ประกาศกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์
พ.ศ. ๒๕๖๗

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร และการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารและการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหาย กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ จึงเห็นควรกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรา ๔๕ กำหนดให้หน่วยงานของรัฐ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้ เรียกว่า “ประกาศกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๗”

๒. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ กำหนดให้มีการดำเนินการครอบคลุมประเด็นสำคัญ ดังต่อไปนี้

๒.๑ การตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์จะต้องดำเนินการ อย่างน้อยปีละ ๑ ครั้ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติ หรือแต่งตั้งโดยกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๒.๒ การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒.๓ การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

๒.๔ การรักษาไว้ซึ่ง ความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมใช้ของสารสนเทศและระบบเทคโนโลยีสารสนเทศ

๓. การเผยแพร่และการทบทวน

๓.๑ นโยบายจะต้องได้รับการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบ โดยการประกาศเวียนในระบบอินทราเน็ต เว็บไซต์ และสื่อสังคมออนไลน์ของหน่วยงาน เพื่อให้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในการปฏิบัติงาน

๓.๒ จัดให้มีการติดตามประสิทธิภาพและประสิทธิผลระบบการบริหารรักษาความมั่นคงปลอดภัยทางไซเบอร์ ด้วยวิธีการตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๓.๓ กำหนดให้...

๓.๓ กำหนดให้ทบทวนนโยบายเป็นประจำ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ เพื่อให้นโยบายมีความเหมาะสม และมีประสิทธิผลต่อการนำไปใช้งาน

๔. การกำหนดความรับผิดชอบ

๔.๑ อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ในฐานะผู้บริหารสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๔.๒ ผู้บริหารที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ของหน่วยงาน เป็นผู้รับผิดชอบสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแลและควบคุม ตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

๕. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและมาตรการป้องกันภัยคุกคามทางไซเบอร์ของหน่วยงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ ให้เจ้าหน้าที่ถือปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๗

(นายอดิทัต วะสีนนท์)
อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

แนวทางปฏิบัติ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์

พ.ศ. ๒๕๖๗

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับหน่วยงาน เพราะเป็นเทคโนโลยีที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงานของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ นอกจากนี้ข้อมูลสารสนเทศขององค์กรถือเป็นทรัพย์สินที่มีมูลค่าของหน่วยงาน การดูแล ป้องกัน รับมือ และลดความเสี่ยงต่อภัยคุกคามให้กับระบบเทคโนโลยีสารสนเทศและข้อมูล จึงเป็นภารกิจที่ต้องให้ความสำคัญอย่างยิ่ง โดยกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ได้ตระหนักถึงความมั่นคงปลอดภัยทางไซเบอร์ว่า เป็นปัจจัยสำคัญในการดำเนินงานตามภารกิจให้ประสบความสำเร็จภายใต้การบริหารจัดการที่ดี ทั้งนี้เพื่อเป็นการกำหนดทิศทาง หลักการและแนวทางในการป้องกันทรัพย์สินที่เกี่ยวข้องทางไซเบอร์และสารสนเทศให้ปลอดภัยจากภัยคุกคามที่ก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลในระบบสารสนเทศ และให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานทำงานอย่างมีประสิทธิภาพและเสถียรภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง ทั้งยังช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หรือถูกบุกรุก โจมตี ตลอดจนช่วยให้หน่วยงานสามารถบริหารจัดการฟื้นฟูระบบอย่างรวดเร็วหลังจากภัยคุกคามได้สิ้นสุดลง

ดังนั้น กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ จึงได้กำหนดมาตรฐานและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้นตามกรอบมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินงานด้วยวธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัย เชื่อถือได้ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และให้ผู้ปฏิบัติงานและหน่วยงานภายในองค์กรใช้ในการดำเนินงานและถือปฏิบัติอย่างเคร่งครัด

