ประกาศกรมป่าไม้
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

เพื่อให้การจัดทำมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมป่าไม้ เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นมาตรฐานในการดำเนินการรักษาความปลอดภัยทางไซเบอร์ของกรมป่าไม้

ฉะนั้นอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ที่แก้ไขเพิ่มเติมและตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมป่าไม้จึงประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “ประกาศกรมป่าไม้เรื่อง แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้”

๒. การจัดทำแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้มีความมั่นคงปลอดภัยทางไซเบอร์ สำหรับการใช้งานระบบเครือข่ายและข้อมูลสารสนเทศของกรมป่าไม้ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมป่าไม้ ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมป่าไม้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องมีการทบทวนให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๓. กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์โดยคณะกรรมการการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมป่าไม้ถือปฏิบัติตามที่ได้มีการแก้ไขหรือเพิ่มเติมนั้น

๔. ให้ใช้แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นายนิกร ศิรโรจนานนท์)
อธิบดีกรมป่าไม้

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนบท้ายประกาศกรมป่าไม้ ลงวันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

คำนำ

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ ฉบับนี้ จัดทำขึ้นเพื่อเป็นกรอบนโยบายและแนวทางในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ให้เป็นระบบ โปร่งใส และสอดคล้องกับกฎหมาย มาตรฐาน และนโยบายภาครัฐที่เกี่ยวข้อง ทั้งนี้ การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจที่มีความสำคัญยิ่ง เนื่องจากระบบเทคโนโลยีสารสนเทศของกรมป่าไม้เป็นกลไกหลักในการสนับสนุนภารกิจด้านการอนุรักษ์ การบริหารจัดการทรัพยากรป่าไม้ การให้บริการประชาชน และการประสานข้อมูลระหว่างหน่วยงานภาครัฐ ภัยคุกคามทางไซเบอร์ในปัจจุบันมีความหลากหลาย ซับซ้อน และเกิดขึ้นได้ตลอดเวลา ทั้งการโจมตีแบบเรียกค่าไถ่ การเจาะระบบ การรั่วไหลของข้อมูลสำคัญ ตลอดจนภัยคุกคามที่มุ่งโจมตีโครงสร้างพื้นฐานด้านข้อมูลสำคัญของรัฐ (Critical Information Infrastructure) ซึ่งอาจส่งผลกระทบต่อความมั่นคงของข้อมูล ความเชื่อมั่นต่อหน่วยงาน และการปฏิบัติงานที่ต้องอาศัยความต่อเนื่องและความถูกต้องของข้อมูลอย่างมีนัยสำคัญ

กรมป่าไม้ ได้ตระหนักถึงความสำคัญดังกล่าว จึงได้จัดทำเอกสารฉบับนี้ขึ้น โดยกำหนดหลักเกณฑ์ มาตรการ แนวทางการควบคุม และขั้นตอนการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมีจุดมุ่งหมายเพื่อให้บุคลากรทุกระดับของกรมป่าไม้ รวมถึงผู้รับจ้าง ผู้พัฒนาระบบ และผู้ให้บริการภายนอกที่เกี่ยวข้อง สามารถยึดถือเป็นแนวทางกลางในการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างถูกต้อง ครอบคลุม และมีประสิทธิผล การป้องกันเหตุการณ์ไม่พึงประสงค์ทางไซเบอร์ และการสนับสนุนให้กรมป่าไม้สามารถปฏิบัติภารกิจได้อย่างต่อเนื่องและปลอดภัยในทุกสถานการณ์

กรมป่าไม้ หวังเป็นอย่างยิ่งว่าเอกสารฉบับนี้จะเป็นประโยชน์ต่อหน่วยงานและบุคลากรทุกฝ่ายที่เกี่ยวข้อง และช่วยยกระดับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ให้มีความเข้มแข็งทันสมัย และสอดคล้องกับแนวทางการพัฒนารัฐบาลดิจิทัลในปัจจุบันและอนาคต

พฤษภาคม ๒๕๖๙

สารบัญ

บทที่ ๑ บทนำ

๑.๑ หลักการ

การดำเนินภารกิจของกรมป่าไม้ต้องพึ่งพาระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศภูมิศาสตร์ในการสนับสนุนการบริหารจัดการทรัพยากรป่าไม้ การให้บริการประชาชน การวิเคราะห์ข้อมูลเชิงนโยบาย และการปฏิบัติงานด้านอนุรักษ์และบังคับใช้กฎหมาย อย่างไรก็ตาม ภัยคุกคามทางไซเบอร์ มีความซับซ้อนและรุนแรงเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในรูปแบบการโจมตีแบบมุ่งเป้า การโจมตีเรียกค่าไถ่ การรั่วไหลของข้อมูล การปลอมแปลงหน้าเว็บไซต์ รวมถึงการโจมตีโครงสร้างพื้นฐานด้านข้อมูลสำคัญ ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องของบริการ ความเชื่อถือได้ของข้อมูล และภาพลักษณ์ของกรมป่าไม้ เพื่อให้สอดคล้องกับ มาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

กรมป่าไม้จึงได้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ เพื่อกำหนดมาตรฐาน แนวทางการบริหารจัดการความเสี่ยง และมาตรการควบคุมด้านความมั่นคงปลอดภัย สำหรับทุกหน่วยงาน โดยครอบคลุมกระบวนการตามหลักสากล ได้แก่ การกำกับดูแล (Governance) การระบุความเสี่ยง (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการฟื้นฟูระบบ (Recover) การกำหนดมาตรฐานกลางดังกล่าว มีวัตถุประสงค์เพื่อยกระดับความพร้อมของกรมป่าไม้ในการรับมือภัยคุกคาม ลดความเสียหายต่อข้อมูลและระบบงานสำคัญ เสริมสร้างความมั่นคงปลอดภัยของข้อมูลภาครัฐ และสนับสนุนการให้บริการประชาชนอย่างมีประสิทธิภาพ โปร่งใส และน่าเชื่อถือ ทั้งนี้ เอกสารฉบับนี้ถือเป็นแนวทางสำคัญสำหรับเจ้าหน้าที่ ผู้ปฏิบัติงานภายนอก และผู้เกี่ยวข้องทุกฝ่ายในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบ ข้อมูล และภารกิจของกรมป่าไม้ได้รับการคุ้มครองอย่างเหมาะสม รองรับการทำงานในทุกสถานการณ์ และสนับสนุนการพัฒนาหน่วยงานสู่ดิจิทัลอย่างมั่นคงและยั่งยืน

๑.๒ วัตถุประสงค์

การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ ฉบับนี้มีวัตถุประสงค์เพื่อ

๑) เพื่อกำหนดมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นหนึ่งเดียวสำหรับการบริหารจัดการ ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลของกรมป่าไม้ ให้สอดคล้องกับกฎหมาย นโยบาย และมาตรฐานสากลที่เกี่ยวข้อง

๒) เพื่อเสริมสร้างความพร้อมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบจากภัยคุกคามทางไซเบอร์ ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อภารกิจและบริการสาธารณะของกรมป่าไม้

๓) เพื่อยกระดับความมั่นคงปลอดภัยของระบบงาน ข้อมูล และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ให้มีความถูกต้อง เชื่อถือได้ และรองรับการปฏิบัติงานอย่างต่อเนื่อง

๔) เพื่อสร้างความตระหนักรู้และกำหนดบทบาทความรับผิดชอบของบุคลากรและผู้เกี่ยวข้องทุกฝ่าย ในการปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมธรรมาภิบาลข้อมูลภาครัฐอย่างยั่งยืน

๑.๓ องค์ประกอบของประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ ประกอบด้วย นโยบายและการกำกับดูแลด้านไซเบอร์ การบริหารจัดการความเสี่ยง มาตรการควบคุมด้านความปลอดภัยเชิงเทคนิคและเชิงบริหาร การเฝ้าระวังและตรวจจับเหตุการณ์ การตอบสนองและฟื้นฟูหลังเกิดเหตุการณ์ รวมถึงมาตรการด้านบุคลากร การสร้างความตระหนักรู้ และการตรวจประเมินเพื่อปรับปรุงอย่างต่อเนื่อง เพื่อให้ระบบ ข้อมูล และภารกิจของกรมป่าไม้มีความมั่นคงปลอดภัยและรองรับการดำเนินงานได้อย่างยั่งยืน

๑.๔ บทบังคับใช้

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ให้มีผลบังคับใช้กับหน่วยงานทุกส่วนราชการภายในกรมป่าไม้ รวมถึงเจ้าหน้าที่ บุคลากร ผู้ปฏิบัติงานภายนอก ผู้รับจ้าง ผู้พัฒนาระบบ และผู้ให้บริการที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและข้อมูลของกรมป่าไม้

๑.๕ การเผยแพร่และทบทวน

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ ฉบับนี้จัดทำขึ้น และมีจะมีการทบทวนเมื่อมีการปรับปรุงกฎหมาย ระเบียบ ประกาศ และอื่นๆ ที่เกี่ยวข้อง โดยประมวลแนวทางปฏิบัติและกรอบมาตรฐานได้นำออกเผยแพร่ โดยการประกาศแจ้งเวียนในระบบงานสารบรรณอิเล็กทรอนิกส์และเว็บไซต์กรมป่าไม้ เพื่อให้บุคลากรกรมป่าไม้ และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

บทที่ ๒ คำนิยาม

๑. **คณะกรรมการ** หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. **กกม.** หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๓. **หน่วยงานของรัฐ** หมายถึง หน่วยงานของรัฐที่ถูกประกาศเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ

๔. **บริการที่สำคัญ** หมายถึง ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙

๕. **สำนักงาน** หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๖. **ดัชนีชี้วัดความเสี่ยงที่สำคัญ** หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยง ในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

๗. **ผู้ให้บริการภายนอก** หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการ ด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับ ระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการ ที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๘. **คอมไพเลอร์** หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรม คอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่ง ไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

๙. **แพตช์** หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่ จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่อง ความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของ ซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่ แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

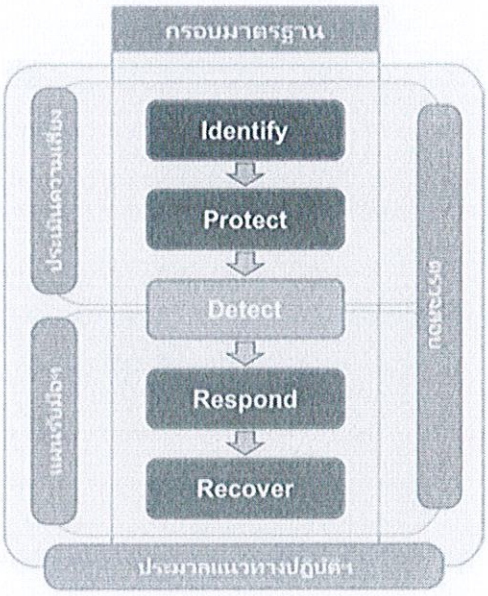
๑๐. Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

๑๑. Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

๑๒. Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับ การดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับ การเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

การจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบ ดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑ หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ หรือด้านไซเบอร์ โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้

๒) แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

๑.๒ ต้องมีการรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก หรือโดย ผู้ตรวจสอบอิสระภายนอก

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่จะเกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการไอซีทีของหน่วยงาน

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ และจัดให้มีการสื่อสารไปยังบุคลากรเกี่ยวข้องอย่างมีประสิทธิผล

๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยดังนี้

๔.๑ แนวนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)

๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)

๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)

๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การรายงานบัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๒ กรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การกำกับดูแล (Govern)

๑.๑ บริบทขององค์กร (Organizational Context)

๑.๑.๑ หน่วยงานจะต้องกำหนดพันธกิจ บทบาท และวัตถุประสงค์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับภารกิจหลักขององค์กร

๑.๑.๒ หน่วยงานจะต้องระบุผู้มีส่วนได้ส่วนเสียภายในและภายนอกที่เกี่ยวข้องกับระบบสารสนเทศและจัดลำดับความสำคัญในการบริหารความเสี่ยงไซเบอร์

๑.๑.๓ หน่วยงานจะต้องศึกษาวิเคราะห์บริบทที่เกี่ยวข้อง เช่น กฎหมาย ข้อบังคับ โครงสร้างพื้นฐาน ทรัพยากร และเทคโนโลยี เพื่อใช้เป็นข้อมูลในการกำหนดนโยบายและแนวปฏิบัติ

๑.๒ กลยุทธ์การบริหารความเสี่ยง (Risk Management Strategy)

๑.๒.๑ หน่วยงานจะต้องจัดทำและทบทวนกลยุทธ์ด้านการบริหารความเสี่ยงไซเบอร์อย่างสม่ำเสมอ โดยคำนึงถึงระดับความเสี่ยงที่ยอมรับได้ (risk tolerance)

๑.๒.๒ หน่วยงานจะต้องดำเนินการประเมินความเสี่ยงด้านไซเบอร์ต่อภารกิจหลัก และใช้ผลการประเมินเพื่อจัดลำดับความสำคัญของมาตรการควบคุม

๑.๒.๓ กลยุทธ์การบริหารความเสี่ยงจะต้องครอบคลุมภัยคุกคามจากภายใน ภายนอก รวมถึงผู้ให้บริการ (ISP) และผู้รับจ้างงานจากภายนอก (Outsource)

๑.๓ บทบาท ความรับผิดชอบ และอำนาจหน้าที่ (Roles, Responsibilities, and Authorities)

๑.๓.๑ หน่วยงานจะต้องกำหนดบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ไว้อย่างชัดเจนในทุกระดับขององค์กร

๑.๓.๒ บุคลากรทุกระดับต้องตระหนักถึงบทบาทของตนเองและปฏิบัติตามนโยบายไซเบอร์ขององค์กรอย่างเคร่งครัด

๑.๓.๓ ผู้บริหารระดับสูงต้องมีส่วนร่วมในการตัดสินใจด้านนโยบายไซเบอร์ และแต่งตั้งเจ้าหน้าที่รับผิดชอบเฉพาะด้าน เช่น CISO หรือ CSIRT (ถ้ามี)

๑.๔ นโยบาย (Policy)

๑.๔.๑ หน่วยงานจะจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมการใช้งาน การเข้าถึง การจัดเก็บ และการถ่ายโอนข้อมูล

๑.๔.๒ นโยบายต้องผ่านความเห็นชอบจากผู้บริหารระดับสูง และประกาศใช้กับบุคลากรทุกระดับ

๑.๔.๓ นโยบายต้องมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์สำคัญด้านความปลอดภัย

๑.๕ การกำกับดูแลและตรวจสอบ (Oversight)

๑.๕.๑ หน่วยงานจะต้องจัดให้มีการกำกับดูแลการดำเนินงานตามนโยบายไซเบอร์อย่างเป็นระบบ โดยอาจตั้งคณะกรรมการหรือกลไกติดตามประเมินผล

๑.๕.๒ จะมีการรายงานความคืบหน้าและความเสี่ยงด้านไซเบอร์ต่อผู้บริหารเป็นระยะๆ เพื่อประกอบการตัดสินใจ

๑.๕.๓ หน่วยงานจะต้องจัดให้มีการตรวจสอบภายใน (internal audit) และ/หรือประเมินจากหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อยกระดับมาตรฐาน

๑.๖ การจัดการความเสี่ยงในห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management)

๑.๖.๑ หน่วยงานจะต้องระบุเสี่ยง ประเมินความเสี่ยง และควบคุมความเสี่ยงที่เกี่ยวข้องกับบุคคลภายนอกหรือผู้ให้บริการด้านเทคโนโลยีสารสนเทศ

๑.๖.๒ สัญญาและข้อตกลงกับผู้ให้บริการต้องระบุข้อกำหนดด้านความปลอดภัยไซเบอร์อย่างชัดเจน เช่น SLA การเข้ารหัสข้อมูล การแจ้งเหตุการณ์ รวมทั้งการทำ Secure Coding ด้วย

๑.๖.๓ หน่วยงานจะตรวจสอบความสอดคล้องของผู้ให้บริการกับนโยบายไซเบอร์ขององค์กรรวมถึงดำเนินการประเมินเป็นระยะ

หัวข้อที่ ๒ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๒.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้โนการวางแผนและการบริหารด้านความมั่งคงปลอดภัยทางไซเบอร์ โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๑.๑ ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สิน แต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อหรือคำอธิบายของทรัพย์สิน
๒) ประเภทของอุปกรณ์/ยี่ห้อ
๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชั่น
๕) การระบุลำดับความสำคัญของทรัพย์สิน
๖) เจ้าของ และ/หรือหน่วยงานเจ้าของทรัพย์สิน
๗) ตำแหน่งทางกายภาพของทรัพย์สิน
๘) การขึ้นต่อประกันของทรัพย์สิน

๒.๑.๒ ต้องมีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ภายในระบบสารสนเทศโดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface

๒.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๒.๑.๔ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการ ที่สำคัญของหน่วยงานซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๒.๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๕ ต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของหน่วยงานและปรับปรุงให้เป็นปัจจุบัน

๒.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management strategy)

การประเมินความเสี่ยงด้านความความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับหน่วยงาน พร้อมทั้งหาแนวทางในการรับมือภัยทคุกคามทางไซเบอร์ เพื่อลดความเสียหายที่จะเกิด โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๒.๑ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง

๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)

๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๒) คำอธิบายของความเสี่ยง (Description of the Risk)

๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๔) การจัดการความเสี่ยง (Risk Treatment)

๖) เจ้าของความเสี่ยง (Risk Owner)

๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๘) ความเสี่ยงที่เหลืออยู่ (Residual Risk)

๒.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

เป็นการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ครอบคลุมทั้งฮาร์ดแวร์

(Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานทราบ ถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศ โดยให้ หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๓.๑ ต้องดำเนินการประเมินช่องโหว่ของอุปกรณ์ของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคง ปลอดภัย และการควบคุมโดยครอบคลุมระบบเทคโนโลยีสารสนเทศ หรือบริการที่สำคัญ

๒.๓.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๒.๓.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลง ระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มระบบสารสนเทศ ระบบงานบริการ ระบบแอปพลิเคชัน การปรับปรุงแก้ไขระบบอย่างมีนัยสำคัญ และการปรับเปลี่ยนด้านเทคโนโลยี

๒.๓.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญ ของหน่วยงานโดยเฉพาะอย่างยิ่ง คือ ระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) ที่เชื่อมต่อ กับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยง จากการทดสอบเจาะระบบด้วย

๒.๓.๕ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๒.๓.๖ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจาเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงาน ก่อนที่ จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยน เทคโนโลยี เป็นต้น

๒.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึง ข้อมูลจากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๔.๑ ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษา ความมั่นคงปลอดภัยไซเบอร์ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตาม ในส่วนของบริการที่สำคัญ ของหน่วยงาน

๒.๔.๒ ต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญา กับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียด อย่างน้อย ดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงาน ตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานจาก ภัยคุกคามทางไซเบอร์

๓) ความเสี่ยงที่เกี่ยวข้องกับบริการ หรือห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๒.๔.๓ ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้อง กับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญาหรือไม่ ตัวอย่างเช่น การตรวจสอบโดยบุคคล ที่สาม และการตรวจสอบผลิตภัณฑ์

๒.๔.๔ ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนด ทางกฎหมายหรือข้อบังคับใหม่

หัวข้อที่ ๓ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๓.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

การอนุญาต การกำหนดสิทธิ หรือการมอบอ านาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้น สำหรับบุคคลภายนอกในการ เข้าถึงบริการที่สำคัญของหน่วยงาน โดยให้หน่วยงานด าเนินการอย่างน้อย ดังนี้

๓.๑.๑ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย อย่างน้อยดังนี้

๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๓.๑.๒ ต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับ การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๓.๑.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับขั้นความลับของข้อมูลรวมทั้งระดับขั้นการเข้าถึงเวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๓.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB หรือ พอร์ตต่างๆ) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางผู้ดูแลระบบสารสนเทศเท่านั้น

๓.๑.๕ ต้องเก็บบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๓.๑.๖ ในการเข้าถึงระบบสารสนเทศของหน่วยงานต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

๓.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๓.๒.๑ ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการ ที่สำคัญของหน่วยงาน

๓.๒.๒ ต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

๔) การลบบริการและแอปพลิเคชันที่ไม่จ าเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตซ์ (Patch) ความมั่นคงปลอดภัยของระบบสารสนเทศ อย่างทันการณ์ และเหมาะสม

๓.๒.๓ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๓.๒.๔ ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration standard) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๓.๒.๕ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาต และตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๓.๓ การเชื่อมต่อระยะไกล (Remote Control)

โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๓.๓.๑ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังงานบริการสำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

๑) เปิดใช้งานการเชื่อมต่อระยะไกล เมื่อจ าเป็นและได้รับการอนุญาตเท่านั้น

๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)

๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)

๔) ในกรณีที่เป็นไปได้ ควรใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication) การก าหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น HTTPS SSH หรือ SCP เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงานเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๓.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๓.๔.๑ ต้องตรวจสอบให้แน่ใจว่า มีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของหน่วยงานโดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

๓.๔.๒ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึกข้อมูลแบบถอดได้

๓.๔.๓ ต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายลือบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๓.๕.๑ ต้องเผยแพร่ ประชาสัมพันธ์เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักรู้ดานไซเบอร์ถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งานในลักษณะของการปฏิบัติตน ข้อหลีกเลี่ยงหรือข้อควรระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้โดยง่าย

๓.๕.๒ ต้องจัดทำหรือปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๓.๕.๓ ต้องจัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ ครั้งหรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศอย่างมีนัยสำคัญ

๓.๕.๔ ต้องสร้างความตระหนัก (Awareness) เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือการใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรในทุกระดับ

๓.๕.๕ ควรจัดให้มีการฝึกอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้แก่เจ้าหน้าที่ที่ปฏิบัติงานดูแลระบบสารสนเทศ

๓.๖ การแบ่งปันข้อมูล (Information Sharing)

โดยให้หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์

หัวข้อที่ ๔. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงาน ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยี สารสนเทศที่ยอมรับได้ที่กำหนดไว้ โดยหน่วยงานต้องมีกระบวนการในการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๔.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

๔.๒ มีกระบวนการในการจัดประเภท และวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่ตรวจพบ

๔.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย ไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

๔.๔ ต้องดำเนินการตรวจสอบกลไก และกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๕ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๕.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องมีการจัดทำการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทาง ไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๕.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

ให้หน่วยงานดำเนินการดังนี้

๕.๒.๑ จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยไซเบอร์

๕.๒.๒ ต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อดำเนินงานในช่วงที่เกิดเหตุการณ์วิกฤตทางไซเบอร์

๒) ระบุสถานการณ์/เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และ แผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์เหตุการณ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญที่จะเป็นตัวแทนขององค์กร เมื่อต้องมีการแถลงการณ์ หรือให้ข้อมูลที่เกี่ยวข้องกับเหตุการณ์

๔) ระบุแพลตฟอร์มหรือช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม สื่อโซเชียลมีเดียสำหรับการเผยแพร่ข้อมูล

๕.๒.๓ ต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๕.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่า สามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผล ในช่วงที่เกิดเหตุวิกฤตอันเนื่องมาจากภัย ทางไซเบอร์

หัวข้อที่ ๖ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานทที่ได้รับผลกระทบ (Containment,

Eradication, and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

๖.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิด การหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ให้สามารถใช้ปฏิบัติงานได้จริง เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตคานิยามและ การกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อยดังนี้

๖.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยต้องพิจารณาจากวิจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงัก ลำดับความสำคัญในการกู้คืนระบบ

๖.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤตสำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สิน สารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงาน ได้อย่างต่อเนื่อง มีการควบคุมดูแลการแก้ไขและกู้คืนระบบเมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย ทางไซเบอร์

๖.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม (Business Continuity Plan : BCP) อย่างน้อย ปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ (Business Continuity Plan : BCP) ต่อภัยคุกคามทางไซเบอร์ และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๖.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงาน ภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการถึงหัวหน้าหน่วยงาน ผ่านผู้บริหารด้านไอซีทีทราบทุกระยะ