



ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๙

โดยที่เป็นการสมควรปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ให้เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๓๖ (๒) แห่งพระราชบัญญัติหลักประกันสุขภาพแห่งชาติ พ.ศ. ๒๕๔๕ ประกอบมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๘

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ประกอบด้วย

- (๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- (๒) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน
- (๓) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ
- (๔) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

ข้อ ๕ ให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดในเอกสารแนบท้ายประกาศนี้

ผู้ฝ่าฝืนหรือไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติตามวรรคหนึ่ง อาจถูกปฏิเสธหรือถูกระงับการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ และต้องรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายทั้งปวงที่เกิดขึ้นจากการฝ่าฝืนหรือไม่ปฏิบัติตาม

ข้อ ๖ กรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ให้เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติเป็นผู้อำนวยการวินิจฉัยชี้ขาด โดยอาจมอบคณะกรรมการบริหารนโยบายดิจิทัลพิจารณาเสนอความเห็นก่อนก็ได้

ประกาศ ณ วันที่ ๒๒ พฤษภาคม พ.ศ. ๒๕๖๔

หมายเลขใบเก็บค่า: d6c1b0911f472f65da032c6ea37590
เวลาทำใบเก็บค่า: 2026-05-22 13:26
ลงนามโดย: เจตน์ ธรรมธัชอารี
หมายเลขเอกสาร: 98c1-5254-93ae



(นายเจตน์ ธรรมธัชอารี)

เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ

เอกสารแนบท้ายประกาศสำนักงานหลักประกันสุขภาพแห่งชาติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔

หลักการและเหตุผล

สำนักงานหลักประกันสุขภาพแห่งชาติเป็นหน่วยงานของรัฐที่มีภารกิจสำคัญในการบริหารจัดการระบบหลักประกันสุขภาพถ้วนหน้า ซึ่งถือเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยต้องมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ประกอบกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวทางนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร และกำหนดให้หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหนึ่งหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายที่อาจเกิดขึ้น ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานหลักประกันสุขภาพแห่งชาติ สอดคล้องกับประกาศและระเบียบภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) รวมถึงมีความมั่นคงปลอดภัยตามมาตรฐานสากล เช่น ISO/IEC 27001:2022 และ NIST CSF2.0 สามารถดำเนินงานได้อย่างต่อเนื่อง (Business Continuity) และป้องกันการถูกคุกคามจากภัยไซเบอร์ในรูปแบบต่าง ๆ สำนักงานหลักประกันสุขภาพแห่งชาติจึงเห็นสมควรปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ให้ครอบคลุมและเป็นปัจจุบัน

วัตถุประสงค์

สำนักงานหลักประกันสุขภาพแห่งชาติได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของสำนักงานหลักประกันสุขภาพแห่งชาติ ให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล

๒. เพื่อกำหนดขอบเขตในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามมาตรฐาน ISO/IEC 27001 หรือมาตรฐานอื่น ๆ ที่เกี่ยวข้องให้เป็นปัจจุบัน และมีการปรับปรุงอย่างต่อเนื่อง

๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมในกรณีฉุกเฉินให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่อง และพร้อมใช้งานอยู่เสมอ ได้ตามปกติ เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของสำนักงานหลักประกันสุขภาพแห่งชาติ

๔. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานหลักประกันสุขภาพแห่งชาติ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๕. เพื่อเผยแพร่ให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานหลักประกันสุขภาพแห่งชาติได้รับทราบและถือปฏิบัติตามนโยบายและแนวปฏิบัตินี้อย่างเคร่งครัด

องค์ประกอบ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นส่วนหนึ่งในการกำหนด ควบคุม ให้เป็นไปตามมาตรฐานทางด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานหลักประกันสุขภาพแห่งชาติ ทั้งนี้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกจะต้องคำนึงถึงการควบคุมในส่วนต่าง ๆ ดังต่อไปนี้

หมวดที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ ๒ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน

หมวดที่ ๓ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ

หมวดที่ ๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

คำนิยามศัพท์

เว้นแต่จะได้กำหนดไว้เป็นอย่างอื่น คำนิยามศัพท์ในแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ให้มีความหมาย ดังต่อไปนี้

“**นโยบาย**” หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“**แนวปฏิบัติ**” หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“**สำนักงาน**” หมายความว่า สำนักงานหลักประกันสุขภาพแห่งชาติ

“**สำนักงานสาขา**” หมายความว่า สำนักงานหลักประกันสุขภาพแห่งชาติเขต ๑ ถึง เขต ๑๓

“**ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)**” หมายความว่า เลขาธิการสำนักงานหลักประกันสุขภาพแห่งชาติ

“**ผู้บริหารข้อมูลระดับสูง (Chief Data Officer: CDO)**” หมายความว่า ผู้บริหารที่ได้รับมอบหมายให้ทำหน้าที่กำกับดูแลบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูลของสำนักงาน

“**คณะกรรมการ**” หมายความว่า คณะกรรมการบริหารนโยบายดิจิทัล ผู้มีอำนาจในการกำกับควบคุม ดูแล บังคับใช้นโยบายด้านเทคโนโลยีสารสนเทศของสำนักงาน

“**คณะทำงาน**” หมายความว่า คณะทำงานพัฒนาระบบบริหารจัดการด้านความปลอดภัยสารสนเทศ ที่ทำหน้าที่จัดทำ ทบทวน ตรวจสอบ ประเมินผล และปรับปรุงนโยบายและแนวปฏิบัติรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ หรือตามมาตรฐานสากลในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

“**ผู้บังคับบัญชา**” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน

“**ผู้ดูแลระบบ**” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“**ผู้พัฒนาระบบ**” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบพัฒนาโปรแกรมประยุกต์ที่ใช้งานภายในสำนักงาน

“ผู้ใช้งาน” หมายความว่า เลขธิการสำนักงานหลักประกันสุขภาพแห่งชาติ และผู้ปฏิบัติงานของสำนักงานหลักประกันสุขภาพแห่งชาติ และสำนักงานสาขา รวมถึง พนักงานสัญญาจ้าง พนักงานโครงการ บุคคลภายใต้การควบคุมดูแลของผู้ให้บริการภายนอกที่ปฏิบัติหน้าที่ตามสัญญาจ้าง เจ้าหน้าที่ของรัฐซึ่งมาปฏิบัติงานในสำนักงานตามมติคณะรัฐมนตรีและรวมถึงพนักงานจ้างเหมาบริการทั้งที่เป็นบุคคล นิติบุคคล

“หน่วยงานภายนอก” หมายความว่า หน่วยงานของรัฐตามมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ที่เข้ามาทำการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ หรือนำข้อมูลสารสนเทศของสำนักงาน ไปใช้ประโยชน์ต่อการบริการต่าง ๆ

“บุคคลภายนอก” หมายความว่า ผู้ที่เข้ามาทำการติดต่อ ประสานงาน ดำเนินงานที่เกี่ยวข้องกับสำนักงานที่อยู่นอกเหนือในส่วนผู้ใช้งาน

“ผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (IT Auditor)” หมายความว่า ผู้ที่ได้รับมอบหมาย จากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และอื่น ๆ ที่ร้องขอเพื่อใช้ในการตรวจสอบ

“ระบบสารสนเทศ (Information System)” หมายความว่า ระบบงานของสำนักงาน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

“โปรแกรมประเภทอรรถประโยชน์ (Utility Program/Software)” หมายความว่า โปรแกรมประยุกต์หรือแอปพลิเคชันที่ทำงานบนระบบปฏิบัติการ ที่มีคุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ ช่วยสนับสนุนเพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น

“ระบบซึ่งไวต่อการรบกวน (Sensitive or Critical system)” หมายความว่า ระบบเทคโนโลยีสารสนเทศที่มีความละเอียดอ่อนต่อการเก็บใช้ รักษาในส่วนของข้อมูลสารสนเทศที่เกี่ยวข้องต่อประชาชน และเป็นระบบที่มีความสำคัญสูงต่อสำนักงานที่ใช้ในการทำธุรกรรมต่าง ๆ

“สารสนเทศ (Information)” หมายความว่า ข้อเท็จจริงที่ได้จากการนำเข้าข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่าย และสามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ

“ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล ข่าวสาร ความรู้ ข้อเท็จจริง ที่นำมาบันทึกไว้ในทรัพยากรสารสนเทศของสำนักงาน ได้แก่ เอกสาร สื่อบันทึกข้อมูล ซึ่งผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอกที่ได้รับอนุญาตให้สามารถรับรู้สารสนเทศจากเอกสารและสื่อบันทึกข้อมูลนั้นได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม โดยในที่นี้เรียกว่า “อุบัติการณ์”

“เวลาอ้างอิงสากล (Stratum o)” หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับสำนักงานมาตรฐาน เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)” หมายความว่า ข้อมูลที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ โดยสำนักงานจะเป็นผู้พิจารณา

“การถ่ายโอนข้อมูล” หมายความว่า การรับ – ส่งข้อมูลสารสนเทศจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งที่ผ่านระบบเครือข่ายหรือผ่านสื่อบันทึกข้อมูล

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด เพื่อให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสำนักงานได้ เช่น ระบบเครือข่าย แบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN)

“ระบบอินทราเน็ต (Intranet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสำนักงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลสารสนเทศภายในสำนักงาน

“ระบบเครือข่ายแบบไร้สาย (Wireless LAN)” หมายความว่า เทคโนโลยีในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ตั้งแต่ ๒ เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ ซึ่งการสื่อสารจะไม่ใช่สายสัญญาณในการเชื่อมต่อ (LAN) แต่จะใช้คลื่นวิทยุในการรับส่งข้อมูลแทน

“ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของสำนักงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ทรัพย์สินหรือสินทรัพย์ (Asset)” หมายความว่า ระบบคอมพิวเตอร์ เครือข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ซอฟต์แวร์ที่มีลิขสิทธิ์ และสิ่งใดก็ตามที่มีคุณค่าสำหรับสำนักงาน

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” หมายความว่า พื้นที่ที่สำนักงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

๑. พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

๒. พื้นที่ควบคุม หมายความว่า พื้นที่ภายในศูนย์คอมพิวเตอร์หลัก (DC) ศูนย์คอมพิวเตอร์สำรอง (DR) และห้องคอมพิวเตอร์ (Server Room) ที่ใช้สำหรับติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย และข้อมูลคอมพิวเตอร์ของสำนักงาน

๓. พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สายที่อยู่ในพื้นที่ทำงาน และพื้นที่ควบคุมของสำนักงาน

“**เครื่องคอมพิวเตอร์**” หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพาที่สำนักงานจัดหาให้ หรือเครื่องคอมพิวเตอร์ส่วนบุคคล ที่นำเข้ามาเพื่อใช้งานในสำนักงาน และต้องได้รับอนุมัติจากส่วนงานที่รับผิดชอบ

“**สื่อบันทึกข้อมูล**” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Drive

“**จดหมายอิเล็กทรอนิกส์ (Electronic mail: e-mail)**” หมายความว่า ระบบที่ผู้ใช้งานผู้ดูแลระบบใช้ในการรับส่งข้อความระหว่างกันโดยผ่านระบบเครือข่าย ในการรับ-ส่งข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย กราฟิก ภาพเคลื่อนไหว และเสียง โดยที่ผู้ใช้งาน ผู้ดูแลระบบสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ ตามมาตรฐานที่ใช้ในการรับส่งข้อมูล ได้แก่ SMTP, POP๓ และ IMAP

“**สิทธิของผู้ใช้งาน**” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ โดยสำนักงานจะเป็นผู้พิจารณา

“**บัญชีผู้ใช้บริการ (Account)**” หมายความว่า รายชื่อผู้มีสิทธิใช้งานระบบคอมพิวเตอร์ระบบเครือข่าย ระบบจดหมายอิเล็กทรอนิกส์และระบบเทคโนโลยีสารสนเทศของสำนักงาน

“**ชื่อผู้ใช้ (Username)**” หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) ในระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของสำนักงาน ที่มีการกำหนดสิทธิการใช้งานไว้

“**รหัสผ่าน (Password)**” หมายความว่า ตัวอักษรหรืออักขระตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลบัญชีผู้ใช้บริการ เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของสำนักงาน

“**เลขที่อยู่ไอพี (IP Address)**” หมายความว่า ตัวเลขประจำเครื่องที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน (IPv๔) หรือ ๕ ส่วน (IPv๖) แต่ละกลุ่มตัวเลขคั่นด้วยเครื่องหมายจุด (.) หรือเครื่องหมายทวิภาค (: หรือ semi-colon)

“**ลงบันทึกเข้า (Login)**” หมายความว่า กระบวนการที่ผู้ใช้งาน ผู้ดูแลระบบ บุคคลภายนอกต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้ เพื่อการเข้าใช้งานระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของสำนักงาน ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

“**ลงบันทึกออก (Logout)**” หมายความว่า กระบวนการที่ผู้ใช้ทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของสำนักงาน

“**โปรแกรมประสงค์ร้าย**” หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่ง และ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาโดยมีวัตถุประสงค์ เพื่อก่อวินาศกรรมหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น มัลแวร์ (Malware)

“Non-Disclosure Agreement (NDA)” หมายความว่า สัญญาที่ทางสำนักงานทำระหว่างผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอกที่ได้รับอนุญาตที่สามารถรับรู้ข้อมูลสารสนเทศไม่ให้เปิดเผยเนื้อหาความรู้หรือข้อมูลใด ๆ ต่อบุคคลที่สาม

“Acceptable Use Policy (AUP)” หมายความว่า ข้อตกลงระหว่างผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอก ที่ยอมรับเงื่อนไขในส่วนของนโยบายและแนวปฏิบัติรักษาความปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง

“บริการข้อมูล (Data Steward)” หมายความว่า ผู้ปฏิบัติงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลคุณภาพ ความถูกต้อง และความมั่นคงปลอดภัยของข้อมูล

“เครื่องมือสื่อสารดิจิทัล” หมายความว่า อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย ซอฟต์แวร์ แอปพลิเคชัน หรือแพลตฟอร์มออนไลน์ เช่น ระบบ O365, SharePoint, Teams และการยืนยันตัวตนแบบ 2FA

หมวดที่ ๑

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น เพื่อให้การดำเนินการใด ๆ ด้านเทคโนโลยีสารสนเทศของสำนักงานมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล สำนักงานจึงเห็นควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามพระราชกฤษฎีกา และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ตลอดจนแนวทางการใช้บริการคลาวด์ พ.ศ. ๒๕๖๒ และมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ สำหรับสำนักงาน และเพื่อให้ประชาชน หน่วยบริการ หรือผู้ใช้งานภายในระบบสารสนเทศของสำนักงาน มีความมั่นใจได้ว่าสำนักงานจะไม่สนับสนุนหรือยินยอมให้มีการกระทำ ความผิดตามที่พระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องกำหนดโดยกำหนดให้มีสาระสำคัญ เพื่อการนำไปดำเนินงานด้านความมั่นคงปลอดภัยในสำนักงาน ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๑.๑.๑ สำนักงาน ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๑.๑.๒ สำนักงาน ต้องควบคุมให้มีการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่รับผิดชอบที่ได้รับมอบหมาย รวมถึงการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑.๑.๓ สำนักงาน ต้องทำการคัดเลือกผู้ปฏิบัติงานตามคุณสมบัติของตำแหน่งงานที่กำหนดไว้ในแต่ละตำแหน่ง รวมถึงต้องตรวจสอบเอกสาร ข้อมูล หรือบุคคลอ้างอิง ประวัติการทำงาน การศึกษา คุณสมบัติ ข้อมูลหลักฐานแสดงตนของผู้ปฏิบัติงาน

๑.๑.๔ สำนักงาน ต้องดำเนินการฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ใช้งาน

๑.๑.๕ สำนักงาน ต้องควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๑.๑.๖ สำนักงาน ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๑.๑.๗ สำนักงาน ต้องควบคุมผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลง ให้มีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถ

ปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

๑.๑.๘ สำนักงาน ต้องควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต

๑.๒ การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

สำนักงาน ต้องจัดทำระบบสำรอง และมาตรการควบคุม เพื่อลดความเสี่ยงต่อภัยคุกคามทางกายภาพที่เหมาะสม พร้อมทั้งอยู่ในสภาพพร้อมใช้งานโดยคัดเลือกกระบวนสารสนเทศที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๑.๓ การตรวจสอบและประเมินความเสี่ยง

