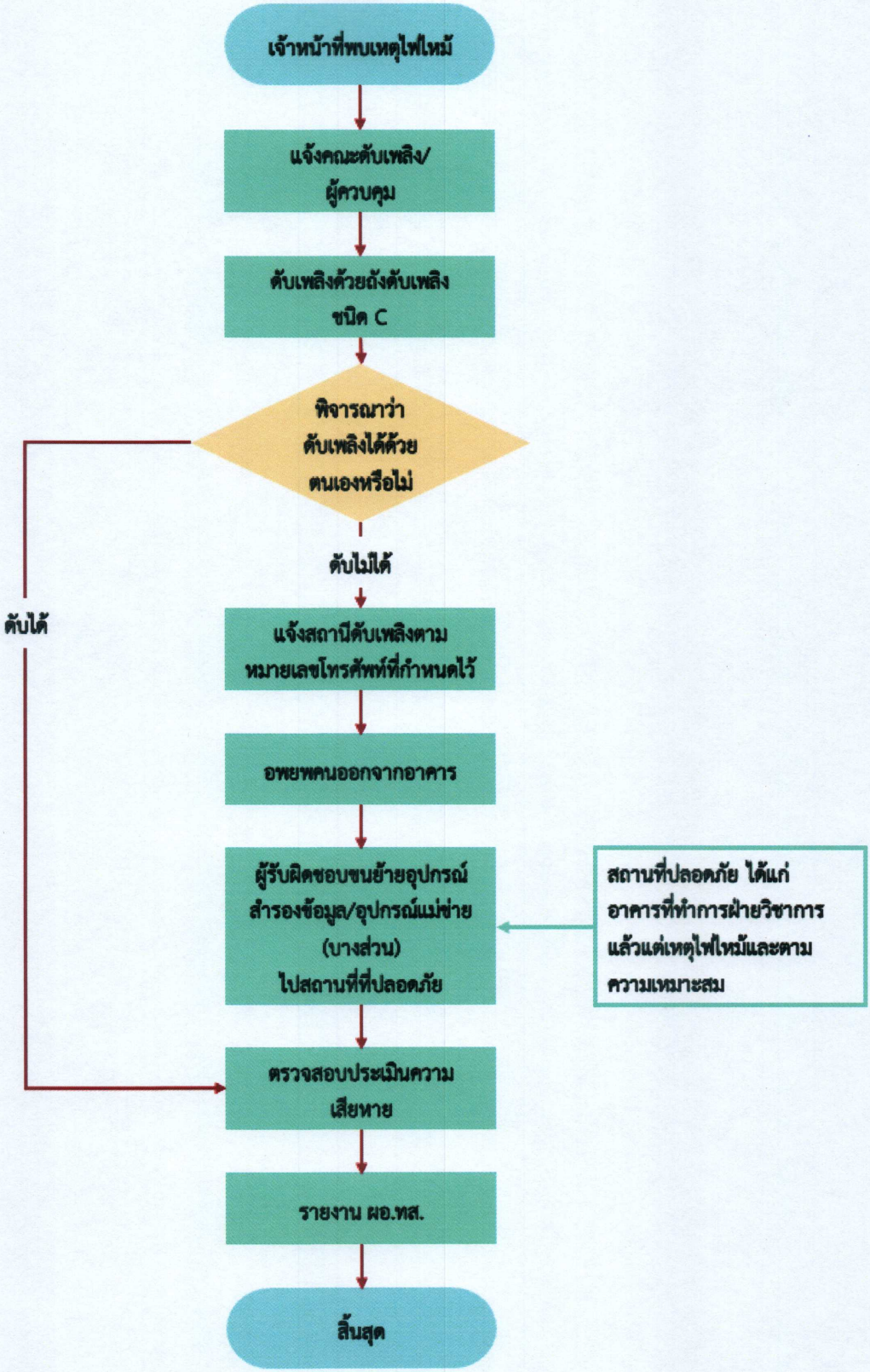
๔. กรณีไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องแจ้งสถานีดับเพลิงที่ใกล้ที่สุด ซึ่งในเขตที่ตั้งนี้คือ สถานีดับเพลิงและกู้ภัยบางโพ เบอร์โทรศัพท์ ๐๒-๕๘๕-๗๒๑๘ เพื่อดำเนินการต่อไป

๕. ประกาศอพยพคนออกจากอาคาร และจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัย ได้แก่ อาคารที่ทำการฝ่ายวิชาการ หรืออาคารอื่นใกล้เคียง แล้วแต่เหตุไฟไหม้และความเหมาะสม

๖. ผู้ควบคุมในข้อ ๒ ดำเนินการรายงาน แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป

๗. เมื่อกลับเข้าสู่สภาวะปกติผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบอุปกรณ์ภายในห้องปฏิบัติงานคอมพิวเตอร์และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศทั้งหมด พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

ผังงานกระบวนการกรณีจากไฟไหม้ห้องปฏิบัติงานคอมพิวเตอร์และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ



๙.๒ กรณีไฟดับ/หม้อแปลงไฟฟ้าระเบิด

เมื่อระบบไฟฟ้าถูกตัดเครื่องกำเนิดไฟฟ้า (Generator) จะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่าย เพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลา ๘ ชั่วโมง และหากเครื่องกำเนิดไฟฟ้าหยุดทำงาน ระบบสำรองไฟฟ้าอัตโนมัติ (UPS) ก็จะทำงานต่ออีก ๑๕-๓๐ นาที

๑. เมื่อพบเหตุไฟดับ

ผู้พบเหตุหรือผู้ที่อยู่เวรรักษาการณ์ต้องแจ้งผู้รับผิดชอบกรณีไฟดับ/หม้อไฟระเบิด ประกอบด้วย

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๒. เมื่อเกิดเหตุไฟดับ

๒.๑ ผู้ที่อยู่เวรรักษาการณ์และผู้รับผิดชอบต้องดำเนินการแก้ไขปัญหาเบื้องต้น ดังนี้

- ตรวจสอบเครื่องกำเนิดไฟฟ้า (Generator) ต้องทำงานทันที
- ตรวจสอบระบบสารสนเทศ ต้องสามารถเข้าถึงและเรียกใช้ได้ปกติ
- ประเมินสถานการณ์ไฟฟ้าว่าเกิดจากระบบไฟฟ้าอาคารของหน่วยงาน หรือการจ่ายไฟจากการไฟฟ้า
- ประเมินพลังงานที่เหลือของเครื่องกำเนิดไฟฟ้า (Generator) ว่าสามารถทำงานต่อได้กี่ชั่วโมง
- สำรองน้ำมันเชื้อเพลิงและแบตเตอรี่ของเครื่องกำเนิดไฟฟ้า

๒.๒ กรณีไฟดับนานมากกว่า ๑ ชั่วโมง หรือตรวจสอบแล้วพบว่าเกิดจากการไฟฟ้า

- แจ้งผู้ควบคุมผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่ที่เกี่ยวข้องเข้าปฏิบัติงาน
- ผู้ควบคุมดำเนินการรายงานแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป
- แจ้งคณะสำรองและกู้คืนข้อมูล เพื่อเตรียมสำรองข้อมูลและปิดระบบ
- แจ้งคณะกู้คืนเครือข่ายและคณะกู้คืนระบบสารสนเทศและแอพพลิเคชั่นเพื่อเตรียมกู้คืนระบบเครือข่ายและระบบสารสนเทศของกรมชลประทาน
- แจ้งการไฟฟ้า
  - การไฟฟ้านครหลวง เขตสามเสน ๐-๒๒๔๓-๐๕๖๔

๒.๓ กรณีไฟดับนานมากกว่า ๕ ชั่วโมง

- กรณีที่สามารถเติมน้ำมันเชื้อเพลิงได้
  - ให้ผู้รับผิดชอบเตรียมสำรองน้ำมัน
  - ดำเนินการเติมน้ำมันเชื้อเพลิงในชั่วโมงที่ ๗ หรือระดับน้ำมันน้อยกว่า ¼
- กรณีที่ไม่สามารถเติมน้ำมันเชื้อเพลิงได้
  - คณะสำรองและกู้คืนข้อมูล (Backup & Recovery) คณะกู้คืนเครือข่ายและคณะกู้คืนระบบสารสนเทศและแอพพลิเคชั่นต้องดำเนินการปิดระบบภายใน ๑ ชั่วโมง

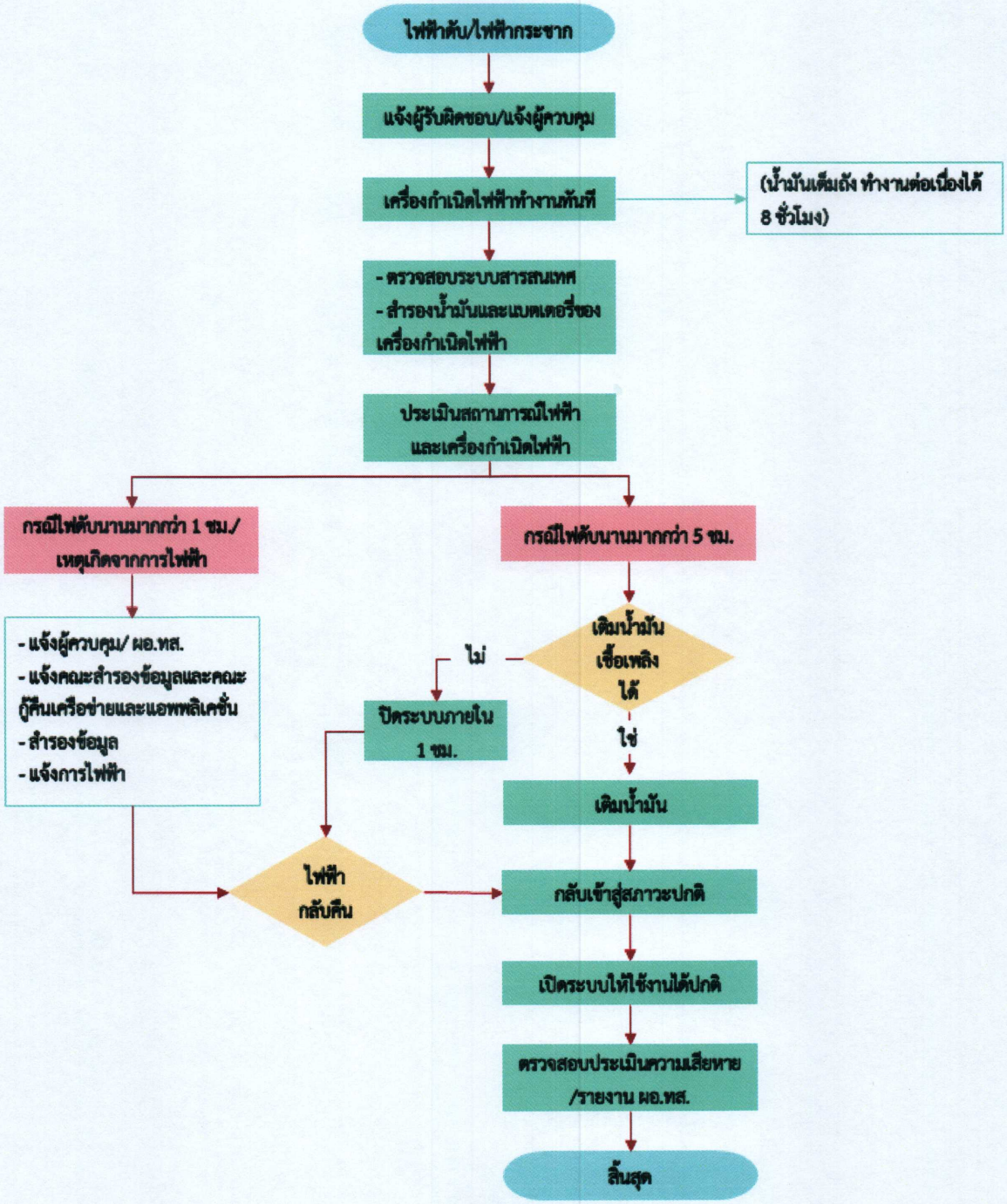
หมายเหตุ : ขั้นตอนปฏิบัติข้างต้นอยู่ภายใต้สมมุติฐานว่าเครื่องกำเนิดไฟฟ้ามีน้ำมันเต็มถัง สามารถทำงานต่อได้ ๘ ชั่วโมง กรณีมีน้ำมันเชื้อเพลิงไม่เต็มถังให้ผู้รับผิดชอบพิจารณาระยะเวลาในการปฏิบัติข้อ ๒.๒ และ ๒.๓ ตามความเหมาะสม

