แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

สารบัญ

คำนิยาม

“กรมฯ” หมายถึง กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

“ผู้บังคับบัญชา” หมายถึง ผู้บริหารในระดับศูนย์/กอง/ฝ่ายของกรมฯ

“ผู้ใช้งาน หรือ พนักงาน” หมายถึง ข้าราชการ เจ้าหน้าที่ ลูกจ้าง หรือผู้บังคับบัญชา ซึ่งปฏิบัติงาน ให้แก่กรมฯ หรือมีกิจที่ต้องปฏิบัติงานกับกรมฯ ในลักษณะใดลักษณะหนึ่ง

“ผู้ดูแลระบบ” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมฯ

“ผู้ดูแลเครือข่าย” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลและบริหารจัดการเครือข่ายของกรมฯ

“ผู้พัฒนาระบบ” หมายถึง พนักงานของกรมฯ หรือผู้ที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวข้องกับการพัฒนาระบบงานของกรมฯ

“ผู้รับผิดชอบระบบสารสนเทศ” หมายถึง ผู้ที่รับผิดชอบการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรมฯ ซึ่งรวมถึงผู้ดูแลระบบ ผู้ดูแลเครือข่าย และผู้พัฒนาระบบ

“ผู้ให้บริการภายนอก (External Service Provider)” หมายถึง หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของกรมฯ เช่น ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการด้านฮาร์ดแวร์ ผู้ให้บริการด้านซอฟต์แวร์ ผู้ให้บริการด้านระบบงาน โดยรวมผู้ให้บริการเหล่านี้มีหน้าที่ที่จะต้องปฏิบัติตามสัญญาจ้างที่มีการจัดทำไว้กับกรมฯ รวมทั้งปฏิบัติตามแนวนโยบายและแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับการให้บริการของตนเอง

“ความมั่นคงปลอดภัยสารสนเทศ” หมายถึง การรักษาความมั่นคงปลอดภัยให้กับสินทรัพย์สารสนเทศของกรมฯ ทั้งนี้เพื่อป้องกันการสูญเสีย การสูญหาย การถูกขโมย การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดชอบ หรือ การกระทำใดๆ ก็ตามที่ก่อให้เกิดความเสียหายต่อองค์ประกอบ ๓ ส่วน ดังนี้ การรักษาความลับ การรักษาความครบถ้วน การรักษาความพร้อมใช้

“การรักษาความลับ (Confidentiality)” หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

“การรักษาความครบถ้วน (Integrity)” หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษาเพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

“การรักษาความพร้อมใช้ (Availability)” หมายถึง การจัดทำให้ทรัพย์สินสารสนเทศ สามารถทำงานเข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

“ความมั่นคงปลอดภัย” หมายถึง ความมั่นคงปลอดภัยสารสนเทศ

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือ ใช้ประโยชน์เพื่อการดำเนินงานต่างๆ ตามภารกิจของกรมฯ

“คณะกรรมการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์” (คณะกรรมการบริหารฯ) หมายถึง กลุ่มบุคลากรซึ่งเป็นผู้บริหารระดับกองหรือฝ่ายที่ได้รับมอบหมายจากกรมฯ ให้มีอำนาจ ในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ ซึ่งมีอำนาจและหน้าที่ดังนี้

- กำหนดให้มีการทบทวนการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ ๑ ครั้ง
- กำหนดให้มีการจัดทำ ทบทวน และปรับปรุงแนวนโยบายและแนวปฏิบัติต่างๆ ในเอกสารฉบับนี้อย่างน้อยปีละ ๑ ครั้ง
- กำกับดูแลให้ผู้ที่อยู่ในขอบเขตของเอกสารฉบับนี้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้กำหนดไว้อย่างเคร่งครัด
- กำหนดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ อย่างน้อยปีละ ๑ ครั้ง
- กำหนดให้มีการประเมินและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ อย่างน้อยปีละ ๑ ครั้ง
- กำหนดให้มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์และปรับปรุงอย่างน้อยปีละ ๑ ครั้ง รวมทั้งจัดให้มีการซ้อมแผนดังกล่าวเป็นระยะๆ เพื่อให้มีความพร้อมในการปฏิบัติเมื่อเกิดเหตุฉุกเฉิน
- ทบทวนรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และให้คำแนะนำที่จะเป็นประโยชน์ในการปรับปรุงการดำเนินการ
- ทบทวนและปรับปรุงโครงสร้างและหน้าที่ความรับผิดชอบของคณะทำงานกู้คืนระบบของกรมฯ
- กำหนดให้มีการจัดทำและปรับปรุงแผนกู้คืนระบบของกรมฯ
- ศึกษา และติดตาม ภัยคุกคามใหม่ๆ ที่อาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ รวมทั้งกำหนดมาตรการรองรับที่จำเป็น

“ระบบงาน (Application systems)” หมายถึง ระบบสารสนเทศที่ทำงานอยู่บนเครื่อง คอมพิวเตอร์เพื่อให้บริการต่างๆ ซึ่งรวมถึงให้บริการงานตามภารกิจของกรมฯ ด้วย เช่น ระบบงาน บุคคลากร ระบบงานบัญชี เป็นต้น

“สินทรัพย์ (Information assets)” หมายถึง ทรัพย์สิน ๕ หมวด ซึ่งประกอบด้วย บุคลากร ฮาร์ดแวร์ (เช่น เครื่องคอมพิวเตอร์อุปกรณ์เครือข่าย อุปกรณ์ต่อพ่วง) ซอฟต์แวร์ (เช่น โปรแกรมคอมพิวเตอร์ โปรแกรมระบบงาน) ข้อมูลและระบบงาน

“เครือข่าย หรือ ระบบเครือข่าย (Computer networks or network systems)” หมายถึง โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่างๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กร สามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์ กร และโครงข่ายบนอินเทอร์เน็ต ซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ของอีกองค์กรหนึ่งได้

“อุปกรณ์คอมพิวเตอร์ หรือ อุปกรณ์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับหรือทำงานเป็นส่วนหนึ่งของคอมพิวเตอร์ ทำงานบนระบบเครือข่าย หรือทำงานเป็นคอมพิวเตอร์อย่างหนึ่ง ซึ่งอาจทำหน้าที่ในการสื่อสารข้อมูล ประมวลผลข้อมูล บันทึกข้อมูล หรือสนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะต่างๆ เช่น อุปกรณ์เครือข่าย (เช่น สวิทช์ เร้าเตอร์) เครื่องพิมพ์ เครื่องสแกนภาพ เครื่องสำรองไฟฟ้า (UPS)

“ระบบเทคโนโลยีสารสนเทศ (Information technology systems)” หมายถึง ระบบงานโปรแกรมประยุกต์ ระบบปฏิบัติการ เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ให้บริการระบบงาน เครือข่าย อุปกรณ์เครือข่าย (เช่น สวิทช์ เร้าเตอร์ ไฟร์วอลล์) และอุปกรณ์คอมพิวเตอร์อื่นๆ

เมื่อกล่าวถึงคำว่า “ระบบเทคโนโลยีสารสนเทศ” มีความมุ่งหมายให้เป็นคำเรียกโดยรวมของ อุปกรณ์ทุกชนิดทุกประเภทที่สามารถประมวลผลหรือสนับสนุนการประมวลผลคอมพิวเตอร์

“ระบบ (Systems)” หมายถึง ระบบเทคโนโลยีสารสนเทศ

“รหัสผ่าน” หมายถึง กลุ่มชุดตัวอักษร ตัวเลข หรือเครื่องหมายต่างๆ ที่กำหนดขึ้นมาโดย ผู้ใช้งานสำหรับใช้ในการพิสูจน์ตัวตนในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีความหมายตรง กับคำในภาษาอังกฤษว่า Password

“บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อของผู้ที่ได้รับสิทธิและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมฯ

“สิทธิการเข้าถึง หรือ สิทธิของผู้ใช้งาน” หมายถึง การอนุญาตให้ผู้ใช้งานสามารถเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศของกรมฯ โดยผู้มีอำนาจ การอนุญาตให้เข้าถึงข้อมูลนี้โดยทั่วไป จะกำหนดจากบทบาทหรือหน้าที่ความรับผิดชอบของผู้ใช้งานหรือตามความจำเป็นในการเข้าถึงข้อมูลนั้น กล่าวคือหากมีบทบาทหรือหน้าที่ความรับผิดชอบ หรือความจำเป็นในการเข้าถึงข้อมูลนั้นก็จะอนุญาตให้เข้าถึงได้หรือที่เรียกว่าได้รับ “สิทธิ” ในการเข้าถึงข้อมูลนั่นเอง การได้รับสิทธิของผู้ใช้งานยังหมายรวมถึงความสามารถของผู้ใช้งานในการที่จะเปลี่ยนแปลง แก้ไข เพิ่มเติม หรือลบ ข้อมูลตามที่ตนเองได้รับสิทธินั้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาตให้ผู้ใช้งานเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของกรมฯ โดยได้รับสิทธิการเข้าถึงตามบทบาทหรือหน้าที่ความรับผิดชอบของผู้ใช้งาน หรือตามความจำเป็นในการเข้าถึง

“ไวรัสคอมพิวเตอร์ (ไวรัส) หรือ โปรแกรมไม่ประสงค์ดี” หมายถึง โปรแกรมที่ได้รับการติดตั้งในเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัว อาจก่อให้เกิดความเสียหายต่อข้อมูลต่างๆ ในเครื่องนั้น อาจทำให้เครื่องคอมพิวเตอร์เสียหาย อาจสร้างความรำคาญ อาจทำให้เครื่องคอมพิวเตอร์ทำงานช้าหรือทำงานผิดปกติ หรือทำงานในลักษณะที่ไม่เป็นประโยชน์ ไม่สร้างสรรค์ หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น โปรแกรมที่ทำงานในลักษณะดังกล่าวอย่างน้อยหมาย รวมถึง

- โปรแกรมที่สามารถสำเนาตัวเองและแพร่กระจายผ่านทางสื่อบันทึกข้อมูลเพื่อข้ามไปยังเครื่องคอมพิวเตอร์อื่น กล่าวคือ เมื่อมีการใช้สื่อบันทึกข้อมูลดังกล่าวกับเครื่องคอมพิวเตอร์หนึ่ง โปรแกรมดังกล่าวก็จะแพร่กระจายหรือติดไปยังเครื่องคอมพิวเตอร์ นั้น
- โปรแกรมที่สามารถสำเนาตัวเองข้ามหรือแพร่กระจายไปยังเครื่องคอมพิวเตอร์ปลายทางหนึ่งเครื่องหรือมากกว่าหนึ่งเครื่องก็ได้ เครื่องปลายทางที่ได้รับการแพร่ระบาดนั้นก็สามารถสำเนาและแพร่กระจายตัวเองได้ต่อไป โปรแกรมที่แพร่กระจายในลักษณะดังกล่าวมีชื่อเรียกกันว่าหนอนเครือข่าย (Worm)
- โปรแกรมที่เคลื่อนที่จากเครื่องคอมพิวเตอร์อื่นมายังเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือที่เรียกกันว่า Mobile Code เช่น โปรแกรมที่เขียนด้วย Java Script, Active เป็นต้น และถูกสั่งให้ทำงานในเครื่องของผู้ใช้งานนั้น โปรแกรมประเภทนี้อาจฝังตัวอยู่กับโปรแกรมอื่นแต่ถูกเรียกทำงานร่วมกัน เช่น กรณีของการเข้าถึงโปรแกรมบนเว็บไซต์หนึ่งซึ่งมีการเรียกใช้ Java Script ด้วย ก็จะทำให้ Java Script นั้นถูกโอนย้าย เข้ามาและสั่งทำงานบนเครื่องของผู้ใช้งาน

“ข้อมูลล็อก (Log)” หมายถึง ข้อมูลเหตุการณ์ต่างๆ ที่เกิดขึ้นบนระบบๆ หนึ่งและได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายามในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่ง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ เป็นต้น ข้อมูลเหล่านี้สามารถใช้ เพื่อตรวจติดตามการทำงานของระบบ เตือนว่ามีเหตุการณ์หนึ่งเกิดขึ้นแล้วในระบบ ดำเนินการเชิงป้องกันหรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐานในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ กรณีการส่งอีเมล์ ซึ่งพาดพิงถึงผู้อื่นและทำให้ผู้นั้นเกิดความเสียหาย เป็นต้น

“ช่องโหว่ (Software/hardware vulnerabilities)” หมายถึง จุดอ่อนที่พบในซอฟต์แวร์ หรือฮาร์ดแวร์ที่กรมฯ ใช้งาน โดยที่ซอฟต์แวร์หรือฮาร์ดแวร์นั้นอาจถูกพัฒนาหรือจัดทำขึ้นมาโดย ผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง โดยทั่วไปผู้ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์นั้นจะเป็นผู้ค้นพบ จุดอ่อน เช่น ในระหว่างที่ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์ และรายงานให้ผู้ผลิตได้รับทราบเพื่อขอให้ช่วยดำเนินการแก้ไขจุดอ่อนดังกล่าวในหลายๆ กรณีทำให้ซอฟต์แวร์หรือฮาร์ดแวร์นั้นทำงานผิดพลาดในลักษณะต่างๆ ซึ่งรวมถึงความผิดพลาดในด้านข้อมูลด้วย ในบางกรณีที่ร้ายแรง ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากจุดอ่อนดังกล่าวเพื่อทำการบุกรุกระบบได้ด้วย ซึ่งหมายถึง สามารถเข้าสู่ระบบได้โดยไม่ได้รับอนุญาต

“โปรแกรมแก้ไขช่องโหว่ (Patch for software/hardware vulnerabilities)” หมายถึง โปรแกรมสำหรับแก้ไข ที่ผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์จัดทำขึ้นมาเพื่อแก้ไขปัญหาช่องโหว่ที่ผู้ใช้งานซอฟต์แวร์หรือฮาร์ดแวร์ค้นพบและรายงานเข้ามาให้ผู้ผลิตได้รับทราบ