สำนักงานต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยผู้ตรวจสอบภายในสำนักงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้สำนักงาน ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๔ การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

สำนักงานต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศนโยบายและแนวปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติได้ และต้องกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน พร้อมทั้งต้องทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สมบูรณ์จะต้องลงนามโดยผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เท่านั้น และต้องจัดเก็บเอกสารภายใต้เอกสารควบคุมคุณภาพ (<http://iso.nhso.go.th>) ในหมวดประกาศแต่งตั้ง เพื่อให้สามารถเข้าถึงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้ตลอดเวลา โดยมาตรฐานดังกล่าวที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน อาจมีการกำหนดหลักเกณฑ์ ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

๑.๔.๑ การรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีการกำหนดทิศทาง การบริหารจัดการและสนับสนุนความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับการดำเนินงานของสำนักงาน และกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

๑.๔.๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการเริ่มต้น และควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในสำนักงาน

๑.๔.๓ ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล เพื่อผู้ปฏิบัติงานของสำนักงานหรือสำนักงานสาขา ตั้งแต่เจ้าหน้าที่ ลูกจ้าง เจ้าหน้าที่ของรัฐซึ่งมาปฏิบัติงานในสำนักงานตามมติคณะรัฐมนตรี และรวมถึงพนักงานจ้างเหมาบริการทั้งที่เป็นบุคคล นิติบุคคล บุคลากรภายใต้การควบคุมดูแลของผู้ให้บริการภายนอกที่ปฏิบัติหน้าที่ตามสัญญาจ้าง เข้าใจหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ ที่รับผิดชอบ

๑.๔.๔ การบริหารจัดการทรัพยากร เพื่อให้มีการระบุนทรัพยากรของสำนักงาน และกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการทรัพยากรอย่างเหมาะสม

๑.๔.๕ การควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของสำนักงาน ให้เกิดความปลอดภัยต่อการเข้าถึงระบบสารสนเทศ

๑.๔.๕ การเข้ารหัสข้อมูล เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและป้องกันข้อมูลไว้ซึ่งความลับ ความถูกต้องของข้อมูล ป้องกันการปลอมแปลงหรือแก้ไขข้อมูลของสำนักงาน

๑.๔.๖ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เพื่อป้องกันการสร้างความเสียหาย หรือการแทรกแซงการปฏิบัติงาน โดยต้องครอบคลุมการปกป้องทรัพยากรสารสนเทศ สิ่งปลูกสร้าง และโครงสร้างพื้นฐานที่สำคัญ จากภัยคุกคามทางกายภาพและสภาพแวดล้อม อาทิ ภัยจากการคุกคามโดยบุคคล ภัยธรรมชาติ อุบัติภัย หรือเหตุอันไม่คาดคิดอื่น ๆ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว เหตุระเบิด และการก่อจลาจล เพื่อป้องกันการสูญหาย ความเสียหาย หรือผลกระทบต่อความต่อเนื่องในการดำเนินงานของสำนักงาน

๑.๔.๗ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน เพื่อให้การปฏิบัติงานกับระบบหรืออุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัยได้รับการป้องกันจากโปรแกรมกำจัดมัลแวร์ รวมถึงการป้องกันการสูญหายของข้อมูล การบันทึกเหตุการณ์และจัดทำหลักฐานต่าง ๆ ในการดำเนินการ

๑.๔.๘ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เพื่อให้มีการป้องกันข้อมูลสารสนเทศภายในระบบเครือข่ายในการถ่ายโอนข้อมูลภายในสำนักงาน และการถ่ายโอนข้อมูลกับหน่วยงานภายนอก

๑.๔.๙ การจัดหา การพัฒนา และการบำรุงรักษาระบบ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบที่สำคัญในการพัฒนาระบบ ตั้งแต่กระบวนการออกแบบ กระบวนการจัดการ พัฒนาระบบ และการบำรุงรักษาระบบให้สามารถดำเนินการได้อย่างต่อเนื่อง

๑.๔.๑๐ ความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก และเพื่อป้องกันทรัพยากรของสำนักงาน ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

๑.๔.๑๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ และตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ได้รับทราบ

๑.๔.๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

๑.๔.๑๓ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องของธุรกิจ เพื่อวางแผน และจัดเตรียมความพร้อมในส่วนต่าง ๆ รวมถึงทำการตรวจสอบ ทบทวน และประเมินเหตุการณ์ ผลกระทบที่จะส่งผลหรืออาจจะส่งผลให้เกิดความไม่ต่อเนื่องในการดำเนินธุรกิจ

๑.๔.๑๔ ความสอดคล้องต่อความต้องการด้านกฎหมาย ระเบียบ ข้อบังคับ เพื่อให้การดำเนินงานภายในสำนักงานมีความสอดคล้องในด้านกฎหมายระเบียบข้อบังคับหรืออื่น ๆ ที่เกี่ยวข้องกับสำนักงาน ที่ส่งผลต่อความมั่นคงปลอดภัยสารสนเทศ และทั้งที่เป็นความต้องการทางด้านความมั่นคงปลอดภัยสารสนเทศกฎหมาย ระเบียบ ข้อบังคับ จากภายนอก โดยให้มีการทบทวนความไม่สอดคล้องอย่างสม่ำเสมอ

๑.๔.๑๕ การปกป้องข้อมูล สิทธิในทรัพย์สินทางปัญญา และลิขสิทธิ์เพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่เกี่ยวข้องเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ มีความสอดคล้องกับกฎหมาย และข้อกำหนดตามสัญญาต่าง ๆ ทั้งการใช้งานภายในสำนักงานและการกำกับผู้ให้บริการภายนอก โดยต้องดำเนินการอย่างน้อย ดังนี้

(๑) จัดทำและปรับปรุงทะเบียนซอฟต์แวร์ลิขสิทธิ์ (Software License Inventory) ให้เป็นปัจจุบัน ครอบคลุมจำนวนสิทธิการใช้งาน (License) ที่ได้รับอนุญาต วันหมดอายุ เงื่อนไขสัญญาอนุญาต และผู้รับผิดชอบ โดยทบทวนอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

(๒) กำหนดขั้นตอนปฏิบัติงานในการตรวจสอบการใช้งานซอฟต์แวร์ให้สอดคล้องกับเงื่อนไขสัญญาอนุญาตใช้สิทธิ (Software License Compliance) รวมถึงการตรวจสอบซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของสำนักงานอย่างสม่ำเสมอ

(๓) กำหนดด้านทรัพย์สินทางปัญญาและลิขสิทธิ์ไว้ในสัญญา ข้อตกลงระดับการให้บริการ (SLA) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยครอบคลุมสิทธิในทรัพย์สินทางปัญญาที่เกิดจากการพัฒนาระบบ การใช้งานซอฟต์แวร์ตามลิขสิทธิ์ และมาตรการควบคุมการใช้งานข้อมูลของสำนักงาน

(๔) ห้ามมิให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ติดตั้งหรือใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ หรือนำข้อมูลอันเป็นทรัพย์สินทางปัญญาของสำนักงานไปใช้นอกเหนือจากที่ได้รับอนุญาต ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ และที่แก้ไขเพิ่มเติม

(๕) ผู้ให้บริการภายนอกที่พัฒนาระบบหรือซอฟต์แวร์ให้แก่สำนักงาน ต้องรับรองว่าผลงานที่ส่งมอบไม่ละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น และต้องระบุสิทธิความเป็นเจ้าของในทรัพย์สินทางปัญญาไว้ในสัญญาอย่างชัดเจน

๑.๔.๑๖ การรักษาความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security) เพื่อให้การกำกับดูแลและการใช้บริการระบบคลาวด์ (Cloud Computing) ของสำนักงาน มีความมั่นคงปลอดภัยเหมาะสมกับสภาพแวดล้อม และสอดคล้องกับมาตรฐานสากล โดยต้องดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดทำข้อตกลงระดับการให้บริการ (SLA) และเงื่อนไขสัญญา โดยกำหนดรูปแบบความรับผิดชอบร่วม (Shared Responsibility Model) ระหว่างสำนักงานและผู้ให้บริการคลาวด์ให้ชัดเจนเป็นลายลักษณ์อักษร

(๒) ดำเนินการประเมินความเสี่ยงและตรวจสอบหลักฐานการรับรองมาตรฐานด้านความมั่นคงปลอดภัยของผู้ให้บริการคลาวด์ ก่อนการพิจารณาใช้บริการ และจัดให้มีการทบทวนอย่างสม่ำเสมอ

(๓) กำหนดมาตรการควบคุมและปกป้องข้อมูลสารสนเทศที่จัดเก็บหรือประมวลผลบนระบบคลาวด์อย่างรัดกุม ครอบคลุมถึงการเข้ารหัสข้อมูล (Encryption) การยืนยันตัวตนแบบหลายปัจจัย (MFA) และการกำหนดตำแหน่งที่ตั้งของศูนย์ข้อมูล (Data Localization)

(๔) จัดให้มีแนวปฏิบัติในการใช้งานและการบริหารจัดการระบบคลาวด์ สำหรับผู้ใช้งานและผู้ดูแลระบบ โดยควบคุมการเข้าถึงและการแชร์ข้อมูลตามหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) เพื่อป้องกันการรั่วไหลของข้อมูลและรองรับการจัดการเหตุละเมิดความมั่นคงปลอดภัย

๑.๕ การรับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศของสำนักงาน

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๖ การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นปัจจุบันอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๗ การปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วนและการรักษาสภาพความพร้อมใช้งานตามที่สำนักงานประกาศใช้ล่าสุด และให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน ลงนามในเอกสาร Non-Disclosure Agreement (NDA) กำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) และ Acceptable Use Policy (AUP) ที่สำนักงานกำหนดขึ้น เพื่อให้ผู้ใช้งานได้รับทราบ และสามารถปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างถูกต้อง

๑.๘ การรับมือภัยคุกคามทางไซเบอร์

๑.๘.๑ สำนักงานต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน อย่างน้อยต้องประกอบด้วยเรื่อง ดังนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

๑.๘.๒ สำนักงานมีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน

๑.๘.๓ สำนักงานต้องกำหนดให้มีกลไก หรือ ขั้นตอน เพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงาน รวมถึงมีมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๘.๔ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของสำนักงาน ให้รายงาน ต่อสำนักงานหรือคณะกรรมการที่กำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน

๑.๘.๕ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของสำนักงาน ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์

และระบบคอมพิวเตอร์ รวมถึงพฤติกรรมแวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๑.๘.๖ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือระงับการดำเนินการใด ๆ เพื่อป้องกัน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทัน่วงทีและเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อสำนักงานหรือคณะกรรมการที่กำกับดูแล โดยเร็ว

๑.๘.๗ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง คณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังนี้

- (๑) เผื่อระงับคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง
- (๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์
- (๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่
- (๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์
- (๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

หมวด ๒

แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน

๒.๑ การปฏิบัติหน้าที่ทั่วไป

๒.๑.๑ ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลอันเป็นความลับของสำนักงาน เว้นแต่จะได้รับการอนุญาตให้เปิดเผยจากสำนักงาน

๒.๑.๒ ผู้ใช้งาน ต้องให้ความร่วมมือในการเข้าร่วมการฝึกอบรมในลักษณะของการติดตามการเปลี่ยนแปลงของเทคโนโลยีด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความตระหนักและมีความรู้เท่าทันเหตุการณ์ที่จะทำให้ละเมิดต่อนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงาน

๒.๑.๓ ผู้ใช้งาน ต้องให้ความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ หรือข้อกำหนดอื่นใดที่เกี่ยวข้องตามที่สำนักงานได้จัดทำขึ้น ตลอดจนให้ข้อเสนอแนะในการปรับปรุงให้มีประสิทธิภาพดีขึ้น

๒.๑.๔ ผู้ใช้งาน ต้องรักษาความลับและความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน จากผู้ไม่ได้รับอนุญาตหรือไม่มีหน้าที่รับผิดชอบตามที่สำนักงานกำหนด

๒.๑.๕ ผู้ใช้งาน ต้องดูแลรักษาป้องกันและใช้งานทรัพย์สินสารสนเทศของสำนักงานอย่างถูกวิธี ทั้งทรัพย์สินในครอบครองและทรัพย์สินส่วนกลางตามมาตรการต่าง ๆ ที่กำหนดไว้ ตามแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

๒.๑.๖ ผู้ใช้งาน ต้องตระหนักการนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย แต่ถ้ายกกระทำเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะส่งผลทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอายก็ได้ แต่หากเป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการดิ้นรนด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำผู้กระทำไม่มีความผิด

๒.๑.๗ ผู้ใช้งาน ต้องปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ในการเข้าถึงข้อมูลการใช้ข้อมูลส่วนบุคคล และเมื่อมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคล ต้องเป็นไปตามสิทธิที่ได้รับมอบหมายตามหน้าที่รับผิดชอบตามที่สำนักงานกำหนด

๒.๒ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๒.๑ ผู้ใช้งาน ต้องใช้ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่สำนักงานเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการปฏิบัติงานตามภารกิจของสำนักงานการใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวน หรือเป็นอุปสรรคต่อการทำงานในระบบสารสนเทศของสำนักงาน

๒.๒.๒ ผู้ใช้งานต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ดังนี้

(๑) ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนโดยทุจริต

หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่น

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตาม ข้อ ๒.๒.๒ (๑) – (๔)

(๖) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย แต่ถ้การกระทำเป็นการนำเข้าสู่ข้อมูลคอมพิวเตอร์โดยสุจริต ผู้ใช้งานไม่มีความผิด

(๗) เข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๘) ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ ๒.๒.๒ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๒.๓ ผู้ใช้งานต้องไม่กระทำการ ดังนี้

(๑) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมีได้มีไว้สำหรับตน

(๒) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นเฉพาะ ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อกดรั่วซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๔) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๕) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๖) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยไม่ปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(๗) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง

ในทางเศรษฐกิจของประเทศ การบริการสาธารณะ การกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

(๘) จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ ๒.๒.๓ (๑) – (๗)

(๙) ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router Switch Hub Wireless access point หรืออื่น ๆ ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักงาน ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๒.๒.๔ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย และอุปกรณ์ต่อพ่วง ผู้ใช้งานควรปฏิบัติ ดังนี้

(๑) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน จะต้องได้รับอนุญาตจากผู้บังคับบัญชาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) แต่งตั้งให้มีบทบาทหน้าที่ในการอนุมัติในการร้องขอจากผู้ใช้งานที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน และต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด

(๒) ห้ามมิให้ทำการแก้ไข ซ่อมแซม ทรัพย์สินสารสนเทศที่ชำรุดเสียหายด้วยตนเองโดยพลการ หรือให้ผู้อื่นที่ไม่มีอำนาจหน้าที่ดำเนินการให้ กรณีที่มีความจำเป็นให้แจ้งฝ่ายวิศวกรรมโครงสร้างพื้นฐาน เป็นผู้ดำเนินการ

(๓) ห้ามมิให้นำอุปกรณ์สารสนเทศหรืออุปกรณ์สื่อสารทั้งแบบใช้สายและไม่ใช้สาย นอกเหนือจากที่ผู้ดูแลระบบติดตั้งไว้เดิม มาเชื่อมต่อกับระบบสารสนเทศของสำนักงานโดยมิได้รับอนุญาต กรณีที่มีความจำเป็นต้องใช้หรือต่อเชื่อมต่อกับระบบสารสนเทศของสำนักงานให้แจ้งฝ่ายวิศวกรรมโครงสร้างพื้นฐานเป็นผู้ดำเนินการ

(๔) การปฏิบัติงานกับอุปกรณ์เทคโนโลยีสารสนเทศให้ปฏิบัติตามแนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย

(๕) กรณีทำงานที่ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของสำนักงานที่ได้รับมอบหมาย ให้คงอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๖) ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของสำนักงานอย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุดแก่ทางสำนักงาน

(๗) อุปกรณ์คอมพิวเตอร์ของสำนักงานต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บังคับบัญชาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงแต่งตั้งให้มีบทบาทหน้าที่ในการอนุมัติการดัดแปลง หรือติดตั้งอุปกรณ์ เพิ่มเติม