๓. เมื่อกลับเข้าสู่สภาวะปกติ

๓.๑ กรณีที่มีการปิดระบบคณะสำรองและกู้คืนข้อมูลร่วมกับคณะกู้คืนเครือข่ายและแอพพลิเคชั่น ต้องดำเนินการเปิดระบบให้ใช้งานได้เป็นปกติดังเดิม

๓.๒ ผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

ผังงานกระบวนการกรณีไฟดับ/หม้อไฟระเบิด



๙.๓ กรณีน้ำท่วม ห้องควบคุมระบบเครือข่าย

๑. กรณีเกิดเหตุน้ำท่วมห้องควบคุมระบบเครือข่าย ผู้พบเหตุรีบแจ้งผู้ที่อยู่เวรรักษาการณ์หรือแจ้งผู้รับผิดชอบ เพื่อแก้ปัญหาและระงับเหตุโดยเร่งด่วน ประกอบด้วย

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

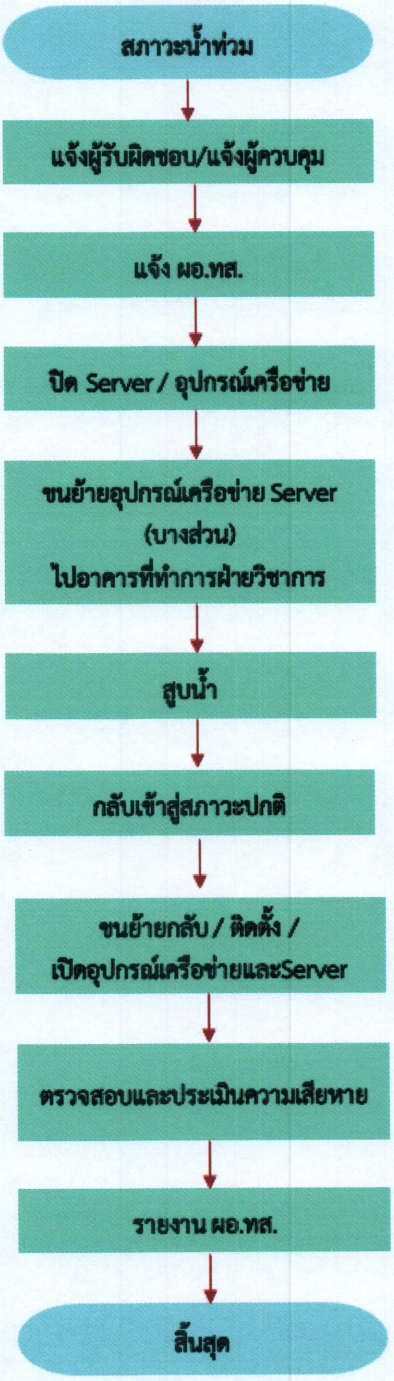
๒. ผู้รับผิดชอบแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบฯ เสียหายน้อยที่สุด

๓. ผู้ที่อยู่เวรรักษาการณ์หรือเจ้าหน้าที่รับผิดชอบ ต้องประเมินสถานการณ์และดำเนินการแก้ไขปัญหาเบื้องต้น ดังนี้

- ผู้ควบคุมในข้อ ๒ ดำเนินการรายงานแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป
- ผู้ที่อยู่เวรรักษาการณ์หรือเจ้าหน้าที่รับผิดชอบ ต้องนำอุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้นโดยจะต้อง
  - จัดหาอุปกรณ์สร้างกำแพงหรืออุปกรณ์กั้นน้ำไม่ให้คอยล์ร้อนจมน้ำ
  - ปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ
  - จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากบริเวณคอยล์ร้อน ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังอาคารที่ทำการฝ่ายวิชาการ หรือ อาคารอื่นใกล้เคียงที่ปลอดภัยจากภัยน้ำท่วมห้องควบคุมระบบเครือข่ายตามความเหมาะสม

๔. เมื่อกลับเข้าสู่สภาวะปกติกรณีน้ำท่วม ผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบฯ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

ผังงานกระบวนการกรณีน้ำท่วมห้องควบคุมระบบเครือข่าย



๙.๔ กรณีโดนเจาะระบบ และภัยคุกคามทางไซเบอร์

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก้ระบบเครือข่าย โดยจะต้องแจ้งผู้ดูแลระบบและผู้รับผิดชอบกรณีนี้ทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ซึ่งผู้รับผิดชอบ ประกอบด้วย

นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
นายกฤช กลมกล่อม	เบอร์โทรศัพท์ติดต่อ	๐๘-๙๑๕๓-๓๖๓๐
นายพูรัตน์ ราชไชย	เบอร์โทรศัพท์ติดต่อ	๐๖-๓๕๑๖-๒๖๘๘

๒. ผู้รับผิดชอบแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้าควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

๓. ผู้ควบคุมในข้อ ๒ ดำเนินการรายงานการถูกโจมตีแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามไซเบอร์มีดังนี้

๑. ควบคุมสถานการณ์ โดยต้องประสานงานกับคณะกู้คืนเครือข่ายด้วย

๑) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

๒) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

๓) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๒. วิเคราะห์การถูกโจมตี โดยต้องประสานงานกับคณะกู้คืนเครือข่ายด้วย

๑) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System File) และไฟล์อื่น ๆ

๒) วิเคราะห์ล็อกไฟล์ (Log File) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้

๓) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

๔) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๓. กู้คืนระบบคอมพิวเตอร์ โดยต้องประสานงานกับคณะสำรองและกู้คืนข้อมูล (Backup & Recovery) และคณะกู้คืนระบบสารสนเทศและแอพพลิเคชั่นด้วย

๑) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

๒) งดใช้เซอร์วิสที่ไม่จำเป็น

๓) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

๔) อุดช่องโหว่ในระบบเครือข่าย

๕) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

๔. เมื่อกลับเข้าสู่สภาวะปกติผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

ผังงานกระบวนการกรณีโดนเจาะระบบ และภัยคุกคามทางไซเบอร์

๙.๕ กรณีแผ่นดินไหว

๑. ผู้ที่อยู่เวรรักษาการณ์หรือผู้พบเหตุเมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้น คณะอาคารสถานที่และคณะแก้ไขปัญหาเนื่องจากแผ่นดินไหว ผู้รับผิดชอบได้แก่

นางสาวไตรทิพย์ มณีโชติ เบอร์โทรศัพท์ติดต่อ ๐๘-๑๘๑๒-๗๙๕๒

นางสันธณา ภูมิสิงหราช เบอร์โทรศัพท์ติดต่อ ๐๙-๑๗๖๕-๙๐๙๐

๒. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือน เจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชา ได้แก่

นางสาวไตรทิพย์ มณีโชติ เบอร์โทรศัพท์ติดต่อ ๐๘-๑๘๑๒-๗๙๕๒

นางสันธณา ภูมิสิงหราช เบอร์โทรศัพท์ติดต่อ ๐๙-๑๗๖๕-๙๐๙๐

๓. เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้

๔. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณี ดังนี้

ขั้นตอนการปฏิบัติกรณีแผ่นดินไหว

๑. การปฏิบัติขณะเกิดแผ่นดินไหว

๑) ควบคุมสติอย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน

๒) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

๓) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร

๔) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้

๕) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น

๗) ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า /สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๘) ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า

๙) ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด

๑๐) หลังจากการสั่นสะเทือนสิ้นสุด ให้รีบออกจากอาคาร

๑๑) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้อง โดยยึดหลัก “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๑๒) ให้อยู่ห่างจากประตูหน้าต่างโดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่

๑๓) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

๑๔) ห้ามใช้ลิฟต์โดยเด็ดขาด

๑๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

๑) ถ้าอาคารมั่นคงแข็งแรง ให้หลบอยู่ในอาคารนั้น

๒) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น

๓) หลังการสั่นสะเทือนสิ้นสุดลง ให้หาทางออกจากอาคารนั้น

๔) ถ้าไม่อยู่ใกล้ทางออกให้ “ หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดชุลมุน

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

๑) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๒) หลีกเลี่ยงสูงของที่อาจโค่นล้มลงมาทำอันตราย เช่น ตู้เสาไฟฟ้า ป้ายโฆษณา ต้นไม้ใหญ่

๓) หลีกเลี่ยงอาคารสูง กำแพง ระวังเศษอิฐ กระจก ชิ้นส่วนของอาคารที่อาจหล่นลงมา

๔) วิ่งไปสู่ที่โล่ง

๕) รีบออกจากอาคารที่ชำรุดเสียหายโดยเร็วที่สุด

๒. เมื่อแผ่นดินไหวสงบลง

๑) ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนำส่งโรงพยาบาล

๒) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ

๓) ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบการทำงานทั้งหมดทันที

๔) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

๓. ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

๑) อยู่กับที่ ป้องกันศีรษะและหน้า จากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ

๒) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกัน วัสดุหล่นใส่

๓) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย

๔) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น

๕) ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย

๔. การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

๑) ควบคุมสติอารมณ์ปฏิบัติตามแผนอพยพ

๒) เชื่อฟังคำแนะนำของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.