“พอร์ต (Ports)” หมายถึง ช่องสัญญาณบนอุปกรณ์เครือข่าย เช่น บนสวิทซ์ เร้าเตอร์ โดยทั่วไปช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่ายคอมพิวเตอร์ และอุปกรณ์เครือข่ายต่างๆ โดยทั่วไปอุปกรณ์เครือข่ายจะมีช่องสัญญาณดังกล่าวจำนวนหนึ่ง

นอกจากนั้นพอร์ตยังหมายถึงบริการต่างๆ บนเครื่องเซิร์ฟเวอร์ให้บริการ โดยทั่วไปบริการเหล่านี้จะได้รับการกำหนดหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต ๘๐ หมายถึงบริการเว็บซึ่ง บริการข้อมูลต่างๆ บนเว็บหนึ่ง พอร์ต ๒๕ หมายถึงบริการรับส่งอีเมล์บนอินเทอร์เน็ต พอร์ต ๕๓ หมายถึงบริการค้นหาไอพีแอดเดรสของเครื่องหรืออุปกรณ์คอมพิวเตอร์ต่างๆ

ในลักษณะของพอร์ตที่เป็นช่องสัญญาณหรือให้บริการต่างๆ ก็ตาม เมื่อไม่มีความจำเป็นต้องใช้ช่องสัญญาณหรือบริการนั้นโดยผ่านทางพอร์ตดังกล่าว และโดยหลักการด้านความมั่นคงปลอดภัย ผู้รับผิดชอบควรจะปิดช่องสัญญาณหรือบริการนั้นทิ้งไป ซึ่งเรียกโดยรวมว่าเป็นการปิดพอร์ตที่ไม่ได้ใช้งาน

“VPN (Virtual Private Network)” หมายถึง การเข้ารหัสข้อมูล เช่น โดยผ่านทาง ซอฟต์แวร์หรือฮาร์ดแวร์หนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย เนื่องจากข้อมูลจะได้รับการเข้ารหัสก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ตหรือเครือข่ายไร้สายนั้น เมื่อกล่าวถึง VPN จะหมายรวมถึงระบบ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้การเข้ารหัสข้อมูลก่อนส่งข้อมูลออกไป

“ความเสี่ยง” หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์ สารสนเทศของกรมฯ เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไข ซึ่งอาจทำให้กรมฯ เสียชื่อเสียง

“ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk)” หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าหรือเท่ากับค่าที่ยอมรับได้นี้ จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม

“แผนการลดความเสี่ยง (Treatment plan)” หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติการดำเนินการ

“สื่อบันทึกข้อมูล” หมายถึง กระดาษ เทป Hard disk Flash Drive และแผ่น CD/DVD หรือสื่อชนิดอื่นๆ ที่ใช้ในการบันทึกข้อมูล

หมวด ๑ ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารฯ กำหนดให้มีการตรวจสอบดังนี้

(๑) จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง ซึ่งมีขอบเขตของการตรวจสอบอย่างน้อยดังนี้

- บริการสำคัญของกรมฯ ที่ประกอบด้วยระบบและอุปกรณ์ที่สนับสนุนการให้บริการดังกล่าว
- การประเมินผลกระทบของบริการสำคัญ (Business Impact Analysis: BIA)
- การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ซึ่งรวมถึงหลักเกณฑ์ใดๆ ที่ สกมช. ประกาศกำหนดให้ปฏิบัติตาม

(๒) กำหนดให้มีการรายงานผลการตรวจสอบให้ได้รับทราบ เพื่อให้คำแนะนำในการดำเนินการปรับปรุงต่างๆ ตามความจำเป็น

(๓) ติดตามผลการปฏิบัติเพื่อแก้ไขตามคำแนะนำหรือข้อคิดเห็นของผู้ตรวจสอบ จนกว่าจะแล้วเสร็จและครบถ้วนทั้งหมด

ส่วนที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารฯ กำหนดให้มีการดำเนินการดังนี้

(๑) จัดให้หน่วยงานผู้รับผิดชอบประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ อย่างน้อยปีละ ๑ ครั้งตามแนวปฏิบัติในการบริหารจัดการความเสี่ยงและการตรวจสอบด้านความมั่นคงปลอดภัย

(๒) กำหนดให้มีการรายงานผลการบริหารความเสี่ยงเป็นระยะๆ จนกว่าความเสี่ยงจะอยู่ในระดับที่กรมฯ ยอมรับได้

(๓) ติดตามและประเมินผล และให้คำแนะนำเพื่อปรับปรุงผลการปฏิบัติ

ส่วนที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์

คณะกรรมการบริหารฯ กำหนดให้มีการดำเนินการดังนี้

(๑) จัดให้หน่วยงานผู้รับผิดชอบทำแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อกำหนดแนวทางในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

(๒) ทบทวนและปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อกรมฯ

(๓) จัดให้มีการซ้อมแผนดังกล่าวเป็นระยะๆ เพื่อให้มีความพร้อมในการปฏิบัติเมื่อเกิดเหตุฉุกเฉิน

หมวด ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารฯ กำหนดให้มีการปฏิบัติดังนี้เพื่อให้สอดคล้องกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- การระบุความเสี่ยงที่มีต่อระบบและอุปกรณ์สำคัญ (Identify)
- การกำหนดมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
- การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๑. การระบุความเสี่ยงที่มีต่อระบบและอุปกรณ์สำคัญ (Identify)

๑.๑ การจัดการสินทรัพย์สารสนเทศ (Asset Management)

ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการสินทรัพย์สารสนเทศของกรมฯ ดังนี้

(๑) ระบุระบบและอุปกรณ์สำคัญ ซึ่งเป็นองค์ประกอบของบริการสำคัญในขอบเขตของการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมถึงระบบและอุปกรณ์สำหรับการรับมือและบริหารจัดการภัยคุกคามทางไซเบอร์ด้วย

(๒) จัดทำทะเบียนสินทรัพย์สารสนเทศของระบบและอุปกรณ์สำคัญ ตลอดจนทบทวนทะเบียนให้เป็นปัจจุบัน

(๓) ตรวจสอบทะเบียนสินทรัพย์สารสนเทศอย่างน้อยปีละ ๑ ครั้ง ทบทวนและปรับปรุงข้อมูลทะเบียนสินทรัพย์ให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

ผู้รับผิดชอบระบบสารสนเทศ ประเมินความเสี่ยงและกำหนดกลยุทธ์ในการจัดการกับความเสี่ยงดังนี้

(๑) ปฏิบัติตามแนวปฏิบัติสำหรับการวิเคราะห์ ประเมิน และจัดการกับความเสี่ยง เพื่อประเมินความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ จัดทำแผนการลดความเสี่ยง นำแผนไปสู่การปฏิบัติ และรายงานผลการปฏิบัติให้ผู้บังคับบัญชาและคณะกรรมการบริหารฯ ได้รับทราบ

