



ประกาศสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)
เรื่อง ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)

โดยที่เป็นการสมควรกำหนดประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีความปลอดภัย และดำเนินงานได้อย่างต่อเนื่อง

อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมาตรา ๒๗ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) พ.ศ. ๒๕๕๘ ซึ่งแก้ไขเพิ่มเติมโดยพระราชกฤษฎีกาจัดตั้งสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) เรื่อง ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) ได้กำหนดขึ้นโดยมีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อให้มีประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)

๓.๒ เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓.๓ เพื่อให้บุคลากรของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) และบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๔ ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) ให้เป็นไปตามแนบท้ายประกาศ โดยมีแนวทางปฏิบัติและแผนรับมือ ดังต่อไปนี้

๔.๑ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

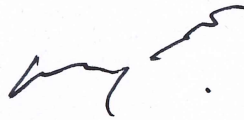
๔.๒ แนวทางปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์

๔.๓ แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๔.๔ แผนรับมือเหตุภัยคุกคามทางไซเบอร์

ข้อ ๕ ให้สำนักบริหารกลางดำเนินการทบทวนและปรับปรุงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๑๓ ตุลาคม พ.ศ. ๒๕๖๗



(นายณัฏฐชัย ปัญญาสุรฤทธิ์)

ผู้อำนวยการสถาบันส่งเสริมความปลอดภัย
อาชีวอนามัย และสภาพแวดล้อมในการทำงาน



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
(องค์การมหาชน)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์
สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)

๑. วัตถุประสงค์และขอบเขต

ตามพระราชบัญญัติการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร และตามพระราชบัญญัติการรักษาความมั่นคงทางไซเบอร์ พ.ศ. ๒๕๖๒ ในมาตรา ๔๔ “ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว” นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) หรือต่อไปนี้จะเรียกว่า “สถาบัน” เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ สถาบันจึงเห็นสมควรกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชบัญญัติการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ฯ และตามพระราชบัญญัติฯ โดยมีวัตถุประสงค์ดังต่อไปนี้

- ๑.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของสถาบันให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
- ๑.๒. แนวปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสถาบันได้รับทราบและเจ้าหน้าที่ทุกคน จะต้องถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด
- ๑.๓. แนวปฏิบัตินี้ควรมีการดำเนินการตรวจสอบและประเมินแนวปฏิบัติทุก ๓-๕ ปี

๒. องค์ประกอบของแนวปฏิบัติ

ส่วนที่ ๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน	๕
ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน	๑๑
ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๑๓
ส่วนที่ ๔ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย	๑๕
ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ	๑๗
ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	๑๘
ส่วนที่ ๗ การจัดทำระบบสำรองข้อมูล	๒๐
ส่วนที่ ๘ การตรวจสอบและประเมินความเสี่ยง	๒๓
ส่วนที่ ๙ นโยบายความมั่นคงปลอดภัยของการใช้งานอินเทอร์เน็ต	๒๔
ส่วนที่ ๑๐ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์	๒๖
ส่วนที่ ๑๑ ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์	๒๘

คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้

๑. **สถาบัน** หมายถึง สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)
๒. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)
๓. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role)
๔. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๕. **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่ายซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
๖. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
๗. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนแนวปฏิบัติด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๘. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
๙. **รหัสผ่าน** (Password) หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๐. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
๑๑. **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) ได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) โดย
- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
 - ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
๑๒. **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศ เป็นต้น
๑๓. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๑๔. **จดหมายอิเล็กทรอนิกส์** (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้
๑๕. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

- ๒.๑. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น
- ๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- ๒.๓. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้
- ๒.๔. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ
- ๒.๕. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- ๓.๑. ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

- ๓.๒. เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น
- ๓.๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้

- ๔.๑. การลงทะเบียนเจ้าหน้าที่ใหม่ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน
- ๔.๒. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ๔.๓. ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด
- ๔.๔. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่
- ๔.๔.๑. ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
- ๔.๔.๒. การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตาม “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
- ๔.๔.๓. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
- ๔.๔.๓.๑. ควรได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ
- ๔.๔.๓.๒. ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น
- ๔.๔.๓.๓. ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๔.๔.๓.๔. ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการทำงาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๔.๕. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๕.๑. ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึง ผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๕.๒. เจ้าของข้อมูลจะต้องมีการสอบถามความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๕.๓. วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๔.๕.๔. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๔.๕.๕. ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๕.๖. ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่สถาบัน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๕.๑. ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๒. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓. ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔. ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

- ๕.๕. ป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- ๕.๖. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบัน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย
- ๕.๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบัน ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- ๕.๘. การเข้าสู่ระบบงานเครือข่ายภายในสถาบันโดยผ่านทางอินเทอร์เน็ต จำเป็นต้องมีการล็อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
- ๕.๙. IP Address ภายในของระบบงานเครือข่ายภายในสถาบัน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย
- ๕.๑๐. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ๕.๑๑. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- ๕.๑๒. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่เทคโนโลยีสารสนเทศเท่านั้น

๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

- ๖.๑. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน
- ๖.๒. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที
- ๖.๓. ต้องเปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet FTP หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

- ๖.๔. ควรดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น
- ๖.๕. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- ๖.๖. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่เทคโนโลยีสารสนเทศเท่านั้น

๗. การบริหารจัดการการบันทึกและตรวจสอบ

- ๗.๑. ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน
- ๗.๒. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ๗.๓. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. การควบคุมการเข้าใช้งานระบบจากภายนอก

ต้องกำหนดให้มีการควบคุมการเข้าใช้งานระบบที่ ผู้ดูแลระบบได้ติดตั้งไว้ในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

- ๘.๑. การเข้าสู่ระบบระยะไกล (Remote access) เข้าสู่ระบบเครือข่ายของสถาบัน ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของสถาบัน จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
- ๘.๒. วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากเจ้าหน้าที่เทคโนโลยีสารสนเทศ และผู้จัดการสำนักอำนวยการ ก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตาม ข้อกำหนดของสถาบันในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
- ๘.๓. การทำให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
- ๘.๔. ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๘.๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ออกนอก

๙.๑. ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรดังนี้

๙.๑.๑. แสดงชื่อผู้ใช้งาน (Username)

๙.๑.๒. ใส่รหัสผ่าน (Password)

ส่วนที่ ๒

การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(User Access Management)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน

๒. การลงทะเบียนผู้ใช้งาน (User Registration)

- ๒.๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของสถาบัน
- ๒.๒. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
- ๒.๓. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- ๒.๔. ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว
- ๒.๕. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน
- ๒.๖. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

- ๓.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ๓.๒. ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ
- ๓.๓. ผู้ดูแลระบบต้องมอบหมายสิทธิควรมีความสอดคล้องกับนโยบายควบคุมการเข้าถึง
- ๓.๔. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

- ๓.๕. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

- ๔.๑. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน
- ๔.๒. ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- ๔.๓. ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น
- ๔.๔. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน
- ๔.๕. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมลเป็นช่องทางในการส่ง และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

- ๕.๑. ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย
- ๕.๒. ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป
- ๕.๓. ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน
- ๕.๔. ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๓

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้ระบบเทคโนโลยีสารสนเทศของสถาบัน เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

- ๒.๑. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- ๒.๒. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง
- ๒.๓. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- ๒.๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- ๒.๕. ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้
- ๒.๖. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ
- ๒.๗. ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม
- ๒.๘. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓ , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑ , aaa เป็นต้น
- ๒.๙. ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด
- ๒.๑๐. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
- ๒.๑๑. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ ๓ เดือน สำหรับผู้ดูแลระบบ และ ๖ เดือน สำหรับผู้ใช้งานระบบ
- ๒.๑๒. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน
- ๒.๑๓. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง
- ๒.๑๔. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๑๕. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

- ๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์โน้ตบุ๊ก
- ๓.๒ ผู้ใช้งานควรล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว
- ๓.๓ ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ส่วนที่ ๔

การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของสถาบัน โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

๒. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๒.๑. การใช้งานบริการเครือข่าย

- ๒.๑.๑. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของสถาบัน
- ๒.๑.๒. สถาบัน ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร
- ๒.๑.๓. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มีใช้ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว สถาบัน ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
- ๒.๑.๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกรานเขตหวงห้าม ของทางราชการ
- ๒.๑.๕. สถาบัน ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินี้ให้กับผู้อื่นไม่ได้

- ๒.๒.๖. บัญชีผู้ใช้งาน (User Account) ที่สถาบัน ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- ๒.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่สถาบันมีแนวทางปฏิบัติดังนี้
- ๒.๒.๑. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น
- ๒.๒.๒. สิทธิในการเข้าออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากเจ้าหน้าที่เทคโนโลยีและสารสนเทศ เป็นลายลักษณ์อักษรโดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย
- ๒.๒.๓. กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย
- ๒.๒.๔. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง
- ๒.๓. ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้
- ๒.๓.๑. ผู้ติดต่อจากหน่วยงานภายนอกต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย
- ๒.๓.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งผู้ติดต่อจากหน่วยงานภายนอกหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

ส่วนที่ ๕

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการใช้งานที่มั่นคงปลอดภัย

- ๒.๑. ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- ๒.๒. ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล๊อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
- ๒.๓. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง
- ๒.๔. ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- ๒.๕. ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

- ๓.๑. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข
- ๓.๒. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- ๓.๓. ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- ๓.๔. ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ส่วนที่ ๒

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application Information Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ได้อย่างถูกต้อง

๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

- ๒.๑. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสถาบัน ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น
- ๒.๒. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ๒.๓. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้
 - ๒.๓.๑. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
 - ๒.๓.๒. ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
 - ๒.๓.๓. กำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)
 - ๒.๓.๔. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๕. กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๔. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๔.๑. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๔.๒. ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๔.๓. กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๔.๔. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๔.๕. กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๔.๖. กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ส่วนที่ ๗

การจัดทำระบบสำรองข้อมูล

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้อง และสามารถกู้คืนระบบได้ในกรณีจำเป็น

๒. แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

- ๒.๑. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของสถาบัน
- ๒.๒. การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น
- ๒.๓. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย
- ๒.๔. ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้
- ๒.๕. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้จัดการสำนักอำนวยการ
- ๒.๖. ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูล ตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- ๒.๗. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
- ๒.๘. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๓. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

- ๓.๑. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
Web Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้ง ต่อสัปดาห์
Database Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลในฐานข้อมูลที่สำคัญ	๑ ครั้ง ต่อสัปดาห์
Firewall, Proxy, IPS, DNS	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูล Rule ในอุปกรณ์	๑ ครั้ง ต่อเดือน
Server ระบบงานอื่น ๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลบน Server อื่น ๆ	๑ ครั้ง ต่อเดือน
หมายเหตุ: ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup		

- ๓.๒. ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ ตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๔. การกู้คืนระบบ

- ๔.๑. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบ เครือข่ายจนเป็นเหตุให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึก และให้รายงานสรุปผลการปฏิบัติงานต่อผู้จัดการสำนักอำนาจการ หรือผู้ที่ได้รับมอบหมายจากผู้จัดการสำนักอำนาจการทราบ
- ๔.๒. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ
- ๔.๓. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๕. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

- ๕.๑. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
- ๕.๒. กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ
- ๕.๓. ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๕.๔. จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕.๕. ทดสอบ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง อย่างน้อย ปีละ ๑ ครั้ง

ส่วนที่ ๘

การตรวจสอบและประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. แนวปฏิบัติการประเมินความเสี่ยง

- ๒.๑. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของสถาบัน เพื่อการประเมินความเสี่ยงนั้น
 - ๒.๑.๑. ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ไวรัสมัลแวร์ (Computer Virus), ระบบไฟฟ้าขัดข้อง, ความเสียหายจากเพลิงไหม้, โจรกรรม และการขโมยอุปกรณ์คอมพิวเตอร์
 - ๒.๑.๒. ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)
- ๒.๒. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
- ๒.๓. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
 - ๒.๓.๑. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
 - ๒.๓.๒. ภัยคุกคามหรือสิ่งนี้อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
 - ๒.๓.๓. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
- ๒.๔. กำหนดมาตรการจัดการความเสี่ยง
 - ๒.๔.๑. ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)
 - ๒.๔.๒. จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของสถาบัน

ส่วนที่ ๙

นโยบายความมั่นคงปลอดภัยของการใช้งานอินเทอร์เน็ต (Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้เกิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสถาบันถูกระงับ ชะลอ ชัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

- ๒.๑. ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากเจ้าหน้าที่เทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษร
- ๒.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอัปเดตช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์
- ๒.๓. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- ๒.๔. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสถาบันเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- ๒.๕. ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสถาบัน
- ๒.๖. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือ ข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสถาบัน
- ๒.๗. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบันที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

- ๒.๘. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- ๒.๙. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๐

แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์

(Use of Electronic Mail)

๑. วัตถุประสงค์

- ๑.๑. เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของสถาบัน สามารถสนับสนุนการปฏิบัติงานของสถาบัน และการบริหารงานของสถาบัน เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล
- ๑.๒. เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของกรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ ของกรมเจ้าท่า

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- ๒.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- ๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใ้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน
- ๒.๓. สำหรับผู้ใ้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- ๒.๔. รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น 'x' หรือ 'o' ในการพิมพ์แต่ละตัวอักษร
- ๒.๕. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง
- ๒.๖. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอาท์ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใ้และรหัสผ่านอีกครั้ง
- ๒.๗. ผู้ใ้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์
- ๒.๘. ผู้ใ้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

- ๒.๙. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อสถาบัน หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน
- ๒.๑๐. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- ๒.๑๑. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของสถาบันเพื่อการทำงานของสถาบันเท่านั้น
- ๒.๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการล็อกเอาต์ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- ๒.๑๓. ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
- ๒.๑๔. ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- ๒.๑๕. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสถาบัน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์
- ๒.๑๖. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- ๒.๑๗. ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- ๒.๑๘. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๑

ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(Term of Use and Disclaimer)

๑. วัตถุประสงค์

- ๑.๑. เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของสถาบัน สามารถสนับสนุนการปฏิบัติงานของสถาบัน เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ
- ๑.๒. เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของสถาบันและหน่วยงานอื่น เป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของสถาบัน

๒. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

- ๒.๑. ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้
 - ๒.๑.๑. พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐
 - ๒.๑.๒. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔
 - ๒.๑.๓. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐
 - ๒.๑.๔. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔
 - ๒.๑.๕. ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗
 - ๒.๑.๖. ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕

๓. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

- ๓.๑. หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของสถาบัน จะต้องใช้จดหมายอิเล็กทรอนิกส์ของสถาบัน เพื่อผลประโยชน์ของทางราชการ
- ๓.๒. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน เพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน
- ๓.๓. ห้ามใช้บริการนี้ ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

- ๓.๔. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของทางราชการ
- ๓.๕. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น
- ๓.๖. ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร
- ๓.๗. ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)
- ๓.๘. ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น
- (๑) การสร้างจดหมายลูกโซ่ (Chain mail)
 - (๒) การส่งจดหมายจำนวนมาก (Spam mail)
 - (๓) การส่งจดหมายต่อเนื่อง (Letter bomb)
 - (๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์
- ๓.๙. ห้ามผู้ให้บริการกระทำการใด ๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของสถาบัน
- ๓.๑๐. ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์ ไว้เป็นความลับ
- ๓.๑๑. ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของสถาบัน
- ๓.๑๒. การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานภายนอก จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่สถาบันกำหนด
- ๓.๑๓. ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน (Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่าน ทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)
- ๓.๑๔. ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์สถาบัน หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์ จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของสถาบันได้อย่างถูกต้อง

๓.๑๕. กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการ ยกเลิก หรือระงับบริการแก่บุคลากรนั้น ๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบ หาสาเหตุของมูลเหตุนั้น ๆ



แนวทางปฏิบัติการตรวจสอบ
ด้านความมั่นคงปลอดภัยไซเบอร์

สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
(องค์การมหาชน)

สารบัญ

เรื่อง

หน้า

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (INTRODUCTION)	๑
๒. วัตถุประสงค์ (PURPOSE).....	๑
๓. กลุ่มเป้าหมาย (AUDIENCE).....	๑
๔. ขอบเขต (SCOPE).....	๑
๕. การอนุมัติผู้ตรวจสอบ (AUDITOR APPROVAL)	๑
๖. ความคาดหวังในการตรวจสอบ (AUDIT EXPECTATIONS)	๒
๗. ขั้นตอนการปฏิบัติในการตรวจสอบ	๖
เอกสารอ้างอิง	๘

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (INTRODUCTION)

การตรวจสอบความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างน้อยปีละหนึ่ง หรือความถี่ที่สูงกว่านั้น ตามที่สถาบันกำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดยสถาบัน

๒. วัตถุประสงค์ (PURPOSE)

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อกำหนดความคาดหวังในการตรวจสอบ และใช้เป็นแนวทางสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

เอกสารนี้ไม่ได้หมายถึงแหล่งข้อมูลที่จะเอื้ออำนวยสำหรับการดำเนินการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในเอกสารนี้ ผู้ตรวจสอบควรใช้ดุลยพินิจกับผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบ

๓. กลุ่มเป้าหมาย (AUDIENCE)

กลุ่มเป้าหมายของเอกสารนี้:

- ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ และ
- ผู้มีส่วนได้ส่วนเสีย (เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบและผู้ขาย หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล ฯลฯ) ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

๔. ขอบเขต (SCOPE)

เอกสารนี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕. การอนุมัติผู้ตรวจสอบ (AUDITOR APPROVAL)

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหน่วยงานและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด ใบสมัครจะถือว่าสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาโดยหน่วยงาน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

เกณฑ์การพิจารณา มี ๒ ประการ ได้แก่ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (audit firm/team) และผู้ตรวจสอบ (auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง:

- ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์ และ
- ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้ และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ หน่วยงานอาจพิจารณาแตกต่างกันไปตามที่หน่วยงานเห็นสมควร ในประเด็นต่อไปนี้

(๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน

(๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น

ในกรณีผู้ตรวจสอบของหน่วยงานที่ลงทะเบียนแล้วลาออกจากการเป็นพนักงานก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงพนักงานที่ลงทะเบียนไว้ให้หน่วยงานแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่ การเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๖. ความคาดหวังในการตรวจสอบ (AUDIT EXPECTATIONS)

ส่วนนี้กำหนดความคาดหวังในการตรวจสอบ มีวัตถุประสงค์เพื่อช่วยให้ผู้อ่านเข้าใจว่าควรดำเนินการ และรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

สกมช. ได้ระบุความคาดหวังในการตรวจสอบไว้ ๗ ด้านในหัวข้อ ๖.๑ ถึง ๖.๗



๖.๑ หลักการตรวจสอบ (Principles of Auditing)

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้ เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity): รากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลกระทบต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง

- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
 - ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน
- ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ
- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
 - ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ
- ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล
- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
 - ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ขอด้วยกฎหมายของผู้ตรวจสอบ
 - จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม
- จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ
- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
 - ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
 - รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ
 - ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๖.๒ วัตถุประสงค์ในการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบ คือ:

- ก. ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง
- ข. ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๖.๓ ขอบเขตการตรวจสอบ (Audit Scope)

การตรวจสอบจะครอบคลุมสิ่งต่อไปนี้:

ขอบเขต (Scope)	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลา การตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็น ลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔ แนวทางการตรวจสอบ (Audit Approach)

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

ก. การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ข. ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๖.๕ ข้อค้นพบการตรวจสอบ (Audit Finding)

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้:

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม และ

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(ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๖.๖ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

- ก. ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ
- ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๖.๗ รูปแบบรายงานการตรวจสอบ (Audit Report Format)

รายงานการตรวจสอบควรมีอย่างน้อยดังต่อไปนี้:

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารนี้

เนื้อหา	คำอธิบาย
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบการวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิภาพของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๖.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๖.๖ ของเอกสารนี้

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 เพื่อรักษารักษาความลับในการตรวจสอบ
๘. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน
๙. คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ 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>
๓. แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Link: <https://dg.th/dcnxmabuiio>



แนวทางปฏิบัติ
การประเมินความเสี่ยง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
(องค์การมหาชน)

สารบัญ

เรื่อง	หน้า
๑. บทนำ (INTRODUCTION)	๓
๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์.....	๓
๒. วัตถุประสงค์ (PURPOSE).....	๓
๓. กลุ่มเป้าหมายและขอบเขต (Audience)	๓
๔. ขอบเขต (SCOPE)	๓
๕. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT).....	๓
๕.๑ นิยามความเสี่ยงทางไซเบอร์.....	๓
๕.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance).....	๕
๕.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)	๖
๖. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT).....	๗
๖.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification).....	๗
๖.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)	๘
๖.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)	๑๓
๗. ตอบสนองต่อความเสี่ยง	๑๔
๗.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options).....	๑๕
๗.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)	๑๕
เอกสารอ้างอิง	๑๗

๑. บทนำ (INTRODUCTION)

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป และความเป็นดิจิทัลที่เพิ่มขึ้น สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อสถาบัน ดังนั้นจึงมีความจำเป็นในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงของสถาบัน โดยการประเมินความเสี่ยงจะสามารถ:

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้สถาบันสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในสถาบัน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๒. วัตถุประสงค์ (PURPOSE)

เพื่อให้สถาบันมีกรอบการดำเนินงานเกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

๓. กลุ่มเป้าหมายและขอบเขต (Audience)

กลุ่มเป้าหมายมีดังต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) (เช่น หัวหน้างาน ผู้ดูแลระบบ ฯลฯ) ภายในสถาบัน
- ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของสถาบัน

๔. ขอบเขต (SCOPE)

ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๕. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

เป็นการสร้างข้อกำหนดที่สำคัญสำหรับการประเมินความเสี่ยง เพื่อให้กลุ่มเป้าหมาย ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๕.๑ นิยามความเสี่ยงทางไซเบอร์

คือแนวโน้มที่จะได้รับผลกระทบจากการหยุดชะงักต่อข้อมูลที่ละเอียดอ่อน การเงิน หรือการดำเนินธุรกิจออนไลน์ รวมถึงการให้บริการบางอย่างที่มีความเกี่ยวข้องต่อการดำเนินงานและการให้บริการประชาชน

โดยทั่วไปความเสี่ยงทางไซเบอร์มีความเกี่ยวข้องกับเหตุการณ์ที่อาจส่งผลให้เกิดการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูลเพื่อให้ไม่สามารถให้บริการได้

การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้ การใช้มาตรการรักษาความปลอดภัยทางไซเบอร์ มีวิธีการคำนวณตาม OWASP Risk Assessment

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน; และ
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

$$\text{Risk} = \text{Function (Likelihood, Impact)}$$

การบ่งชี้ความเสี่ยง

เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อเป้าหมายของสถาบันหรือการปฏิบัติงาน เช่น ทรัพย์สิน ภัยคุกคาม ช่องโหว่ด้านความปลอดภัย

สินทรัพย์สารสนเทศ

หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ได้แก่ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น มีวัตถุประสงค์เพื่อสนับสนุนงานเผยแพร่ ประชาสัมพันธ์ งานอบรม ประชุม สัมมนาของสถาบัน

เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์การโจมตี (Threat Vector)) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

- **Ransomware (แรนซัมแวร์)** ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูลไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความนิยมเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware
- **Phishing (ฟิชชิง)** คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่ กรุณาลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียง

แค่รอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังดีนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล

- **Malware (มัลแวร์)** หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น
- **Virus (ไวรัส)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างดีโดยมุ่งเน้นในการโจมตี ขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้
- **Worms (เวิร์ม)** เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้
- **Trojan (โทรจัน)** เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลกระทบต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้
- **Spyware (สปายแวร์)** ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล
- **Adware (แอดแวร์)** คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้
- **Data leaks (ข้อมูลรั่วไหล)** ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสียหายที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ

๕.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าสถาบันยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนจำเป็น ต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับการพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

๕.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

ผู้บริหาร (Head of Organization)

เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในสถาบันที่มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของสถาบัน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

ฟังก์ชันการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในสถาบันที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งสถาบัน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชันเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในสถาบันที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมทางธุรกิจ พวกเขาควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชันความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

บุคคลหรือกลุ่มภายในสถาบันที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุม ความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมทางธุรกิจ โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

๖. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)



รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๖.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

งาน A: ระบุทรัพย์สิน (Identify Assets)

ดังสุภาษิตความมั่นคงปลอดภัยโบราณที่ว่า “คุณไม่สามารถปกป้องสิ่งที่คุณไม่รู้ได้” ดังนั้น สิ่งแรก ที่ควรดำเนินการคือการระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็น ระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง เมื่อระบุทรัพย์สิน สิ่งสำคัญคือต้องจัดบันทึกทรัพย์สิน เหล่านั้น

- ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์ทาง ธุรกิจโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์

ตัวอย่าง: ในระบบควบคุมแบบกระจาย (Distributed Control System (DCS)) ของโรงไฟฟ้า โปรแกรมควบคุมลอจิกแบบตั้งโปรแกรมได้ (Programmable Logic Controller (PLC)) ที่ควบคุมระบบไฟฟ้ามักจะได้รับการพิจารณาว่าเป็นทรัพย์สินสำคัญ เนื่องจากมีผลโดยตรงต่อการผลิตไฟฟ้า ซึ่งเป็นวัตถุประสงค์ทางธุรกิจโดยรวมของโรงไฟฟ้า

ผู้โจมตีที่ต้องการขัดขวางการผลิตไฟฟ้ามีแนวโน้มที่จะโจมตีและควบคุมตรรกะภายใน PLC

- ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

ตัวอย่าง: ในสภาพแวดล้อม Windows ทั่วไป เซิร์ฟเวอร์ Active Directory (AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ไปยังเซิร์ฟเวอร์หลายเครื่องมักจะได้รับการพิจารณาว่าเป็นทรัพย์สินที่เกี่ยวข้อง เนื่องจากเป็นสะพานเชื่อมให้ผู้โจมตีเปลี่ยนเข้าสู่เซิร์ฟเวอร์เหล่านี้

ใช้รายการทรัพย์สินที่รวมเข้าด้วยกันเพื่อสร้างแผนผังสถาปัตยกรรมเครือข่ายที่ให้การแสดงภาพของเส้นทางการเชื่อมต่อระหว่างกันและการสื่อสารระหว่างทรัพย์สิน ระบุจุดเข้าทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายในระบบ รวมถึงทรัพย์สินที่เกี่ยวข้องและทรัพย์สินสำคัญ สิ่งนี้จะช่วยอำนวยความสะดวกในงานต่อไปในการระบุภัยคุกคาม

งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

ด้วยรายการทะเบียนทรัพย์สินและไดอะแกรมสถาปัตยกรรมเครือข่าย ควรระบุเหตุการณ์ภัยคุกคามที่อาจใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการเพื่อการวิเคราะห์เชิงลึก เทคนิคประการหนึ่งที่สถาบันควรใช้คือการสร้างแบบจำลองภัยคุกคาม โดยการสร้างแบบจำลองภัยคุกคามเป็นกระบวนการที่มีโครงสร้างสำหรับการระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับระบบ เพื่อให้สถาบันสามารถสร้างการป้องกันที่มุ่งเน้นมากขึ้นเพื่อปกป้องระบบ

การสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) – สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำในงาน A

๒. การระบุภัยคุกคาม (Threat Identification) – สถาบันควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว สถาบันควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้สถาบันสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อไป ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้:

- **ทรัพย์สิน (Asset)** - สิ่งที่มีค่าที่ได้รับการระบุในงาน A
- **เหตุการณ์ภัยคุกคาม (Threat event)** - เหตุการณ์การโจมตีที่ระบุในงาน B
- **ช่องโหว่ (Vulnerability)** - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง
- **ผลที่ตามมา (Consequence)** - ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

๖.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

- (๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น; และ

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

งาน A: กำหนดโอกาส (Determine Likelihood)

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าวเพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- **ความสามารถในการค้นพบ (Discoverability)** – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- **ความสามารถในการใช้ประโยชน์ (Exploitability)** – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- **ความสามารถในการทำซ้ำ (Reproducibility)** – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปเพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: - สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) - สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: - สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย - สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไปโดยไม่ต้องมีความรู้	การโจมตี: - สามารถทำซ้ำได้ตามต้องการโดยไม่มีข้อกำหนดค่า (Configuration) หรือเงื่อนไขของเหตุการณ์ (Event Condition) - สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์