๓) เก็บทรัพย์สิน/เอกสารสำคัญ ไว้ในลิ้นชักโต๊ะและล็อคกุญแจ

๔) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด

๕) ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ

๖) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า

๗) ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ ๒ คน

๘) ห้ามพูดคุยสายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่นห้ามดันหรือแซง

๙) ห้ามใช้ลิฟต์โดยเด็ดขาด

๑๐) เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที

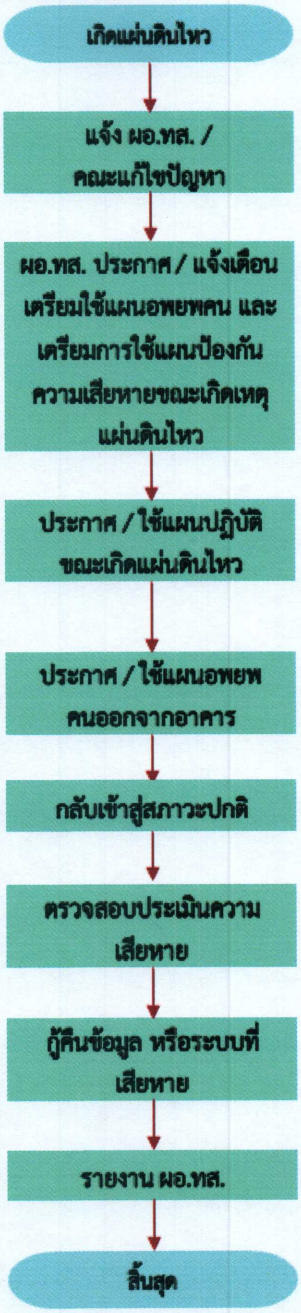
๑๑) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้

๑๒) ตรวจสอบจำนวนผู้อพยพ

๕. เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้บังคับบัญชา และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป

๖. เมื่อกลับเข้าสู่สภาวะปกติผู้รับผิดชอบและคณะประเมินความเสียหายต้องดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบและสั่งการให้กู้คืนระบบทั้งด้านอาคารสถานที่ Network Hardware และ Software กลับคืนสู่สภาพเดิมต่อไป

ผังงานกระบวนการกรณีแผ่นดินไหว



๙.๖ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

๑. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้นของ คณะอาคารสถานที่และคณะแก้ไขปัญหาเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ผู้รับผิดชอบ ได้แก่

นางสาวไตรทิพย์ มณีโชติ เบอร์โทรศัพท์ติดต่อ ๐๘-๑๘๑๒-๗๙๕๒

นางสันธณา ภูมิสิงหราช เบอร์โทรศัพท์ติดต่อ ๐๙-๑๗๖๕-๙๐๙๐

๒. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชา ได้แก่

นางสาวไตรทิพย์ มณีโชติ เบอร์โทรศัพท์ติดต่อ ๐๘-๑๘๑๒-๗๙๕๒

นางสันธณา ภูมิสิงหราช เบอร์โทรศัพท์ติดต่อ ๐๙-๑๗๖๕-๙๐๙๐

๓. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่เตรียมไว้ล่วงหน้าตามควรแก่กรณี ดังนี้

๓.๑ ก่อนเกิดเหตุ

๑) ตรวจเช็คความพร้อมของระบบไฟฟ้าเครื่องกำเนิดไฟฟ้า ระบบสำรองไฟฟ้า และระบบรักษาความปลอดภัย สำหรับห้องควบคุมระบบเครือข่าย ได้แก่

- ตรวจเช็คความพร้อมของเครื่องกำเนิดไฟฟ้า
- สำรองน้ำมันเชื้อเพลิงและแบตเตอรี่ของเครื่องกำเนิดไฟฟ้า
- ตรวจสอบระบบดับเพลิงอัตโนมัติ
- ตรวจสอบระบบสำรองไฟฟ้าอัตโนมัติ
- ตรวจสอบระบบแจ้งเตือนภัย
- ตรวจสอบระบบปรับอากาศระบบ Precision air conditioner
- ตรวจสอบระบบควบคุมอุณหภูมิและความชื้น
- ตรวจสอบกล้องวงจรปิด

๒) สำรองข้อมูลระบบสารสนเทศของเครื่องคอมพิวเตอร์แม่ข่ายในห้องควบคุมระบบเครือข่าย กรมชลประทานลงบนอุปกรณ์จัดเก็บข้อมูล SAN Storage /สำรองลงสื่อบันทึกภายนอก จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๓) ประชาสัมพันธ์แจ้งเวียนหน่วยงานให้สำรองข้อมูลที่สำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกและจัดเก็บไว้ในสถานที่ที่เหมาะสม

๔) จัดเตรียมระบบประกาศแจ้งเตือนเหตุการณ์ผิดปกติหน้าเว็บไซต์กรมชลประทาน พร้อมขึ้นประกาศทันทีขณะมีเหตุฉุกเฉิน

๕) จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่รับผิดชอบ สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันทีโดยไม่ต้องเดินทางมาปฏิบัติงานที่กรมชลประทาน

๖) จัดเตรียมการเฝ้าระวังระบบอินเตอร์เน็ตของผู้ให้บริการที่กรมชลประทานเช่าใช้บริการได้แก่ NT ให้สามารถดำเนินการให้บริการเจ้าหน้าที่กรมชลประทานและประชาชนได้อย่างต่อเนื่อง

๗) จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้

๘) ประสานงานในเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศ กับหน่วยงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย : ThaiCERT ไทยเซิร์ต เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน

๙) จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๑๐) กำหนดเจ้าหน้าที่ดูแลรับผิดชอบ/จัดเวรยามรักษาการณ์ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ วันเสาร์-อาทิตย์และวันหยุดนักขัตฤกษ์

๓.๒ ขณะเกิดเหตุ

๑) เจ้าหน้าที่ผู้พบเหตุแจ้งผู้บังคับบัญชาทราบถึงเหตุผิดปกติ/ฉุกเฉิน

๒) ประกาศแจ้งเตือนกรณีที่มีเหตุการณ์ผิดปกติ/ฉุกเฉิน หน้าเว็บไซต์หรือ Facebook ของกรมชลประทาน หรือประกาศเสียงตามสาย