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

ผู้รับผิดชอบระบบสารสนเทศ ประเมินช่องโหว่และทดสอบเจาะระบบและอุปกรณ์สำคัญดังนี้

(๑) ติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ของระบบและอุปกรณ์สำคัญอย่างสม่ำเสมอ เพื่อให้ทราบถึงความจำเป็นในการที่จะต้องแก้ไขช่องโหว่ของระบบและอุปกรณ์สำคัญในขอบเขต

(๒) ประเมิน พิจารณาผลการประเมิน และดำเนินการแก้ไขช่องโหว่โดยประมาณปีละ ๑ ครั้ง ของระบบและอุปกรณ์สำคัญที่ตรวจพบตามความจำเป็น

(๓) ทดสอบเจาะระบบและอุปกรณ์สำคัญในทุกๆ ๓-๕ ปี พิจารณาผลการทดสอบเจาะระบบและดำเนินการแก้ไขช่องโหว่ที่ตรวจพบตามความจำเป็น

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการผู้ให้บริการภายนอกดังนี้

(๑) ปฏิบัติตามแนวปฏิบัติในการควบคุมการปฏิบัติงานของผู้ให้บริการภายนอกของกรมฯ

(๒) กำหนดให้มีการดำเนินการและระบุประเด็นดังต่อไปนี้ ที่จำเป็นต้องให้ผู้ให้บริการภายนอกปฏิบัติตามลงในสัญญาจ้าง

- กำหนดวัตถุประสงค์ของการจ้างผู้ให้บริการภายนอก
- กำหนดบทบาทและหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบและอุปกรณ์สำคัญ
- ประเมินความเสี่ยงที่เกี่ยวข้องกับการให้บริการโดยผู้ให้บริการภายนอกโดยพิจารณาจากวัตถุประสงค์ของการจ้าง
- กำหนดเป็นข้อตกลงระดับการให้บริการ (Service Level Agreement) เช่น ระบบและอุปกรณ์ต้องมีความพร้อมใช้อย่างต่อเนื่องมากที่สุดและมีระยะเวลาที่หยุดชะงักได้น้อยที่สุดตามที่กรมฯ กำหนด
- กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ
- กำหนดเป็นความร่วมมือในการบริหารจัดการภัยคุกคามทางไซเบอร์นับตั้งแต่เหตุเกิดขึ้นจนกระทั่งเหตุยุติลงระหว่างผู้ให้บริการภายนอกและกรมฯ
- กำหนดระยะเวลาในการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเมื่อได้รับการประสานงานหรือแจ้งจากกรมฯ
- ระบุการขอสงวนสิทธิของกรมฯ ในการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก ซึ่งรวมถึงระบบ อุปกรณ์ และสถานที่ปฏิบัติงานของผู้ให้บริการภายนอก
- ทบทวนเนื้อหาของสัญญาจ้างให้มีความสอดคล้องกับกฎหมายหรือข้อบังคับที่เกี่ยวข้องที่กรมฯ ต้องปฏิบัติตาม เช่น พรบ. ไซเบอร์ พรบ. คุ้มครองข้อมูลส่วนบุคคล เป็นต้น และอ้างถึงกฎหมายหรือข้อบังคับดังกล่าวลงในสัญญาจ้าง

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการเข้าถึงระบบและอุปกรณ์สำคัญดังนี้

(๑) ปฏิบัติตามแนวปฏิบัติในการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมฯ เพื่อจำกัดสิทธิการเข้าถึงระบบและอุปกรณ์สำคัญตามบทบาทและหน้าที่ความรับผิดชอบของพนักงานหรือผู้ที่เกี่ยวข้องนั้น พนักงานหรือผู้ที่เกี่ยวข้องนั้นจะสามารถเข้าถึงได้ก็ต่อเมื่อมีบทบาทหรือหน้าที่ความรับผิดชอบเท่านั้น

(๒) ดำเนินการตรวจสอบและปรับปรุงสิทธิการเข้าถึงระบบและอุปกรณ์สำคัญอย่างสม่ำเสมอในทุกๆ ๖ เดือน เพื่อให้มั่นใจว่าพนักงานหรือผู้ที่เกี่ยวข้องนั้นได้รับสิทธิการเข้าถึงอย่างถูกต้องและเป็นปัจจุบัน

(๓) ปฏิบัติตามแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยของระบบ เพื่อให้มีการบันทึกข้อมูลล็อกของระบบและอุปกรณ์สำคัญอย่างต่อเนื่อง รวมทั้งตรวจสอบข้อมูลล็อก

เหล่านั้นอย่างสม่ำเสมอเพื่อติดตามกิจกรรมต่างๆ ที่เกิดขึ้น และประเมินปัญหาหรือความผิดปกติที่อาจจะเกิดขึ้น

(๔) ตรวจสอบและปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งานของระบบและอุปกรณ์สำคัญอย่างสม่ำเสมอ

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

ผู้รับผิดชอบระบบสารสนเทศ จัดเตรียมให้ระบบและอุปกรณ์สำคัญมีความมั่นคงปลอดภัย ดังนี้

(๑) กำหนดมาตรฐานขั้นต่ำสำหรับการตั้งค่าระบบและอุปกรณ์สำคัญ ได้แก่

- การตั้งค่าขั้นต่ำสำหรับระบบปฏิบัติการ
- การตั้งค่าขั้นต่ำสำหรับแอปพลิเคชัน
- การตั้งค่าขั้นต่ำสำหรับอุปกรณ์เครือข่าย

(๒) ทบทวนและปรับปรุงมาตรฐานการตั้งค่าตามความจำเป็น หรือเมื่อเทคโนโลยีที่เกี่ยวข้องมีการเปลี่ยนแปลง

(๓) กำหนดมาตรฐานการตั้งค่าขั้นต่ำให้อย่างน้อยต้องครอบคลุมถึง

- การให้สิทธิการเข้าถึงในระดับน้อยที่สุด
- การแบ่งแยกหน้าที่ความรับผิดชอบออกจากกัน
- การตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย
- การลบหรือถอดถอนบัญชีที่ไม่ได้มีการใช้งาน
- การลบโปรแกรมหรือซอฟต์แวร์ที่ไม่ได้มีการใช้งาน
- การปิดพอร์ตของระบบและอุปกรณ์ที่ไม่ได้มีการใช้งาน
- การป้องกันไวรัสคอมพิวเตอร์
- การแก้ไขช่องโหว่ของระบบและอุปกรณ์

(๔) กำหนดให้ผู้ที่ได้รับมอบหมายตั้งค่าระบบและอุปกรณ์สำคัญตามมาตรฐานขั้นต่ำที่กำหนดไว้

(๕) ตรวจสอบการตั้งค่าของระบบและอุปกรณ์สำคัญให้เป็นไปตามมาตรฐานขั้นต่ำก่อนนำขึ้นให้บริการ รวมทั้งทบทวนการตั้งค่าให้เป็นไปตามมาตรฐานขั้นต่ำปีละ ๑ ครั้ง