สารบัญ

เรื่อง		หน้า
คำนำ		ก
สารบัญ		ข
คำนิยาม		๑
หมวดที่ ๑	การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๔
	ส่วนที่ ๑ การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๔
	ส่วนที่ ๒ ขั้นตอนการปฏิบัติในการตรวจสอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๑๑
หมวดที่ ๒	การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๑๔
	ส่วนที่ ๑ องค์ประกอบการประเมินความเสี่ยง	๑๔
	ส่วนที่ ๒ ขั้นตอนการปฏิบัติในการประเมินความเสี่ยง	๑๕
หมวดที่ ๓	การรับมือภัยคุกคามทางไซเบอร์	๑๗
	ส่วนที่ ๑ แผนการรับมือภัยคุกคามทางไซเบอร์	๑๗
	ส่วนที่ ๒ มาตรการในการรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามทางไซเบอร์	๑๘
	ส่วนที่ ๓ มาตรการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์	๑๙
	ส่วนที่ ๔ มาตรการเพื่อระงับภัยคุกคาม ปราบปรามภัยคุกคามทางไซเบอร์ และ ฟื้นฟูระบบงานที่ได้รับผลกระทบ	๒๐
	ส่วนที่ ๕ การดำเนินงานที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์	๒๑
หมวดที่ ๔	การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางไซเบอร์	๒๒
หมวดที่ ๕	บทบาท หน้าที่ และความรับผิดชอบ	๒๔

คำนิยาม

๑. **คณะกรรมการ** หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. **บริการที่สำคัญ** หมายถึง ภารกิจหรือบริการของหน่วยงานของรัฐ

๓. **การรักษาความมั่นคงปลอดภัยไซเบอร์** หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๔. **ภัยคุกคามทางไซเบอร์ (Cyber Threats)** หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๕. **ไซเบอร์ (Cyber)** หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

๖. **หน่วยงานของรัฐ** หมายถึง ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

๗. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๘. **มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์** หมายถึง การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๙. **หน่วยงาน** หมายถึง กรม สำนัก ศูนย์ กอง และหน่วยงานที่มีฐานะเทียบเท่า กรม/กอง รวมถึง หน่วยงานส่วนภูมิภาคที่อยู่ในสังกัดกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑๐. **ผู้บริหารระดับสูงสุดของหน่วยงาน** หมายถึง อธิบดี หรือเทียบเท่า

๑๑. **ผู้บริหาร** หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ อธิบดี หรือเทียบเท่า ผู้อำนวยการสำนัก ศูนย์ กอง หรือเทียบเท่า

๑๒. **ผู้ดูแลระบบ** หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๓. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

๑๔. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๑๕. **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย ระบบเครือข่ายแบบไร้สาย ระบบอินทราเน็ต และระบบอินเทอร์เน็ต เป็นต้น

๑๖. **ชื่อผู้ใช้ (User Name)** หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิการใช้งานไว้

๑๗. **รหัสผ่าน (Password)** หมายถึง กลุ่มตัวอักษรหรือตัวเลขหรืออักขระที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล สารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

๑๘. **บัญชีผู้ใช้ (User Account)** หมายถึง รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑๙. **การเข้ารหัส (Encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password)

๒๑. **VPN (Virtual Private Network)** หมายถึง เครือข่ายส่วนตัวเสมือน โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๒. **SSID (Service Set Identifier)** หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๒๓. **WEP (Wire Equivalent Privacy)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันต้องรู้ค่าชุดตัวเลขนี้

๒๔. **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๒๕. **MAC Address (Media Access Control Address)** หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๒๖. **ไฟล์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๒๗. **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๒๘. **ช่องโหว่ (Vulnerability)** หมายถึง ช่องโหว่ในทรัพย์สินสารสนเทศที่อาจเกิดจากความบกพร่องในการผลิตหรือออกแบบ ทำให้เกิดจุดอ่อนและมีความเสี่ยงในการคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน

๒๙. **การเฝ้าระวัง (Monitoring)** หมายถึง การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบความผิดปกติจากการประมวลผล กิจกรรมต่าง ๆ ของระบบสารสนเทศ

๓๐. **บันทึกเหตุการณ์ (Logs)** หมายถึง บันทึกเหตุการณ์การใช้งานของระบบเทคโนโลยีสารสนเทศและการสื่อสาร การเข้าใช้งานระบบ การประมวลผล กิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึงประสิทธิภาพ ความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓๑. **โปรแกรมไม่พึงประสงค์** หมายถึง โปรแกรมหรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความเสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) สปายแวร์ (Spyware)