๓) เฝ้าระวังระบบอินเตอร์เน็ตของผู้ให้บริการที่กรมชลประทานเช่าใช้บริการ NT กรณีเกิด เหตุขัดข้องต่อผู้ให้บริการรายใดรายหนึ่ง ผู้ดูแลระบบหรือเจ้าหน้าที่รับผิดชอบจะต้องดำเนินการกำหนด DNS และ ปรับโหลดอินเตอร์เน็ตให้ไปใช้อินเตอร์เน็ตจากผู้ให้บริการรายที่เหลือได้อย่างต่อเนื่อง

๔) ปฏิบัติหน้าที่อยู่เวรยามรักษาการณ์ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศวันทำการวันเสาร์-อาทิตย์ และวันหยุดนักขัตฤกษ์

๕) กรณีตรวจพบวัตถุต้องสงสัย หรือเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของกรมชลประทาน ให้แจ้งไปยังสถานีตำรวจที่ใกล้เคียง หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้บังคับบัญชาทราบ

๓.๓ หลังเกิดเหตุ

๑) ตรวจสอบระบบเครือข่ายระบบเทคโนโลยีสารสนเทศ และความเสียหายด้านอื่น ๆ โดยละเอียดพร้อมทั้งประเมินความเสียหาย

๒) กรณีตรวจพบว่าระบบสารสนเทศหรือข้อมูลมีความเสียหาย ให้กู้คืนระบบกลับสู่สภาพปกติโดยใช้ข้อมูลที่สำรองไว้ให้ข้อมูลกลับมาใช้ได้ปกติโดยเร็ว

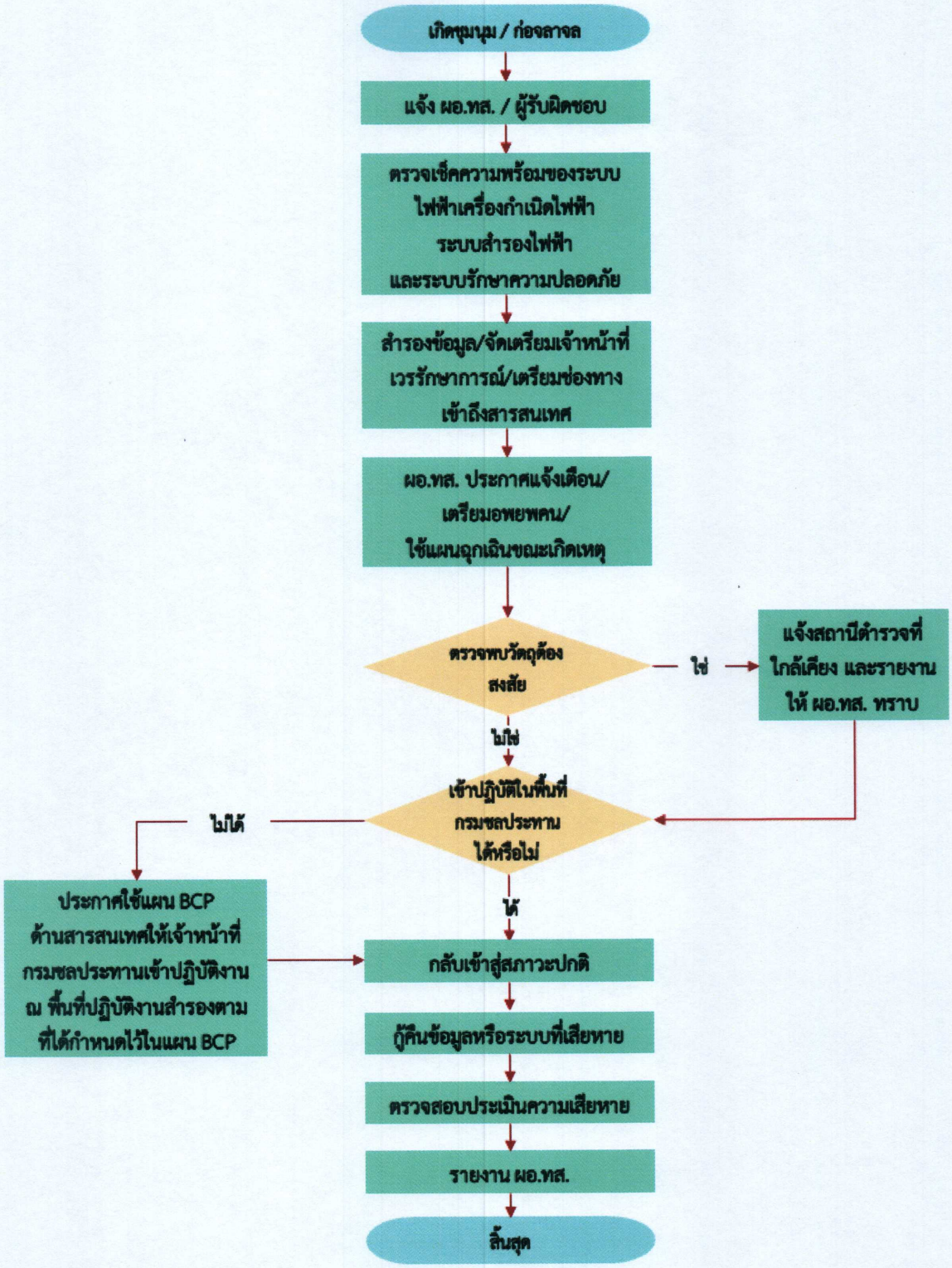
๓) กรณีตรวจพบระบบคอมพิวเตอร์เสียหาย ให้ดำเนินการซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย/ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย/จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน/ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๔) รายงานผลความเสียหาย และสรุปผลการดำเนินการให้ผู้บังคับบัญชาทราบ