(๖) ทบทวนและปรับปรุงมาตรฐานขั้นต่ำอย่างน้อยปีละ ๑ ครั้ง

(๗) ปฏิบัติตามแนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบ เพื่อบริหารจัดการและควบคุมการเปลี่ยนแปลงการตั้งค่าระบบและอุปกรณ์ให้เป็นไปตามมาตรฐานขั้นต่ำที่กำหนดไว้

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

ผู้รับผิดชอบระบบสารสนเทศ จัดเตรียมการเข้าถึงระบบและอุปกรณ์สำคัญจากระยะไกลให้มีความมั่นคงปลอดภัยดังนี้

(๑) ปฏิบัติตามแนวปฏิบัติสำหรับการบริหารจัดการการเข้าถึงเครือข่ายจากระยะไกล เพื่อควบคุมการเข้าถึงระบบและอุปกรณ์สำคัญจากระยะไกลให้มีความมั่นคงปลอดภัย

๒.๔ สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)

ผู้รับผิดชอบระบบสารสนเทศ ควบคุมและจำกัดการใช้สื่อบันทึกข้อมูลที่ถอดแยกได้บนระบบและอุปกรณ์สำคัญดังนี้

(๑) ควบคุมการเชื่อมต่อเพื่อใช้งานสื่อบันทึกข้อมูลที่ถอดแยกได้จากระบบและอุปกรณ์สำคัญ ปิดการใช้งานไม่ว่าจะเป็นพอร์ตหรือช่องสำหรับการเชื่อมต่อสื่อบันทึกข้อมูลที่ถอดแยกได้ และให้เปิดการใช้งานเมื่อมีความจำเป็นเท่านั้น

(๒) ตรวจสอบระบบและอุปกรณ์สำคัญดังกล่าวเพื่อให้ระบบป้องกันไวรัสยังคงทำงานอยู่เสมอ เพื่อป้องกันข้อมูลที่เข้าและออกจากระบบ ซึ่งรวมถึงโดยผ่านทางสื่อบันทึกข้อมูลด้วย

(๓) จำกัดสื่อบันทึกข้อมูลที่อนุญาตให้ใช้งานกับระบบและอุปกรณ์สำคัญ

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารฯ มอบหมายหน่วยงานผู้รับผิดชอบให้มีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ดังนี้

(๑) สร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้งให้แก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่นๆ ที่สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศของกรมฯ ได้

(๒) ติดตามข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ใหม่ๆ เป็นระยะๆ และสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์เหล่านั้นตามความจำเป็น เพื่อให้พนักงานและผู้ที่เกี่ยวข้องมีความรู้และความเข้าใจ และสามารถป้องกันตนเองได้ในระดับหนึ่ง

(๓) สื่อสารและสร้างความตระหนักเกี่ยวกับแผนการรับมือเกี่ยวกับภัยคุกคามทางไซเบอร์และโครงสร้างของการบริหารจัดการภัยคุกคามทางไซเบอร์ ให้พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องได้รับทราบ

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

คณะกรรมการบริหารฯ กำหนดให้มีการแบ่งปันข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ดังนี้

(๑) แบ่งปันข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังหน่วยงานทั้งภายในและภายนอกกรมฯ เพื่อประโยชน์ในการเรียนรู้และป้องกันตนเอง

(๒) สร้างเครือข่ายความร่วมมือทั้งภายในและภายนอกกรมฯ เพื่อแบ่งปันข้อมูลและประสานงานกันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

ผู้รับผิดชอบระบบสารสนเทศ กำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ดังนี้

(๑) กำหนดกลไก มาตรการ ระบบ หรืออุปกรณ์เพื่อใช้ในการตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นกับระบบและอุปกรณ์ต่างๆ บันทึกและจัดหมวดหมู่เหตุการณ์ดังกล่าว วิเคราะห์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่

(๒) กำหนดให้กลไกดังกล่าวสามารถแจ้งเตือนการตรวจพบเหตุการณ์ที่ผิดปกติได้โดยอัตโนมัติ

(๓) ทบทวนกลไกดังกล่าวที่ใช้ในการตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์เพื่อปรับปรุงให้มีประสิทธิภาพมากยิ่งขึ้นอย่างน้อยปีละ ๑ ครั้ง

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์

คณะกรรมการบริหารฯ มอบหมายหน่วยงานผู้รับผิดชอบเพื่อจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ดังนี้

(๑) จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ทบทวนและปรับปรุงแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๒) สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่นๆ ได้รับทราบ อธิบายถึงความจำเป็นที่จะต้องมีแผนการรับมือฯ และความต้องการหรือความคาดหวังของกรมฯ ที่มีต่อบุคลากรเหล่านั้นในการจัดการและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

๔.๒ แผนการสื่อสารในสภาวะวิกฤต

คณะกรรมการบริหารฯ มอบหมายหน่วยงานผู้รับผิดชอบเพื่อจัดทำแผนการสื่อสารในสภาวะวิกฤตดังนี้

(๑) จัดทำแผนการสื่อสารในสภาวะวิกฤตเป็นส่วนหนึ่งของแผนการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อใช้ในการสื่อสารและประสานงานไปยังผู้มีส่วนได้ส่วนเสียของกรมฯ โดยแผนการสื่อสารต้องครอบคลุมข้อมูลสำหรับการติดต่อไปยังผู้ที่เกี่ยวข้องเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ทบทวนและปรับปรุงแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๒) ฝึกซ้อมแผนการสื่อสารในสภาวะวิกฤต ร่วมกับแผนการรับมือกับภัยคุกคามทางไซเบอร์หรือเป็นการฝึกซ้อมแผนการสื่อสารแยกก็ตาม

(๓) ประเมินผลภายหลังการฝึกซ้อมเพื่อให้มั่นใจว่าสามารถสื่อสารและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ และปรับปรุงแผนการสื่อสารจากผลการประเมินดังกล่าว

๔.๓ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารฯ กำหนดให้มีการดำเนินการดังนี้ เกี่ยวกับการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) ฝึกซ้อมแผนการรับมือกับภัยคุกคามทางไซเบอร์เป็นประจำอย่างน้อยในทุกๆ ๒-๓ ปี ต่อ ๑ ครั้ง

(๒) ฝึกอบรมผู้ที่เกี่ยวข้องเพื่อให้มีความรู้ ทักษะ การเตรียมความพร้อมเพื่อให้สามารถรับมือกับสถานการณ์ฉุกเฉิน (ซึ่งกรณีนี้คือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น) รวมทั้งเพื่อให้ทราบถึงบทบาทและความรับผิดชอบของตนเองเมื่อจำเป็นต้องรับมือกับสถานการณ์ที่เกิดขึ้น

(๓) เข้าร่วมการฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับคำสั่งจาก สกมช. และหน่วยงานกำกับดูแลของกรมฯ

(๔) ให้ข้อมูลเกี่ยวกับระบบและอุปกรณ์สำคัญของกรมฯ แผน และการซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับคำร้องขอจาก สกมช. และหน่วยงานกำกับดูแลของกรมฯ