(๘) การใช้งานอุปกรณ์เคลื่อนที่แบบพกพา เช่น Notebook และอุปกรณ์สื่อสารอื่น ๆ ของผู้ใช้งาน จะต้องระมัดระวังเป็นพิเศษเพื่อให้มั่นใจได้ว่าข้อมูลที่มีความสำคัญของสำนักงานที่บันทึกอยู่ในอุปกรณ์ จะไม่ถูกเปิดเผย เปลี่ยนแปลง แก้ไข หรือถูกทำลาย

(๙) ไม่ทำการเปลี่ยนแปลง เพิ่มเติมหมายเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพาภายในสำนักงานโดยไม่ได้รับอนุญาต

(๑๐) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจาก ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน หรือผู้ที่ได้รับมอบหมาย

(๑๑) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๒.๕ ผู้ใช้งาน ต้องให้ความร่วมมือกับสำนักงานในการบำรุงรักษาอุปกรณ์สารสนเทศ ที่เป็นประจำอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๒.๓ การควบคุมเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

๒.๓.๒ ผู้ใช้งาน ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานร่วมกัน

๒.๓.๓ ผู้ใช้งาน ควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการ ล็อกหน้าจอภาพ เมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ใช้งาน ควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๓.๕ ผู้ใช้งาน ต้องปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อไม่มีการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๒.๓.๖ ผู้ใช้งาน ต้องให้ความร่วมมือในการปฏิบัติตามข้อกำหนดที่ทางผู้ดูแลระบบ กำหนดขึ้นตามแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศเพื่อให้ระบบสารสนเทศของสำนักงานมีความมั่นคงปลอดภัยอย่างเคร่งครัด

๒.๔ การใช้งานบัญชีผู้ใช้งาน (Account)

๒.๔.๑ ผู้ใช้งาน ที่เป็นเจ้าของบัญชีผู้ใช้งานต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งานของตนเอง จากเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๔.๒ ผู้ใช้งาน ต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่ายจ่ายแจก ให้กับผู้อื่น

๒.๔.๓ ผู้ใช้งาน ต้องลงบันทึกการเข้าใช้ (Login) โดยบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดงานชั่วคราว

๒.๕ การบริหารจัดการรหัสผ่านและข้อมูลการพิสูจน์ตัวตน (Identity and Password Management)

๒.๕.๑ รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยผสมกันระหว่างตัวเลข และตัวอักษรภาษาอังกฤษ ที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักษรพิเศษ (เช่น @ # \$ %) และสัญลักษณ์ต่าง ๆ ด้วย

๒.๕.๒ ไม่ควรกำหนดรหัสผ่านจากข้อมูลส่วนตัว เช่น ชื่อ หรือนามสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ วันเดือนปีเกิด

๒.๕.๓ เมื่อผู้ใช้งานได้รับรหัสผ่านจากระบบสารสนเทศ หรือได้รับจากผู้ดูแลระบบ ต้องทำการเปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานครั้งแรก และแนะนำให้เปลี่ยนรหัสผ่านทุก ๑ ปี หรือเปลี่ยนทันทีเมื่อมีเหตุอันควรสงสัยว่าความลับของรหัสผ่านถูกล่วงรู้

๒.๕.๔ ผู้ใช้งาน ต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคลและจะต้องไม่เปิดเผยหรือกระทำใดให้ผู้อื่นทราบโดยมิได้รับอนุญาต จากผู้บังคับบัญชา

๒.๕.๕ ไม่ทำการบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ หรือในรูปแบบอื่น ๆ ที่ไม่ได้ป้องกันการเข้าถึง

๒.๕.๖ ในกรณีที่ระบบสารสนเทศหรือเครื่องมือสื่อสารดิจิทัลมีการกำหนดให้ใช้การยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication: ๒FA) ผู้ใช้งานต้องปฏิบัติให้ครบถ้วนทุกขั้นตอนตามที่ระบบกำหนด เพื่อเพิ่มความปลอดภัยในการพิสูจน์ตัวตนเข้าสู่ระบบ

๒.๕.๗ รหัสผ่านชุดที่ ๒ หรือรหัสผ่านแบบใช้ครั้งเดียว (One-Time Password: OTP) หรือข้อมูลพิสูจน์ตัวตนที่ส่งไปยังอุปกรณ์เคลื่อนที่ (Mobile Device) ของผู้ใช้งาน ถือเป็นความลับเฉพาะบุคคล และเป็นความรับผิดชอบของเจ้าของบัญชีผู้ใช้งาน ห้ามมิให้เปิดเผยหรือโอนสิทธิการใช้งานรหัสประเภทดังกล่าวให้แก่บุคคลอื่นโดยเด็ดขาด

๒.๖ การป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๒.๖.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในสำนักงาน หรือเครื่องคอมพิวเตอร์ที่ต้องการใช้ระบบเครือข่ายของสำนักงาน ต้องติดตั้งโปรแกรมกำจัดมัลแวร์ (Anti Malware) ที่สำนักงานจัดหา หรืออนุญาต รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๖.๒ ผู้ใช้งาน ควรทำการอัปเดต (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ ตามคำแนะนำ ที่ผู้ดูแลระบบจะแจ้งให้ทราบเป็นระยะ ๆ

๒.๖.๓ ห้ามมิให้ผู้ใช้งานทำการปิด ยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator) หรือฝ่ายวิศวกรรมโครงสร้างพื้นฐาน

๒.๖.๔ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ และให้แจ้งฝ่ายวิศวกรรมโครงสร้างพื้นฐาน เพื่อทำการแก้ไข

๒.๖.๕ ก่อนการใช้งานสื่อบันทึกพกพา ควรมีการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

๒.๖.๖ ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันแล้วกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๒.๖.๗ ผู้ใช้งาน ควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยโปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Anti-Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .inf .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe & .xls.exe

๒.๗ การใช้ระบบอินเทอร์เน็ต (Internet)

๒.๗.๑ สำนักงานจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงานและอำนวยความสะดวกแก่ผู้ใช้งาน ผู้เข้าร่วมประชุม และบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงาน และการให้บริการของสำนักงาน

๒.๗.๒ ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้น ต้องไม่เป็นสาเหตุให้สำนักงานและบุคคลผู้ที่เกี่ยวข้องกับสำนักงาน เสื่อมเสียชื่อเสียง หรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๒.๗.๓ การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต ทั้งนี้สำนักงานขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งาน ในลักษณะที่ไม่เหมาะสม

๒.๗.๔ ผู้ใช้งาน ควรระมัดระวังในการคลิกหน้าต่างโฆษณาแบบป๊อปอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมัลแวร์ร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๒.๗.๕ ผู้ใช้งาน ควรระมัดระวังในการเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือขัดต่อกฎหมาย

๒.๗.๖ ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญาตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ และที่แก้ไขเพิ่มเติม

๒.๗.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นที่ใช้ข้อความยั่วๆ ให้อารมณ์ ซึ่งจะก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับบุคลากรของสำนักงานทั้งภายในและภายนอก รวมถึงหน่วยงานอื่น ๆ

๒.๗.๘ หลังจากการใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้วให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการใช้งานโดยบุคคลอื่น ๆ

๒.๗.๙ สำนักงานไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (อาทิ ผ่านทางเว็บบอร์ดหรือบล็อก) ของผู้ใช้งาน ผู้เข้าร่วมประชุม และบุคคลภายนอก ทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้น จากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของผู้ใช้งาน ผู้เข้าร่วมประชุม และบุคคลภายนอกผู้นั้น

๒.๗.๑๐ สำนักงานไม่สนับสนุนผู้ใช้งาน ที่ใช้ระบบอินเทอร์เน็ต (Internet) ของสำนักงาน ไปกระทำการใด ๆ ที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๒.๘ การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของสำนักงาน

๒.๘.๑ ผู้ใช้งานอีเมลทั้งหมดของสำนักงานต้องมี e-mail account เป็นของตนเอง

๒.๘.๒ e-mail account ต้องได้รับการป้องกันด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิด และการนำอีเมล ไปใช้ในทางที่ผิด

๒.๘.๓ ผู้ใช้งาน ต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนเป็นประจำ เพื่อเป็นการรักษาพื้นที่ เก็บข้อมูล ทั้งนี้ให้เก็บรักษาไว้เฉพาะอีเมลที่เกี่ยวข้องกับการปฏิบัติงาน หรือตามระยะเวลาที่กฎหมายกำหนดไว้เท่านั้น

๒.๘.๔ ห้ามใช้ e-mail account ของสำนักงานเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่าง เช่น เพื่อการโฆษณาขายสุบ สิ่งมีนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์

๒.๘.๕ ห้ามใช้ e-mail account ของสำนักงานในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ อาทิ เว็บบอร์ด บล็อก กระดานข่าว เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับสำนักงาน

๒.๘.๖ ผู้ใช้งาน ต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ e-mail account ของตน โดยเด็ดขาดไม่ว่าบุคคลนั้นจะเป็นผู้ใด

๒.๘.๗ ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ เช่น อีเมลขยะ (Junk mail) หรือโฆษณาสินค้า หรือโฆษณาสินค้าต่าง ๆ (Spam mail)

๒.๘.๘ ห้ามผู้ใช้งานนำ e-mail account ของสำนักงาน สร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมลหลอกลวง หรือการส่งอีเมลในลักษณะลูกโซ่ โดยเด็ดขาด

๒.๘.๙ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ช่มชู้ ลามก อนาจาร การยั่วยู่ทางเพศ หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

๒.๘.๑๐ ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใด ที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อสำนักงาน

๒.๘.๑๑ ผู้ใช้งาน ต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์หรือโปรแกรมแฝง (ม้าโทรจัน)

๒.๘.๑๒ เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมลโดยทันทีจนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

๒.๙ การจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๒.๙.๑ ให้ผู้ใช้งานตรวจสอบและสังเกตพฤติกรรมของระบบหรือบุคคลที่น่าสงสัย และแจ้งเจ้าหน้าที่ผู้ดูแลระบบที่รับผิดชอบ เมื่อสังเกตเห็นสิ่งผิดปกติหรืออาจเป็นเหตุละเมิดความมั่นคงปลอดภัย เช่น การใช้สิทธิของผู้ดูแลระบบจากระยะไกลเพื่อเข้าถึงระบบสารสนเทศ การแก้ไขข้อมูลบนเว็บไซต์ การพยายามสอบถามหรือหลอกลามรหัสผ่าน การเข้ามาใช้อุปกรณ์สารสนเทศโดยไม่ได้รับอนุญาต

๒.๙.๒ เมื่อเกิดหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัย เช่น ทรัพย์สินสารสนเทศสูญหาย มีความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต ให้ผู้ใช้งานที่พบเหตุปฏิบัติตาม แนวปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย และห้ามมิให้เจ้าหน้าที่ที่ไม่ได้รับมอบหมาย ปฏิบัติการอื่นใดที่ไม่ได้กำหนดไว้ในขั้นตอนรับมือเหตุละเมิดโดยพลการและดำเนินการแจ้งเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศตามช่องทางแจ้งเหตุที่ฝ่ายวิศวกรรมโครงสร้างพื้นฐานกำหนด

๒.๙.๓ ห้ามมิให้ผู้ใช้งานที่ไม่ได้รับอนุญาต ทำการทดสอบระบบรักษาความมั่นคงปลอดภัย โดยเด็ดขาด ถ้าพบว่าการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๙.๔ ห้ามมิให้ผู้ใช้งานที่ไม่ได้อนุญาต ทำการตรวจจับ เผ่าฟิง ติดตาม ถอดรหัส บันทึก การสื่อสารข้อมูลทั้งในเครือข่ายคอมพิวเตอร์และระบบสื่อสารโดยเด็ดขาด และให้ถือว่าการกระทำดังกล่าว เป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๙.๕ ผู้ใช้งาน ที่ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ และบุกรุกทรัพย์สินทางสำนักงานหรืออื่น ๆ แล้วแต่กรณีจะมีความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๒.๙.๖ เมื่อฝ่ายวิศวกรรมโครงสร้างพื้นฐาน ขอความร่วมมือในการปรับปรุงเวอร์ชันหรือระบบการใช้ทรัพยากรสารสนเทศเพื่อป้องกันการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัยให้ผู้ใช้งานปฏิบัติตามโดยทันที

๒.๙.๗ ภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน ต้องจัดทำรายงานตามที่คุณดูแลระบบตรวจพบการละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เสนอต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) การละเลยไม่ทำรายงานในเวลาที่กำหนดถือเป็นความบกพร่องในหน้าที่

๒.๑๐ การเคลื่อนย้ายและการทำสำเนาสารสนเทศ

๒.๑๐.๑ ห้ามมิให้คัดลอกหรือทำสำเนา เอกสาร ข้อมูลคอมพิวเตอร์ หรือข้อมูลสารสนเทศที่มีระดับลับขึ้นไป ในระบบสารสนเทศของสำนักงาน โดยไม่ได้รับอนุญาต ถ้าพบว่ามีกรกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๐.๒ ห้ามมิให้ส่งข้อมูลสารสนเทศของระบบสารสนเทศของสำนักงานออกไปนอกเครือข่ายของสำนักงาน หรือนำสำเนาสารสนเทศระดับลับขึ้นไปในระบบสารสนเทศของสำนักงานออกนอกพื้นที่รักษาการณโดยไม่ได้รับอนุญาต ถ้าพบว่ามีกรกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๐.๓ การทำสำเนาข้อมูลและการส่งข้อมูลของระบบสารสนเทศ ที่มีระดับความลับตามข้อ ๒.๑๐.๑ ของสำนักงานออกไปนอกเครือข่ายหรือระบบสารสนเทศของสำนักงาน ตามที่ผู้ร้องขอหรือผู้ที่ต้องการใช้สำเนาหรือรับข้อมูลดังกล่าวเพื่อใช้ในทางราชการ จะต้องได้รับอนุญาตจากผู้บริหารระดับสูง (CEO) หรือตัวแทนที่ผู้บริหารระดับสูง (CEO) แต่งตั้ง และให้ผู้ที่ได้รับอนุญาตจากผู้บังคับบัญชา ในการเข้าถึงเอกสารลับเป็นผู้ทำสำเนาออกจากระบบสารสนเทศของสำนักงาน โดยส่งสำเนาดังกล่าวให้กับผู้ร้องขอด้วยแผ่น CD DVD e-mail หรือสื่อบันทึกข้อมูลอื่น ๆ ที่สำนักงานอนุญาตเท่านั้น และห้ามมิให้คัดลอกหรือทำสำเนาส่งต่อให้ผู้ที่มีได้รับอนุญาต

๒.๑๐.๔ การใช้งานการสื่อสารข้อมูลในระบบอีเมลหรือจดหมายอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของสำนักงาน

๒.๑๑ การควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูล

๒.๑๑.๑ ควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูลเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

๒.๑๑.๒ ผู้ใช้งาน ห้ามปล่อยทิ้งอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูลไว้ในที่สาธารณะโดยไม่มีผู้ดูแล หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๒.๑๑.๓ ผู้ใช้งาน ต้องสำรองข้อมูลสำคัญสูงที่อยู่ภายในอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูลอย่างสม่ำเสมอและมีการเข้ารหัสข้อมูลที่สำคัญอย่างเหมาะสม

๒.๑๑.๔ ผู้ใช้งาน ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและไฟร์วอลล์สำหรับอุปกรณ์ส่วนตัวที่เชื่อมต่อเครือข่ายจากภายนอก และต้องเชื่อมต่อผ่านช่องทางที่มีการเข้ารหัสที่เป็นมาตรฐานสากล ได้แก่ VPN (Virtual Private Network)

๒.๑๑.๕ ผู้ใช้งาน ต้องแจ้งต่อผู้บังคับบัญชาเพื่อดำเนินการถอดถอนสิทธิในการเข้าถึงจากภายนอกสำนักงาน เมื่อเสร็จสิ้นการปฏิบัติงานที่ได้รับมอบหมาย

๒.๑๒ การทำลายสื่อบันทึกข้อมูลหรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป

๒.๑๒.๑ ผู้ใช้งาน ต้องไม่ทิ้งเอกสารที่เป็นลำดับชั้นความลับ ลับมาก และลับที่สุด ไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นเตอร์ หรือเครื่องสแกนเนอร์ เมื่อส่งพิมพ์หรือสำเนาแล้วต้องเก็บเอกสารทันที