๔. กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่สำนักงานกรมชลประทาน ได้ให้ผู้บังคับบัญชาสั่งการใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ กรมชลประทานเพื่อจัดเตรียมทรัพยากรที่จำเป็นและให้เจ้าหน้าที่กรมชลประทานเข้าปฏิบัติงาน ณ พื้นที่ปฏิบัติงานสำรองตามที่กรมชลประทานได้กำหนดไว้

๕. เมื่อกลับเข้าสู่สภาวะปกติการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ผู้รับผิดชอบและคณะประเมินความเสียหายต้องดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ และสำรวจความเสียหายทุกด้านอย่างละเอียดทำการประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหายเพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบและสั่งการต่อไป

ผังงานกระบวนการกรณีเกิดการชุมนุมประท้วงและก่อจลาจล



๙.๗ กรณีเกิดโรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง

เมื่อเกิดโรคระบาดให้ดำเนินการเตรียมพร้อม ตรวจสอบ และเฝ้าระวังการใช้งานระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

นายราชพล หิรัญรักษ์	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๓
นายเกรียงไกร ภูมิสิงหราช	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๖๒๔-๙๑๙๑
นางสาวไตรทิพย์ มณีโชติ	เบอร์โทรศัพท์ติดต่อ	๐๘-๑๘๑๒-๗๙๕๒
นางอัจฉรา ดาวัน	เบอร์โทรศัพท์ติดต่อ	๐๘-๔๗๐๐-๕๓๒๐
นายสิริวัฒน์ หญีตสอน	เบอร์โทรศัพท์ติดต่อ	๐๙-๘๒๘๕-๘๖๔๘
ว่าที่ร้อยตรีหญิงณฐมน อยู่เล่ห์	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๓๖๕-๔๙๔๙
นายภาคภูมิ อิงคปรัชญากุล	เบอร์โทรศัพท์ติดต่อ	๐๙-๕๑๔๕-๔๖๖๔

ตามแผนเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่เตรียมไว้ล่วงหน้า ดังนี้

๑. ก่อนเกิดเหตุ

๑.๑ จัดทำแนวทางการใช้เทคโนโลยีสนับสนุนการปฏิบัติงานนอกสถานที่ตั้งราชการ

๑.๒ เพื่อเป็นการเฝ้าระวัง และตรวจสอบให้ระบบสารสนเทศของกรมชลประทานพร้อมใช้งานอย่างต่อเนื่อง จึงต้องมีการจัดเวรยามรักษาการณ์เฝ้าระวัง ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตรวจสอบความพร้อมใช้งานของห้องควบคุมเครือข่ายคอมพิวเตอร์ ได้แก่

- ห้องควบคุมเครือข่ายคอมพิวเตอร์
- เครื่องสำรองไฟฟ้าอัตโนมัติ (UPS)
- ระบบเครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น (Precision Air Conditioning System)
- เครื่องกำเนิดไฟฟ้า

๑.๓ จัดเตรียมช่องทาง SSL VPN เพื่อให้ดูแลระบบสามารถเข้าถึงระบบฯ หรือเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างปลอดภัย

๑.๔ จัดเตรียมระบบอินเทอร์เน็ตความเร็วสูง (Fiber Optic) หรือ เทคโนโลยี MPLS (Multiprotocol Label Switching) หรือ Leased Line

๑.๕ จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่พร้อมกล้องวีดีโอ หูฟังและลำโพง หรือ Device อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายภายในสำนักงานได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติราชการนอกสถานที่

๑.๖ จัดเตรียมแอปพลิเคชัน และเทคโนโลยีที่สนับสนุนการทำงานต่าง ๆ สำหรับการปฏิบัติงานร่วมกันระหว่างผู้ที่ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

๑.๗ จัดเตรียมระบบสนับสนุนการทำงานร่วมกันจากทางไกล จัดเก็บเอกสารไฟล์เข้าถึงไฟล์งานได้จากภายนอก รองรับการจัดเก็บข้อมูลต่าง ๆ แบบรวมศูนย์

๑.๘ จัดเตรียมระบบประชุม Conference สนับสนุนการประชุมทางไกลออนไลน์นอกสถานที่

๑.๙ จัดเตรียมบัญชีรายชื่อติดต่อ ของหน่วยงาน บุคลากร สำหรับการติดต่อประสานระหว่างผู้ที่ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

๑.๑๐ จัดเตรียมเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) ที่มีการป้องกันและความเป็นส่วนตัวที่สูงเมื่อใช้งานผ่านอินเทอร์เน็ต สำหรับการเข้าใช้งานแอปพลิเคชันระบบงานภายในหน่วยงานของผู้ปฏิบัติงานจากนอกสถานที่

๑.๑๑ ผู้ปฏิบัติงานจัดเตรียมอินเทอร์เน็ตความเร็วสูง (Fiber Optic) หรืออินเทอร์เน็ตไร้สาย (Mobile broadband) หรือ 4G/5G Mobile

๑.๑๒ ผู้ปฏิบัติงานจัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่ พร้อมกล้องวีดีโอ หูฟัง และลำโพง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายความเร็วสูงได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติงาน ณ สำนักงาน