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

คณะกรรมการบริหารฯ กำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ดังนี้

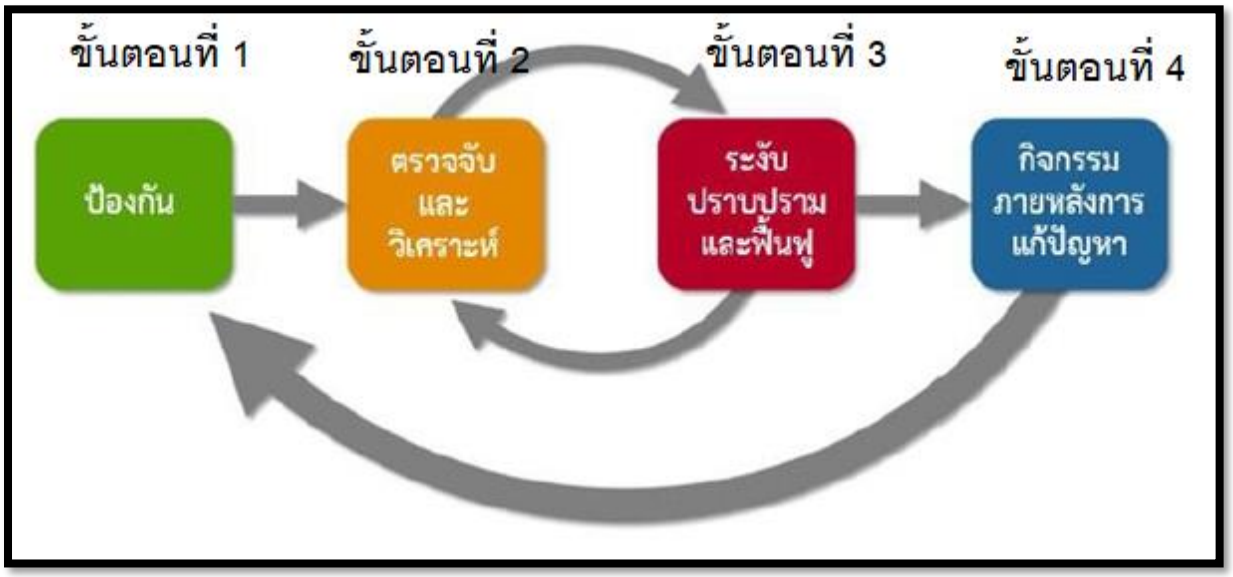
(๑) ปฏิบัติตามแนวปฏิบัติสำหรับการบริหารจัดการการกู้คืนระบบ เพื่อจัดทำแผนกู้คืนระบบและอุปกรณ์สำคัญ ซึ่งครอบคลุมถึงการประเมินผลกระทบที่มีต่อระบบและอุปกรณ์สำคัญ การกำหนดระยะเวลาเป้าหมายของการกู้คืน (Recovery Time Objective (RTO)) ความถี่ของการสำรองข้อมูลของระบบและอุปกรณ์สำคัญ (Recovery Point Objective (RPO)) ตามแนวปฏิบัติสำหรับการสำรองข้อมูลและทดสอบคู้คืนข้อมูล และการซ้อมแผนการกู้คืนระบบ

(๒) ทบทวนให้แผนการกู้คืนระบบของกรมฯ มีความสอดคล้องกับแผนงานที่เกี่ยวข้องของผู้ให้บริการภายนอกในการให้บริการระบบและอุปกรณ์สำคัญของกรมฯ

(๓) กำหนดให้มีการซ้อมแผนการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้งเพื่อประเมินความเชื่อมโยงกับแผนการรับมือกับภัยคุกคามทางไซเบอร์ และปรับปรุงแผนกู้คืนระบบหรือแผนการรับมือกับภัยคุกคามทางไซเบอร์ตามความจำเป็น

หมวด ๓ มาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์

วงจรชีวิตที่แสดงลำดับของการดำเนินการเพื่อบริหารจัดการกับภัยคุกคามทางไซเบอร์ (Incident Handling Cycle) ประกอบด้วย ๔ ขั้นตอนตามที่ปรากฏในรูปด้านล่าง



ลักษณะภัยคุกคามทางไซเบอร์แบ่งตามระดับผลกระทบได้เป็น ๓ ประเภท ซึ่งประกอบด้วย

- ระดับไม่ร้ายแรง ซึ่งหมายถึง ผลกระทบน้อย
- ระดับร้ายแรง ซึ่งหมายถึง ผลกระทบปานกลาง
- ระดับวิกฤต ซึ่งหมายถึง ผลกระทบมากที่สุด

ดูคำนิยามของผลกระทบได้จากเอกสาร ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ซึ่งจะขอเรียกโดยย่อว่า “เอกสารลักษณะภัยคุกคามทางไซเบอร์”

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในแต่ละระดับมีขั้นตอนการจัดการครอบคลุมครบทั้ง ๔ ขั้นตอนตามที่ปรากฏในรูป

เอกสารลักษณะภัยคุกคามทางไซเบอร์ได้กำหนดให้ เมื่อเหตุการณ์ที่เกิดขึ้นมีผลกระทบที่สูงกว่า เช่น ระดับร้ายแรง จะสูงกว่า ระดับไม่ร้ายแรง ระดับวิกฤต จะสูงกว่า ระดับไม่ร้ายแรงและระดับร้ายแรง เป็นต้น เหตุการณ์ที่มีผลกระทบที่สูงกว่าจะต้องรวมวิธีปฏิบัติของเหตุการณ์ที่มีผลกระทบที่ต่ำกว่า เช่น เหตุการณ์ในระดับวิกฤตจะต้องรวมวิธีปฏิบัติของเหตุการณ์ระดับไม่ร้ายแรงและระดับร้ายแรงเข้าไปด้วย

เอกสารลักษณะภัยคุกคามทางไซเบอร์ได้กำหนดวิธีปฏิบัติที่จะต้องดำเนินการให้สอดคล้องมีจำนวนด้วยกันทั้งสิ้น ๗ ชุด ตั้งแต่ชุด ก. จนถึง ชุด ช. ตารางที่ตามมาด้านล่างแสดงวิธีปฏิบัติของแต่ละระดับความรุนแรง ยกตัวอย่างเช่น

- ระดับไม่ร้ายแรง ใช้แนวทางปฏิบัติชุด ก. ชุด ข. ชุด ง. และชุด ช.
- ระดับร้ายแรง ใช้แนวทางปฏิบัติชุด ก. ชุด ข. ชุด จ. ร่วมกับชุด ง. และชุด ช.
- ระดับวิกฤต ใช้แนวทางปฏิบัติชุด ก. ชุด ค. ร่วมกับชุด ข. ชุด ฉ. ร่วมกับชุด ง. และ จ. และชุด ช.