๓๒. **ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Cyber and Information Security)** หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของไซเบอร์และสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

๓๓. **ความเสี่ยงเรื่องความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Cyber and Information Security Risk)** หมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานหน่วยงาน รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วยแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อใช้ในการรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ให้สามารถกลับมาใช้งานได้อย่างปกติ

การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ มีประเด็นสำคัญในการดำเนินการ ๕ หมวด ดังนี้

หมวดที่ ๑
การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑. ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๒) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ ๑)

๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติมาตรฐานการปฏิบัติงาน และที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การตรวจสอบความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างน้อยปีละหนึ่งครั้ง หรือความถี่ที่สูงกว่านั้นตามที่กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่กำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดยกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ โดยแนวทางการตรวจสอบ มีดังนี้

๑. วัตถุประสงค์ (PURPOSE)

การตรวจสอบนี้มีวัตถุประสงค์เพื่อกำหนดความคาดหวังในการตรวจสอบ และใช้เป็นแนวทางสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในแนวทางปฏิบัตินี้ ผู้ตรวจสอบควรใช้ดุลยพินิจเยี่ยงผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบ

๒. กลุ่มเป้าหมาย (AUDIENCE)

กลุ่มเป้าหมาย มีดังนี้

ก. ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ และ

ข. ผู้มีส่วนได้ส่วนเสีย เช่น หัวหน้าหน่วยงานที่ดูแลรับผิดชอบข้อมูลสารสนเทศ เจ้าของระบบงานสารสนเทศ หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูลที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

๓. ขอบเขต (SCOPE)

การตรวจสอบมีขอบเขตครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔. การอนุมัติผู้ตรวจสอบ (AUDITOR APPROVAL)

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหน่วยงานและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด ใบสมัครจะถือว่าสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาโดยหน่วยงาน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

การพิจารณามีเกณฑ์ ๒ ประการ ได้แก่ เกณฑ์ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (Audit Firm/Team) และเกณฑ์ผู้ตรวจสอบ (Auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง :

ก. ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์ และ

ข. ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้ และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่อาจพิจารณาแตกต่างกันไปตามที่หน่วยงานเห็นสมควรในประเด็นต่อไปนี้

(๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน

(๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น

ในกรณีผู้ตรวจสอบของหน่วยงานที่ลงทะเบียนแล้วลาออกจากการเป็นพนักงานก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงพนักงานที่ลงทะเบียนไว้ ให้หน่วยงานแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่มีการเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๕. ความคาดหวังในการตรวจสอบ (AUDIT EXPECTATIONS)

การกำหนดความคาดหวังในการตรวจสอบ มีวัตถุประสงค์เพื่อช่วยให้ผู้อ่านเข้าใจว่าควรดำเนินการและรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ระบุความคาดหวังในการตรวจสอบไว้ ๗ ด้านในหัวข้อ ๕.๑ ถึง ๕.๗ ดังนี้

๕.๑ หลักการตรวจสอบ (Principles of Auditing)

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity) เป็นรากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation) เป็นหน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care) การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality) เป็นความมั่นคงปลอดภัยของข้อมูล

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence) เป็นพื้นฐานสำหรับความเป็นกลางของการตรวจสอบ และความเที่ยงธรรมของข้อสรุปการตรวจสอบ

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

๕.๒ วัตถุประสงค์ในการตรวจสอบ

ก. ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

ข. ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๕.๓ ขอบเขตการตรวจสอบ (Audit Scope)

การตรวจสอบจะครอบคลุม สิ่งต่อไปนี้

ขอบเขต (Scope)	**คำอธิบาย (Description)**
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๕.๔ แนวทางการตรวจสอบ (Audit Approach)

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

ก. การตรวจสอบการปฏิบัติตามข้อกำหนด

การดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ข. การตรวจสอบตามความเสี่ยง

การระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และการตรวจสอบการควบคุมที่เหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบได้ชัดเจนและภัยที่ไม่อาจคาดการณ์ได้