๑.๑๓ จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้

๑.๑๔ ผู้ปฏิบัติงานจัดเตรียมโปรแกรมประยุกต์ และเทคโนโลยีที่สนับสนุนการทำงานต่าง ๆ

๒. ขณะเกิดเหตุ

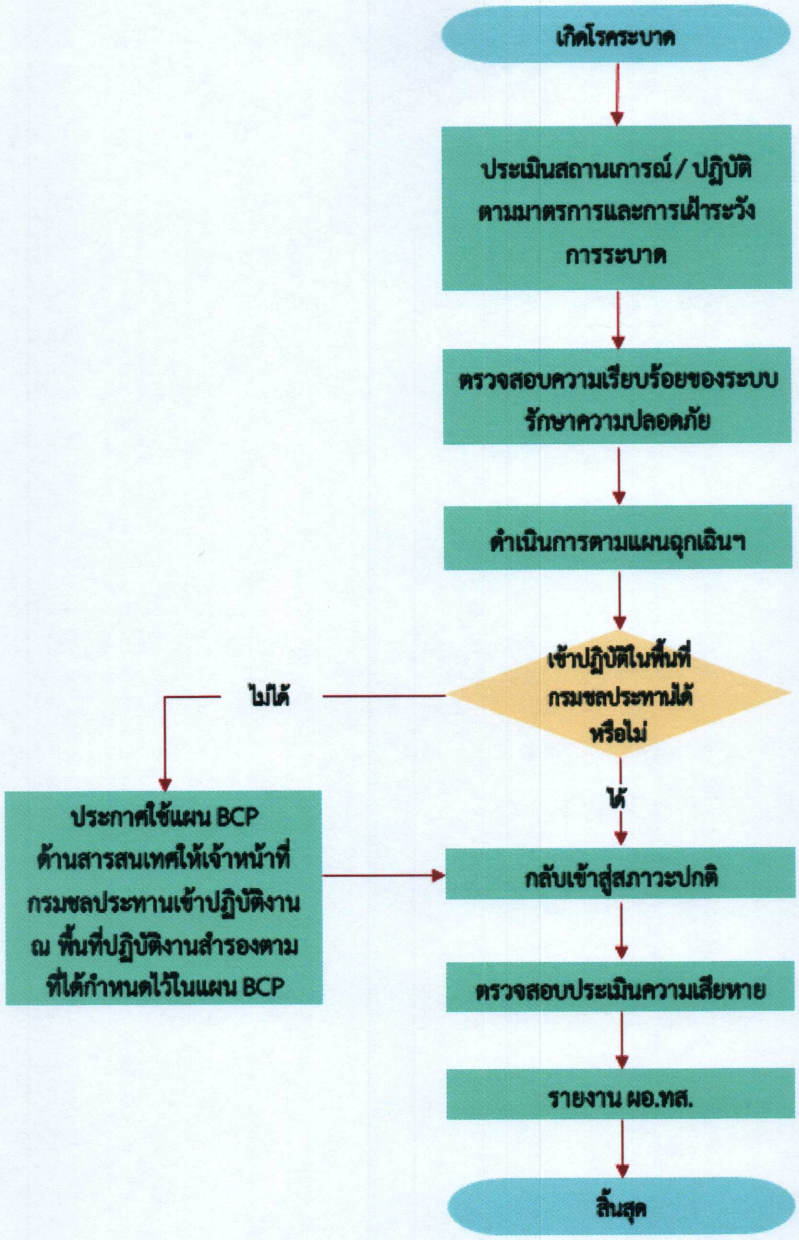
๒.๑ กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่สำนักงานกรมชลประทานได้ ให้ผู้บังคับบัญชาสั่งการใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ กรมชลประทาน เพื่อจัดเตรียมทรัพยากรที่จำเป็นและให้เจ้าหน้าที่กรมชลประทานเข้าปฏิบัติงาน ณ พื้นที่ปฏิบัติงานสำรองตามที่กรมชลประทานได้กำหนดไว้

๒.๒ ดำเนินการป้องกันภัยตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติเทคโนโลยีสารสนเทศ กรมชลประทาน

๓. หลังเกิดเหตุ

เมื่อกลับเข้าสู่สภาวะปกติ การเกิดโรคระบาดสิ้นสุดลง ผู้รับผิดชอบและคณะประเมินความเสียหายต้อง ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ และสำรวจความเสียหายทุกด้านอย่างละเอียด ทำการประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบและสั่งการต่อไป

ผังงานกระบวนการกรณีเกิดโรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง



๑๐. การกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ Backup Device / CD-ROM / Harddisk ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้คณะกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ หน่วยงานจึงมีแผนจัดทำการสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งได้ ๓ ไซต์ คือ

๑. Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลักมีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำที่สูง

๒. Warm Site เป็นไซต์ที่คล้ายกับ Hot site แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่ำกว่า Hot site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า Hot site

๓. Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง Hardware และ Software ในการกู้คืนมีต้นทุน การจัดทำต่ำแต่ระยะเวลาในการกู้คืนนาน

ขั้นตอนการดำเนินการ

๑. สำรวจความต้องการของระบบสำรอง

๒. สำรวจไซต์สำรองที่เหมาะสม

๓. การประเมินความเสี่ยงจากสิ่งต่างๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง

๔. การจัดลำดับผลกระทบขององค์กร

๕. การจัดทำไซต์สำรอง

๖. การจัดทำแผนกู้คืน

๗. การวางแผนการแต่งตั้งคณะทำงานลำดับการทำงานหลังระบบได้รับความเสียหาย

๘. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่รวมถึงการฝึกอบรมทางด้านเทคนิค

๙. การทดสอบแผนกู้คืนอาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง

๑๑. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบเพื่อนำเสนอรายงานสรุปให้อธิบดีกรมชลประทานหรือ DCIO และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) รักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติ ทั้งนี้ เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศต่อไป

ผู้จัดทำ/ผู้รับผิดชอบแผน

(นางอัจฉรา ดาวัน)

ผยม.ทส.

วันที่ - ๒ ธ.ค. ๒๕๖๗

ผู้อนุมัติแผน

(นายราชพล หิรัญรักษ์)

ผชช.ทส. รักษาราชการแทน ผอ.ทส.

วันที่ - ๒ ธ.ค. ๒๕๖๗