Likelihood Rating	Discoverability	Exploitability	Reproducibility
		ด้านเทคนิค	(Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: - สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ต เครือข่าย การดักจับเครือข่าย (Network Sniffing)) - สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน	การโจมตี: - สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/Root) - สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: - สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง - สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: - สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย - สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิกัลโลคัล	การโจมตี: - สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root) - สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	การโจมตี: - สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุมบางอย่าง - สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

ตัวอย่างตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

งาน B: กำหนดผลกระทบ (Determine Impact)

โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้:

- **ระดับชาติ (National)** – ในระดับประเทศ ผลกระทบอาจถูกมองว่าเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ

- **องค์กร (Organisational)** – ในระดับองค์กร ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงักในการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

- **บุคคล (Individual)** – ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิตและการบาดเจ็บ

ตารางด้านล่าง คือ ตัวอย่างตารางประเมินสำหรับการพิจารณาผลกระทบของความเสียหายในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่างเป็นข้อมูลทั่วไป เมื่อใช้ตารางผลกระทบที่คล้ายกัน สถาบันควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการเพื่อให้แน่ใจว่า

- **เกี่ยวข้องกับบริบททางธุรกิจ (Relevant to business context)** – เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของสถาบันหรือวัดผลงาน

- **ไม่กำกวม (Unambiguous)** – ใช้คำอธิบายที่เป็นเลขฐานสองหรือที่มีช่วงเชิงปริมาณ (เช่น การรั่วไหลของข้อมูลที่ถูกจัดประเภทเป็น “ความลับ” หรือทำให้การบริการของลูกค้ามากกว่าร้อยละ ๕๐ หยุดชะงัก)

- **มุมมองที่หลากหลาย (Multi-perspectives)** – ระบุประเภทย่อยของผลกระทบจากแต่ละระดับจาก ๓ ระดับ (เช่น ระดับประเทศ องค์กร และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสียหาย

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ ^{น้อยหรือ} อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
	มีผลกระทบต่อข้อมูลที่ ^{ลับ} (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ ^{ลับ} มาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ ^{ลับ} ที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
ด้านการรักษาความถูกต้องครบถ้วน(Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ <u>น้อยหรืออย่างจำกัด</u> (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ <u>อย่างร้ายแรง</u> (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบ <u>อย่างร้ายแรงมาก</u> (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ <u>น้อยหรืออย่างจำกัด</u> (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ <u>อย่างร้ายแรง</u> (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูล ข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบ <u>อย่างร้ายแรงมาก</u> (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่มีผู้ให้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ให้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ให้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ให้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของ	ไม่มีผลกระทบ หรือมีผลกระทบต่อ	การดำเนินการตามหน้าที่หลักของสถาบันด้อย	การดำเนินการตามหน้าที่หลักของสถาบันต้องหยุดชะงัก ไม่

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
สถาบัน	การดำเนินการตามหน้าที่ของสถาบันเพียงเล็กน้อย	ประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน	ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของสถาบัน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

๖.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับ ความเสี่ยง และประกอบด้วยการกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

งาน A: กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยงสำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง (หัวข้อ ๔.๒)

IMPACT	High (๓)	M๓๑	H๓๒	H๓๓
	Medium (๒)	L๒๑	M๒๒	H๒๓
	Low (๑)	L๑๑	L๑๒	L๑๓
		Low (๑)	Medium (๒)	High (๓)
		LIKELIHOOD		

รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยสถาบัน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

งาน B: ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้านี้จะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของสถาบันมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- สถานการณ์ความเสี่ยง (Risk Scenario) – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร
- วันที่ระบุความเสี่ยง (Identification Date) – วันที่ที่ระบุสถานการณ์ความเสี่ยง
- มาตรการที่มีอยู่ (Existing Measures) – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง
- ความเสี่ยงในปัจจุบัน (Current Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)
- แผนจัดการความเสี่ยง (Treatment Plan) – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของสถาบัน)
- สถานะความคืบหน้า (Progress Status) – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

- **ความเสี่ยงที่คงเหลืออยู่ (Residual Risk)** – ระดับความเสี่ยงที่กำหนด (การรวมกันของความ เป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

- **เจ้าของความเสี่ยง (Risk Owner)** – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยง ที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของสถาบัน

๗. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุ และกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของสถาบัน

๗.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลด ความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของสถาบันเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้สถาบันมีความเสี่ยง ที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยง ที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไป ตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่ของการแบ่งปัน ความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้ โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยง ของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และ ความรับผิดชอบที่เหมาะสม) ภายในสถาบันจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๗.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุม ความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม สถาบัน ควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่า ตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย สถาบันอาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลง

หรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกัน
ปลายทางที่มีราคาแพง

เมื่อสถาบันเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบ
ให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ
ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยง
หรือการลดผลกระทบจากความเสี่ยง

เอกสารอ้างอิง

๑. GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, FEBRUARY ๒๐๒๑
Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf
๒. NIST SP ๘๐๐-๓๐ Rev. ๑ Guide for Conducting Risk Assessments, NIST, September ๒๐๑๒
Link: <https://csrc.nist.gov/publications/detail/sp/๘๐๐-๓๐/rev-๑/final>
๓. ISO ๓๑๐๐๐:๒๐๑๘(en) Risk management — Guidelines, ISO, FEBRUARY ๒๐๑๘
Link: <https://www.iso.org/obp/ui/#iso:std:iso:๓๑๐๐๐:ed-๒:v๑:en>
๔. ISO/IEC ๒๗๐๐๕:๒๐๑๘ Information technology — Security techniques — Information security risk management, ISO/IEC, July ๒๐๑๘
Link: <https://www.iso.org/standard/๗๕๒๘๑.html>
๕. ตัวอย่างแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Link: <https://dg.th/dcnxmabui๐>



แผนรับมือเหตุภัยคุกคามทางไซเบอร์

สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
(องค์การมหาชน)

สารบัญ

เรื่อง	หน้า
คำนำ.....	๑
หลักการและเหตุผล.....	๒
วัตถุประสงค์.....	๒
ขอบเขต.....	๒
หน้าที่การทบทวนแผน.....	๒
หน้าที่ในการดำเนินการตามแผน.....	๒
ความเกี่ยวข้องกับเอกสารอื่น.....	๒
นิยาม.....	๓
โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)	๓
ขั้นตอนการรับมือ.....	๔

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทาง ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์การประเมินความเสี่ยงด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อดำเนินการตาม พรบ. การรักษาความ มั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์โดยการมุ่งเน้นการตรวจสอบ ควบคุม ปกป้อง และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถใช้งานได้

สำนักบริหารกลาง งานเทคโนโลยีสารสนเทศจึงได้จัดทำ “แผนรับมือเหตุภัยคุกคามทางไซเบอร์สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)” เพื่อใช้เป็นแผนในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญด้านบริการ ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน) ได้อย่างมีประสิทธิภาพและทันต่อเหตุการณ์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน (องค์การมหาชน)

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของ สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแผนปฏิบัติการดิจิทัลของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน ด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใน สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับกลุ่มงานต่าง ๆ ภายใน สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของ สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

สำนักบริหารกลาง งานเทคโนโลยีสารสนเทศ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้อำนวยการสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน

๕. หน้าที่ในการดำเนินการตามแผน

สำนักบริหารกลาง งานเทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย สำนักบริหารกลาง งานเทคโนโลยีสารสนเทศ รวมถึง สำนักอื่น ๆ ของสถาบันฯ

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน

๖.๒ แนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

สถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	นายมานิชญ์ เหล็ก ดำรง (084-5254136)	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นางสาวดวงกมล ปทุม รังษี (0868553084)	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นายเฉลิมชัย บุญเลี้ยง (0863768203)	เจ้าหน้าที่รับมือฯ (Incident lead)	- ทำหน้าที่ช่วยเหลือ สถาบันส่งเสริม ความมั่นคง อาชีวอนามัย และ สภาพแวดล้อมในการทำงาน ให้ สามารถควบคุมผลกระทบจากภัย คุกคามทางไซเบอร์ได้ - ทำหน้าที่ตรวจสอบและควบคุมความ เสี่ยงที่เกี่ยวข้อง
๔	นายธนยุทธ สุนา (092-8855545)	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทาง ที่เหมาะสมในการควบคุมผลกระทบ จากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับที่	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๑	นายพรเทพ ศิริฤกษ์ อุดมพร (081-9069059)	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตาม ให้คำปรึกษาด้านกฎหมายที่เกี่ยวข้อง
๒	นางสาวณิชาณาด เมฆ พงศ์พันธ์ (086-3575647)	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตรวจสอบข้อกฎหมายที่เกี่ยวข้อง
๒	บริษัท แมกซ์ เซฟวิงส์ (ประเทศไทย) จำกัด (087-7190040)	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามทดสอบและประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
๕	นายพิษณุ จันทรัส (0814250586)	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ประชาสัมพันธ์ให้กับผู้มีส่วนได้ส่วนเสีย

๙. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึง นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันส่งเสริมความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน ดังนี้

๙.๑ ขั้นการเตรียมการ เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่ต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันทั่วทั้งที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
- NIST SP 800-61r2 Computer Security Incident Handling Guide

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง
ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน
ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้ (ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ (ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT (ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process) (ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ (ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน (ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ (ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๘ ข้อที่ ๙.๑ (๒) ข้อที่ ๙.๑ (๓) ข้อที่ ๙.๓ (๑) ข้อที่ ๙.๓ (๒) ข้อที่ ๙.๓ (๓) ข้อที่ ๙.๓ (๔) ข้อที่ ๙.๓ (๕) ข้อที่ ๙.๔ (๑)