๕.๕ ข้อค้นพบการตรวจสอบ (Audit Finding)

ผู้ตรวจสอบควรเน้น สิ่งต่อไปนี้

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุมการตรวจสอบ

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน และดำเนินการแก้ไข (Corrective Action) ไปแล้วก็ตาม

ง. เน้นแนวปฏิบัติที่ดี (Good Practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

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

๕.๖ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่อง ต่อไปนี้

ก. ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๕.๗ รูปแบบรายงานการตรวจสอบ (Audit Report Format)

รายงานการตรวจสอบควรมีอย่างน้อย ดังต่อไปนี้

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๕.๒ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๕.๓ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๕.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๕.๖ ของเอกสารนี้

ส่วนที่ ๒ ขั้นตอนการปฏิบัติในการตรวจสอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑. ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒. ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

๓. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมเปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

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

๕. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๖. คณะทำงานรับทราบผลการตรวจสอบ

๗. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-Conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษาความลับในการตรวจสอบ

๘. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๙. คณะทำงานดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๑๐. ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

๗. ขั้นตอนการปฏิบัติในการตรวจสอบ

๑. ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒. ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

๓. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

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

๕. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๖. คณะทำงานรับทราบผลการตรวจสอบ

๗. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-Conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษาความลับในการตรวจสอบ

๘. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๙. คณะทำงานดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๑๐. ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

เอกสารอ้างอิง

๑. GUIDELINES FOR AUDITING CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, JANUARY ๒๐๒๐
Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guidelines_for_auditing_critical_information_infrastructure.pdf

๒. ISO ๑๙๐๑๑:๒๐๑๘ Guidelines for auditing management systems, ISO, July ๒๐๑๘
Link: https://www.iso.org/standard/๗๐๐๑๗.html

หมวดที่ ๒
การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

แนวปฏิบัติ

เพื่อให้หน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑ องค์ประกอบการประเมินความเสี่ยง

๑. การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจของหน่วยงาน ภารกิจและกิจกรรมสิ่งแวดล้อมด้านกฎหมาย วัฒนธรรม สังคม ปัจจัยที่มีต่อความสำเร็จของหน่วยงาน โอกาส และภัยคุกคามที่มีต่อหน่วยงาน การระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ควรดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุก ๆ ด้านของ

หน่วยงาน ซึ่งรวมถึงการพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีต หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ และการตรวจช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าว อาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒. การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๓. การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๔. การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

ส่วนที่ ๒ ขั้นตอนการปฏิบัติในการประเมินความเสี่ยง

๑. การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ มีการตรวจสอบอย่างน้อยดังนี้

๑) ตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศและข้อมูล (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๑) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓) มีการตรวจสอบและประเมินความเสี่ยงให้จัดทำรายงานพร้อมข้อเสนอแนะ

๔) มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างดี

๓. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๑) ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ

๒) ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๔) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๔. ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๕. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้นซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

๖. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวดที่ ๓
การรับมือภัยคุกคามทางไซเบอร์

วัตถุประสงค์

๑. เพื่อให้มีแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา
๒. เพื่อลดความเสี่ยง ลดความเสียหาย และป้องกันเหตุที่อาจจะเกิดขึ้นจากภัยคุกคามทางไซเบอร์
๓. เพื่อให้ระบบสารสนเทศและข้อมูลสามารถให้บริการอย่างต่อเนื่อง

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบและเจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

แนวปฏิบัติ

ส่วนที่ ๑ แผนการรับมือภัยคุกคามทางไซเบอร์

๑. ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังนี้

๑) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

๒) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใดๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

๖) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๗) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

๘) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ

๙) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๒. ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๔. ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยวงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ มาตรการในการรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามทางไซเบอร์

การกำหนดมาตรการในการรับมือภัยคุกคามทางไซเบอร์ให้สามารถตอบสนองได้อย่างทันเหตุการณ์ ต้องดำเนินการ ดังนี้

๑. การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคล หรือองค์กรต่างๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใดที่ช่วยสนับสนุนการรายงานเมื่อเกิดภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น

๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์

๓) จัดให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ตลอดจนสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

๔) จัดเตรียมรายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network Diagrams) เพื่อข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (Discovery Protocol) เป็นต้น

๖) จัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (Configuration Management Plan) ที่มีผลกระทบกับความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน และดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่างๆ (Configuration Change Control) โดยจะต้องมีการบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร

๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่างๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง

๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใดๆ

๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยต้องมีการคัดกรองนักพัฒนา (Developer Screening) ที่ได้รับมอบหมายได้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ เท่านั้น

๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Respond Capability Testing)

๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (Treat Intelligence)

๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อพบช่องโหว่หรือจุดอ่อนต่าง ๆ

๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์

๑๔) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (Simulated Event) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตน เมื่อต้องรับมือกับสถานการณ์ดังกล่าว

๑๕) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

ส่วนที่ ๓ มาตรการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

๑. จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้

๒. จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๓. จัดให้มีข้อควรปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยทางไซเบอร์ และการตรวจสอบระบบที่มีความสำคัญ (Critical Systems) และจัดให้มีข้อควรปฏิบัติที่สูงขึ้นสำหรับระบบงานที่มีความสำคัญมากขึ้น

๔. วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (Profile Networks and Systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (Normal Behaviors) ทำการศึกษา และค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (Event Correlation)

๕. ทันทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์ ช่องโหว่ที่อาจถูกใช้ในการโจมตี สถานการณ์ของการโจมตี จำนวนระบบหรือบริการที่ได้รับผลกระทบ โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับข้อมูล และข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (Safeguard Incident Data) เป็นพยานหลักฐานในการดำเนินคดี และจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

๖. ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยพิจารณาอ้างอิงจากข้อมูล ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗. จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ ผลกระทบต่อข้อมูล และความสามารถในการกู้คืน เป็นต้น

๘. ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี

๙. ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัยหรือช่องทางที่กรมกำหนด โดยต้องคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้ผู้รับผิดชอบดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

๑๐. รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่กรมกำหนด

ส่วนที่ ๔ มาตรการเพื่อระงับภัยคุกคาม ปราบปรามภัยคุกคามทางไซเบอร์ และฟื้นฟูระบบงานที่ได้รับผลกระทบ

๑. ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ

๑) การดำเนินการเชิงเทคนิค เช่น ลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี เป็นต้น

๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของกรม การสื่อสารทั้งภายในและภายนอกกรม เป็นต้น

๒. ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่างๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์การเก็บข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี

๓ ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (Attacking Host) เช่น การระบุหมายเลขประจำเครื่อง การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น

๔. ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอรด์และความคืบหน้าในการตอบสนองยังบุคคลหรือหน่วยงานที่เกี่ยวข้องผ่านทางช่องทางที่มีความเหมาะสมและปลอดภัย ภายในระยะเวลาที่กรมกำหนด

๕. ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม

๖. ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ การสร้างระบบงานขึ้นใหม่ การแทนที่ไฟล์ที่ได้รับผลกระทบ การติดตั้งโปรแกรมคอมพิวเตอร์ การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย เป็นต้น

๗. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต

๘. ดำเนินการตามแผนการทำงานในการกู้คืนระบบต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่กำหนด โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของกรมทำได้อย่างรวดเร็ว

ส่วนที่ ๕ การดำเนินงานที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

๑. นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีผลกระทบรุนแรงมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของกรม นโยบายและกระบวนการฝึกบุคลากร การระบุผู้มีอำนาจ การดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง

๒. รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์เป็นรายเดือน เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในกรม

๓. ปรับปรุงมาตรการและเตรียมการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน

๔. เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการเก็บรักษา หลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่กรมได้กำหนด

หมวดที่ ๔
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของหน่วยงาน ได้ใช้งานอย่างปลอดภัย

๒. เพื่อป้องกัน รับมือ และลดความเสี่ยงต่อภัยคุกคามทางไซเบอร์และมีแนวทางการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์อย่างถูกต้อง

๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบและเจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