<table>
<tr><th></th><th>ขั้นตอนที่ ๑</th><th>ขั้นตอนที่ ๒</th><th>ขั้นตอนที่ ๓</th><th>ขั้นตอนที่ ๔</th></tr>
<tr><td>ไม่ร้ายแรง</td><td rowspan="3">ใช้แนวทางปฏิบัติชุด ก.</td><td rowspan="2">ใช้แนวทางปฏิบัติชุด ข.</td><td>ใช้แนวทางปฏิบัติชุด ง.</td><td rowspan="3">ใช้แนวทางปฏิบัติชุด ช.</td></tr>
<tr><td>ร้ายแรง</td><td>ใช้แนวทางปฏิบัติชุด จ. ร่วมกับชุด ง.</td></tr>
<tr><td>วิกฤต</td><td>ใช้แนวทางปฏิบัติชุด ค. ร่วมกับชุด ข.</td><td>ใช้แนวทางปฏิบัติชุด ฉ. ร่วมกับชุด ง. และชุด จ.</td></tr>
</table>

แต่ละขั้นตอนและวิธีปฏิบัติชุดต่างๆ เรียงตามลำดับเป็นดังนี้

ขั้นตอนที่ ๑: การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

<u>ไม่ร้ายแรง/ร้ายแรง/วิกฤต</u>

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ก. ดังนี้

(๑) จัดเตรียมข้อมูลและอุปกรณ์สำหรับการติดต่อสื่อสารไปยังผู้ที่เกี่ยวข้อง

(๒) จัดเตรียมระบบและอุปกรณ์สำคัญเพื่อใช้ในการรับมือกับภัยคุกคามทางไซเบอร์

(๓) จัดชั้นความลับของข้อมูลที่เกี่ยวข้องกับการรับมือกับภัยคุกคามทางไซเบอร์

(๔) จัดทำทะเบียนสินทรัพย์สารสนเทศของระบบและอุปกรณ์สำคัญเพื่อใช้ในการรับมือกับภัยคุกคามทางไซเบอร์ (อ้างอิงข้อ ๑.๑.๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๕) ปิดพอร์ตของระบบและอุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน (อ้างอิงข้อ ๒.๑.๔ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๖) ควบคุมการเปลี่ยนแปลงการตั้งค่าของระบบและอุปกรณ์สำคัญ (Configuration Change Control) (อ้างอิงข้อ ๒.๒.๗ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๗) กำหนดบุคลากรผู้ทำหน้าที่เปลี่ยนแปลงการตั้งค่าของระบบและอุปกรณ์สำคัญ (อ้างอิงข้อ ๒.๒.๔ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๘) กำหนดวิธีการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสูง โดยต้องใช้การเข้ารหัสข้อมูลใน session ของการติดต่อเพื่อเข้าถึงระบบและอุปกรณ์สำคัญจากระยะไกล

(๙) ตรวจสอบการพัฒนาระบบสำคัญให้มีความมั่นคงปลอดภัย (อ้างอิงหมวด ๗ แนวปฏิบัติในการพัฒนาระบบให้มีความมั่นคงปลอดภัยในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ)

(๑๐) ฝึกซ้อมแผนการรับมือกับภัยคุกคามทางไซเบอร์เป็นประจำ (อ้างอิงข้อ ๔.๓.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๑๑) ติดตามข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ใหม่ๆ เป็นระยะๆ (อ้างอิงข้อ ๒.๕.๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๑๒) ตรวจสอบช่องโหว่และทดสอบเจาะระบบและอุปกรณ์สำคัญอย่างสม่ำเสมอ (อ้างอิงข้อ ๑.๓.๒-๑.๓.๓ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๑๓) เก็บข้อมูลและหลักฐานทางคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นไว้เป็นระยะเวลาไม่น้อยกว่า ๑๐ ปีเพื่อเป็นประโยชน์ในการเรียนรู้สำหรับเหตุการณ์ที่เกิดขึ้น

(๑๔) ควบคุมการเปลี่ยนแปลงการตั้งค่าของระบบและและอุปกรณ์สำคัญ (มีเนื้อหาเช่นเดียวกับข้อ ๖) โดยต้อง

- จัดเก็บประวัติการเปลี่ยนแปลงการตั้งค่าระบบและอุปกรณ์สำคัญ
- กำหนดให้มีการแจ้งเตือนอัตโนมัติเมื่อมีการเปลี่ยนแปลงการตั้งค่าระบบและอุปกรณ์สำคัญ (อ้างอิงข้อ ๒.๒.๗ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๑๕) ฝึกอบรมเพื่อเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉิน (ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น) เพื่อให้ผู้ที่เกี่ยวข้องรับทราบในบทบาทและความรับผิดชอบของตนเอง เมื่อจำเป็นต้องรับมือกับสถานการณ์ที่เกิดขึ้น (อ้างอิงข้อ ๔.๓.๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานกันเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (อ้างอิงข้อ ๒.๖.๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

ขั้นตอนที่ ๒: การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

<u>ไม่ร้ายแรง/ร้ายแรง</u>

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ข. ดังนี้

(๑) จัดให้มีกลไกลการตรวจจับภัยคุกคามทางไซเบอร์ที่กำลังจะเกิดขึ้นหรือที่ได้เกิดขึ้นแล้ว ซึ่งรวมถึง ลักษณะหรือสิ่งบ่งชี้สำหรับเหตุการณ์ที่เกิดขึ้น (อ้างอิงข้อ ๓.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๒) แจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นไปยังผู้ที่เกี่ยวข้อง

(๓) วิเคราะห์ข้อมูลล็อกบนระบบและอุปกรณ์สำคัญ รับการแจ้งเตือนจากระบบและอุปกรณ์ต่างๆ ตลอดจนตรวจสอบการทำงานของระบบและอุปกรณ์เหล่านั้นอย่างสม่ำเสมอ

(๔) ติดตาม วิเคราะห์ และประเมินประวัติการเข้าถึงหรือใช้งานระบบและอุปกรณ์ เพื่อให้เข้าใจลักษณะของการใช้งานหรือพฤติกรรมการใช้งานที่เป็นปกติ หรือไม่ปกติ

(๕) เมื่อคาดว่าอาจจะมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้เก็บรวบรวมข้อมูล ได้แก่ ภัยคุกคามที่เกิดขึ้น ช่องโหว่ที่ใช้ในการบุกรุก สถานการณ์ของการบุกรุก (กำลังเกิดเหตุหรือสถานการณ์สิ้นสุดลงแล้ว) จำนวนระบบและอุปกรณ์ที่ได้รับผลกระทบ ชื่อเครื่องคอมพิวเตอร์ IP Address

ของระบบที่ได้รับผลกระทบ ข้อมูลการแจ้งเตือนจากระบบป้องกันการบุกรุก ข้อมูลล็อกของระบบและอุปกรณ์

(๖) จัดเก็บและรักษาข้อมูลในย่อหน้าที่แล้วให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ ใช้เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

(๗) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยพิจารณาใช้แนวทางการจัดหมวดหมู่ตามที่ปรากฏในตารางด้านล่าง

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)[4]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

(๘) จัดลำดับความสำคัญของการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เช่น กรณีที่มีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นมากกว่า ๑ เหตุการณ์ในเวลาที่ไล่เลี่ยกันหรือในเวลาเดียวกัน

(๙) ศึกษาวิธีการและลักษณะของการบุกรุกที่เกิดขึ้น และระบุสาเหตุของการเกิดขึ้น รวมถึงจุดอ่อนของระบบและอุปกรณ์ที่ถูกบุกรุก

(๑๐) แจ้งประสานงานไปยังผู้ที่เกี่ยวข้องโดยผ่านช่องทางที่มีความมั่นคงปลอดภัย และคำนึงถึงระดับชั้นความลับของข้อมูลที่สื่อสารไปยังผู้ที่เกี่ยวข้องเหล่านั้น

(๑๑) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นให้ผู้ที่เกี่ยวข้องได้รับทราบภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกรมฯ ได้กำหนดไว้ โดยพิจารณาระยะเวลาของการรายงานตามแนวทางในตารางด้านล่างนี้

ข้อ ๓ ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	**ทุกเหตุการณ์**	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	**๓๐ นาที**	**๒ ชั่วโมง**	**๘ ชั่วโมง**
๔	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๖	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๗	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๑๐ นาที**	**๑ ชั่วโมง**	**๑ ชั่วโมง**
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	**๒๐ นาที**	ตามเวลาที่ต้องใช้ในการสืบสวน	**๔ ชั่วโมง**
๙	-	-	**๔ ชั่วโมง**	**๑๒ ชั่วโมง**

ขั้นตอนที่ ๒: การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

วิกฤต

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ค. ดังนี้

(๑) แจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในลักษณะ Real Time

(๒) จัดให้มีระบบสำหรับการตรวจจับ (และแจ้งเตือน) ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยอัตโนมัติ ติดตามการเกิดขึ้น และจัดเก็บข้อมูลผลการวิเคราะห์ต่างๆ

(๓) กำหนดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบและอุปกรณ์สำคัญ เช่น การใช้ซีพียู หน่วยความจำ และฮาร์ดดิสก์ที่ผิดปกติ

(๔) วิเคราะห์หาความสัมพันธ์ของข้อมูลที่ได้รับจากระบบและอุปกรณ์ต่างๆ เช่น ข้อมูลล็อกที่ได้รับจากระบบและอุปกรณ์เหล่านั้น เพื่อหาความสัมพันธ์ของเหตุการณ์ที่เกิดขึ้นบนระบบและอุปกรณ์เหล่านั้น

ขั้นตอนที่ ๓ : การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ไม่ร้ายแรง

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ง. ดังนี้

(๑) จำกัดขอบเขตและผลกระทบของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยครอบคลุมถึงการดำเนินการดังนี้

- ดำเนินการทางเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย
- ดำเนินการเชิงบริหาร เช่น กำหนดแนวทางการดำเนินการจัดการกับภัยคุกคามที่เกิดขึ้น กำหนดให้มีการสื่อสารทั้งภายในและภายนอก
- เตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด

(๒) เก็บรวบรวมหลักฐานทางคอมพิวเตอร์ต่างๆ ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เช่น ข้อมูลหลักฐาน ที่อยู่ในหน่วยความจำที่อาจสูญหายได้หากปิดเครื่อง เก็บข้อมูลล็อกของกิจกรรมที่เกิดขึ้น เก็บข้อมูลเกี่ยวกับไวรัสที่ตรวจพบ เก็บข้อมูลสถานะของระบบ และข้อมูลอื่นๆ ที่จำเป็นเพื่อนำไปใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี

(๓) ระบุแหล่งที่มาของการบุกรุก เช่น การระบุหมายเลข IP Address การระบุ Port ที่ใช้ในการเข้าถึง

(๔) ประสานงานแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์ไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่ได้รับผลกระทบ และให้ดำเนินการแจ้งภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดไว้

(๕) จัดการกับช่องโหว่ที่พบ (ที่ทำให้เกิดการบุกรุก) เช่น ดำเนินการตามวิธีการป้องกันระบบที่กำหนดไว้ การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ การปรับการตั้งค่าไฟร์วอลล์) การติดตั้ง virus signature เพิ่มเติม การแก้ไขช่องโหว่ของระบบปฏิบัติการ เป็นต้น

(๖) ดำเนินการตรวจสอบระบบและอุปกรณ์สำคัญต่างๆ เพื่อให้มั่นใจว่ายังสามารถใช้งานได้ตามปกติ

(๗) กำหนดมาตรการเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์นี้ซ้ำอีก หรือมีลักษณะที่คล้ายคลึงกันเกิดขึ้นอีกในอนาคต

ขั้นตอนที่ ๓ : การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ร้ายแรง

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด จ. ดังนี้

(๑) ใช้ระบบสำรองกรณีมีความจำเป็น เช่น กรณีที่ระบบหลักหยุดให้บริการ (อ้างอิงข้อ ๕.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

(๒) ประสานงานขอความช่วยเหลือไปยังหน่วยงานหรือผู้ให้บริการภายนอกที่เกี่ยวข้อง (Supply Chain Coordination) รวมถึงขอความช่วยเหลือจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติตามความจำเป็น

(๓) จัดทำรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๔) ปฏิบัติหน้าที่ร่วมกับสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ ตามแต่กรณีและความจำเป็น

(๕) จัดให้มีการรับมือภัยคุกคามทางไซเบอร์แบบอัตโนมัติ (อ้างอิงขั้นตอนที่ ๒ ในแบบวิกฤต ข้อ ๒)

ขั้นตอนที่ ๓ : การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

<u>วิกฤต</u>

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ฉ. ดังนี้

(๑) ใช้แผนกู้คืนระบบเพื่อให้ระบบสามารถให้บริการได้ทันภายในระยะเวลาเป้าหมายที่กำหนดไว้ (อ้างอิงข้อ ๕.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์)

ขั้นตอนที่ ๔ : การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

<u>ไม่ร้ายแรง/ร้ายแรง/วิกฤต</u>

ผู้รับผิดชอบระบบสารสนเทศ ใช้แนวทางปฏิบัติชุด ช. ดังนี้

(๑) ประเมินและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น นำบทเรียนที่ได้รับไปปรับปรุงการรับมือกับภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันภัยคุกคามดังกล่าวที่อาจจะเกิดขึ้นอีก รวมทั้งภัยคุกคามในลักษณะเดียวกัน (อ้างอิงขั้นตอนที่ ๓ ในแบบร้ายแรง ข้อ ๓)

(๒) สรุปข้อมูลภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในรอบระยะเวลาที่ผ่านมา เช่น จำนวนครั้งที่เกิดขึ้น ระยะเวลาที่ใช้ในการดำเนินการ สาเหตุของการถูกบุกรุก เป็นต้น

(๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น

(๔) เก็บรักษาข้อมูลและหลักฐานทางคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี (อ้างอิงขั้นตอนที่ ๑ ในแบบ ไม่ร้ายแรง/ร้ายแรง/วิกฤต ข้อ ๑๓)