๒.๑๒.๒ ผู้ใช้งาน ต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ไว้ที่โต๊ะทำงาน โดยไม่มีผู้ดูแล หรือไม่ได้ใช้งาน และต้องจัดหาสถานที่จัดเก็บอย่างปลอดภัย เช่น เก็บในตู้ที่มีอุปกรณ์ล็อก

๒.๑๒.๓ ห้ามมิให้คัดลอกหรือทำสำเนา เอกสาร ข้อมูลคอมพิวเตอร์ หรือข้อมูลสารสนเทศที่มีระดับลับขึ้นไป ในระบบสารสนเทศของสำนักงาน โดยไม่ได้รับอนุญาต ถ้าพบว่ามีกรกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๒.๔ กรณีผู้ร้องขอสำเนาข้อมูล และได้รับสำเนาข้อมูลตาม ๒.๑๐.๓ ทาง e-mail ของสำนักงาน เมื่อใช้งานตามภารกิจแล้วให้ทำการลบ e-mail นั้น ใน Inbox และ Trash ออกจากระบบ

๒.๑๒.๕ หากผู้ที่ร้องขอหรือผู้ที่ต้องการใช้สำเนาหรือรับข้อมูล ได้รับสำเนาข้อมูล มีระดับลับขึ้นไปจากผู้ที่ได้รับอนุญาตจากผู้บังคับบัญชา ลงสื่อบันทึกข้อมูลอื่น ๆ เช่น Flash Drive, Hard disk ฯลฯ เพื่อใช้ในราชการตามภารกิจเรียบร้อยแล้ว ให้ทำการลบหรือล้างไฟล์ข้อมูลนั้น ๆ ด้วยโปรแกรมเขียนทับ (Wiping) ด้วย บิต ๐ หรือ ๑ ในไฟล์ข้อมูลดังกล่าว ทั้งนี้ต้องแจ้งให้ผู้บังคับบัญชาของผู้ที่ได้รับอนุญาตตาม ๒.๑๐.๓ ทราบว่าได้ทำลายข้อมูลแล้ว เป็นลายลักษณ์อักษร

๒.๑๓ การเข้ารหัสข้อมูลที่มีระดับลับขึ้นไป

การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล การเข้ารหัสข้อมูลแบบสมมาตร เช่น AES 256 การเข้ารหัสข้อมูลแบบอสมมาตร เช่น public key cryptography และมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้กันยังคงมีความแข็งแรงเพียงพอ

๒.๑๔ การใช้งานปัญญาประดิษฐ์อย่างมีธรรมาภิบาลและปลอดภัย (Responsible and Secure AI Adoption)

๒.๑๔.๑ ควบคุมการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้เพิ่มประสิทธิภาพการทำงาน ให้เป็นไปตามหลักธรรมาภิบาลปัญญาประดิษฐ์ภาครัฐ เพื่อคุ้มครองข้อมูลของสำนักงานและข้อมูลส่วนบุคคล

๒.๑๔.๒ ผู้ใช้งานต้องใช้เทคโนโลยีหรือระบบปัญญาประดิษฐ์ (AI) ที่สำนักงานจัดหา หรืออนุมัติให้ใช้งานอย่างเป็นทางการเท่านั้น เช่น ระบบ AI ระดับองค์กร (Enterprise License) บริการ AI ผ่าน API ที่มีการทำสัญญาคุ้มครองข้อมูล หรือระบบอื่นที่สำนักงานรับรอง

ทั้งนี้ ห้ามมิให้ ผู้ใช้งานนำข้อมูลที่มีชั้นความลับตั้งแต่ระดับชั้นลับ (Confidential) ขึ้นไป ข้อมูลการเงิน หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว ไปประมวลผลบนระบบปัญญาประดิษฐ์สาธารณะ แบบให้ใช้ฟรี เช่น ChatGPT รุ่นฟรี Gemini รุ่นทั่วไป หรือ AI อื่นที่ไม่ได้ระบุในบัญชีอนุญาต ที่ไม่มีการรับประกันความปลอดภัยของข้อมูลโดยเด็ดขาด

๒.๑๔.๓ การนำข้อมูลเข้าสู่ระบบปัญญาประดิษฐ์ที่ได้รับอนุญาต เพื่อการประมวลผล วิเคราะห์ หรือร่างเอกสาร ผู้ใช้งานต้องปฏิบัติตามนโยบายธรรมาภิบาลข้อมูล (Data Governance) ของสำนักงาน โดยพิจารณาตามการจัดระดับชั้นความลับของข้อมูล และต้องได้รับการอนุมัติตามลำดับชั้น ดังนี้

(๑) ข้อมูลระดับชั้นเผยแพร่ภายในสำนักงาน (Private) และ ชั้นลับ (Confidential) ต้องได้รับความเห็นชอบจาก ผู้อำนวยการสำนัก ฝ่ายต้นสังกัด หรือ บริกรข้อมูล (Data Steward) ของส่วนงานนั้น

(๒) ข้อมูลระดับชั้นลับมาก (Secret) ต้องได้รับความเห็นชอบจากผู้บริหารข้อมูลระดับสูง (Chief Data Officer: CDO) เป็นลายลักษณ์อักษรก่อนดำเนินการทุกครั้ง

(๓) ข้อมูลระดับชั้นลับที่สุด (Top Secret) ห้ามมิให้นำเข้าประมวลผลในระบบปัญญาประดิษฐ์หรือระบบสารสนเทศใด ๆ โดยเด็ดขาด ทั้งนี้ให้ดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น ตามระเบียบกรอบธรรมาภิบาลข้อมูล

๒.๑๔.๔ ผู้ใช้งานต้องตรวจสอบความถูกต้อง (Fact-check) ของผลลัพธ์ที่ได้จาก AI ก่อนนำไปอ้างอิงหรือใช้งานจริงทุกครั้ง โดยห้ามนำผลลัพธ์จาก AI มาใช้งานโดยตรงโดยไม่มีการตรวจสอบจากมนุษย์ (Human-in-the-loop)

๒.๑๕ การบริหารจัดการข้อมูลบนระบบจัดเก็บเอกสารบนคลาวด์ (Corporate Cloud Storage)

๒.๑๕.๑ ผู้ใช้งานต้องถือว่าระบบจัดเก็บเอกสารบนคลาวด์ส่วนกลางที่สำนักงานจัดหาให้ หรืออนุมัติให้ใช้งาน เป็นพื้นที่หลักสำหรับการจัดเก็บและบริหารจัดการข้อมูลเพื่อการปฏิบัติงานภายในสำนักงาน โดยต้องมีการกำหนดสิทธิการเข้าถึงให้สอดคล้องกับภารกิจหน้าที่จริง (Least Privilege)

๒.๑๕.๒ ผู้ใช้งานห้ามจัดเก็บหรือแชร์ข้อมูลที่ผิดกฎหมาย ข้อมูลที่ละเมิดลิขสิทธิ์ ซอฟต์แวร์ หรือข้อมูลไฟล์ส่วนตัวที่ไม่เกี่ยวข้องกับการปฏิบัติงาน เช่น รูปภาพครอบครัว ไฟล์วิดีโอส่วนตัว หรือสื่อบันเทิง ลงในระบบคลาวด์ของสำนักงาน

๒.๑๕.๓ ผู้ใช้งานสามารถใช้พื้นที่จัดเก็บข้อมูลบนคลาวด์ส่วนบุคคลที่สำนักงานจัดหาให้ สำหรับการจัดเก็บเอกสารร่าง (Draft) หรือข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานส่วนบุคคลเท่านั้น และห้ามตั้งค่าการแชร์ไฟล์ในลักษณะ “ทุกคนที่มีลิงก์” (Anyone with the link) สูภายนอกสำนักงานโดยเด็ดขาด

๒.๑๕.๔ ผู้ใช้งานมีหน้าที่โอนย้ายข้อมูลราชการทั้งหมดจากพื้นที่จัดเก็บส่วนบุคคลไปยังพื้นที่จัดเก็บส่วนกลางทันทีเมื่อต้องใช้งานร่วมกันในระดับส่วนงาน หรือก่อนวันสุดท้ายของการปฏิบัติงาน กรณีพ้นสภาพการปฏิบัติงาน

๒.๑๖ การสื่อสารและการทำงานร่วมกันผ่านสื่ออิเล็กทรอนิกส์ (Digital Communication and Collaboration)

๒.๑๖.๑ ผู้ใช้งานต้องใช้อีเมลของสำนักงาน (Office e-Mail) และระบบการสื่อสารและทำงานร่วมกันที่สำนักงานจัดหาให้ เป็นช่องทางหลักในการสื่อสารและประสานงานภายในสำนักงาน

๒.๑๖.๒ ผู้ใช้งานห้ามส่งข้อมูลที่มีชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่มีความละเอียดอ่อน (Sensitive Data) ผ่านแอปพลิเคชันสื่อสารส่วนบุคคลหรือแพลตฟอร์มภายนอก เช่น LINE Facebook Messenger โดยเด็ดขาด

๒.๑๖.๓ ผู้ใช้งานที่ทำหน้าที่จัดประชุม (Organizer) ต้องตรวจสอบสิทธิผู้เข้าร่วมและเปิดใช้งานฟังก์ชัน “Waiting Room” หรือ “Lobby” เพื่อคัดกรองบุคคลภายนอกก่อนเริ่มการสนทนาในหัวข้อที่มีชั้นความลับ

๒.๑๖.๔ ผู้ใช้งานต้องใช้วิธีการส่ง “ลิงก์” (Link) จากระบบจัดเก็บข้อมูลคลาวด์ที่กำหนดสิทธิการเข้าถึงไว้แล้วแทนการแนบไฟล์โดยตรงในระบบสนทนา

ในกรณีที่มีความจำเป็นต้องแนบไฟล์ข้อมูลเพื่อส่งผ่านระบบอีเมลหรือระบบสนทนาของสำนักงาน ผู้ใช้งานต้องดำเนินการระบุป้ายกำกับชั้นความลับ (Mark Label หรือ Sensitivity Label) ให้กับไฟล์ดังกล่าวก่อนทุกครั้ง เพื่อความปลอดภัยในการควบคุมข้อมูลและป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต

หมวด ๓

แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ

๓.๑ การปฏิบัติหน้าที่โดยทั่วไปของผู้ดูแลระบบ

๓.๑.๑ เจ้าหน้าที่ผู้ดูแลระบบมีหน้าที่ปฏิบัติต่อระบบสารสนเทศ ต้องปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศระดับผู้ใช้งานทั่วไป อีกทั้งยังต้องทำการบริหารและจัดการสารสนเทศหรือระบบสารสนเทศตามบทบาทหน้าที่ที่ทางผู้อำนวยการฝ่ายวิศวกรรมโครงสร้างพื้นฐาน หรือผู้รับผิดชอบในส่วนงานอื่น ๆ ที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงมอบหมายหน้าที่โดยจำเป็นต้องปฏิบัติเพิ่มเติมในส่วนของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

(๑) ต้องตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่ายของสำนักงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกัน และบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่เกิดขึ้นแก่สำนักงาน ให้ผู้ดูแลระบบพิจารณาแจ้งการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

(๒) ต้องติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์ และระบบบนเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

(๓) สำหรับระบบงานที่ต้องมีการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลผ่านระบบ Internet ควรมีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบเครือข่าย (Network Penetration Test) โดยผู้เชี่ยวชาญอย่างน้อยปีรายไตรมาส และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัย หรือมีการเปลี่ยนแปลงความเสี่ยงทางเทคโนโลยีที่มีนัยสำคัญ รวมทั้งควรจะมีการพิจารณาตามความเหมาะสม

(๔) จัดทำแผนการเปลี่ยนแปลงและแก้ไขซอฟต์แวร์ ระบบสารสนเทศ และระบบปฏิบัติการล่วงหน้า เพื่อใช้ในการดูแลและบำรุงรักษาระบบในอนาคตและให้ผู้เกี่ยวข้องมีเวลาในการทดสอบก่อนการเปลี่ยนแปลงและแก้ไข

(๕) แจ้งผลการตรวจสอบและประเมินแนวโน้มระดับการใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Capacity) และสรุปประเด็นปัญหาให้กับผู้บริหารอย่างสม่ำเสมอทุกเดือน เพื่อที่จะสามารถปรับปรุงประสิทธิภาพและความเพียงพอของอุปกรณ์ประมวลผลสารสนเทศให้ตอบสนองความต้องการของผู้เป็นเจ้าของสารสนเทศทั้งในปัจจุบันและในอนาคต

(๖) ต้องตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

(๗) ต้องดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(๘) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน ก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของสำนักงาน

(๙) ต้องดูแลรักษาและปรับปรุงบัญชีผู้ใช้งานระบบยืนยันตัวตน (Authentication) และระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

(๑๐) ต้องตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือเครื่องคอมพิวเตอร์แม่ข่าย ที่ให้บริการไคลเอนต์สำหรับเครือข่ายโดเมนในส่วนนโยบายรหัสผ่าน (Password Policy) ให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password) ให้สอดคล้องตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศระดับผู้ใช้งานทั่วไป ในข้อ ๒.๕

(๑๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้ระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(๑๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้ระบบคอมพิวเตอร์ หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(๑๓) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

(๑๔) เมื่อผู้ดูแลระบบ พ้นจากหน้าที่จะต้องคืนทรัพย์สินของสำนักงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้หัวหน้ากลุ่มงานที่บังคับบัญชาผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายทำการตรวจสอบการคืนทรัพย์สิน

๓.๑.๒ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ดูแลระบบ จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานที่สำนักงานให้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังนี้

(๑) เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริงและระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยสื่อที่ใช้ในการเก็บต้องสามารถใช้ในการยืนยันทางกฎหมายได้และไม่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของสำนักงานหรือบุคคลที่สำนักงานมอบหมาย

(๓) ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) นั้น ต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๔) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ดูแลระบบ ต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลามาตรฐานประเทศไทย (Stratum 1) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

(๕) การให้สิทธิเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log file) แก่ผู้ดูแลระบบ ผู้ให้บริการภายนอก และผู้ที่มีสิทธิที่เกี่ยวข้อง จะต้องถูกควบคุมตามหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege) โดยต้องเข้าถึงผ่านบัญชีผู้ใช้งานรายบุคคล (Individual Account) เท่านั้น และต้องมีกระบวนการสอบทานสิทธิการเข้าถึงอย่างสม่ำเสมอ

๓.๑.๓ ผู้ดูแลระบบมีหน้าที่ควบคุมและการบริหารจัดการการเปลี่ยนแปลง (Change Management) ดังนี้

(๑) จัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) ของผู้ที่เกี่ยวข้องในกระบวนการอย่างเหมาะสม เพื่อป้องกันไม่ให้อำนาจหน้าที่ใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการเพียงลำพัง

(๒) คำขอการเปลี่ยนแปลง (Change Request) ต้องได้รับการอนุมัติจากเจ้าของระบบ (System Owner) หรือผู้มีอำนาจอนุมัติ เพื่อให้มั่นใจว่าได้รับการพิจารณาความจำเป็นและผลกระทบอย่างเหมาะสม

(๓) ต้องมีการประเมินผลกระทบและทำการทดสอบก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง (Production Environment) เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

(๔) จัดทำแผนการถอยกลับ (Rollback Plan) หรือขั้นตอนการปฏิบัติงานสำรอง (Fallback Procedure) พร้อมระบุหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการกู้คืนระบบ กรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

(๕) ต้องมีการติดตามและทบทวนผลหลังการเปลี่ยนแปลง (Post-implementation Review) เพื่อให้มั่นใจว่าการเปลี่ยนแปลงสำเร็จตามวัตถุประสงค์และไม่ส่งผลกระทบต่อการให้บริการ

๓.๑.๔ ผู้ดูแลระบบ ต้องควบคุมให้มีการแยกสภาพแวดล้อมสำหรับการพัฒนา (Development) และสภาพแวดล้อมสำหรับการทดสอบ (Testing) ออกจากสภาพแวดล้อมที่ใช้งานจริง (Production) อย่างชัดเจน เพื่อป้องกันผลกระทบต่อความมั่นคงปลอดภัยและความถูกต้องของข้อมูล โดยต้องจัดให้มีการควบคุม ดังนี้

(๑) จัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) ของบุคลากรที่เกี่ยวข้องอย่างชัดเจน โดยกำหนดให้ ผู้พัฒนาระบบ (Developer) ผู้ทดสอบระบบ (Tester) และผู้ที่มีสิทธิในการนำระบบขึ้นใช้งานจริง (Deployer หรือ Authorized Personnel) เป็นบุคคลคนละกลุ่มกัน เพื่อป้องกันความขัดแย้งทางผลประโยชน์และลดความเสี่ยงจากการกระทำที่มิชอบ

(๒) ซอร์สโค้ด (Source Code) ของระบบสารสนเทศ ต้องไม่จัดเก็บไว้ในสภาพแวดล้อมที่ใช้งานจริง (Production) เว้นแต่มีข้อจำกัดทางเทคนิคของภาษาที่ใช้ในการพัฒนา โดยในกรณีดังกล่าว ต้องมีการกำหนดสิทธิในการเข้าถึง (Access Control) ให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๓) ต้องใช้ระบบควบคุมเวอร์ชันของชุดคำสั่ง (Source Code Version Control) เพื่อบริหารจัดการการแก้ไขปรับปรุง และป้องกันความเสี่ยงจากการใช้งานชุดคำสั่งผิดเวอร์ชัน

(๔) กำหนดแนวทางการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล ที่นำมาใช้ในการทดสอบ โดยต้องมีการปกปิดข้อมูล (Data Masking) หรือใช้ข้อมูลจำลอง เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญหรือข้อมูลส่วนบุคคล (Sensitive หรือ Personal Data)

(๕) การนำระบบขึ้นใช้งานจริง (Deployment) ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) ตามระเบียบที่สำนักงานกำหนดอย่างเคร่งครัด

(๖) หน่วยงานที่เกี่ยวข้องต้องสอบถามความถูกต้องครบถ้วนตามความต้องการทางธุรกิจ (Business Requirement) และต้องครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirement) รวมถึงจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) ให้เป็นปัจจุบัน

(๗) ต้องจัดทำขอบเขตการทดสอบ (Test Scenarios) ให้ครอบคลุมทั้งด้านการทำงาน (Functional Test) ประสิทธิภาพของระบบ (Performance Test) และการทดสอบความมั่นคงปลอดภัย (Security Test) เพื่อให้มั่นใจว่าระบบพร้อมใช้งานตามความต้องการของหน่วยงาน

๓.๒ การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

๓.๒.๑ กำหนดประเภทข้อมูลหลัก ๆ ดังนี้

(๑) ความลับที่สุด (Top Secret) เป็นข้อมูลสารสนเทศที่มีความสำคัญอย่างสูงต่อการดำเนินธุรกิจ และกำหนดให้เฉพาะผู้บริหารระดับสูงหรือบางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้สารสนเทศดังกล่าวได้

(๒) ความลับมาก (Secret) เป็นข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่สำนักงานอย่างร้ายแรง เช่น ข้อมูลรหัสผ่านของผู้ดูแลระบบ

(๓) ความลับ (Confidential) เป็นข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจ และกำหนดให้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึง หรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยหรือการเข้าถึงสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหาย ทางด้านการเงิน หรือกระทบต่อการดำเนินงานประจำวัน หรือความก้าวหน้าทางธุรกิจ และอาจก่อให้เกิดความเสียหายต่อชื่อเสียง และภาพลักษณ์ เช่น ข้อมูลส่วนบุคคล ข้อมูลค่า Configuration ของอุปกรณ์ ข้อมูลรหัสผ่าน ข้อมูลการประเมินความเสี่ยง

(๔) ใช้ภายใน (Internal Use Only) เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในสำนักงานเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบต่อการปฏิบัติงานประจำวันของสำนักงานได้ แต่ไม่กระทบต่อการดำเนินธุรกิจ เช่น เอกสารนโยบาย มาตรฐานและขั้นตอนการปฏิบัติงาน รายละเอียดเบอร์โทรศัพท์ภายในสำนักงาน เอกสารคู่มือการใช้งานระบบต่าง ๆ บันทึกการปฏิบัติงานประจำวัน

(๕) เปิดเผยต่อบุคคลภายนอก (Public) เป็นข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารระดับสูงอนุมัติให้ เปิดเผยต่อสาธารณะได้อย่างไรก็ได้ สารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกันหรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับลูกค้า รวมทั้งรักษาภาพลักษณ์และชื่อเสียง เช่น รายงานประจำปี ข้อมูลบนเว็บไซต์

๓.๒.๒ ลำดับความสำคัญของข้อมูล หรือชั้นความลับของข้อมูลผู้ดูแลระบบ จะต้องปฏิบัติอย่างเคร่งครัด โดยให้กำหนดประเภทของข้อมูลตามหลักเกณฑ์ข้อ ๓.๒.๑

๓.๒.๓ ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศตามชั้นความลับ ต้องแบ่งสิทธิตามตำแหน่ง และตามบทบาทหน้าที่ความรับผิดชอบ โดยแบ่งระดับชั้นการเข้าถึงออกเป็น ๓ ลำดับ ดังนี้

(๑) ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลสารสนเทศในทุกลำดับชั้นความลับ

(๒) ระดับชั้นสำหรับผู้ใช้งาน หรือผู้ดูแลระบบ สามารถเข้าถึงข้อมูลสารสนเทศเฉพาะที่ได้รับมอบหมายตามหน้าที่ความรับผิดชอบ

(๓) ระดับชั้นสำหรับบุคคลภายนอก สามารถเข้าถึงข้อมูลสารสนเทศในลำดับชั้นความลับข้อมูลเปิดเผยได้ (Public)

๓.๒.๔ ระยะเวลาการเข้าถึงข้อมูลสารสนเทศ ได้แก่

(๑) ระบบอินเทอร์เน็ต และระบบภายในของสำนักงาน สำหรับผู้ใช้งาน หรือผู้ดูแลระบบ สามารถเข้าถึงได้ตลอดเวลา

(๒) ระบบเว็บไซต์ (www.nhso.go.th) สำหรับบุคคลภายนอกสามารถเข้าถึงได้ตลอดเวลา

๓.๒.๕ ช่องทางการเข้าถึงข้อมูลสารสนเทศ โดยผู้ต้องการเข้าถึงข้อมูลสารสนเทศจะต้องได้รับอนุญาตจากผู้บังคับบัญชา และทุกครั้งที่มีการเข้าถึงข้อมูลสารสนเทศ จะต้องผ่านการยืนยันตัวบุคคล รวมถึงผู้ดูแลระบบต้องกำกับ ติดตาม และทบทวนสิทธิตามที่ผู้ต้องการเข้าถึงข้อมูลร้องขอ โดยช่องทางการเข้าถึงข้อมูลสารสนเทศของสำนักงาน มีดังนี้

(๑) ช่องทางที่สามารถเข้าถึงข้อมูลสารสนเทศจากภายนอกสำนักงานจะต้องผ่านเครือข่ายทางไกลจากภายนอก (VPN)

(๒) ช่องทางที่สามารถเข้าถึงข้อมูลสารสนเทศจากภายในจะต้องผ่านระบบเครือข่ายภายในสำนักงาน

(๓) ช่องทางการรับส่งข้อมูลสารสนเทศสำคัญ โดยผ่านระบบเครือข่ายสาธารณะทั้งจากภายในหรือภายนอกสำนักงานโดยช่องทางและข้อมูลสำคัญดังกล่าว ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อย หรือ XML Encryption ตามความเหมาะสมของธุรกรรมที่ใช้ในการรับส่งข้อมูลสารสนเทศ

๓.๒.๖ ผู้ดูแลระบบต้องบริหารจัดการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดรหัสยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกสำนักงาน เพื่อให้สามารถเข้าถึงเครือข่าย และระบบสารสนเทศของสำนักงานโดยการให้ผู้ใช้งานยืนยันแบบคำขอรหัสการเข้าใช้งาน VPN ตามแบบคำขอใช้งาน VPN โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

(๕) กำหนดค่าการเปลี่ยนรหัส (Password) ตามระยะเวลาที่กำหนดของความปลอดภัยของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ ออกนอกพื้นที่ของสำนักงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๓.๒.๗ ผู้ดูแลระบบ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องข้อมูลสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

๓.๒.๘ ผู้ดูแลระบบ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศในกรณีที่น่าเครื่องคอมพิวเตอร์ ออกนอกพื้นที่ของสำนักงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูล

๓.๒.๙ ผู้ดูแลระบบ ต้องปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ในการเข้าถึงข้อมูลการใช้ข้อมูลส่วนบุคคล และเมื่อมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคล ต้องเป็นไปตามสิทธิที่ได้รับมอบหมายตามหน้าที่รับผิดชอบตามที่สำนักงานกำหนด

๓.๒.๑๐ ผู้ดูแลระบบ ต้องควบคุม ตรวจสอบ แจ้งเตือนการละเมิดการเข้าใช้งาน การโอนถ่ายข้อมูล หรือการกระทำใด ๆ ของผู้ที่เข้าถึงข้อมูลส่วนบุคคลที่ขัดต่อนโยบายในการคุ้มครองข้อมูลส่วนบุคคลให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

๓.๓ การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๓.๑ ให้ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของสำนักงานเพื่อดูแลรักษาความปลอดภัย โดยที่ผู้ดูแลระบบจะต้องกำหนดสิทธิในการเข้าใช้งานระบบสารสนเทศของสำนักงานนั้น ผู้เข้าใช้งานในส่วนต่าง ๆ จะต้องขออนุญาตเป็นลายลักษณ์อักษร และให้ผู้บังคับบัญชาที่รับผิดชอบในการกำกับควบคุมผู้ดูแลระบบที่มีหน้าที่ในการให้เข้าถึงระบบสารสนเทศ โดยที่ผู้ดูแลระบบ

ต้องตรวจสอบการดำเนินการ และเสนอความผิดปกติต่อผู้อำนวยการฝ่ายวิศวกรรมโครงสร้างพื้นฐานรับทราบทันที โดยให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของสำนักงาน ดังนี้

(๑) ให้สำนักงานจัดทำทะเบียนควบคุมสิทธิที่เหมาะสม รวมถึงรายชื่อหรือกลุ่มผู้มีสิทธิใช้งานทั้งที่ต้องขออนุมัติและไม่ต้องขออนุมัติก่อนเริ่มใช้งานอย่างเป็นลายลักษณ์อักษรในแต่ละระบบสารสนเทศ โดยการเข้าถึงของผู้ใช้งานทั้งหมดต้องสอดคล้องกับการดำเนินงานของสำนักงานและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(ก) ผู้บังคับบัญชา พิจารณาให้สิทธิตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน รวมทั้งกำหนดให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(ข) ผู้ดูแลระบบ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานตามที่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๓.๒ ให้ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน ควบคุมให้มีขั้นตอนการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนสิทธิการเข้าใช้งาน ดังนี้

(๑) การลงทะเบียนผู้ใช้งาน

(ก) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน ก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของสำนักงาน

(ข) การลงทะเบียนผู้ใช้งาน กรณีที่จ้างบุคคลภายนอกพัฒนาระบบ (Outsource) โดยกำหนดให้มีการแสดงหลักฐานที่สามารถระบุตัวบุคคลได้ และการเข้าถึงระบบสารสนเทศต้องได้รับอนุมัติจากสำนักต้นสังกัดของผู้ใช้งานนั้น ๆ ก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของสำนักงาน

(ค) ผู้ดูแลระบบต้องสร้างบัญชีผู้ใช้งานแยกเป็นรายบุคคล ในกรณีที่มีความจำเป็นต้องใช้งานบัญชีผู้ใช้งานร่วมกันให้ขออนุมัติเป็นกรณีไปผู้ดูแลระบบ ต้องจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยจัดส่งแยกเป็นรายบุคคล

(๒) การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งาน

(ก) กรณีที่ผู้ใช้งานในส่วนเจ้าหน้าที่ลาออก สิ้นสุดการจ้าง ให้ยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามรอบที่ฝ่ายบริหารทรัพยากรบุคคล แจ้งต่อฝ่ายวิศวกรรมโครงสร้างพื้นฐาน

(ข) กรณีที่ผู้ใช้งานในส่วนอื่น ๆ ลาออก สิ้นสุดการจ้าง ให้ยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามรอบที่สำนักต้นสังกัดของผู้ใช้งานนั้น ๆ แจ้งต่อฝ่ายวิศวกรรมโครงสร้างพื้นฐาน

(ค) กรณีปรับเปลี่ยนตำแหน่งหน้าที่ภายในหน่วยงาน โอนย้ายหน่วยงาน หรือหมดความจำเป็นในการใช้งาน ให้เปลี่ยนแปลงสิทธิตามรอบที่ฝ่ายบริหารทรัพยากรบุคคล หรือสำนักต้นสังกัดแจ้งต่อฝ่ายวิศวกรรมโครงสร้างพื้นฐาน

(ง) ผู้ดูแลระบบ ต้องยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามเงื่อนไข (ก) – (ค) ภายใน ๗ วัน ตามการร้องขอจากฝ่ายบริหารทรัพยากรบุคคล หรือสำนักต้นสังกัดที่แจ้งต่อฝ่ายวิศวกรรมโครงสร้างพื้นฐาน

(๓) การทบทวนสิทธิ

(ก) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบของผู้ใช้งานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และระงับการใช้งานบัญชีผู้ใช้ที่ไม่ได้ใช้งาน

(ข) ให้ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน ควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๑. ผู้ดูแลระบบ ต้องกำหนดสิทธิผู้ใช้งานตามคำร้องขอที่ได้รับอนุมัติ การขอเข้าใช้งานระบบจากผู้บังคับบัญชา โดยผู้ใช้งานต้องเข้าใช้งานระบบตามสิทธิที่ตนเองได้รับเท่านั้น

๒. ผู้บังคับบัญชาต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่รับผิดชอบ

๓. หัวหน้าหน่วยงานเจ้าของระบบ หรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย ต้องตรวจสอบและมอบหมายสิทธิเฉพาะตามที่ได้รับการร้องขอ

๔. ในกรณีมีความจำเป็นต้องให้สิทธิจำเพาะ สิทธิพิเศษกับผู้ใช้งาน ได้แก่ สิทธิสูงสุดในการเข้าถึงระบบหรือข้อมูล และสิทธิที่เข้าถึงระบบหรือข้อมูลได้มากกว่าหน้าที่รับผิดชอบ ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา และได้รับการตรวจสอบจากหัวหน้าหน่วยงานเจ้าของระบบ หรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง รวมทั้งต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕. หัวหน้าหน่วยงานเจ้าของระบบ หรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย ต้องมีการบันทึก จัดเก็บหลักฐานในการขอใช้สิทธิระดับสูงเพื่อการทบทวนและตรวจสอบสิทธิ

(ค) ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสารสนเทศ

(ง) ผู้ดูแลระบบ ต้องจัดบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาต และไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

(จ) ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านและสิทธิการใช้งาน ระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน ดังนี้

๑. รหัสผู้ใช้งานและรหัสผ่าน ผู้ดูแลระบบจัดส่งให้กับผู้ใช้งานเริ่มต้นเป็นรหัสชั่วคราว โดยชื่อผู้ใช้งานหรือรหัสผ่านต้องไม่ซ้ำกัน และกำหนดให้ระบบจัดการรหัสผ่านตรวจสอบรหัสผ่านว่าต้องประกอบด้วย อักขระ ตัวเลขและอักขระพิเศษ ความยาวรวมกันไม่น้อยกว่า ๘ ตัวอักษร กรณีที่ผู้ใช้งานทำการเปลี่ยนรหัสเอง (สามารถตั้งค่า การจัดการรหัสผ่าน)

๒. ส่งมอบรหัสผ่านชั่วคราว (Temporary Password) ให้กับผู้ใช้บริการ ด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓. เมื่อมีการส่งมอบรหัสผ่านตามข้อ ๕ (จ) (๒) ให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน และกำหนดและแจ้งผู้ใช้บริการให้ทำการเปลี่ยนรหัสผ่านใหม่

๔. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๕. แจ้งผู้ใช้งานไม่ให้ทำการบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๗. กำหนดให้ระบบแจ้งเตือนให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน

๘. กำหนดระยะเวลาการใช้งานระบบสารสนเทศภายในของสำนักงาน โดยผู้ใช้งานต้องใช้งานระบบสารสนเทศอย่างต่อเนื่อง หากว่างเว้นจากการใช้งานระบบสารสนเทศมากกว่า ๓๐ นาที หรือแล้วแต่ความเหมาะสมของระบบสารสนเทศนั้น ๆ โดยต้องกำหนดให้โปรแกรม Browser ปิดการทำงาน และกำหนดให้ผู้ใช้งานกรอกรหัสผู้ใช้งานและ รหัสผ่าน เพื่อเข้าสู่ระบบสารสนเทศใหม่

(ฉ) ผู้ดูแลระบบ ต้องควบคุมระบบซึ่งไวต่อการรบกวน (Sensitive or Critical system) มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน โดยต้องแยกระบบซึ่งไวต่อการรบกวน ออกจากระบบอื่น และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยจัดแบ่งโซนของเครือข่าย และติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่าง ๆ ของระบบไว้ในศูนย์คอมพิวเตอร์ หรือพื้นที่ปลอดภัย ที่ได้มีการจำกัดสิทธิผู้เข้าถึงทางกายภาพที่เหมาะสม

(ช) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานต่อสำนักงาน ดังนี้

๑. จำกัดการเข้าถึงระบบซึ่งไวต่อการรบกวนจากอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่ เฉพาะผู้ได้รับอนุญาต หรือโปรแกรมประยุกต์หรือแอปพลิเคชันที่ต้องเชื่อมต่อกันเท่านั้น และต้องกำหนดให้มีการระบุและยืนยันตัวตนผ่านระบบที่สำนักงานกำหนด เช่น AD (Active Directory), LDAP (Lightweight Directory Access Protocol), ระบบ SSO (Single Sign On) ของสำนักงานทุกครั้ง

๒. กำหนดให้มีการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากล ได้แก่ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อย หรือ XML Encryption ในส่วนการรับส่งข้อมูลผ่านเครือข่าย (encryption protocol) เข้าสู่ระบบซึ่งไวต่อการรบกวนเพื่อปฏิบัติงานจากภายนอกสำนักงาน

๓. กำหนดให้ใช้สายสัญญาณที่มีคุณสมบัติป้องกันสนามแม่เหล็กไฟฟ้า หรือใช้สายใยแก้วนำแสง (Fiber Optic) ติดตั้งท่อหุ้มสายชนิดควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel) และห้องพักสาย (Cable Room) และมีการตรวจสอบระบบสาย เพื่อตรวจจับอุปกรณ์แปลกปลอม

๔. จัดให้มีการบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๔.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้ระบบเครือข่ายไร้สายน้อยที่สุด

๓.๔.๒ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๓.๔.๓ ผู้ดูแลระบบต้องกำหนดค่า WPA หรือ WPA-๒ (Wi-Fi Protected Access) เป็นระดับเบื้องต้นในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๓.๔.๔ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุมการเข้าใช้งานระบบเครือข่ายไร้สาย โดยมีการพิสูจน์ตัวตนด้วยชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย หรือการระบุตัวตนด้วยวิธีอื่นใดตามที่กำหนดไว้เท่านั้น เพื่อให้เข้าใช้งานระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๓.๔.๕ ผู้ดูแลระบบควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สาย กับระบบเครือข่ายในสำนักงาน

๓.๔.๖ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งาน เข้าใช้บริการในระบบเครือข่ายไร้สาย ของสำนักงานด้วยช่องทางที่ปลอดภัยในการติดต่อสื่อสาร เช่น VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๓.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัย ของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นจากในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อผู้บังคับบัญชาส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลทราบทันที

๓.๔.๘ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของสำนักงาน

๓.๕ การควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓.๕.๑ ให้กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์คอมพิวเตอร์ ตรวจสอบกำหนดมาตรการ ควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง และให้สำนักงานสาขาทั้ง ๑๓ แห่ง แต่งตั้งเจ้าหน้าที่ควบคุมห้องคอมพิวเตอร์ (Server Room) และผู้ให้บริการภายนอก เพื่อควบคุมการเข้าถึง ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงาน

๓.๕.๒ ให้กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์คอมพิวเตอร์ กำหนดมาตรฐานและควบคุม ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมสำหรับศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และห้องคอมพิวเตอร์ (Server Room) ดังนี้

(๑) จัดให้มีระบบกล้องวงจรปิด (CCTV) บันทึกภาพการเข้า-ออกและเหตุการณ์ บริเวณพื้นที่ควบคุม โดยให้ถือว่าศูนย์คอมพิวเตอร์และห้องคอมพิวเตอร์เป็นพื้นที่หวงห้ามที่มีความสำคัญระดับวิกฤต (Critical Restricted Area) จึงต้องกำหนดนโยบายระยะเวลาการจัดเก็บข้อมูลภาพจากระบบกล้องวงจรปิด (CCTV Retention Policy) สำหรับพื้นที่ดังกล่าวอย่างเคร่งครัด โดยให้มีระยะเวลาจัดเก็บไม่น้อยกว่า ๖๐ วัน เพื่อให้มีข้อมูลหลักฐานที่เพียงพอสำหรับการตรวจสอบย้อนกลับ (Traceability) และรองรับกระบวนการสืบสวนสอบสวนกรณีเกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัย

(๒) ในกรณีที่สำนักงานมีการใช้บริการพื้นที่ศูนย์คอมพิวเตอร์ หรือบริการอื่นใด จากผู้ให้บริการภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางกายภาพ ต้องระบุเงื่อนไขการให้บริการ (SLA) หรือสัญญา (Contract) ให้ผู้ให้บริการภายนอกต้องดำเนินการจัดเก็บข้อมูลภาพจากกล้องวงจรปิด ให้สอดคล้อง และเป็นไปตามนโยบายและมาตรฐานระยะเวลาการจัดเก็บข้อมูลของสำนักงาน

(๓) ต้องกำหนดมาตรการกำกับดูแล ติดตาม และตรวจสอบผู้ให้บริการภายนอก ให้ปฏิบัติตามนโยบายและมาตรฐานระยะเวลาการจัดเก็บข้อมูลของสำนักงานอย่างเคร่งครัดและสม่ำเสมอ

๓.๕.๓ การอนุญาตใช้พื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่สำนักงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อผู้บังคับบัญชาส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ให้บริการอื่น ๆ

๓.๕.๔ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ให้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ให้บริการสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของสำนักงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System หรือ Intrusion System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงานในลักษณะที่ผิดปกติ

(๖) ผู้ดูแลระบบต้องดูแลการเข้าสู่ระบบเครือข่ายภายในสำนักงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวบุคคล (Authentication) เพื่อการตรวจสอบความถูกต้องของผู้ใช้งาน

(๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของสำนักงานจำเป็นต้องมีการป้องกันมิให้สำนักงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๘) การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะที่จำเป็น

(๙) ผู้ดูแลระบบต้องดำเนินการทบทวนกฎของระบบไฟร์วอลล์ (Firewall Rule Review) อย่างน้อยปีละ ๑ ครั้ง เพื่อคัดกรองและยกเลิกกฎที่ไม่ได้ใช้งาน (Unused Rules) หรือกฎที่ให้สิทธิการเข้าถึงเกินความจำเป็น (Overly Permissive Rules) รวมทั้งต้องตรวจสอบและปรับปรุงฐานข้อมูลรูปแบบภัยคุกคามของระบบตรวจจับและป้องกันการบุกรุก (IDS หรือ IPS Signatures) ให้เป็นปัจจุบัน พร้อมทั้งปรับแต่งระบบ (Tuning) เพื่อลดอัตราการแจ้งเตือนที่ผิดพลาด (False Positive) อย่างสม่ำเสมอ

๓.๕.๕ ผู้ดูแลระบบ ต้องบริการควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (System Software)

๓.๕.๖ ให้ผู้ดูแลระบบที่ดูแลความมั่นคงปลอดภัยสารสนเทศที่สำนักงานแต่งตั้งกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้อง และสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังนี้

(๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย ทั้งนี้การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๓) ควรตรวจสอบบันทึกการปฏิบัติงานหรือรายงานการเข้าถึงของผู้ใช้งานระบบสารสนเทศของสำนักงานอย่างสม่ำเสมอ

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๕) ให้กลุ่มระบบคอมพิวเตอร์และความมั่นคง ฝ่ายวิศวกรรมโครงสร้างพื้นฐาน กำหนดมาตรการควบคุมบุคคลจากสำนักงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสำนักงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บังคับบัญชาส่วนขึ้นตรงเลขาธิการด้านดิจิทัล

(๖) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมและมีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้

(ก) กำหนดให้มีการเข้ารหัสในลักษณะของ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อย สำหรับการเข้าถึงพอร์ตที่ใช้ปรับแต่งระบบ

(ข) กำหนดรหัสผู้ใช้และรหัสผ่านสำหรับผู้ที่มีสิทธิ

(ค) ติดตั้งอุปกรณ์สำหรับการป้องกันตรวจสอบระบบเครือข่ายจากภายนอก

(ง) กำหนดให้มีการระบุอุปกรณ์บนเครือข่ายต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน ดังนี้

๑. มีการจัดทำทะเบียนรายการเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๒. ทบทวนทะเบียนรายการเครื่องคอมพิวเตอร์และอุปกรณ์บนเครือข่ายอย่างสม่ำเสมออย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

(๗) ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ รวมถึงระบบสารสนเทศที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อสำนักงานต้องได้รับ การแยกออกจากระบบอื่น ๆ ดังนี้

(ก) แบ่งแยกเครือข่ายด้วยอุปกรณ์ป้องกันการบุกรุก (Firewall) โดยเฉพาะในส่วน of ระบบฐานข้อมูล และระบบโปรแกรมประยุกต์ (Application) ด้วยพอร์ตการใช้งานเฉพาะ

(ข) กำหนดกลุ่มของเครือข่ายเสมือน (VLAN) เพื่อแบ่งแยก

๑. ผู้ใช้งานระหว่างกลุ่มหรือสำนักงานหรือพื้นที่การใช้งาน

๒. กลุ่มผู้ใช้งานกับระบบสารสนเทศหลัก

๓. ระบบสารสนเทศหลักกับเครือข่ายภายนอก

(๘) การควบคุมการเชื่อมต่อทางเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างสำนักงาน ดังนี้

(ก) กำหนดให้แต่ละกลุ่มหรือสำนักงานภายในมีเครือข่ายเสมือนของตนเอง

(ข) การเชื่อมต่อระหว่างเครือข่ายกำหนดโดยอุปกรณ์สลับเส้นทางหลัก (Core Switch)

(ค) เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศของสำนักงาน

(๙) การควบคุมการจัดเส้นทางบนเครือข่าย มีดังนี้

(ก) กำหนดการควบคุมการจัดการเส้นทางบนเครือข่ายผ่านอุปกรณ์สลับเส้นทางหลัก (Core Switch)

(ข) เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศส่วนกลาง

(๑๐) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากกระยะทางไกล ต้องได้รับการอนุญาต จากผู้บังคับบัญชาส่วนงานขึ้นตรงเลขานุการด้านดิจิทัล

(๑๑) การเข้าสู่ระบบจากกระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(ก) การใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของสำนักงาน

(ข) ควบคุมและป้องกันการใช้งานพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

๑. ผู้ใช้งานต้องมีการขออนุญาตเข้าถึงพอร์ตดังกล่าวอย่างเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบต้องควบคุมให้มีการบันทึกการเข้าใช้งานทุกครั้ง รวมถึงตรวจสอบ บันทึกการเข้าใช้งานอย่างสม่ำเสมอ

๓. ผู้ดูแลระบบต้องเปิดพอร์ตสื่อสาร (Port) เท่าที่จำเป็นต้องใช้งานเท่านั้น โดยผู้ดูแลระบบต้องดำเนินการตรวจสอบพอร์ตสื่อสาร (Port) และปิดพอร์ตสื่อสาร (Port) ที่ไม่มีความจำเป็นในการใช้งานของระบบหรืออุปกรณ์ และกรณีที่ต้องใช้งานพอร์ตสื่อสาร (Port) จะต้องมีการยืนยันตัวตนทุกครั้ง ก่อนอนุญาตให้ใช้งาน

๓.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๖.๑ ให้กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์คอมพิวเตอร์ ควบคุมการเข้าถึงระบบปฏิบัติการ โดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) ควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต และอนุญาตให้มีการใช้งานได้ เฉพาะผู้ใช้งานที่ได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษร

(๒) ควบคุมให้ไม่มีการเปิดเผยข้อมูลที่เกี่ยวข้องกับระบบหรือแอปพลิเคชันจนกว่าผู้ใช้งานจะผ่านขั้นตอนการยืนยันตัวตนเพื่อเข้าใช้งานระบบอย่างสมบูรณ์

(๓) ควบคุมให้มีการแจ้งเตือนโดยระบุว่าอนุญาตเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ที่มีสิทธิเข้าใช้งาน และให้มีการบันทึกล็อก (Log) การเข้าใช้งานทุกครั้ง ที่ผู้ใช้งานทำการเข้าถึงระบบทั้งที่ดำเนินการสำเร็จ และดำเนินการไม่สำเร็จ

(๔) ระงับการล็อกอินเป็นระยะเวลาตามที่กำหนดหากตรวจสอบพบว่ามีกรยืนยันตัวตน ไม่ถูกต้องติดต่อกัน

(๕) ควบคุมไม่ให้มีการส่งรหัสผ่านโดยไม่มีการเข้ารหัสระหว่างการยืนยันการเข้าถึงระบบหรือแอปพลิเคชันผ่านระบบเครือข่าย

(๖) ควบคุมให้มีการตัดการใช้งาน หลังจากที่ไม่มิกิจกรรมการใช้งานเป็นเวลาอย่างน้อย ๓๐ นาที หรือตามความจำเป็นของระบบสารสนเทศที่กำหนด

๓.๖.๒ ผู้ดูแลระบบต้องควบคุมให้มีการระบุและยืนยันตัวตนด้วยชื่อผู้ใช้งาน ดังนี้

(๑) ต้องกำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคล เพื่อใช้ในการยืนยันตัวตนในการเข้าถึงระบบสารสนเทศ

(๒) ต้องควบคุมให้มีการยืนยันตัวตนของผู้ใช้งานผ่านระบบที่สำนักงานกำหนด เช่น AD (Active Directory), LDAP (Lightweight Directory Access Protocol), ระบบ SSO (Single Sign On) ของสำนักงานทุกครั้ง พร้อมบันทึกข้อมูลการเข้าถึง

(๓) ในกรณีที่มีความจำเป็นต้องมีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared User ID) ผู้ใช้งานต้องได้รับการอนุมัติจากผู้บังคับบัญชา และต้องมีตรวจสอบการใช้งานของบัญชีผู้ใช้งานดังกล่าวอย่างสม่ำเสมอ

๓.๖.๓ ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งรองรับการบริหารจัดการรหัสผ่าน อย่างน้อย ดังนี้

(๑) การตั้งบัญชีผู้ใช้งานของแต่ละบุคคล

(๒) การกำหนดรหัสผ่านที่มีความซับซ้อน

(๓) การเปลี่ยนรหัสผ่านตามรอบที่กำหนด

(๔) ไม่อนุญาตให้ใช้รหัสผ่านซ้ำตามจำนวนครั้งที่กำหนด

(๕) ตัดการเชื่อมต่อหากตรวจสอบพบว่ามีกำรยืนยันตัวตนไม่ถูกต้องติดต่อกัน

(๖) ไม่แสดงรหัสผ่านจริงบนหน้าจอในขณะที่มีการเข้าสู่ระบบรับส่ง และเก็บรหัสผ่านแยกจากข้อมูลอื่นในรูปแบบที่ปลอดภัย โดยการเข้ารหัส

๓.๖.๔ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทมัลแวร์ประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ดังนี้

(๑) ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมมัลแวร์ประโยชน์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของสำนักงาน เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา โดยต้องพิจารณาให้สิทธิตามหน้าที่ความรับผิดชอบและความจำเป็นที่ต้องใช้งานเท่านั้น และโปรแกรมมัลแวร์ประโยชน์ที่นำมาใช้ จะต้องถูกต้องตามลิขสิทธิ์การใช้งาน

(๒) หากโปรแกรมมัลแวร์ประโยชน์ใด ๆ จำเป็นต้องใช้สิทธิสูงในการดำเนินงานจะต้องมีการบันทึก จัดเก็บหลักฐานในการขอใช้สิทธิระดับสูงเพื่อการทบทวนและตรวจสอบสิทธิตามรอบการทบทวนสิทธิที่สำนักงานได้กำหนด

(๓) ต้องมีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมมัลแวร์ประโยชน์ และตรวจสอบอย่างสม่ำเสมอ

(๔) ต้องทำการเพิกถอนหรือระงับโปรแกรมมัลแวร์ประโยชน์เมื่อไม่จำเป็นต้องใช้งาน

๓.๖.๕ ผู้ดูแลระบบต้องให้ยุติการใช้งานระบบสารสนเทศนั้น เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-Out) ดังนี้

(๑) กำหนดให้มีการตัดการใช้งาน หลังจากที่ไม่มิกิจกรรมการใช้งานอุปกรณ์ที่เชื่อมต่อเข้าระบบสารสนเทศเป็นเวลา ๓๐ นาทีโดยอัตโนมัติ หรือแล้วแต่ความเหมาะสมของระบบสารสนเทศ

(๒) หากระบบไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติต้องกำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่าน หรือกำหนดให้มีการล็อกหน้าจอหลังจากไม่มีการใช้งานเป็นเวลา ๑๐ นาที

๓.๖.๖ ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ หรือโปรแกรมประเภทมัลแวร์ประโยชน์ที่มีความเสี่ยงสูง หรือมีความสำคัญสูง ดังนี้

(๑) การเข้าถึงระบบสารสนเทศหรือโปรแกรมประเภทรถประโยชน์ที่มีความเสี่ยงสูง หรือมีความสำคัญสูงทั้งจากภายในสำนักงาน และการใช้งานในสถานที่สาธารณะหรือพื้นที่นอกสำนักงาน ต้องกำหนดให้มีการยืนยันตัวตนซ้ำหลังจากเข้าใช้งานต่อเนื่องอย่างน้อยทุก ๘ ชั่วโมง

(๒) กำหนดให้มีการตัดการใช้งานหรือการเชื่อมต่อผ่านระบบอินเทอร์เน็ต หรือเครือข่ายเสมือน (VPN) หลังจากที่ไม่มีการใช้งานเป็นเวลา ๑๕ นาที

๓.๗ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๗.๑ ผู้ดูแลระบบ ต้องควบคุมให้มีการติดตั้งโปรแกรมป้องกันไวรัสในอุปกรณ์ คอมพิวเตอร์และสื่อสารเคลื่อนที่ และต้องปรับปรุงให้โปรแกรมดังกล่าวทันสมัยอยู่เสมอ

๓.๗.๒ ผู้ดูแลระบบต้องมีการเข้ารหัสไฟล์ข้อมูลที่มีการเข้ารหัสอัลกอริทึม (Algorithm) ที่เป็นมาตรฐานสากล ได้แก่ Triple DES หรือ RSA ในส่วนการจัดเก็บข้อมูล (file encryption) ที่มีความสำคัญ ต่อสำนักงาน

๓.๗.๓ ผู้ดูแลระบบ ต้องควบคุมให้มีการระบุและยืนยันตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของหน่วยงานจากภายนอกสำนักงาน ผ่านระบบ Active Directory หรือ Lightweight Directory Access Control ของสำนักงานทุกครั้ง

๓.๗.๔ ผู้ดูแลระบบ ต้องดำเนินการทบทวนสิทธิในการเข้าถึงของผู้ใช้งานจากภายนอก สำนักงานอย่างสม่ำเสมอ

๓.๘ การปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย (กรณีการเข้าถึงระบบ โดยไม่ได้รับอนุญาต)

๓.๘.๑ เมื่อผู้ดูแลระบบได้รับแจ้งเหตุให้วิเคราะห์ว่าเป็นเหตุละเมิดประเภทใด เกิดผลกระทบอย่างไร มีวิธีการรับมืออย่างไรบ้าง

๓.๘.๒ ผู้ดูแลระบบรายงานให้บุคคลและสำนักงานที่เกี่ยวข้องรับทราบทันที ตามขั้นตอน การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal data breach management procedure)

๓.๘.๓ ผู้ดูแลระบบปฏิบัติตามวิธีรับมือกับเหตุละเมิดตามความเหมาะสม ในกรณีนี้ อาจได้แก่การเปลี่ยนแปลงรหัสผ่าน การแยกระบบที่มีปัญหาออกจาการบริการที่สงสัย การปิดเส้นทาง การเข้าสู่ระบบสารสนเทศ การยกเลิกบัญชีผู้ใช้งานที่ถูกใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต ในบางกรณี เจ้าหน้าที่ที่เกี่ยวข้องจะต้องค้นหาและจับกุมผู้ก่อเหตุละเมิด

๓.๘.๔ ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องรวบรวมข้อมูลและหลักฐานของเหตุการณ์

๓.๘.๕ ผู้ดูแลระบบตรวจสอบว่าวิธีการรับมือที่ใช้ได้ผลหรือมีประสิทธิภาพหรือไม่ แล้วเพิ่มเติมมาตรการเพื่อลดช่องโหว่ หรือถอดแยกส่วนของระบบสารสนเทศที่มีปัญหาออก

๓.๘.๖ ผู้ดูแลระบบกู้คืนระบบสารสนเทศสู่สภาพเดิม และทำรายงานแจ้งผู้ที่เกี่ยวข้อง

๓.๙ การปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย

หลังจากเกิดเหตุละเมิดความมั่นคงปลอดภัย กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์ คอมพิวเตอร์หรือกลุ่มงานที่ได้รับมอบหมายจากฝ่ายวิศวกรรมโครงสร้างพื้นฐาน จะต้องปฏิบัติตามกระบวนการ ดังนี้

(๑) รวบรวมการเรียนรู้รูปแบบของสถานการณ์ วิเคราะห์รายงานเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

(๒) สำนวจความเสียหายที่เกิดจากเหตุละเมิดการรักษาความมั่นคงปลอดภัย ตรวจสอบสาเหตุและจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ทำรายงานและทบทวนมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง เสนอคณะกรรมการเพื่อพิจารณา

๓.๑๐ การสำรองข้อมูล

การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม เจ้าหน้าที่ผู้ดูแลระบบจะต้องปฏิบัติ ดังนี้

(๑) พิจารณาและจัดหมวดหมู่ของข้อมูล โดยกำหนดระดับความสำคัญของข้อมูล ที่จำเป็นต้องทำสำรอง

(๒) สำหรับข้อมูลที่มีความลับสูงให้ทำการเข้ารหัสก่อนทำการสำรอง

(๓) พิจารณากำหนดวิธีการสำรองในประเด็น ดังนี้

(ก) ขนาด (สำรองทั้งหมดหรือสำรองเฉพาะส่วนที่แตกต่าง)

(ข) ความถี่ของการสำรอง ควรกำหนดโดยคำนึงถึงความต้องการใช้หากข้อมูลสูญหายหรือเรียกใช้งานไม่ได้ และความจำเป็นของข้อมูลเพื่อให้ธุรกิจของสำนักงานดำเนินต่อไปได้อย่างไม่ติดขัดหรือเพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

(ค) วางขั้นตอนการเรียกกลับมาใช้อย่างเป็นลายลักษณ์อักษร

(๔) ระหว่างทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติ ดังนี้

(ก) ตรวจสอบผลการสำรองข้อมูล ว่าได้ข้อมูลที่ต้องการและครบถ้วนสมบูรณ์หรือไม่

(ข) จัดทำบันทึกการสำรองข้อมูลให้ชัดเจนครบถ้วนสมบูรณ์ และง่ายต่อการสืบค้น

(๕) หลังทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติ ดังนี้

(ก) เก็บข้อมูลที่สำรองเอาไว้ในพื้นที่ที่ห่างออกไปไกลพอที่จะไม่ได้รับความเสียหายอันเกิดจากภัยพิบัติในพื้นที่หลัก

(ข) ข้อมูลที่สำรองจะต้องได้รับการป้องกันทั้งทางกายภาพและสภาพแวดล้อมที่เหมาะสมตามมาตรฐานเดียวกับที่ใช้ในข้อมูลหลัก มาตรการที่ใช้ป้องกันสื่อบันทึกข้อมูลในพื้นที่หลักก็ควรนำมาใช้กับพื้นที่สำรองด้วย

(ค) ทำการทดสอบสื่อบันทึกข้อมูลสำรองและขั้นตอนในการนำข้อมูลสำรองกลับมาใช้ ควรได้รับการตรวจสอบและทดสอบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้มั่นใจว่ามีประสิทธิภาพเพียงพอและสามารถทำได้เสร็จสิ้นภายในระยะเวลาที่ถูกจัดสรรไว้ตามกระบวนการกู้คืน เพื่อให้มั่นใจว่าสามารถนำข้อมูลกลับมาใช้อีกได้เมื่อเกิดเหตุการณ์ฉุกเฉินจริง

(ง) จัดหาตู้เก็บหรือที่จัดเก็บสื่อบันทึกข้อมูลสำรอง เพื่อให้เป็นหมวดหมู่ และเป็นระเบียบ เรียบร้อย ง่ายต่อการค้นหาหรือนำกลับมาใช้ และจัดให้มีการควบคุมการนำสื่อบันทึกไปใช้ที่สามารถตรวจสอบได้

๓.๑๑ การสำรองและกู้คืนข้อมูล

๓.๑๑.๑ รับผิดชอบในการสำรองและกู้คืนข้อมูลต้องมีขั้นตอนปฏิบัติ ดังนี้

(๑) ผู้อำนวยการฝ่ายวิศวกรรมโครงสร้างพื้นฐาน เป็นผู้กำกับดูแลการปฏิบัติงานในการสำรอง และกู้คืนข้อมูล และกำหนดแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๒) ผู้ดูแลระบบ ที่ได้รับมอบหมายจากฝ่ายวิศวกรรมโครงสร้างพื้นฐาน เป็นเจ้าหน้าที่ผู้ปฏิบัติงานในการสำรองและกู้คืนข้อมูล และเป็นผู้จัดทำวิธีปฏิบัติการสำรองและกู้คืนข้อมูลของสำนักงาน

๓.๑๑.๒ ผู้ดูแลระบบร่วมกับผู้บังคับบัญชา ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

(๑) ดำเนินการวิเคราะห์และคัดเลือกระบบที่มีความสำคัญสูง

(๒) ดำเนินการวิเคราะห์เหตุการณ์ที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัด หรือไม่สามารถทำงานได้อันเป็นผลมาจากภัยพิบัติ

(๓) ดำเนินการวิเคราะห์ผลกระทบอันเป็นผลมาจากภัยพิบัติต่อระบบที่มีความสำคัญสูง

(๔) ผู้ดูแลระบบ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ

(๕) ผู้ดูแลระบบ ต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และดำเนินการปรับปรุงแผนให้เป็นปัจจุบัน โดยในการทดสอบ ผู้ดูแลระบบต้องสื่อสารแผนเตรียมความพร้อมกรณีฉุกเฉินให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ และผู้ใช้งานที่เกี่ยวข้องกับแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องเข้าร่วมการทดสอบแผน และดำเนินงานตามแผนที่กำหนดไว้เมื่อเกิดเหตุการณ์ฉุกเฉิน

๓.๑๒ การสร้างความตระหนัก

ผู้รับผิดชอบต้องอบรม เรียนรู้เพื่อสร้างความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ ดังนี้

(๑) ผู้ดูแลระบบต้องมั่นฝึกอบรม เรียนรู้ในส่วนของงานที่รับผิดชอบในด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง และนำมาประยุกต์ใช้อย่างเคร่งครัด เสมอ

(๒) ผู้บังคับบัญชาส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลเป็นผู้ให้การสนับสนุนในการอบรมสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศอย่างน้อย ๑ ครั้งต่อปี

(๓) ผู้รับผิดชอบการอบรม ต้องมีการจัดเก็บบันทึกเอกสารในการจัดฝึกอบรมไว้เป็นหลักฐานด้วย เช่น บันทึกการฝึกอบรม เอกสารฝึกอบรม

๓.๑๓ การตรวจสอบและการประเมินผล

๓.๑๓.๑ สำนักงานต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยผู้ตรวจสอบภายใน (internal auditor) เพื่อให้สำนักงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ และเพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ รวมถึงจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ โดยต้องมีการวางแผนการตรวจสอบ และกำหนดกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ

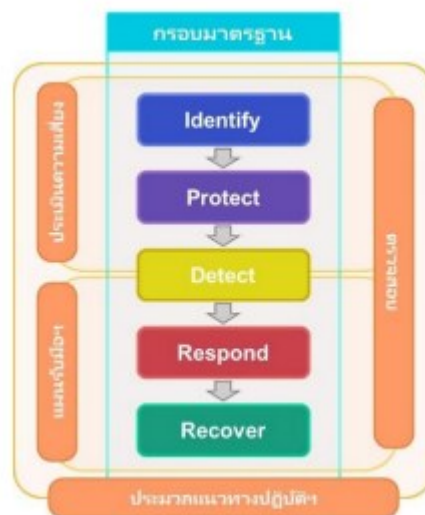
๓.๑๓.๒ สำนักงานต้องควบคุมการเข้าถึงและใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ และประเมินความเสี่ยง เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) เพื่อลด

ความเสี่ยงที่อาจเกิดขึ้นกับระบบ เช่น การหยุดชะงักของการให้บริการ การใช้งานผิดประเภท หรือถูกละเมิดการใช้งาน

๓.๑๔ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑๔.๑ การจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังนี้

- (๑) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (๒) ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคง ปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้
 - (ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
 - (ข) บริการที่สำคัญที่สำนักงานเป็นเจ้าของและใช้หรือให้บริการ ตามผลการวิเคราะห์ในข้อ ๓.๑๔.๑ (๒) (ก)
 - (๓) จัดส่งผลสรุปรายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์เสนอสำนักงานหรือคณะกรรมการที่กำกับดูแล



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑๔.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ เพื่อให้สำนักงานสามารถประเมิน ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ และต่อเนื่อง สำนักงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงาน ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

- (๑) การประเมินความเสี่ยง (Risk Assessment)

(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการ ปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการทำงาน และการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

(๒) การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมิน ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

(๓) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยอมรับได้ตามที่กำหนดไว้

(๔) การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากลอย่างมีนัยสำคัญ

๓.๑๔.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

แนวปฏิบัติ

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

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

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่า สำนักงานจะปฏิบัติตามภาระหน้าที่ ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจน ภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

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

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติ การบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ เช่น ผู้ขายสำหรับบริการ ด้านนิติวิทยาศาสตร์ หรือการกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(ณ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุ และแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพ ไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของสำนักงาน

(๓) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

(๔) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของสำนักงาน

๓.๑๔.๔ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) กรอบมาตรฐาน ประกอบไปด้วย ๕ หัวข้อหลัก (ดังรูปที่ ๑) ดังนี้

(ก) การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

(ข) การจัดการทรัพย์สิน (Asset Management)

(ค) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(ง) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(จ) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(๒) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

(ก) การควบคุมการเข้าถึง (Access Control)

(ข) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ค) การเชื่อมต่อระยะไกล (Remote Connection)

(ง) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(จ) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ฉ) การแบ่งปันข้อมูล (Information Sharing)

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
โดยการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
(Respond)

(ก) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident
Response Plan)

(ข) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(ค) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์
(Recover)

(ก) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์
(Cybersecurity Resilience and Recovery)

(ข) การสื่อสารและประสานงานระหว่างกระบวนการฟื้นฟู (Recovery
Communications)

(ค) การทบทวนและปรับปรุงแผนฟื้นฟู (Recovery Improve)

๓.๑๔.๕ หัวข้อหลักที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์
ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกาย
ของบุคคล (Identify)

กรอบมาตรฐาน

(๑) การจัดการทรัพย์สิน (Asset Management)

(ก) ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ
ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สิน
ให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

๑. ชื่อหรือคำอธิบายของทรัพย์สิน บริการที่สำคัญของสำนักงาน

๒. ฟังก์ชันที่สำคัญของทรัพย์สิน บริการที่สำคัญของสำนักงาน

๓. การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญ

ของสำนักงาน

๔. เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน บริการที่สำคัญของสำนักงาน

๕. ตำแหน่งทางกายภาพของทรัพย์สิน บริการที่สำคัญของสำนักงาน

๖. การขึ้นต่อกันของทรัพย์สิน บริการที่สำคัญของสำนักงานบนระบบ

หรือเครือข่ายภายใน และ/หรือภายนอก

(ข) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของสำนักงานและระบบ
คอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

(ค) ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง
หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของสำนักงาน ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

(ง) ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์ของบริการที่สำคัญของสำนักงาน ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน
ในข้อ ๓.๑๔.๕ (๑) (ก) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

(๒) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(ก) ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของสำนักงานทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

(ข) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังนี้

๑. วันที่ระบุความเสี่ยง (Date the Risk is Identified)
๒. คำอธิบายของความเสี่ยง (Description of the Risk)
๓. โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
๔. ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
๕. การจัดการความเสี่ยง (Risk Treatment)
๖. เจ้าของความเสี่ยง (Risk Owner)
๗. สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
๘. ความเสี่ยงที่เหลือ (Residual Risk)

(๓) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(ก) ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของสำนักงาน อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญของสำนักงาน ซึ่งเป็น

๑. ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
๒. ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial

Control System: ICS)

(ข) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

๑. การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
๒. การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
๓. การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

(ค) ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของสำนักงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของสำนักงาน การเปลี่ยนแปลงระบบที่สำคัญ

ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

(ง) ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของสำนักงาน โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

(จ) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชัน บริการที่สำคัญของสำนักงาน โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

(ฉ) ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ บริการที่สำคัญของสำนักงาน ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบ ที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

(ช) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรอง และได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบ ที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และ วิธีการที่หน่วยงาน ควบคุมหรือกำกับดูแลกำหนด

(ซ) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการ ทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

(ฌ) ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุไว้ในผลการประเมินช่องโหว่และในการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

(๔) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(ก) ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแล รักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอก จะดำเนินงานใด ๆ ก็ตามในส่วนของการบริการที่สำคัญของสำนักงาน

(ข) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้อง กับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญา กับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑. ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของสำนักงานตามความต้องการทางธุรกิจของสำนักงาน และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของสำนักงานจากภัยคุกคามทางไซเบอร์

๓. ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๔. สิทธิของสำนักงาน ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์
ของผู้ให้บริการภายนอก

(ค) ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการ
ภายนอกว่า สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา เช่น การตรวจสอบโดย
บุคคลที่สามและการตรวจสอบผลิตภัณฑ์

(ง) ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้อง
กับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๓.๑๔.๖ หัวข้อหลักที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

กรอบมาตรฐาน

(๑) การควบคุมการเข้าถึง (Access Control)

(ก) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของสำนักงานถูกจำกัดไว้
ดังนี้

๑. บุคลากรและกิจกรรมที่ได้รับอนุญาต

๒. อุปกรณ์และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

(ข) ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๓.๑๔.๖ (๑) (ก) สำนักงาน
ต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ
ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญของสำนักงาน

(ค) ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access)
และความพยายาม ทั้งหมดในการเข้าถึงบริการที่สำคัญของสำนักงาน และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรม
ที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอ
ของกิจกรรมการเข้าถึงดังกล่าว

(ง) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการ
ที่สำคัญของสำนักงาน เช่น USB พอร์ตอนุกรม และ การเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแล ดังนี้

๑. ทำภายใต้การดูแลของสำนักงานทางสารสนเทศเท่านั้น

๒. ดำเนินการในสถานที่ หากเป็นไปได้

(๒) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ก) ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย
(Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย
ทั้งหมดของบริการที่สำคัญของสำนักงานที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Risk Profile) ของบริการที่สำคัญของสำนักงาน

(ข) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security
Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

๑. สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒. การแบ่งแยกหน้าที่ (Separation of Duties)

๓. การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔. การลบบัญชีที่ไม่ได้ใช้

๕. การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖. การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗. การป้องกันมัลแวร์ (Malware)

๘. การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัย

ของระบบอย่างทันการณ์และเหมาะสม

(ค) ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพยากรใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของสำนักงาน

(ง) ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของสำนักงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพ ต่อภัยคุกคามทางไซเบอร์

(จ) ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของสำนักงาน

(๓) การเชื่อมต่อระยะไกล (Remote Connection)

(ก) ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของสำนักงาน มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(ข) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของสำนักงานต้องปฏิบัติตามแนวทางปฏิบัติ ดังนี้

๑. ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

๒. ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

๓. ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp

๔. ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการทำงานของบริการที่สำคัญของสำนักงาน เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

๕. จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

(๔) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(ก) ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แฟลชไดรฟ์ กับบริการที่สำคัญของสำนักงาน โดยใช้มาตรการอย่างน้อย ดังนี้

๑. ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒. ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๓.๑๔.๖ (๔) (ก) ๑. เท่านั้น

๓. ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของสำนัก

(ข) ต้องเข้ารหัสข้อมูลที่จะเฝ้าติดตามทั้งหมดของบริการที่สำคัญของสำนักงานบนสื่อบันทึกข้อมูลแบบถอดได้

(๕) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ก) ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังนี้

๑. กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

๑.๑ พนักงานใหม่ (New Employees)

๑.๒ ผู้ใช้และระดับบริหาร (Users and Management)

๑.๓ เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เช่น ผู้ให้บริการ IT และ ICS

๑.๔ ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

๒. การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของสำนักงาน

๓. การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนว ปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔. การสื่อสารอย่างสม่ำเสมอและทันทั่วถึงที่ครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

(ข) ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

(๖) การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของสำนักงาน และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของสำนักงาน เพื่อให้สามารถ

ใช้มาตรการป้องกันที่จำเป็นได้ ทั้งนี้รายละเอียด แนวทาง และรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐาน ในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงาน ประกาศกำหนด

๓.๑๔.๗ หัวข้อหลักที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

กรอบมาตรฐาน

(๑) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(ก) ต้องสร้างกลไกและกระบวนการเพื่อ

๑. ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมด ที่เกี่ยวข้องกับการบริการที่สำคัญของสำนักงาน

๒. การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ที่ตรวจพบ

๓. การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศหรือไม่

(ข) ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๓.๑๔.๗ (๑) (ก) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๓.๑๔.๘ หัวข้อหลักที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

กรอบมาตรฐาน

(๑) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

(ก) ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือ ภัยคุกคาม ทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการ ได้อย่างมีประสิทธิภาพและประสิทธิผล

(ข) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๑. ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤต ที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

๒.๑ จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒.๒ ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๒.๓ ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์ จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๒.๔ ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทน ของสำนักงานเมื่อกล่าวแถลง กับสื่อมวลชน

๒.๕ ระบุแพลตฟอร์มหรือช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อ
ดั้งเดิม และโซเชียลมีเดีย สำหรับการเผยแพร่ข้อมูล

๓. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึง
การประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกัน
ในช่วงวิกฤต

๔. ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อย
ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิภาพ
ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๓.๑๔.๙ หัวข้อหลักที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคาม
ทางไซเบอร์ (Recover)

กรอบมาตรฐาน

(๑) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์
(Cybersecurity Resilience and Recovery)

(ก) ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
เพื่อให้แน่ใจว่าบริการที่สำคัญของสำนักงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก
เนื่องจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผน
ของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของสำนักงาน เช่น ความสอดคล้องกัน
ของขอบเขตค่านิยมและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption
(MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) และให้เป็นไปตามหลักเกณฑ์
และวิธีการที่สำนักงานประกาศกำหนด

(ข) ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง
เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๓.๑๕ การรักษาความมั่นคงปลอดภัยระบบคลาวด์

ผู้ดูแลระบบที่มีหน้าที่กำกับดูแลการใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ ต้องปฏิบัติตาม
ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ดังนี้

๓.๑๕.๑ การกำกับดูแลและบริหารจัดการผู้ให้บริการคลาวด์ (Cloud Security
Governance)

(๑) ต้องกำหนดข้อตกลงระดับการให้บริการ (SLA) และเงื่อนไขสัญญา
ที่ระบุบทบาทความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศระหว่างสำนักงาน (ผู้ให้บริการ)
และผู้ให้บริการคลาวด์อย่างชัดเจน

(๒) ต้องร้องขอและตรวจสอบหลักฐานการรับรองมาตรฐานด้านความมั่นคง
ปลอดภัยจากผู้ให้บริการคลาวด์ เช่น ISO/IEC 27001, 27017, 27018, 27701 หรือ CSA STAR โดยต้องเป็น
รายงานการตรวจสอบอิสระ (Independent Review) หรือเอกสารรับรองตามมาตรฐานสากลที่มีระบุขอบเขต
ในการรับรองอย่างชัดเจน

(๓) ต้องมีกระบวนการตรวจสอบและติดตามการเปลี่ยนแปลงระบบ
(Change Management) ของผู้ให้บริการคลาวด์ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ
ของสำนักงาน

๓.๑๕.๒ การควบคุมการเข้าถึงและการเข้ารหัสข้อมูล (Access Control & Cryptography)

(๑) ต้องใช้เทคนิคการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ (Cloud Administrator) ทุกครั้ง

(๒) ต้องมีการเข้ารหัสข้อมูล (Encryption) ที่มีความแข็งแรงเพียงพอทั้งข้อมูลขณะจัดเก็บ (Data at rest) และระหว่างโอนถ่าย (Data in transit)

(๓) การจัดการกุญแจเข้ารหัส (Key Management) ในกรณีที่สำนักงานใช้กุญแจเข้ารหัสของตนเอง ห้ามมิให้ผู้ให้บริการคลาวด์เป็นผู้จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสนั้น

๓.๑๕.๓ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical & Environment Security)

(๑) การกำหนดตำแหน่งศูนย์ข้อมูล (Data Center Location) ต้องใช้ศูนย์ข้อมูลหลักที่ตั้งอยู่ในประเทศไทย (Data Localization) และศูนย์ข้อมูลสำรองต้องอยู่ในประเทศไทย หรือภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้ที่สุด รวมถึงสิงคโปร์และฮ่องกง

(๒) ต้องตรวจสอบให้แน่ใจว่าผู้ให้บริการคลาวด์มีขั้นตอนการทำลายข้อมูลหรือสื่อจัดเก็บข้อมูลที่มีข้อมูลส่วนบุคคลอย่างปลอดภัย และไม่สามารถกู้คืนได้เมื่อสิ้นสุดการใช้งาน

๓.๑๕.๔ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

(๑) ต้องควบคุมให้ผู้ให้บริการคลาวด์มีการแยกสภาพแวดล้อม (Segregation) สำหรับการพัฒนา (Development), การทดสอบ (Testing) และการปฏิบัติงานจริง (Production) ออกจากกันอย่างเด็ดขาด

(๒) ต้องตรวจสอบให้แน่ใจว่ามีการแบ่งแยกผู้เช่า (Tenant Isolation) อย่างชัดเจนในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน (Public Cloud)

(๓) ต้องจัดให้มีการบันทึกเหตุการณ์ (Audit Log) ที่ครอบคลุมการเปลี่ยนแปลงข้อมูลและเก็บรักษานับที่กตามระยะเวลาที่กฎหมายกำหนด (Log Retention) พร้อมจำกัดการเข้าถึงบันทึกดังกล่าว

๓.๑๕.๕ การจัดการเหตุภัยคุกคามทางสารสนเทศระบบคลาวด์ (Cloud Incident Management) ต้องระบุขอบเขตและขั้นตอนการแจ้งเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศร่วมกับผู้ให้บริการคลาวด์ รวมถึงกำหนดระยะเวลาเป้าหมาย (SLA) ที่ผู้ให้บริการต้องแจ้งให้สำนักงานทราบเมื่อเกิดเหตุ

หมวด ๔

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

๔.๑ การปฏิบัติการเข้าออกพื้นที่ภายในสำนักงาน

๔.๑.๑ บุคคลภายนอกที่มีความจำเป็นจะต้องติดต่อสำนักงาน จะต้องติดบัตรผู้มาติดต่อจากเจ้าหน้าที่รักษาความปลอดภัยของทางอาคารที่ทางบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด รับผิดชอบ และต้องติดบัตรผ่านตรงจุดที่สามารถมองเห็นได้ชัดเจน

๔.๑.๒ บุคคลภายนอกที่มีความจำเป็นจะต้องนำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตที่สำนักงานให้บริการ จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์เชื่อมต่อ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนามในการอนุญาตหรือพิสูจน์ตัวตนของบุคคลภายนอกก่อนทำการเชื่อมต่ออินเทอร์เน็ต โดยต้องไม่กระทำ ดังนี้

(๑) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

(๒) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นเฉพาะไปเปิดเผย โดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่ดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์

(๔) และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๕) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน

(๖) ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๗) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่น

(๘) ถูกกระทบ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๙) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยไม่ปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(๑๐) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ ของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อ ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้ เพื่อประโยชน์สาธารณะ

๔.๑.๓ บุคคลภายนอกที่มีความจำเป็นจะต้องเข้าออกศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และห้องคอมพิวเตอร์ (Server Room) ต้องนำบัตรผู้ติดต่อที่ได้จากเจ้าหน้าที่รักษาความปลอดภัยของทางอาคาร หรือผู้ดูแลพื้นที่ภายในสำนักงาน โดยสิทธิจะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าไปยังพื้นที่ปฏิบัติงานภายในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และห้องคอมพิวเตอร์ (Server Room) นั้น ๆ

๔.๑.๔ บุคคลภายนอกจะต้องมีเจ้าหน้าที่ติดตาม (Escort) ตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในพื้นที่ของสำนักงาน และ สำนักงานจะต้องจัดทำทะเบียนคุมสำหรับลงบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญและวัตถุประสงค์ของบุคคลภายนอก

๔.๒ การกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสำนักงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานได้ ดังนี้

๔.๒.๑ ทำการเชื่อมต่อระบบเครือข่ายภายในกับระบบเครือข่ายภายนอกสำนักงาน ด้วยการใช้เทคโนโลยีที่เรียกว่า Secure Socket Layer VPN หรือ SSL-VPN โดยการนำโครงข่ายสาธารณะมาใช้เป็นสื่อในการส่งข้อมูลระหว่างบุคคลภายนอกและระบบงานภายในสำนักงาน โดยใช้การเข้ารหัสข้อมูลสร้างเป็นระบบเครือข่ายเสมือนขึ้น ซึ่งเป็นการทำ VPN ในระดับ Application Layer ผ่านพอร์ต ๔๔๓ โดยจะใช้กลไกในการแลกเปลี่ยน Key สำหรับการเข้ารหัสข้อมูล โดยจะรับ Public Key ที่ถูกแจกจ่ายมาผ่านทาง Certificate Authority (CA) เพื่อใช้ในการถอดรหัสจาก Private Key ที่อุปกรณ์ที่เปิดใช้งาน SSL VPN ทำให้สามารถควบคุมและกำหนดสิทธิการเข้าใช้งานระบบงานภายในของสำนักงาน ในแต่ละบุคคลได้โดยสามารถระบุชนิดของ Application ที่ผู้ใช้งานแต่ละคนสามารถใช้ได้

๔.๒.๒ บุคคลภายนอกที่ต้องการขอใช้บริการการตรวจสอบข้อมูลหรือใช้ระบบสารสนเทศของสำนักงานผ่านระบบเครือข่ายเสมือน (VPN) ต้องผ่านตรวจสอบตามขั้นตอนที่ทางสำนักงานกำหนดเพื่อระบุตัวตนของผู้ใช้งาน โดยฝ่ายวิศวกรรมโครงสร้างพื้นฐาน จะเป็นผู้ตรวจสอบและเก็บหลักฐานการระบุตัวตนของบุคคลภายนอกที่ใช้งาน

๔.๒.๓ บุคคลภายนอกที่ได้รับชื่อผู้ให้รหัสผ่านในการเข้าใช้บริการ VPN ต้องรักษาไว้ซึ่งความลับของชื่อผู้ให้รหัสผ่านและไม่เผยแพร่ให้ผู้อื่นรับทราบ หากมีเกิดความเสียหายต่อสำนักงานบุคคลภายนอกที่ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