แนวปฏิบัติ

๑. กำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามเหมาะสม

๓. จัดฝึกอบรมการใช้งานสารสนเทศของหน่วยงานอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๔. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๗. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎระเบียบของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ อย่างเคร่งครัด

๘. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๕
บทบาท หน้าที่ และความรับผิดชอบ

วัตถุประสงค์

๑. เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยทางไซเบอร์ของกรม ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความปลอดภัย

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ ทั้งระดับนโยบาย ระดับปฏิบัติการ ได้แก่ ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้งานได้รับรู้เข้าใจ บทบาทหน้าที่ ความรับผิดชอบ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ผู้รับผิดชอบ

ทุกหน่วยงานภายในกรม

แนวปฏิบัติ

การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งานและความรับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร โดยมีการกำหนดหน้าที่ ความรับผิดชอบ ดังนี้

๑. ระดับนโยบาย

รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ผู้รับผิดชอบ ได้แก่

(๑) ผู้บริหารระดับสูงสุด (Chief Executive Office: CEO) เป็นผู้ลงนามอนุมัติแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรม และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่กรม หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) เป็นผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรม และทบทวนภาพรวมของนโยบายดังกล่าวของกรม

(๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเทียบเท่าระดับผู้อำนวยการ

- กำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศรับผิดชอบการดูแลระบบสารสนเทศที่กรมใช้งานให้มีความมั่นคงปลอดภัย
- ควบคุมตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติ เพื่อให้คงไว้ซึ่งการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อหน่วยงาน
- จัดให้มีช่องทางการติดต่อสื่อสารสำหรับใช้รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

๒. ระดับปฏิบัติ

(๑) หัวหน้ากลุ่ม/ฝ่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบ

- กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดูแลให้มีการติดตาม ตรวจสอบในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ พร้อมทั้งรายงานแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบกับหน่วยงาน
- ศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง ควบคุม ดูแล การใช้ระบบสารสนเทศต่าง ๆ ให้เป็นไปตามแผน ป้องกัน แก้ไขและสำรองฉุกเฉิน ให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงในส่วนที่สำคัญ และรายงานผลการทดสอบและการปฏิบัติตามแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

(๒) ผู้ดูแลระบบระดับ Administrator ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ

- ดูแลรักษาและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- ตรวจสอบและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติหรือมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ไม่คาดคิด ให้รีบดำเนินการแก้ไขในทันที เพื่อป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้น ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการละเมิดหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและพิจารณาระงับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศในทันที
- ติดตั้งเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบการเข้ารหัสสารสนเทศ ระบบป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่จำเป็นเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างมั่นคง
- ตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และติดตั้งปรับปรุงการแก้ไขข้อบกพร่อง (Patch) ของระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงและทันสมัยอยู่เสมอ

- ดำเนินการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) พร้อมทั้งทำการทดสอบตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่กำหนดไว้
- ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication Port) ของระบบเทคโนโลยีและปิดช่องทางการสื่อสารที่ไม่มีความจำเป็นใช้งานในทันที เพื่อป้องกันการถูกเจาะเข้าระบบจากบุคคลภายนอกที่ไม่ได้รับอนุญาต
- ดูแลรักษาและปรับปรุงบัญชีรายชื่อผู้ใช้งานของระบบเทคโนโลยีสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิของผู้ใช้งานทันทีที่พ้นสภาพจากเป็นผู้ใช้งาน
- จัดทำรายงานการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทส และนำเสนอต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อรับทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการแก้ไขการปรับปรุงประสิทธิภาพและการให้บริการต่อไป
- ปฏิบัติงานอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมตามที่ได้รับมอบหมาย

(๓) ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอกหน่วยงาน ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรม รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

เอกสารอ้างอิง

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๓. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ สำนักงานมาตรฐาน สินค้าเกษตรและอาหารแห่งชาติ พ.ศ. ๒๕๖๕

๔. มาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

๕. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕ สำนักงานสภาความมั่นคงแห่งชาติ

๖. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข

๗. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ กรมสุขภาพจิต

๘. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ กรมสนับสนุนบริการสุขภาพ

๙. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

๑๐. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๑ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

๑๑. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่