แผนรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ กรมทรัพยากรทางทะเลและชายฝั่ง

สารบัญ

หน้า

๑. บทนำ ๑
๒. วัตถุประสงค์ ๑
๓. การวิเคราะห์ความเสี่ยง ๑
๔. แผนรองรับสถานการณ์ฉุกเฉิน ๒
๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค ๒
๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว ๒
๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว ๓
๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว ๓
๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย ๔
๔.๑.๕ กรณีไฟฟ้าขัดข้อง ๔
๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล ๕
๔.๒.๑ กรณีโจรกรรม ๕
๔.๒.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้ ๕
๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ ๖
๔.๓.๑ กรณีไฟไหม้ ๖
๔.๓.๒ กรณีน้ำท่วม ๗
๔.๓.๓ กรณีแผ่นดินไหว ๗
๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง ๘
๔.๔.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง ๘
๕. การกำหนดผู้รับผิดชอบ ๘

แผนรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ

๑. บทนำ

ปัจจุบันทุกหน่วยงานราชการ ได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานเพิ่มมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและการสร้างข้อมูลสารสนเทศและฐานข้อมูลต่างๆ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ นับวันจะมีจำนวนมากขึ้น ดังนั้น การจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้รวดเร็ว แม่นยำ ถูกต้องและมีประสิทธิภาพจึงนับเป็นสิ่งที่ต้องให้ความสำคัเพิ่มมากขึ้นไปด้วย

กรมทรัพยากรทางทะเลและชายฝั่ง ถือเป็นหน่วยงานราชการที่มีฐานข้อมูล องค์ความรู้เฉพาะด้านและมีข้อมูลที่หลากหลาย จำเป็นต้องดำเนินการเก็บข้อมูลเป็นประจำอย่างต่อเนื่อง และได้นำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานเพิ่มมากขึ้น เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของทั้งหน่วยงานและเครือข่ายอนุรักษ์ที่เกี่ยวข้อง ดังนั้น การป้องกันระบบสารสนเทศจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีบริหารจัดการที่ดี โดยเฉพาะความสามารถในการป้องกันและรักษาระบบสารสนเทศของกรมให้มั่นคง ปลอดภัย จึงได้กำหนดแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกรมขึ้น

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่ง

๖. เพื่อการให้บริการระบบเครือข่าย (Internet) ที่มีความรวดเร็ว มีประสิทธิภาพ และปลอดภัย

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของกรมทรัพยากรทางทะเลและชายฝั่งที่มีความหลากหลาย และมีการพัฒนาระบบเทคโนโลยีสารสนเทศเข้ามาช่วยอำนวยความสะดวกในการปฏิบัติงานเพิ่มมากขึ้น เมื่อมีระบบและมีการใช้งานที่เพิ่มมากขึ้น ความเสี่ยงในการถูกโจมตีก็จะมีเพิ่มมากขึ้นไปด้วย ซึ่งจำเป็นอย่างยิ่งที่กรมฯ จะต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา การลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบ การประเมินความเสี่ยงด้านสารสนเทศ และการกู้คืนระบบ อันจะส่งต่อความเชื่อมั่นในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่ง ให้สามารถใช้ระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุดได้ตามวัตถุประสงค์

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของกรมทรัพยากรทางทะเลและชายฝั่ง พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๓.๑ ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ที่อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมที่ไม่ประสงค์ดี ถูกก่อกวนจาก **Hacker** ถูกเจาะทำลายระบบจาก **Cracker** และจากระบบเครือข่าย **(Internet)** ล่มอันเกิดจากผู้ให้บริการ **(ISP)** หรือการเสื่อมสภาพของอุปกรณ์ เป็นต้น

๓.๒ ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓.๓ ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๔ ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมทรัพยากรทางทะเลและชายฝั่ง ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่งมีประสิทธิภาพที่ดี มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่ง

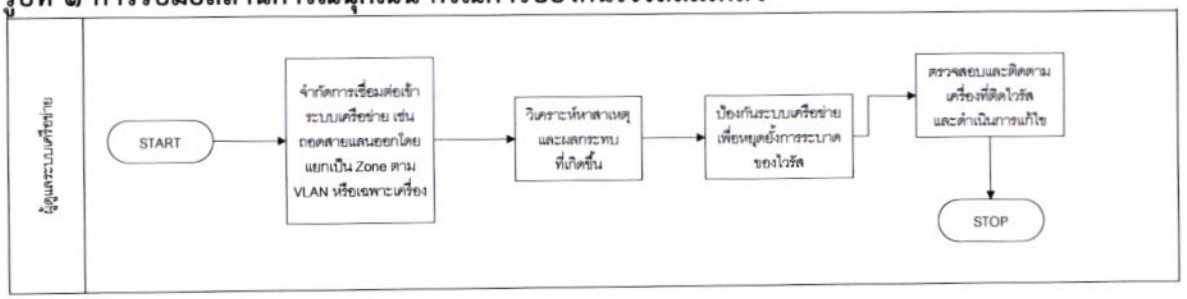
๔. แผนรองรับสถานการณ์ฉุกเฉิน

๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ศูนย์สารสนเทศจะประกาศให้ทุกหน่วยงานในสังกัดทราบ

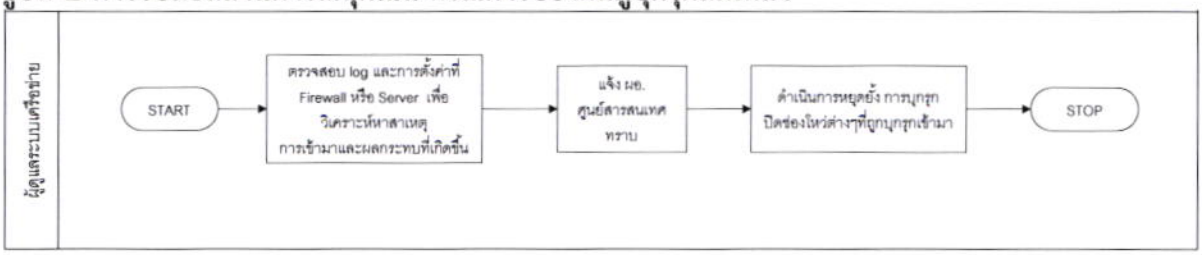
รูปที่ ๑ การรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall หรือ Server
- ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์สารสนเทศให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

รูปที่ ๒ การรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย (บริษัท CTC หรือ TOT หรือ CAT) เพื่อดำเนินการแก้ไขปัญหาและซ่อมแซมอุปกรณ์ให้เสร็จเรียบร้อยโดยเร็ว และในกรณีที่ไม่สามารถเชื่อมโยงเครือข่ายได้ บางชั้นหรือบางจุด ให้ดำเนินการแจ้งข้อมูลไปยังบริษัท CTC หรือ TOT เพื่อดำเนินการแก้ไข

รูปที่ ๓ การรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว