ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล
พ.ศ. ๒๕๖๙

โดยที่เป็นการสมควรปรับปรุงเนื้อหาสาระและองค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) พ.ศ. ๒๕๖๒ ลงวันที่ ๒๑ พฤศจิกายน ๒๕๖๒ เพื่อให้การดำเนินภารกิจด้านป้องกัน ปราบปราม และแก้ไขปัญหายาเสพติดเกิดประสิทธิภาพสูงสุดและสอดคล้องกับพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ หลักเกณฑ์ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ และมาตรฐานที่ได้รับการยอมรับในระดับสากลที่เกี่ยวข้อง อาทิ มาตรฐาน ISO/IEC 27001:2022 และกรอบงานการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (The National Institute of Standards and Technology Cybersecurity Framework: NIST CSF) ครอบคลุมทั้งในด้านความมั่นคงปลอดภัยทางไซเบอร์ การบริหารจัดการความปลอดภัยของข้อมูล ตลอดจนการจัดการระบบสารสนเทศในยุคดิจิทัล

อาศัยอำนาจตามความในมาตรา ๓๒ มาตรา ๓๖ และมาตรา ๓๗ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) พ.ศ. ๒๕๖๒ ลงวันที่ ๒๑ พฤศจิกายน พ.ศ. ๒๕๖๒

ข้อ ๔ นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล มีวัตถุประสงค์ ดังนี้

(๑) เพื่อกำหนดกรอบแนวทาง และมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงาน ป.ป.ส. อย่างเป็นระบบ สอดคล้องต่อภารกิจด้านการป้องกัน ปราบปราม และแก้ไขปัญหายาเสพติดของสำนักงาน ป.ป.ส. และมาตรฐานที่เกี่ยวข้อง

(๒) เพื่อสร้างความเชื่อมั่นต่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลของสำนักงาน ป.ป.ส. แก่ผู้บริหาร บุคลากร ผู้มีส่วนได้ส่วนเสีย และประชาชนผู้รับบริการ

(๓) เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามต่อระบบสารสนเทศและไซเบอร์ ทั้งจากภายในและภายนอกองค์กร รวมถึงป้องกันการรั่วไหลของข้อมูล และการป้องกันการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น

ข้อ ๕ สาระ...

ข้อ ๕ สาระสำคัญของนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล ดังนี้

(๑) การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๑.๑) การควบคุมการเข้าถึงระบบสารสนเทศ กำหนดให้ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลที่คำนึงถึงการใช้งานและความมั่นคงปลอดภัยของระบบสารสนเทศเป็นหลัก โดยกำหนดให้มีข้อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตการเข้าถึง และการกำหนดสิทธิในการใช้งานเพื่อให้ผู้ใช้งานถือปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด รวมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และข้อมูลของสำนักงาน ป.ป.ส.

(๑.๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน กำหนดให้ต้องมีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน โดยต้องเป็นผู้ใช้งานที่ได้รับการอนุมัติเท่านั้น จึงจะสามารถเข้าใช้งานระบบสารสนเทศของสำนักงาน ป.ป.ส. ได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิในการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับ ต้องทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

(๑.๓) การควบคุมการเข้าถึงเครือข่าย โดยต้องกำหนดสิทธิในการเข้าถึงเครือข่ายที่เหมาะสมกับผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงเครือข่ายของสำนักงาน ป.ป.ส. รวมทั้ง ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ สำหรับการใช้งานอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัยตามที่สำนักงาน ป.ป.ส. กำหนด และออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อการควบคุมและการป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างเป็นระบบและมีประสิทธิภาพ

(๑.๔) การควบคุมการเข้าถึงระบบปฏิบัติการ โดยต้องกำหนดสิทธิผู้เข้าใช้งานอย่างเหมาะสม มีการพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนการเข้าใช้งานระบบปฏิบัติการทุกครั้ง และต้องจัดให้มีการระงับใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out) รวมทั้ง ต้องกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เกิดการละเมิดลิขสิทธิและป้องกันโปรแกรมไม่ประสงค์ดี

(๑.๕) การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิเพื่อการปฏิบัติงานในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบจากหัวหน้าส่วนราชการเป็นลายลักษณ์อักษร รวมทั้งต้องจัดให้มีการทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๒) การจัดทำระบบสำรองข้อมูล กำหนดให้ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมและพร้อมใช้งาน เพื่อให้ระบบสารสนเทศของสำนักงาน ป.ป.ส. สามารถใช้งานได้อย่างต่อเนื่องและมีเสถียรภาพ โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นจากมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล จัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบ...

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กำหนดให้ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในขององค์กร (Internal Audit) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Audit) เป็นประจำ เพื่อให้องค์กรได้ทราบถึงระบบความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

(๔) การพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนการพิจารณาทบทวนเพื่ออนุมัติ การสร้าง การติดตั้ง การใช้งาน โดยระบบต้องมีคุณสมบัติ ดังนี้

(๔.๑) สอดคล้องกับสถาปัตยกรรมระบบขององค์กร (Enterprise Architecture: EA)

(๔.๒) สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศดิจิทัลของสำนักงาน ป.ป.ส. และสามารถทำงานร่วมกันกับระบบเดิมได้อย่างราบรื่น

(๔.๓) ต้องผ่านการทดสอบระบบบนสภาวะแวดล้อมเดียวกันกับสภาวะแวดล้อมในการใช้งานจริงของผู้ใช้งาน

(๔.๔) ต้องเปรียบเทียบการตั้งค่าระบบ Active Directory (AD) ของสำนักงาน ป.ป.ส. หรือระบบอื่น ๆ ที่กำหนดกับการตั้งค่าของ Center for Internet Security (CIS Benchmarks) พร้อมทั้งวิเคราะห์ถึงภัยคุกคาม (Threat) และช่องโหว่ (Vulnerability)

(๕) สำนักงาน ป.ป.ส. ต้องกำหนดการแบ่งประเภทและลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และที่แก้ไขเพิ่มเติม รวมถึงประกาศ กฎ ระเบียบ ข้อบังคับอื่นที่เกี่ยวข้อง

ข้อ ๖ กรอบแนวทางการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัลให้เป็นไปตามแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๙

พันตำรวจตรี

(สุริยา สิงหกมล)

เลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติด

เอกสารแนบท้ายประกาศ

กรอบแนวทางการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล

พ.ศ. ๒๕๖๙

สารบัญ

หมวดที่ ๓...

สารบัญ

บทนิยาม

คำนิยามที่ใช้ในกรอบแนวทางการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล ประกอบด้วย

องค์กร หมายถึง สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด หรือสำนักงาน ป.ป.ส.

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

ผู้บริหารสูงสุดขององค์กร (Chief Executive Officer: CEO) หมายถึง เลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติด หรือเลขาธิการ ป.ป.ส.

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) หมายถึง ผู้บริหารระดับสูงขององค์กรที่ได้รับมอบหมาย มีทำหน้าที่กำหนดทิศทางนโยบายและยุทธศาสตร์ด้านดิจิทัลขององค์กร ให้สอดคล้องกับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศ รวมถึงบริหารจัดการทรัพยากรสารสนเทศให้เกิดความมั่นคงปลอดภัย และประสิทธิภาพสูงสุด

เจ้าหน้าที่สำนักงาน ป.ป.ส. หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานและลูกจ้างของกองทุนป้องกันและปราบปรามยาเสพติด และลูกจ้างเหมาเอกชนในสังกัดสำนักงาน ป.ป.ส.

ผู้ใช้งาน หมายถึง เจ้าหน้าที่สำนักงาน ป.ป.ส. ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีดิจิทัลขององค์กร โดยมีสิทธิการใช้งานตามหน้าที่ที่ได้รับมอบหมาย โดยหมายรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานระบบเทคโนโลยีสารสนเทศ

หน่วยงานภายนอก หมายถึง องค์กรภายนอกที่สำนักงาน ป.ป.ส. อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ขององค์กร โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ขององค์กรและต้องรับผิดชอบในการรักษาความลับของข้อมูล

ผู้ดูแลระบบ หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุมดูแลบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

ผู้ประสานงาน หมายถึง เจ้าหน้าที่องค์กรที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการสนับสนุนด้านการดูแลรักษาความปลอดภัย หรือด้านเทคนิคในการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ร่วมกับผู้ดูแลระบบ (Administrator)

เทคโนโลยีดิจิทัล หมายถึง การใช้เครื่องมือ ระบบ และกระบวนการดิจิทัลในการสร้าง จัดเก็บ ประมวลผล และสื่อสารข้อมูล ซึ่งครอบคลุมเทคโนโลยีในวงกว้างตั้งแต่ซอฟต์แวร์ ฮาร์ดแวร์ เทคโนโลยีอินเทอร์เน็ต และแพลตฟอร์มดิจิทัล

ระบบเทคโนโลยีสารสนเทศ หมายถึง ระบบงานขององค์กรที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่องค์กรสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการปฏิบัติงานขององค์กร

ปัญญาประดิษฐ์ (Artificial Intelligence) หมายถึง ศาสตร์ทางวิทยาการคอมพิวเตอร์ที่มุ่งเน้นการพัฒนาระบบให้มีความสามารถในการประมวลผล เรียนรู้ และตัดสินใจได้คล้ายคลึงหรือเหนือกว่ามนุษย์ (Human-like Intelligence) ผ่านกระบวนการรับรู้ข้อมูล (Perception) การให้เหตุผล (Reasoning) และการกระทำ (Action) เพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ในสถานการณ์ต่าง ๆ อย่างมีประสิทธิภาพ

การรักษาความมั่นคงปลอดภัย หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความสงบเรียบร้อยภายในประเทศ เศรษฐกิจ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเป็นการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

ข้อมูล (Data) หมายถึง รูปแบบตัวแทนของสารสนเทศที่สามารถตีความใหม่ได้ (Reinterpretable representation) ซึ่งถูกจัดให้อยู่ในรูปแบบที่เป็นทางการ (Formalized manner) เพื่อให้เหมาะสมสำหรับการสื่อสาร การตีความ หรือการประมวลผลโดยมนุษย์หรือโดยวิธีอัตโนมัติ

สารสนเทศ (Information) หมายถึง ข้อมูลที่ได้ผ่านกระบวนการประมวลผลแล้ว เปลี่ยนแปลงสภาพข้อมูลให้อยู่ในรูปแบบที่มีความสัมพันธ์ หรือมีความเกี่ยวข้องกัน เพื่อนำไปใช้ประโยชน์ในการตัดสินใจหรือตอบปัญหาต่าง ๆ

ระบบสารสนเทศ หมายถึง ระบบงานที่ใช้จัดเก็บและประมวลผลข้อมูล ซึ่งทำงาน ประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสารได้

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร ได้แก่

ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในองค์กรเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในองค์กร

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ขององค์กรเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ห้องระบบคอมพิวเตอร์ หมายถึง สถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และหรืออุปกรณ์จัดการเครือข่าย

ระบบปฏิบัติการ หมายถึง ซอฟต์แวร์ที่ควบคุมการทำงานของโปรแกรมต่าง ๆ และอาจให้บริการต่าง ๆ เช่น การจัดสรรทรัพยากร (Resource allocation) การจัดลำดับงาน (Scheduling) การควบคุมอินพุต/เอาต์พุต และการจัดการข้อมูล

โปรแกรมประยุกต์...

โปรแกรมประยุกต์ หมายถึง ซอฟต์แวร์หรือโปรแกรมที่เจาะจงสำหรับการแก้ปัญหาในงานประยุกต์ด้านใดด้านหนึ่ง (Specific to the solution of an application problem) หรือเพื่อตอบสนองความต้องการของผู้ใช้งานกลุ่มใดกลุ่มหนึ่ง

การเรียนรู้ของเครื่อง (Machine Learning) หมายถึง กระบวนการที่ใช้เทคนิคการคำนวณเพื่อให้ระบบสามารถเรียนรู้จากข้อมูลหรือประสบการณ์ เพื่อปรับปรุงประสิทธิภาพในการตัดสินใจ

การประมวลผลแบบคลาวด์ (Cloud Computing) หมายถึง กระบวนทัศน์สำหรับการเปิดให้เข้าถึงเครือข่ายไปยังกลุ่มทรัพยากรทางกายภาพหรือเสมือน (Physical or virtual resources) ที่ปรับขนาดได้และมีความยืดหยุ่น ซึ่งสามารถจัดสรรและบริหารจัดการได้ด้วยตนเองตามความต้องการ

ข้อมูลจราจรคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วัน เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลสารสนเทศและเป็นผู้รับผิดชอบโดยตรงหากข้อมูลสารสนเทศขององค์กรเกิดการละเมิดต่อความมั่นคงปลอดภัย

สินทรัพย์ หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับองค์กร และสินทรัพย์ด้านเทคโนโลยีดิจิทัล หรือสิ่งอื่นใดที่มีคุณค่าต่อองค์กร

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่เกิดขึ้นและมีส่วนเกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศ เช่น การกู้ระบบกลับคืนเป็นปกติ การป้องกันการบุกรุกทำลายข้อมูล เป็นต้น

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด หมายถึง เหตุการณ์ที่เกิดขึ้นโดยไม่ได้กำหนดให้เกิดขึ้น แล้วมีผลเสียต่อการให้บริการ หรือทำให้การบริการระบบสารสนเทศติดขัด/ขัดข้อง

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

เครือข่ายสังคมออนไลน์ (Social Network) หมายถึง การใช้โปรแกรม หรือเว็บไซต์ที่มีผู้ให้บริการทั้งจากภายนอก หรือภายในองค์กร เพื่อใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารในการสื่อข้อมูลแบบออนไลน์ผ่านระบบอินเทอร์เน็ต

SSL หมายถึง Secure Socket Layer คือ เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ ระบบสารสนเทศที่ใช้งาน เพื่อให้ข้อมูลปลอดภัยจากการเข้าถึงข้อมูลโดยผู้ไม่ประสงค์ดี

VPN หมายถึง Virtual Private Network คือ เป็นฟังก์ชั่นหนึ่งในระบบเครือข่ายคอมพิวเตอร์เพื่อการรับส่งข้อมูลที่ปลอดภัย โดยใช้โครงสร้างของอินเทอร์เน็ตเป็นตัวส่งผ่านข้อมูล มีการเข้ารหัสข้อมูลทั้งหมด และมี Gateway เฉพาะในการส่งข้อมูล

SLA หมายถึง Service Level Agreement คือ ข้อตกลงในการให้บริการว่าจะทำการรักษาระดับคุณภาพการให้บริการแก่ผู้ใช้งาน ตามข้อตกลงที่ศูนย์เทคโนโลยีสารสนเทศให้ไว้กับผู้ใช้งาน

OLA หมายถึง Operational Level Agreement คือ ข้อตกลงในการให้บริการระหว่างองค์กรภายในศูนย์เทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อสามารถให้บริการผู้ใช้งานได้อย่างมีประสิทธิภาพ

หมวดที่ ๑...

หมวดที่ ๑
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ ๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

ข้อ ๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศเป็นหลัก

ข้อ ๒ ผู้ดูแลระบบ อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ก็ต่อเมื่อได้รับอนุญาตจากเจ้าของข้อมูลตามความจำเป็นต่อการใช้งานเท่านั้น โดยมีหลักเกณฑ์ ดังนี้

๒.๑ ต้องเป็นผู้ใช้งาน หรือผู้ใช้งานภายนอกที่มีบัญชีรายชื่อที่ออกโดยศูนย์เทคโนโลยีสารสนเทศ และ/หรือองค์กรภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์ขององค์กร และยังไม่สิ้นสุดสถานภาพ

๒.๒ ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูล และได้รับมอบหมายจากผู้บังคับบัญชาหรือผู้บริหาร

๒.๓ ได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย พร้อมทั้ง กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ

๒.๔ การตัดออกจากทะเบียน การโยกย้ายองค์กร การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

๒.๕ การใช้งานที่ขัดต่อข้อกำหนดการใช้งานเครือข่าย

ข้อ ๓ เจ้าของข้อมูล ต้องจัดให้มีการแบ่งประเภทของข้อมูล และการจัดลำดับความสำคัญของข้อมูล โดยอ้างอิงตามแนวปฏิบัติการเข้าถึง เข้าใช้ และการดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลสารสนเทศของสำนักงาน ป.ป.ส. และจัดให้มีการทบทวนอยู่เสมอ

ข้อ ๔ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทนตามแนวปฏิบัติการเข้าถึง เข้าใช้ และการดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลสารสนเทศของสำนักงาน ป.ป.ส.

ข้อ ๕ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งาน รวมทั้ง โดยรวมถึงเกณฑ์การระงับสิทธิการใช้งานชั่วคราว และการถอนสิทธิการใช้งานระบบสารสนเทศ

ข้อ ๖ ผู้ดูแลระบบ ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน และกำหนดรหัสผ่านเบื้องต้นสำหรับการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้

ข้อ ๗ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

ข้อ ๘ ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๙ ผู้ดูแลระบบ ต้องกำหนดวิธีการบริหารจัดการกับข้อมูลสารสนเทศแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการจำหน่ายหรือการนำอุปกรณ์กลับมาใช้ใหม่

ส่วนที่ ๒...

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงสิทธิผู้ใช้งาน (User Access Management)

ข้อ ๑๐ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

๑๐.๑ ให้สำนักงานเลขานุการกรมมีหนังสือแจ้งรายชื่อเจ้าหน้าที่สำนักงาน ป.ป.ส. เพื่อลงทะเบียนบัญชีผู้ใช้งานใหม่ถึงผู้ดูแลระบบ

๑๐.๒ ต้องตรวจจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๑๐.๓ ต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ ตามข้อ ๕

๑๐.๔ แจ้งสิทธิในการใช้งานต่อผู้ใช้งานใหม่ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศพื้นฐาน (Default) ขององค์กร

ข้อ ๑๑ ในกรณีที่ต้องการเข้าถึงระบบสารสนเทศนอกเหนือจากระบบสารสนเทศพื้นฐาน (Default) ขององค์กร ผู้ใช้งาน ต้องขอการเข้าถึงระบบสารสนเทศผ่านระบบสนับสนุนงานให้บริการสารสนเทศ (Helpdesk) ของสำนักงาน ป.ป.ส.

ทั้งนี้ การขอเข้าถึงระบบสารสนเทศอื่นใดที่ไม่ตรงตามสิทธิที่เจ้าของข้อมูลกำหนดไว้ ให้ผู้ใช้งานขอหนังสือรับรอง พร้อมเหตุผลความจำเป็นในการเข้าถึงระบบสารสนเทศนั้นเป็นลายลักษณ์อักษรจากผู้บริหารระดับผู้อำนวยการกอง/สำนัก ผ่านระบบสนับสนุนงานให้บริการสารสนเทศ (Helpdesk) ของสำนักงาน ป.ป.ส.

ข้อ ๑๒ ผู้ดูแลระบบ ต้องดำเนินการทบทวนสิทธิการเข้าถึงระบบสารสนเทศ และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกัน การเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

๑๒.๑ จัดทำบัญชีรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามกอง/สำนัก หรือแยกตามสังกัดกรณีผู้ใช้งานภายนอก ภายใน ๓๑ มกราคม ของทุกปี

๑๒.๑.๑ กรณีระบบสารสนเทศพื้นฐาน (Default) กำหนดให้ทบทวนตามระบบสารสนเทศทรัพยากรบุคคลระดับกรมของสำนักงาน ป.ป.ส. ระบบ NCMAN และระบบ HRO หรือคำสั่งมอบหมายภายในขององค์กร หรือจัดทำหนังสือสอบถามกอง/สำนัก กรณีผู้ใช้งานเป็นลูกจ้างชั่วคราว และลูกจ้างเหมาบริการบุคคลธรรมดา

๑๒.๑.๒ กรณีระบบสารสนเทศที่เกี่ยวข้องกับภารกิจด้านการป้องกันปราบปราม และแก้ไขปัญหายาเสพติด กำหนดให้ผู้ดูแลระบบ จัดทำหนังสือสอบถามกอง/สำนัก

๑๒.๒ จัดส่งรายชื่อนั้นให้กับผู้อำนวยการกอง/สำนัก หรือผู้บังคับบัญชาต้นสังกัดของผู้ใช้งานภายนอก เพื่อทบทวนรายชื่อและสิทธิการใช้งาน

๑๒.๓ แก้ไขข้อมูล และสิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากกอง/สำนัก หรือหน่วยงานภายนอก

ข้อ ๑๓ การบริหารจัดการบัญชีผู้ใช้

๑๓.๑ ให้ยกเลิกบัญชีผู้ใช้ (User Account) เมื่อผู้ใช้งานลาออก หรือ พ้นจากตำแหน่ง หรือ ยกเลิกการใช้งาน นับแต่ทราบ

๑๓.๑.๑ เมื่อลาออกต้องดำเนินการภายใน ๓ วัน

๑๓.๑.๒ เมื่อเปลี่ยนตำแหน่งงานภายใน ต้องดำเนินการภายใน ๗ วัน

๑๓.๑.๓ เมื่อถูกให้พักราชการ หรือออกจากราชการภายใน ๑ วัน ภายหลังได้รับหนังสือแจ้งจากกอง/สำนัก

๑๓.๑.๔ กรณีการยกเลิก...

๑๓.๑.๔ กรณีการยกเลิกสัญญาของลูกจ้างเหมา ให้กอง/สำนักแจ้งรายชื่อการยกเลิกสัญญานั้น ถือเสมือนการลาออกหรือให้ออก

๑๓.๒ กำหนดการสร้างชื่อบัญชีผู้ใช้และรหัสผ่าน (Password) เป็นไปตามข้อกำหนดขององค์กร ดังนี้

๑๓.๒.๑ การกำหนดรหัสผ่านต้องประกอบไปด้วยอักษร ภาษาอังกฤษตัวพิมพ์เล็กและพิมพ์ใหญ่ อย่างน้อย อย่างละ ๑ ตัวอักษร อักขระพิเศษ เช่น ! # $ % ^ & เป็นต้น อย่างน้อย ๑ ตัวอักษร ตัวเลขอย่างน้อย ๑ ตัว และมีความยาวของรหัสผ่านไม่น้อยกว่า ๘ ตัวอักษร

๑๓.๒.๒ รหัสผ่านห้ามซ้ำกันจากรหัสผ่านเดิมที่เคยใช้ ๕ รหัสผ่านล่าสุด หรือใช้ ๒ factor authen เช่น ThaiD เป็นต้น

๑๓.๒.๓ หากผู้ใช้งานใส่รหัสผ่านผิดเกิน ๕ ครั้ง ระบบจะระงับบัญชีผู้ใช้งานชั่วคราว (Lock Username) ไม่ให้ทำการล็อกอิน (Log in) จนกว่าจะครบ ๑๕ นาที หรือติดต่อผู้ดูแลระบบหรือดำเนินการด้วยตัวเองผ่านระบบบริหารจัดการบัญชีผู้ใช้งานด้วยตนเองเพื่อปลดล็อก

๑๓.๒.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๑๓.๓ ผู้ใช้งาน ต้องไม่บันทึกหรือเก็บรหัสผ่านในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงโดยบุคคลอื่น

๑๓.๔ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และแจ้งรหัสผ่านให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย

๑๓.๕ การให้สิทธิสูงสุดเฉพาะกาลกับผู้ใช้งานคนใดก็ตาม จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน โดยต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานในทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อบุคคลนั้นพ้นจากตำแหน่ง โดยให้กำหนดว่าผู้ใช้งานนั้นสามารถเข้าถึงได้ระดับใด และต้องกำหนดกลุ่มบัญชีผู้ใช้งานต่างจากผู้ใช้งานตามปกติ

๑๓.๖ ผู้ดูแลระบบต้องกำหนดให้มีการเปลี่ยนรหัสผ่าน (Password) ทุก ๙๐ วัน กรณีมีการแจ้งเตือนให้เปลี่ยนรหัสผ่านล่วงหน้าอย่างน้อย ๑๔ วัน โดยผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ทันที

ข้อ ๑๔ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทตามชั้นความลับ

ข้อ ๑๕ ผู้ดูแลระบบ ต้องจัดให้มีการเข้ารหัส (Encryption) ในข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะที่เป็นมาตรฐานสากล เช่น SSL หรือ VPN หรือ XML Encryption เป็นต้น

ข้อ ๑๖ ผู้ดูแลระบบกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกองค์กร เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๑๗ เจ้าของข้อมูล ต้องตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ ๑๘ การเชื่อมโยงแลกเปลี่ยนข้อมูล ให้ผู้บริหารระดับสูงพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกันในระบบสารสนเทศ ดังนี้

๑๘.๑ กำหนดนโยบาย...

๑๘.๑ กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกัน

๑๘.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลลับ

๑๘.๓ พิจารณากำหนดผู้ใช้งานใดที่มีสิทธิหรือได้รับอนุญาตให้เข้าถึง

๑๘.๔ พิจารณาการลงทะเบียนผู้ใช้งาน

๑๘.๕ ต้องไม่อนุญาตการใช้งานข้อมูลสำคัญหรือข้อมูลลับ ในกรณีที่ระบบที่เชื่อมโยงไม่มีมาตรการป้องกันเพียงพอ

ข้อ ๑๙ มาตรการและวิธีการปกปิดข้อมูล (Masking Techniques)

๑๙.๑ จัดให้มีการปกปิดข้อมูลตามมาตรฐานการจัดการ ISO/IEC 27001:2022 (Control 8.11) โดยต้องจัดให้มีการปกปิดข้อมูลตามประเภทงาน อย่างน้อยดังนี้

ประเภทงาน	วิธีการปกปิดที่แนะนำ	ตัวอย่างการใช้งาน
การทดสอบระบบ (UAT/Dev)	**Static Data Masking (SDM)**	การจำลองฐานข้อมูลชุดใหม่ เพื่อใช้ในระบบทดสอบโดยเปลี่ยนค่าข้อมูลจริงเป็นค่าสมมติ
การสืบค้นข้อมูลหน้าจอ	**Dynamic Data Masking (DDM)**	การซ่อนตัวเลขบางส่วน เช่น เลขบัตรประจำตัวประชาชน “๑-๑๐xx-xxxx-xx-๑” เมื่อแสดงผลผ่านแอปพลิเคชัน
การวิเคราะห์ข้อมูล (Big Data/AI)	**Pseudonymization / Anonymization**	การแทนที่ชื่อจริงด้วยรหัสสัญลักษณ์ เพื่อให้นักวิเคราะห์ข้อมูลใช้งานได้โดยไม่ทราบตัวตนจริง

๑๙.๒ กำหนดให้ผู้ดูแลระบบ (Administrator) หรือผู้ประสานงาน ไม่ควรเห็นข้อมูลดิบ (Raw Data) ทั้งหมดโดยไม่มีเหตุจำเป็น และต้องมีการบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log) ทุกครั้งที่มีการเข้าถึง

๑๙.๒.๑ ห้ามใช้ข้อมูลจริงในสภาพแวดล้อมที่ไม่ปลอดภัย: ห้ามนำข้อมูลคดีที่ไม่ได้ปกปิดไปใช้ในระบบทดสอบ หรือบนอุปกรณ์คอมพิวเตอร์ส่วนบุคคล

๑๙.๒.๒ ต้องกำหนดวิธีการและระดับของการปกปิดข้อมูลก่อนเริ่มดำเนินการ

๑๙.๒.๓ ข้อมูลที่ผ่านการปกปิดแล้ว หากต้องมีการส่งผ่านเครือข่ายอินเทอร์เน็ต ต้องมีการเข้ารหัส (Encryption) ผ่านช่องทาง VPN หรือ SSL เสมอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

ข้อ ๒๐ การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

๒๐.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้ง ห้ามเผยแพร่ แจกจ่าย หรือให้ผู้อื่นล่วงรู้รหัสผ่านของตน

๒๐.๒ การกำหนด...

๒๐.๒ การกำหนดรหัสผ่านให้เป็นไปตามข้อ ๑๓.๒

๒๐.๓ ไม่กำหนดรหัสผ่านของบัญชีผู้ใช้ของตนเองจากชื่อหรือนามสกุลของตนเอง

๒๐.๕ ห้ามบันทึกรหัสผ่านบนอุปกรณ์หรือเบราว์เซอร์ที่ไม่ปลอดภัย และอุปกรณ์ดังกล่าวต้องได้รับการอนุมัติใช้งานจากองค์กรเท่านั้น

๒๐.๖ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒๐.๗ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านในทุก ๙๐ วัน หรือทุกครั้งได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๒๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งานที่มีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบในการดูแลบัญชีผู้ใช้งานของตน และต้องแจ้งศูนย์เทคโนโลยีทราบโดยทันทีเมื่อทราบ หรือสงสัยว่าบัญชีผู้ใช้งานถูกเข้าถึงและเข้าใช้โดยผิดปกติ ทั้งนี้ ความรับผิดทางวินัยพิจารณาจากเจตนา ความประมาท และการฝ่าฝืนข้อกำหนดดังกล่าว

ข้อ ๒๒ ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์หรือระบบสารสนเทศขององค์กร หากเกิดปัญหาในการพิสูจน์ตัวตนนั้น ไม่ว่าจากการล็อกของรหัสผ่าน หรือความผิดพลาดอื่นใด ผู้ใช้งานจะต้องแจ้งให้ ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

๒๒.๑ ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนเข้าถึงระบบปฏิบัติการของคอมพิวเตอร์

๒๒.๒ ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานระบบคอมพิวเตอร์อื่นในเครือข่าย

๒๒.๓ ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานอินเทอร์เน็ต และต้องบันทึกข้อมูลซึ่งสามารถระบุตัวตนของผู้ใช้งานได้ และห้ามใช้วิธีใด ๆ เพื่อหลบเลี่ยงการตรวจสอบตัวตนและการเก็บ log

๒๒.๔ ต้องล็อกหน้าจอทุกครั้ง เมื่อผู้ใช้งานไม่อยู่ที่คอมพิวเตอร์ และต้องพิสูจน์ตัวตนทุกครั้ง ก่อนกลับมาใช้งานระบบสารสนเทศ

๒๒.๕ ต้องตั้งเวลาพักหน้าจอ (screen saver) คอมพิวเตอร์ทุกเครื่อง โดยเริ่มพักหน้าจอ หลังจากที่ผู้ใช้หยุดการใช้งานเป็นเวลา ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

ข้อ ๒๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กรหรือเป็นของบุคคลภายนอก

ทั้งนี้ ผู้ใช้งานมีหน้าที่ในการดูแลรักษาและรับผิดชอบต่อข้อมูลขององค์กร และข้อมูลของบุคคลภายนอก หากเกิดการสูญหายหรือนำไปใช้ในทางที่ผิดหรือเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๔ ห้ามไม่ให้เผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครองดูแลขององค์กร โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๒๕ ผู้ใช้งานต้องดูแลป้องกัน และรักษาไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้งานของข้อมูล ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยมิชอบ

ข้อ ๒๖ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต จากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่องค์กรต้องการตรวจสอบข้อมูลนั้น ซึ่งองค์กรอาจแต่งตั้งหรือมอบหมายผู้ทำหน้าที่ตรวจสอบ เพื่อตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๗ ห้ามใช้...

ข้อ ๒๗ ห้ามใช้สินทรัพย์ขององค์กรเผยแพร่ข้อมูล ข้อความ รูปภาพ เพื่อรบกวน ก่อให้เกิดความเสียหาย ใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

ข้อ ๒๘ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์ หรือระบบเครือข่าย หรือระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๒๙ การควบคุมการทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ปลอดภัย (Clear desk and clear screen policy) ผู้ใช้งานต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

ข้อ ๓๐ การห้ามใช้งานโปรแกรมแบบ Peer-to-Peer (P2P) และโปรแกรมที่มีความเสี่ยงเทียบเท่าผู้ใช้งาน ต้องไม่ติดตั้ง ใช้งาน หรือทำให้มีการใช้งาน โปรแกรมหรือบริการที่มีลักษณะเป็น P2P ซึ่งเป็นการสื่อสารหรือแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์โดยตรง หรือโปรแกรม/บริการอื่นใด ที่มีความเสี่ยงในระดับเดียวกัน แต่ไม่จำกัดเพียงบิททอร์เรนท์ (BitTorrent) อีมูล (eMule) หรือซอฟต์แวร์ประเภทเดียวกัน ทั้งนี้ เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และต้องปฏิบัติตามเงื่อนไขหรือมาตรการควบคุมที่องค์กรกำหนดอย่างเคร่งครัด

ข้อ ๓๑ การห้ามใช้สินทรัพย์ขององค์กรเพื่อประโยชน์ทางการค้า ผู้ใช้งานต้องไม่ใช้สินทรัพย์ขององค์กรเพื่อประโยชน์ทางการค้า หรือเพื่อแสวงหาผลประโยชน์ส่วนตนหรือของบุคคลภายนอก เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจขององค์กร

ข้อ ๓๒ ห้ามดักรับข้อมูลในระบบเครือข่ายขององค์กร ผู้ใช้งานต้องห้ามดักรับ เข้าถึง หรือเก็บข้อมูลที่รับส่งในระบบเครือข่ายขององค์กรไม่ว่าด้วยวิธีการใด ๆ เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจขององค์กร

ข้อ ๓๓ การห้ามกระทำการที่กระทบต่อความพร้อมใช้งานของระบบสารสนเทศขององค์กร ผู้ใช้งานต้องไม่กระทำการใด ๆ อันเป็นการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศขององค์กรขัดข้อง หยุดชะงัก หรือไม่สามารถให้บริการได้ ไม่ว่าทางตรงหรือทางอ้อม

ข้อ ๓๔ ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อควบคุมระบบภายนอก โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องไม่ใช้ระบบสารสนเทศหรือทรัพยากรขององค์กร เพื่อควบคุม เข้าถึง หรือดำเนินการใด ๆ ต่อคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ส่วนที่ ๔ การบริหารจัดการทรัพย์สิน

ข้อ ๓๕ ผู้ใช้งาน ต้องไม่เข้าไปในห้องระบบคอมพิวเตอร์ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๓๖ ผู้ใช้งาน ต้องไม่นำอุปกรณ์หรือชิ้นส่วนใด ออกจากห้องระบบคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๗ ผู้ใช้งาน...

ข้อ ๓๗ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลของผู้อื่น ก่อนได้รับอนุญาตจากเจ้าของแฟ้มข้อมูล และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

ข้อ ๓๘ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับการจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้น และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	เครื่องทำลายเอกสาร
Flash Drive/Memory Stick/Memory Card	สำหรับอุปกรณ์ที่จะนำกลับมาใช้งานในองค์กร หรืออุปกรณ์ที่ต้องใช้ในส่วนงานอื่นที่มีระดับชั้นความลับที่ต่ำกว่า ให้เลือกใช้วิธีการทำลายข้อมูลตามมาตรฐาน NIST 800-88 โดยใช้คำสั่งมาตรฐานในการเขียนทับ (Overwrite) ทุกตำแหน่งที่ผู้ใช้เข้าถึงได้ (User-addressable) หรือการล้างข้อมูลระดับลึก (Purge) โดยใช้คำสั่งเฉพาะระดับ Firmware เช่น Secure Erase หรือ Cryptographic Erase เพื่อทำลายข้อมูลแม้ในส่วนที่เข้าถึงไม่ได้
แผ่น CD/DVD	ให้ทำลายด้วยเครื่องทำลายเอกสาร
เทป	ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ให้ทำลายข้อมูลบนฮาร์ดดิสก์ตาม DoD 5220.22-M หรือมาตรฐาน NIST 800-88 เก็บรักษาไว้อย่างน้อย ๑ ปี หรือตามที่กฎหมายกำหนด ดังนี้ ๑. สำหรับอุปกรณ์ที่จะนำกลับมาใช้ใหม่ภายในองค์กรเดิม ใช้วิธีการล้างข้อมูล (Clear) โดยใช้คำสั่งมาตรฐานในการเขียนทับ (Overwrite) ทุกตำแหน่งที่ผู้ใช้เข้าถึงได้ (User-addressable) ๒. สำหรับอุปกรณ์ที่จะขายต่อหรือบริจาค หรือไปแผนกอื่นที่มีระดับชั้นความลับของข้อมูลต่างกัน ให้ใช้การล้างข้อมูลระดับลึก (Purge) โดยใช้คำสั่งเฉพาะระดับ Firmware เช่น Secure Erase หรือ Cryptographic Erase เป็นต้น เพื่อทำลายข้อมูลแม้ในส่วนที่เข้าถึงไม่ได้ ๓. สำหรับข้อมูลที่เป็นความลับสุดยอด หรืออุปกรณ์ที่เสียจนเข้าถึงข้อมูลด้วยซอฟต์แวร์ไม่ได้ ใช้วิธีการทำลายทางกายภาพ เช่น การบด (Shredding) การเผา หรือการหลอมละลาย

ข้อ ๓๙ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ที่องค์กรมอบไว้ให้ใช้งาน เสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยรายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์จะต้องได้รับการบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่องค์กรมอบหมาย

ข้อ ๔๐ กรณีที่ผู้ใช้งานนำสินทรัพย์ออกนอกองค์กร ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ขององค์กรที่ได้รับไว้ใช้งาน

ทั้งนี้ ผู้ใช้งานต้องชดใช้ค่าเสียหาย ไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าของสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ใช้งาน

ข้อ ๔๑ ผู้ใช้งาน...

ข้อ ๔๑ ผู้ใช้งานมีสิทธิใช้สินทรัพย์หรือระบบสารสนเทศที่องค์กรจัดเตรียมไว้ให้ใช้งานตามภารกิจขององค์กร และห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศไปใช้ในกิจกรรมที่องค์กรมิได้กำหนดหรือในกิจกรรมที่ก่อให้เกิดความเสียหายต่อองค์กร

ข้อ ๔๒ กรณีการยืมทรัพย์สินสารสนเทศในความครอบครองของผู้ใช้งาน ต้องจัดให้มีการลงทะเบียนยืมคืนสินทรัพย์นั้นเสมอ

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๓ ผู้ดูแลระบบ ต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

ข้อ ๔๔ มาตรการควบคุมการเข้าออกห้องระบบคอมพิวเตอร์

๔๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกต้องแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๔๔.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์มาใช้ในการปฏิบัติงานที่ห้องระบบคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในหนังสือขออนุญาตเข้าออก ตามที่ระบุไว้ในเอกสารขอเข้าพื้นที่ให้ถูกต้องชัดเจน

ข้อ ๔๕ ผู้ใช้งานที่จะนำคอมพิวเตอร์อุปกรณ์ใด ๆ มาเชื่อมต่อกับระบบคอมพิวเตอร์ ระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๔๖ การขอใช้พื้นที่บนเครื่องแม่ข่ายเว็บ (Web Server) หรือขอใช้ชื่อโดเมนย่อย (Subdomain) ภายใต้ความรับผิดชอบขององค์กร ให้จัดทำหนังสือขออนุญาตหรือยื่นคำขอผ่านระบบสนับสนุนงานให้บริการสารสนเทศ (Helpdesk) ของสำนักงาน ป.ป.ส. ทั้งนี้ โปรแกรมหรือระบบที่จะติดตั้งต้องไม่ก่อให้เกิดผลกระทบต่อการทำงานของระบบคอมพิวเตอร์/ระบบสารสนเทศขององค์กร หรือการใช้งานของผู้ใช้งานรายอื่น

ข้อ ๔๗ ห้ามผู้ใดเคลื่อนย้าย ติดตั้ง หรือกระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๔๘ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้สามารถบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๔๘.๑ ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานได้เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ดังนี้

๔๘.๑.๑ ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๔๘.๑.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๔๘.๑.๓ ควบคุม...

๔๘.๑.๓ ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๔๘.๑.๔ ต้องจัดลำดับความสำคัญของช่องบริการเครือข่าย (Quality of Service : QOS) สำหรับเครื่องคอมพิวเตอร์ให้เหมาะสม ตามข้อตกลงการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement: SLA และ Operational Level Agreement: OLA)

๔๘.๒ ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่ใช้งานร่วมกัน โดยผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ (Switch) เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๔๘.๓ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อมิให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๔๘.๔ ระบบเครือข่ายทั้งหมดขององค์กรที่เชื่อมต่อกับระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่านระบบป้องกันเครือข่าย (Firewall) ที่สามารถในการตรวจจับโปรแกรมที่ไม่พึงประสงค์ รวมทั้งสามารถตรวจสอบการใช้งานในลักษณะที่ผิดปกติของผู้ใช้งานระบบเครือข่ายขององค์กรได้

๔๘.๕ การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องลงบันทึกเข้าใช้งาน โดยแสดงตัวเข้าใช้งาน (Login) ด้วยชื่อบัญชีผู้ใช้งาน (User Account) เพื่อพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนทุกครั้ง

๔๘.๖ ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายขององค์กรสามารถมองเห็น IP Address ของระบบเครือข่ายภายในองค์กร

๔๘.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ตลอดจนอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

๔๘.๘ การระบุอุปกรณ์บนเครือข่าย

๔๘.๘.๑ ผู้ดูแลระบบต้องเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้งาน รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้ หมายเลขอุปกรณ์ (Serial Number) IP Address และสถานที่ติดตั้ง

๔๘.๘.๒ ผู้ดูแลระบบต้องจำกัดสิทธิของผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔๘.๘.๓ ต้องระบุหมายเลขอุปกรณ์ (Serial Number) ที่เชื่อมต่อจากเครือข่ายภายนอกว่าสามารถให้เข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

๔๘.๘.๔ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๔๘.๘.๕ ผู้ขอใช้งานต้องกรอกแบบฟอร์มขอเชื่อมต่อเครือข่ายผ่านระบบสนับสนุนงานให้บริการสารสนเทศ (Helpdesk) ของสำนักงาน ป.ป.ส.

๔๘.๘.๖ การใช้งานอุปกรณ์บนเครือข่ายต้องพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๙ ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้งานสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศขององค์กร ได้แก่

๔๙.๑ การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๔๙.๒ การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password) ร่วมกับ ๒ Factor หรือ One Time Password (OTP)

๔๙.๓ การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๔๙.๔ การเข้าสู่ระบบจากระยะไกล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL VPN เพื่อเพิ่มความปลอดภัยของระบบสารสนเทศ

ข้อ ๕๐ ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกัน ระหว่างองค์กรกับองค์กรภายนอก

ข้อ ๕๑ ผู้ดูแลระบบต้องบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการกำหนด แก้ไข หรือ เปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software) ของคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๕๒ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องขออนุมัติจากผู้บังคับบัญชา

ข้อ ๕๓ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ถูกต้อง เพื่อใช้ระบุตัวบุคคลผู้เข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่าย ได้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

ข้อ ๕๔ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

๕๔.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ขององค์กรจะต้องขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นอย่างเพียงพอ

๕๔.๒ มีการควบคุมช่องทาง (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม ต้องตรวจสอบและปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ ทั้งนี้ การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมไว้ให้

๕๔.๓ การเข้าถึงข้อมูล หรือระบบข้อมูลได้จากระยะไกล ต้องเป็นวิธีที่ได้รับการอนุญาต

๕๔.๔ ต้องจัดทำบันทึกเข้าสู่ระบบเครือข่ายภายใน หรือระบบสารสนเทศ (Login) ขององค์กรจากระยะไกล โดยระบุชื่อผู้ใช้งานที่ผ่านการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนใช้งานอย่างถูกต้อง

ข้อ ๕๕ ระบบเครือข่ายทั้งหมดที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรต้องเชื่อมต่อผ่านระบบป้องกันการบุกรุกเครือข่าย (Firewall) ที่มีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware) ด้วย

ข้อ ๕๖ ต้องติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๗ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๕๘ ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่าย เพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

ข้อ ๕๙ ต้องเก็บ...

ข้อ ๕๙ ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้อง หรือตู้ RACK ที่มีการควบคุมการเข้าถึง และเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ข้อ ๖๐ การขอเข้าถึงเครือข่าย โดยอุปกรณ์ที่องค์กรมิได้จัดหาให้ ให้ผู้ใช้งานขออนุญาตการเข้าถึงผ่านผู้บริหารระดับสูง พร้อมข้อตกลงการยอมรับความเสี่ยงที่อาจจะเกิดขึ้นจากอุปกรณ์ภายนอกนั้น

ข้อ ๖๑ การจัดสรรไอพีแอดเดรส (IP Address) ให้ศูนย์เทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการ ดังนี้

๖๑.๑ ไอพีแอดเดรสสาธารณะที่จดทะเบียนขององค์กร (Public IP Address) รุ่น ๔ (IPV๔) ๒๐๒.๕๘.๑๒๖.๐/๒๔ และไอพีแอดเดรส รุ่น ๖ (IPV๖) ที่จัดหาใช้งานต่อไป ของระบบเครือข่ายอินเทอร์เน็ต เป็นสินทรัพย์ขององค์กร

๖๑.๒ สำหรับเครือข่ายภายในองค์กร ให้กำหนดและใช้งานไอพีแอดเดรสรุ่น ๔ (IPV๔) ในช่วงเครือข่ายส่วนบุคคล (Private Network) ตามความเหมาะสม และให้จัดหาและรองรับการใช้งานไอพีแอดเดรสรุ่น ๖ (IPV๖) ตามที่องค์กรกำหนด

๖๑.๓ องค์กรจะจัดสรรไอพีแอดเดรสให้แก่เจ้าหน้าที่ตามคำขอให้เพียงพอและเหมาะสมต่อการใช้งาน และอาจปรับเปลี่ยนไอพีแอดเดรสที่จัดสรรให้กอง/สำนัก/กลุ่มขึ้นตรงเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้การบริหารจัดการเครือข่ายมีประสิทธิภาพ

ข้อ ๖๒ การจัดการชื่อโดนเมน โดยมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศ ดำเนินการ ดังนี้

๖๒.๑ ขึ้นทะเบียนชื่อโดเมนอินเทอร์เน็ต (Internet) บริการจดทะเบียนชื่อโดเมนขององค์กรภายใต้ชื่อ “oncb.go.th” รวมทั้งการบำรุงรักษาโดเมนขององค์กรให้ปลอดภัย และใช้งานได้อย่างมีประสิทธิภาพ

๖๒.๒ องค์กรมีสิทธิในการขอใช้ชื่อโดเมน oncb.go.th โดยยื่นเรื่องขออนุมัติต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ คำขออนุมัติจะต้องลงนามรับรองโดยผู้อำนวยการกอง/สำนักและกลุ่มขึ้นตรง

๖๒.๓ โครงการพิเศษหรือโครงการใด ๆ ที่ได้รับอนุมัติจากองค์กร สามารถขอจดชื่อโดเมนประจำโครงการได้ โดยให้จดทะเบียนภายใต้ชื่อโดเมนย่อยประจำกอง/สำนัก/กลุ่มขึ้นตรงนั้น สามารถยื่นขอจดชื่อโดเมนภายใต้ชื่อโดเมนขององค์กร กรณีที่เป็นโครงการระดับองค์กร

๖๒.๔ การใช้ไอพีแอดเดรสขององค์กร เพื่อจดทะเบียนชื่อโดเมนนอกระบบชื่อโดเมนขององค์กร โดยมิได้รับอนุญาตเป็นสิ่งต้องห้าม ยกเว้นกรณีมีเหตุผลความจำเป็นอย่างยิ่ง

ทั้งนี้ ให้ผู้อำนวยการกอง/สำนัก/กลุ่มขึ้นตรง ดำเนินการยื่นคำร้องต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยชี้แจงเหตุผลและความจำเป็นที่ต้องขอจดทะเบียนชื่อโดเมนนอกระบบการอนุมัติจดทะเบียนให้อยู่ในดุลยพินิจของผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๖๓ ในการเข้าถึงเครือข่ายของสำนักงาน ป.ป.ส. ให้ผู้ใช้งานเลือกใช้ช่องทางการเชื่อมต่อเพียงหนึ่งช่องทางที่สามารถใช้งานได้ ได้แก่ เครือข่ายไร้สาย (Wi-Fi) หรือเครือข่ายแบบสาย (LAN) ตามที่องค์กรกำหนด

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๔ ผู้ดูแลระบบ ต้องกำหนดวิธีการลงทะเบียนบุคลากรใหม่ขององค์กร ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือพ้นจากตำแหน่ง การยกเลิกการใช้งาน หรือ การเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น ให้เป็นไปตามความในส่วนที่ ๒

ข้อ ๖๕ กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

๖๕.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ได้รับมอบ

๖๕.๒ หลังจากติดตั้งระบบเสร็จ ต้องยกเลิกบัญชีผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกรายที่ถูกกำหนดเอาไว้เป็นค่าเริ่มต้นที่มาพร้อมกับระบบในทันที

๖๕.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมพักหน้าจอ (Screen saver) เพื่อล็อกหน้าจอภาพเมื่อไม่ได้ใช้งาน ซึ่งผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานต่อ

๖๕.๔ ผู้ใช้งานต้องบันทึกเข้าใช้งาน (Login) ทุกครั้งก่อนเข้าใช้ระบบปฏิบัติการ และต้องลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๖๕.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อบัญชีผู้ใช้งาน (User Account) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ขององค์กรร่วมกัน

๖๕.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๖๕.๗ ผู้ใช้งานสามารถขอใช้งานซอฟท์แวร์ได้ตามหน้าที่หรือความจำเป็น เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยผู้ดูแลระบบจะเป็นผู้ติดตั้งให้เท่านั้น

๖๕.๘ ห้ามผู้ใช้งานติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล

๖๕.๙ ซอฟท์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๖๕.๑๐ ห้ามใช้สินทรัพย์ที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า

๖๕.๑๑ ห้ามสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดง ข้อความ รูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

๖๕.๑๒ ห้ามผู้ใช้งานควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศของหน่วยงานภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๖๖ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความสำคัญสูงหรือมีความเสี่ยงสูงการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวสำหรับระบบสารสนเทศ ดังนี้

๖๖.๑ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๖๖.๒ จำกัดเข้าถึงระบบปฏิบัติการเฉพาะระบบอินทราเน็ต

๖๖.๓ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

๖๖.๓.๑ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้งาน (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๖๖.๓.๒ ผู้ใช้งาน...

๖๖.๓.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบผลอันเกิดจากการใช้ชื่อผู้ใช้งาน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ ๖๗ ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

๖๗.๑ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน ตามข้อ ๑๓.๒

๖๗.๒ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๖๗.๓ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๖๗.๔ กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

ข้อ ๖๘ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาขององค์กรเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

ข้อ ๖๙ กำหนดให้มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านล่วงหน้าอย่างน้อย ๑๔ วัน

ข้อ ๗๐ ให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งานและพิสูจน์ยืนยันตัวตน (User Identification and Authentication) ด้วยรหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๗๑ การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๗๑.๑ จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น ต้องผ่านการรับรองให้ใช้จากผู้ดูแลระบบ และต้องมีความสามารถในการพิสูจน์ยืนยันตัวตนผู้ใช้งานในการเข้าใช้งานโปรแกรม

๗๑.๒ ต้องจัดเก็บชุดติดตั้งโปรแกรมอรรถประโยชน์ แยกจากชุดติดตั้งซอฟต์แวร์ระบบสารสนเทศ

๗๑.๓ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ

๗๑.๔ การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้มีการติดตั้งระบบเตือนภัยให้กับผู้ใช้งานที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

๗๑.๕ ต้องป้องกันมิให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้ และต้องถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์ รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศเมื่อไม่จำเป็นต้องใช้งาน

ข้อ ๗๒ การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน ๓๐ นาที

ข้อ ๗๓ องค์กรอาจไม่กำหนดข้อจำกัดช่วงเวลาในการเข้าถึงระบบสารสนเทศ เพื่อรองรับภารกิจ อย่างไรก็ตามผู้ใช้งานต้องพิสูจน์ตัวตนผ่านระบบจัดการบัญชีผู้ใช้และสิทธิส่วนกลาง (Active Directory) และยืนยันตัวตนแบบหลายปัจจัย (MFA) ตามที่องค์กรกำหนด และผู้ดูแลระบบต้องจัดให้มีการบันทึกและเฝ้าระวังการใช้งานที่ผิดปกติตลอดเวลา โดยเพิ่มระดับการติดตามกรณีใช้งานนอกเวลาราชการ ทั้งนี้ ให้มีการกำหนดเวลาไม่ใช้งาน (Idle timeout) และการล็อกหรือตัดช่วงการเชื่อมต่อ (session) ตามมาตรการขององค์กร

ส่วนที่ ๗ การควบคุม...

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)

ข้อ ๗๔ ผู้ดูแลระบบ ต้องกำหนดวิธีการลงทะเบียนบุคลากรใหม่ขององค์กร ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือพ้นจากตำแหน่ง การยกเลิกการใช้งาน หรือ การเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น ให้เป็นไปตามความในส่วนที่ ๒

ข้อ ๗๕ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ตามที่องค์กรกำหนดเท่านั้น หากเป็นสิทธิการใช้งานพิเศษ ต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๗๖ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานต่าง ๆ เมื่อผู้ใช้งานไม่ใช้งานระบบสารสนเทศเป็นเวลา ๓๐ นาที ระบบจะต้องตัดการใช้งาน โดยผู้ใช้งานต้องลงบันทึกเข้าใช้งาน (Login) อีกครั้งก่อนใช้งานต่อ

ข้อ ๗๗ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน (Password) ของผู้ใช้งาน ดังต่อไปนี้

๗๗.๑ ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ โดยใช้ชื่อผู้ใช้งานและรหัสผ่านเป็นอย่างน้อย

๗๗.๒ ต้องเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน เมื่อผู้ใช้งาน ลาออก หรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๗๗.๓ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงโดยบุคคลอื่น นอกจากตนเอง

๗๗.๔ กำหนดให้ชื่อบัญชีผู้ใช้งานต้องไม่ซ้ำกัน

๗๗.๕ การให้สิทธิสูงสุดเฉพาะกาลกับผู้ใช้งานคนใดก็ตาม จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานในทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อบุคคลนั้นพ้นจากตำแหน่ง โดยให้กำหนดว่าผู้ใช้งานนั้นสามารถเข้าถึงระดับใดได้ และต้องกำหนดกลุ่มบัญชีผู้ใช้งานต่างจากผู้ใช้งานตามปกติ

ข้อ ๗๘ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทตามชั้นความลับ

ข้อ ๗๙ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ตามมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

ข้อ ๘๐ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกองค์กร เช่น บำรุงรักษา ตรวจซ่อม โดยให้สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๘๑ ระบบที่ไวต่อการรบกวน (Sensitive System) มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติ ดังนี้

๘๑.๑ แยกระบบที่ไวต่อการรบกวนออกจากระบบอื่น ๆ โดยการจัดทำบัญชีรายชื่อแยกประเภทโดยแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในองค์กร

๘๑.๒ ควบคุมสภาพแวดล้อมของระบบ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

๘๑.๓ กำหนดสิทธิการใช้ระบบ ให้เป็นการเฉพาะกับผู้ใช้งานที่เกี่ยวข้องเท่านั้น

๘๑.๔ การเข้าถึงระบบสารสนเทศที่มีความสำคัญสูง อนุญาตให้ทำผ่านช่องทางที่องค์กรกำหนดให้เท่านั้น

ข้อ ๘๒ การใช้งานอุปกรณ์พกพา (Mobile Device) ต้องปฏิบัติดังต่อไปนี้

๘๒.๑ ตรวจสอบความพร้อมของอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ

๘๒.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากอุปกรณ์พกพาที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๘๒.๓ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายขององค์กร ต้องพิสูจน์ตัวตนก่อนเข้าใช้งานโดยการพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่านแบบการยืนยันตัวตนแบบสองปัจจัย (2FA) โดยใช้รหัสผ่านใช้ครั้งเดียว (OTP) เป็นอย่างน้อย

๘๒.๔ การเข้าสู่ระบบจากระยะไกลต้องใช้การเข้ารหัสข้อมูล ได้แก่ SSL หรือ VPN และหรือกระบวนการเข้ารหัสวิธีอื่นที่เหมาะสม เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล

๘๒.๕ การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องตรวจสอบผู้ใช้งานอีกครั้ง

๘๒.๖ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว กำหนดการเชื่อมต่อเข้าสู่ระบบไม่เกิน ๑ ชั่วโมง

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing Intellectual Property and Prevention Malware)

ข้อ ๘๓ ซอฟต์แวร์ที่องค์กรอนุญาตให้ใช้งาน หรือที่องค์กรมีลิขสิทธิ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ และความจำเป็น โดยห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๘๔ ซอฟท์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ หรือผู้ที่มีสิทธิในลิขสิทธิ

ข้อ ๘๕ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus หรือ Endpoint Security) ตามที่องค์กรกำหนด เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องที่ใช้เพื่อการศึกษาหรือทดสอบที่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๘๖ ต้องตรวจสอบข้อมูล แฟ้มข้อมูล ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น เพื่อตรวจจับไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๘๗ ผู้ใช้งานต้องปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) อยู่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๘๘ ผู้ใช้งาน...

ข้อ ๘๘ ผู้ใช้งานต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้ง เมื่อพบสิ่งผิดปกติ ผู้ใช้งานจะต้องแจ้งเหตุแก่ผู้ดูแลระบบทราบโดยไม่ชักช้า ทั้งนี้ หากผู้ใช้งานพบว่า เครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งผู้ดูแลระบบทราบ

ข้อ ๘๙ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้งซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ขององค์กรหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๙๐ ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ขององค์กร แต่การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ อาจกระทำได้โดยห้ามดำเนินการดังนี้

๙๐.๑ การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศ รวมทั้ง การกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลของบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๙๐.๒ การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๙๐.๓ การพัฒนาโปรแกรมใด ๆ ที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๙๐.๔ การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ซอฟต์แวร์

๙๐.๕ การสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความ รูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

ข้อ ๙๑ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๙๑.๑ จัดให้มีกระบวนการควบคุมโครงการพัฒนาซอฟต์แวร์ที่จัดจ้างผู้รับจ้างพัฒนาภายนอก

๙๑.๒ องค์กรถือสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดของซอฟต์แวร์ที่ได้รับการพัฒนาโดยผู้รับจ้างพัฒนาภายนอก

๙๑.๓ กำหนดการสงวนสิทธิที่จะตรวจสอบคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะพัฒนา โดยให้ระบุไว้ในสัญญาจ้างที่จะทำกับผู้รับจ้างพัฒนาภายนอกนั้น

๙๑.๔ ให้ตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่จะติดตั้งก่อนติดตั้งทุกครั้ง

๙๑.๕ หลังจากติดตั้งระบบเพื่อใช้งาน ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกรายที่ถูกกำหนดเอาไว้เป็นค่าเริ่มต้นที่มาพร้อมกับระบบในทันที

ข้อ ๙๒ ป้องกันจากโปรแกรมประสงค์ร้าย (Malware) ผู้ใช้งานต้องปฏิบัติ ดังนี้

๙๒.๑ หลีกเลี่ยงการเข้าถึงเว็บไซต์ที่มีความเสี่ยงหรือเกี่ยวข้องกับการละเมิดลิขสิทธิ

๙๒.๒ ไม่เปิดไฟล์แนบจากอีเมล์ของผู้ส่งที่ไม่ทราบแหล่งที่มา

๙๒.๓ ไม่คลิกลิงก์จากอีเมลที่น่าสงสัย และให้ตรวจสอบปลายทางของลิงก์ก่อนทุกครั้ง โดยเฉพาะลิงก์แบบย่อ (URL Shortener)

๙๒.๔ ก่อนเปิดใช้งานไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ต อีเมล FTP หรือบริการแชร์ไฟล์ ให้สแกนตรวจหาโปรแกรมประสงค์ร้ายทุกครั้ง

ส่วนที่ ๙ การปฏิบัติงาน...

ส่วนที่ ๙ การปฏิบัติงานภายนอก

ข้อ ๙๓ ต้องตรวจสอบว่าอุปกรณ์ซึ่งเป็นของส่วนตัวที่จะใช้เข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลว่าได้รับการติดตั้งโปรแกรมป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรกำหนดหรือไม่

ข้อ ๙๔ ผู้ใช้งานจากระยะไกล ต้องพิสูจน์ตัวตนก่อนเข้าใช้งาน เพื่อเพิ่มความปลอดภัยด้วยการใช้รหัสผ่านแบบ ๒ Factor หรือ One time Password (OTP) เป็นอย่างน้อย

ข้อ ๙๕ ไม่อนุญาตให้ใช้งานอุปกรณ์ซึ่งเป็นของส่วนตัวที่ไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยขององค์กรในการเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกล

ข้อ ๙๖ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตหรือไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๙๗ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิในการเข้าถึงระบบสารสนเทศ และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ข้อ ๙๘ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว โดยกำหนดการเชื่อมต่อเข้าสู่ระบบไม่เกิน ๑ ชั่วโมง

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๙๙ ผู้ดูแลระบบ ต้องออกแบบควบคุมอุปกรณ์เครือข่ายแบบไร้สาย (Access Point) ให้กระจายสัญญาณออกนอกพื้นที่ใช้งานให้น้อยที่สุด เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตี (Hacker) สามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

ข้อ ๑๐๐ ทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) จากผู้ผลิต และให้ซ่อนค่าดังกล่าวด้วย

ข้อ ๑๐๑ ผู้ดูแลระบบต้องกำหนดให้เครือข่ายไร้สายขององค์กรใช้การเข้ารหัสข้อมูลที่มีความมั่นคงปลอดภัย โดยใช้มาตรฐาน WPA3 หรือ WPA2 (AES) เป็นอย่างน้อย ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client)

ข้อ ๑๐๒ ผู้ดูแลระบบต้องตั้งค่าอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ให้ไม่แสดงชื่อเครือข่ายไร้สาย (SSID) ตามที่องค์กรกำหนด เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูล และกำหนดให้ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าใช้งานเครือข่ายไร้สายทุกครั้ง

ข้อ ๑๐๓ ผู้ดูแลระบบต้องควบคุมการเข้าถึงเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่ลงทะเบียน MAC Address และผู้ใช้งานที่มีบัญชีผู้ใช้ พร้อมสิทธิการใช้งานตามที่องค์กรกำหนดเท่านั้น

ข้อ ๑๐๔ ต้องลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ ๑๐๕ องค์กร...

ข้อ ๑๐๕ องค์กรกำหนดให้ผู้ใช้งาน ๑ บัญชี สามารถลงทะเบียนและใช้งานอุปกรณ์เพื่อเชื่อมต่อระบบหรือเครือข่ายขององค์กรได้ไม่เกิน ๓ อุปกรณ์ ได้แก่ คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ แท็บเล็ต เว้นแต่ได้รับอนุมัติจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมาย โดยให้เป็นไปตามหลักเกณฑ์และมาตรการควบคุมที่องค์กรกำหนด

ข้อ ๑๐๖ ผู้ดูแลระบบต้องติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในขององค์กร

ข้อ ๑๐๗ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารกับเครือข่ายภายในองค์กรผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๑๐๘ ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เข้าถึงระบบเครือข่ายไร้สาย

ข้อ ๑๐๙ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย เมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที

ข้อ ๑๑๐ ผู้ดูแลระบบต้องจัดให้มีระบบตรวจจับและป้องกันการบุกรุกเครือข่ายไร้สาย (WIDS/WIPS) เพื่อเฝ้าระวังและตรวจพบจุดกระจายสัญญาณไร้สายแปลกปลอม (Rogue Access Point) ภายในพื้นที่ขององค์กร และต้องสามารถระงับการเชื่อมต่อที่ผิดปกติได้โดยทันที โดยไม่กระทบต่อการใช้งานเครือข่ายไร้สายที่ได้รับอนุญาต

ข้อ ๑๑๑ ผู้ดูแลระบบต้องระงับหรือปิดกั้นการสื่อสาร การเชื่อมต่อของผู้ใช้งานหรืออุปกรณ์ที่เป็นต้นเหตุได้ทันที โดยไม่ต้องแจ้งล่วงหน้า เมื่อพบการใช้งานนอกวัตถุประสงค์ มีพฤติการณ์เสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร หรือมีเหตุอันควรสงสัยว่าอาจเกี่ยวข้องกับการกระทำความผิดตามกฎหมาย ทั้งนี้ ให้รายงานผู้บังคับบัญชาตามลำดับชั้น และให้คงการปิดกั้นไว้จนกว่าจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๑๑๒ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของอุปกรณ์ป้องกันเครือข่ายทั้งหมด

ข้อ ๑๑๓ ผู้ดูแลระบบต้องกำหนดค่าเริ่มต้นของอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้เป็นปฏิเสธทั้งหมด ตามหลักการปฏิเสธโดยปริยาย (Default Deny) โดยจะอนุญาตเฉพาะการสื่อสารที่ระบุไว้ในนโยบายการอนุญาต (Whitelist) เท่านั้น

ข้อ ๑๑๔ บริการและช่องทางการเชื่อมต่ออินเทอร์เน็ตที่ไม่ได้รับอนุญาตตามนโยบายความมั่นคงปลอดภัยขององค์กร ต้องถูกปิดกั้นหรือจำกัดการเข้าถึงด้วยไฟร์วอลล์

ข้อ ๑๑๕ ผู้ใช้งานอินเทอร์เน็ตจะต้องพิสูจน์ตัวตน (Authentication) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๑๖ ผู้ดูแลระบบจะต้องบันทึกการเปลี่ยนแปลงค่าบริการและการเชื่อมต่อที่อนุญาตทุกครั้งที่เปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย เช่น ค่า Parameter เป็นต้น และต้องมีการประเมินผลกระทบด้านความปลอดภัย (Security Impact Analysis) ก่อนอนุมัติเสมอ

ข้อ ๑๑๗ ให้เฉพาะ...

ข้อ ๑๑๗ ให้เฉพาะผู้ได้รับมอบหมายให้ดูแลจัดการเท่านั้น ที่สามารถเข้าถึงตัวอุปกรณ์ป้องกันเครือข่าย

ข้อ ๑๑๘ จะต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ป้องกันเครือข่าย ไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๑๙ การให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน หากผู้ใช้งานมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อที่นอกเหนือไปจากที่กำหนด จะต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๑๒๐ จะต้องกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อกำหนดตามนโยบายการป้องกันเครือข่าย (Policy) จะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องที่ให้บริการจริง

ข้อ ๑๒๑ ผู้ดูแลระบบต้องจัดให้มีการสำรองข้อมูลการตั้งค่า (Configuration) ของอุปกรณ์ป้องกันเครือข่ายเป็นประจำ และเก็บไว้อย่างปลอดภัยในสื่อบันทึกภายนอกหรือระบบที่แยกต่างหาก เพื่อรองรับกรณีเกิดภัยพิบัติ (Disaster Recovery)

ข้อ ๑๒๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศขององค์กรซึ่งใช้งานภายในเครือข่ายอินทราเน็ต ห้ามเปิดให้เข้าถึงผ่านอินเทอร์เน็ต เว้นแต่มีความจำเป็นและได้รับอนุมัติเป็นรายกรณีตามที่องค์กรกำหนด

ข้อ ๑๒๓ ควรจัดให้มีการแบ่งแยกเขตเครือข่ายระหว่างเขตบริการสาธารณะ (DMZ) และเครือข่ายภายในที่มีข้อมูลสำคัญให้ชัดเจน เพื่อป้องกันการบุกรุกลุกลามภายในเครือข่าย (Lateral Movement)

ข้อ ๑๒๔ องค์กรมีสิทธิที่จะระงับหรือจำกัดการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายการป้องกันเครือข่าย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๒๕ ผู้ดูแลระบบจะต้องบันทึกรายการของการเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ก่อน

ข้อ ๑๒๖ ผู้ดูแลระบบต้องกำหนดให้การเชื่อมต่อเข้าใช้งานระบบจากระยะไกล (Remote Access) ทุกกรณีต้องยืนยันตัวตนแบบหลายปัจจัย (MFA) อย่างน้อย ๒ ปัจจัยทุกครั้ง เพื่อป้องกันการเข้าถึงบัญชีผู้ใช้งานโดยมิชอบ

ข้อ ๑๒๗ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์ป้องกันเครือข่ายเปิดใช้คุณสมบัติความปลอดภัยขั้นสูง (Next-Generation Features) เช่น ระบบป้องกันการบุกรุก (IPS) การควบคุมระดับแอปพลิเคชัน (Application Control) และการกรองเว็บไซต์/URL อันตราย (URL Filtering) เป็นต้น ให้เหมาะสมกับระดับความเสี่ยงของระบบ ดังนี้

๑๒๗.๑ ผู้ดูแลระบบต้องกำหนดการควบคุมการเข้าถึงในระดับแอปพลิเคชัน (Layer ๗) โดยปิดกั้นการใช้งานแอปพลิเคชันที่มีความเสี่ยงสูงหรือใช้หลีกเลี่ยงการตรวจสอบ เช่น บริการตัวกลาง (Proxy) เครือข่ายส่วนตัวเสมือนส่วนบุคคล (Private VPN) เว้นแต่ได้รับอนุญาตเป็นกรณีเฉพาะเพื่อการสืบสวนคดีเท่านั้น เป็นต้น

ข้อ ๑๒๗.๒ ผู้ดูแล...

๑๒๗.๒ ผู้ดูแลระบบต้องเปิดใช้งานระบบป้องกันการบุกรุก (IPS) บนอุปกรณ์ไฟร์วอลล์รุ่นใหม่ (NGFW) และตั้งค่าให้อัปเดตฐานข้อมูลลายเซ็นภัยคุกคาม (Threat Signature) จากผู้ผลิตโดยอัตโนมัติ เพื่อให้สามารถตรวจจับและยับยั้งการโจมตีช่องโหว่ได้แบบทันที (Real-time)

๑๒๗.๓ เมื่อมีความจำเป็นด้านความมั่นคงปลอดภัย องค์กรอาจกำหนดให้มีการถอดรหัสและตรวจสอบข้อมูลที่รับ–ส่งผ่าน HTTPS (Decryption/Inspection) เพื่อป้องกันภัยคุกคามที่แฝงมากับทราฟฟิก ทั้งนี้ ต้องดำเนินการเท่าที่จำเป็นและเหมาะสม โดยคำนึงถึงความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๑๒๗.๔ ผู้ดูแลระบบต้องกำหนดให้มีการกรองเว็บไซต์ตามหมวดหมู่ (Category-based Filtering) โดยปิดกั้นอย่างน้อยเว็บไซต์อันตราย (Malicious Sites) เว็บไซต์เกี่ยวกับการพนันและเว็บไซต์ที่อาจเป็นช่องทางให้ข้อมูลรั่วไหล ตามที่องค์กรกำหนด

๑๒๗.๕ ผู้ดูแลระบบ ต้องเปิดใช้งานระบบตรวจสอบไฟล์แนบ (Sandboxing) สำหรับไฟล์ที่ถูกส่งผ่านเครือข่าย เพื่อนำไฟล์ต้องสงสัยไปจำลองการทำงานในสภาพแวดล้อมที่ปลอดภัยก่อนอนุญาตให้เข้าสู่เครือข่ายภายใน

๑๒๗.๖ ผู้ดูแลระบบต้องเชื่อมต่ออุปกรณ์ไฟร์วอลล์รุ่นใหม่ (NGFW) กับฐานข้อมูลข่าวกรองภัยคุกคามภายนอก (Threat Intelligence) เพื่อปิดกั้น IP Address หรือโดเมนที่อยู่ในบัญชีดำ (Blacklist) ของหน่วยงานด้านความมั่นคงหรือแหล่งข้อมูลสากลโดยอัตโนมัติ

ข้อ ๑๒๘ ผู้ละเมิดนโยบายด้านความปลอดภัยของอุปกรณ์ป้องกันเครือข่ายจะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๒๙ ผู้ดูแลระบบต้องทบทวนกฎการทำงานของไฟร์วอลล์ (Rule Base Review) อย่างน้อยทุก ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง เพื่อปรับปรุงและยกเลิกกฎที่ไม่จำเป็นหรือไม่ได้ใช้งานแล้ว

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

ข้อ ๑๓๐ ผู้ใช้งานต้องลงทะเบียนและการอนุมัติจากผู้บริหารก่อนใช้งาน โดยต้องใช้บัญชีไปรษณีย์อิเล็กทรอนิกส์ภาครัฐ (.go.th) ในการปฏิบัติราชการเท่านั้น

ข้อ ๑๓๑ ต้องเปลี่ยนรหัสผ่านทันทีเมื่อใช้งานครั้งแรก และต้องเปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA) สำหรับการเข้าถึงจากภายนอกองค์กร

ข้อ ๑๓๒ ห้ามจดบันทึกหรือจัดเก็บรหัสผ่านไว้ในรูปแบบที่ผู้อื่นเข้าถึงได้ง่าย

ข้อ ๑๓๓ ให้เปลี่ยนรหัสผ่านทันทีเมื่อพบความผิดปกติหรือสงสัยว่าข้อมูลรั่วไหล

ข้อ ๑๓๔ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่น เพื่ออ่าน รับ หรือส่งข้อความ ยกเว้น แต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์นั้น

ข้อ ๑๓๕ หลังจากเสร็จสิ้นการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องลงบันทึกออก (Logout) จากระบบทุกครั้ง

ข้อ ๑๓๖ หลังจากเสร็จสิ้นการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องลงบันทึกออก (Logout) จากระบบทุกครั้ง โดยอ้างตามประเภทข้อมูลที่ได้รับการจำแนก (Data Classification) ขององค์กร

ข้อ ๑๓๗ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๓๘ ห้ามส่ง...

ข้อ ๑๓๘ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๓๙ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๔๐ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๔๑ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อ ๑๔๒ ให้สำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๔๓ ผู้ใช้งานต้องใช้ความระมัดระวังในการเปิดไฟล์แนบและลิงก์ แม้จะมาจากผู้ส่งที่คุ้นเคย และผู้ดูแลระบบต้องมีเครื่องมือตรวจสอบมัลแวร์อัตโนมัติ (Email Security Sandbox) ก่อนถึงผู้ใช้

ข้อ ๑๔๔ หากพบไปรษณีย์อิเล็กทรอนิกส์ต้องสงสัยหรือไปรษณีย์อิเล็กทรอนิกส์หลอกลวง (Phishing) ห้ามตอบกลับหรือคลิกลิงก์ และต้องรายงาน (Report) ให้ศูนย์เทคโนโลยีสารสนเทศทราบทันที

ข้อ ๑๔๕ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กรหรือทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๔๖ ผู้ใช้งานควรบริหารจัดการกล่องจดหมายให้มีพื้นที่เพียงพอต่อการใช้งานเสมอ โดยลบไปรษณีย์อิเล็กทรอนิกส์ที่ไม่จำเป็นหรือไปรษณีย์อิเล็กทรอนิกส์ขยะออกตามวงจรชีวิตข้อมูล (Data Retention Policy)

ข้อ ๑๔๗ การสำรองข้อมูลไปรษณีย์อิเล็กทรอนิกส์เพื่ออ้างอิง ต้องทำบนระบบจัดเก็บข้อมูลที่องค์กรจัดเตรียมไว้ให้เท่านั้น ห้ามโอนย้ายไปเก็บในอุปกรณ์ส่วนตัวที่ไม่มีการควบคุมความปลอดภัย

ข้อ ๑๔๘ ต้องใช้ไปรษณีย์อิเล็กทรอนิกส์กลางภาครัฐในการรับส่งข้อมูลราชการตามมติคณะรัฐมนตรี และห้ามใช้อีเมล์ส่วนตัว เช่น Gmail Hotmail เป็นต้น ในการส่งข้อมูลลับของทางราชการโดยเด็ดขาด

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๔๙ ผู้ใช้งานต้องได้รับการอนุญาตจากผู้บังคับบัญชา และต้องลงทะเบียนกับผู้ดูแลระบบแล้วเท่านั้น ผู้ใช้งานต้องใช้รหัสผู้ใช้งานและรหัสผ่านของตนเองตามที่กำหนดโดยศูนย์เทคโนโลยีสารสนเทศเท่านั้น และผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

ข้อ ๑๕๐ ผู้ใช้งานต้องเชื่อมต่ออินเทอร์เน็ตผ่านเครือข่ายและอุปกรณ์รักษาความมั่นคงปลอดภัยที่องค์กรกำหนดเท่านั้น เช่น Proxy/Firewall/IPS เป็นต้น และห้ามใช้งานฮอตสปอตส่วนบุคคล (Personal Hotspot) หรือเครือข่ายหรืออุปกรณ์เชื่อมต่อภายนอกที่ไม่ได้รับอนุญาต (Shadow Network) กับอุปกรณ์ขององค์กร เพื่อหลีกเลี่ยงมาตรการรักษาความมั่นคงปลอดภัย

ข้อ ๑๕๑ คอมพิวเตอร์และอุปกรณ์พกพาที่ใช้เข้าถึงอินเทอร์เน็ต ต้องติดตั้งระบบป้องกันภัยคุกคามอัจฉริยะ เช่น EDR หรือ Next-Gen Antivirus เป็นต้น และต้องได้รับการปรับปรุงช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน (Patch Management) อย่างสม่ำเสมอ

ข้อ ๑๕๒ ข้อมูล...

ข้อ ๑๕๒ ข้อมูลที่รับ-ส่งผ่านอินเทอร์เน็ตต้องผ่านการตรวจสอบมัลแวร์และสิ่งแปลกปลอม โดยระบบรักษาความปลอดภัยเครือข่าย และผู้ใช้งานต้องหลีกเลี่ยงการเข้าถึงเว็บไซต์ที่ไม่ได้ใช้โปรโตคอลความปลอดภัย (HTTPS)

ข้อ ๑๕๓ ห้ามใช้ระบบอินเทอร์เน็ตขององค์กรเพื่อหาประโยชน์เชิงพาณิชย์ส่วนตัว หรือเข้าถึงเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม ความมั่นคงของชาติ ศาสนา และสถาบันพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นแหล่งแพร่กระจายมัลแวร์ เป็นต้น

ข้อ ๑๕๔ ห้ามเปิดเผยข้อมูลลับคดียาเสพติด ข้อมูลการสืบสวน หรือข้อมูลส่วนบุคคลที่อ่อนไหว ผ่านระบบอินเทอร์เน็ต กระดานสนทนา หรือสื่อสังคมออนไลน์ (Social Media) โดยไม่ได้รับอนุญาต และต้องปฏิบัติตามนโยบายการจัดชั้นความลับข้อมูลอย่างเคร่งครัด

ข้อ ๑๕๕ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน และต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

ข้อ ๑๕๖ ห้ามนำข้อมูลของทางราชการไปจัดเก็บหรือประมวลผลบนบริการคลาวด์ส่วนตัว และการดาวน์โหลดซอฟต์แวร์ต้องกระทำผ่านช่องทางที่ได้รับอนุญาต เพื่อป้องกันการละเมิดลิขสิทธิและมัลแวร์แฝง

ข้อ ๑๕๗ การใช้บริการปัญญาประดิษฐ์สาธารณะ (Public AI) เช่น ChatGPT เป็นต้น เพื่อช่วยในการปฏิบัติงาน ห้ามกรอกข้อมูลลับ ข้อมูลบุคคล หรือข้อมูลคดีขององค์กร ลงในระบบ AI เว้นแต่จะเป็นระบบ AI ภายในที่องค์กรจัดเตรียมไว้ให้เท่านั้น

ข้อ ๑๕๘ ผู้ใช้งานต้องไม่เสนอความคิดเห็น ยั่วยุ หรือใช้ข้อความที่ไม่สุภาพ ซึ่งส่งผลกระทบต่อภาพลักษณ์ขององค์กร ผ่านสื่อสังคมออนไลน์ และต้องระมัดระวังการถูกโจมตีแบบหลอกลวง

ข้อ ๑๕๙ ผู้ใช้งานต้องไม่นำเข้าหรือส่งต่อข้อมูลที่เป็นเท็จ ข้อมูลที่กระทบต่อความมั่นคงหรือข้อมูลลามกอนาจาร และต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

ข้อ ๑๖๐ หลังจากเสร็จสิ้นการใช้งาน ให้ทำการออกจากระบบ (Logout) และควรทำการล้างข้อมูลการใช้งาน (Clear Cache) หากมีการเข้าถึงข้อมูลสำคัญผ่านเว็บเบราว์เซอร์ เพื่อป้องกันการสวมสิทธิจากผู้อื่น

ข้อ ๑๖๑ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๖๒ แนวทางปฏิบัติการใช้งานทั่วไป

๑๖๒.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ใช้งาน เป็นสินทรัพย์ขององค์กรเพื่อใช้ในงานราชการ

๑๖๒.๒ โปรแกรมที่จะติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรซื้อลิขสิทธิมาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๖๒.๓ ไม่อนุญาต...

๑๖๒.๓ ไม่อนุญาตให้ผู้ใช้งานติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

๑๖๒.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลไปตรวจซ่อมจะต้องกระทำโดยเจ้าหน้าที่ขององค์กรหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับองค์กรเท่านั้น

๑๖๒.๕ ต้องตรวจสอบหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนใช้งานสื่อบันทึกพกพาต่าง ๆ

๑๖๒.๖ ผู้ใช้งาน มีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ที่ตนเองได้รับมอบให้ใช้งาน

๑๖๒.๗ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อเสร็จสิ้นการใช้งานประจำวัน หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๑๖๒.๘ ตั้งค่าพักหน้าจอ (Screen Saver) ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๑๖๒.๙ ห้ามนำเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินส่วนตัว มาใช้กับระบบเครือข่ายขององค์กร ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบขององค์กรก่อนใช้งาน ยกเว้นจะได้รับการลงทะเบียนและตรวจสอบมาตรฐานความปลอดภัย (Endpoint Compliance) จากผู้ดูแลระบบก่อนเชื่อมต่อเครือข่าย

ข้อ ๑๖๓ ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ข้อ ๑๖๔ การป้องกันจากโปรแกรมไม่ประสงค์ดี (Malware)

๑๖๔.๑ การป้องกันโปรแกรมประสงค์ร้ายจากสื่อบันทึกข้อมูล ผู้ใช้งานต้องตรวจสอบสื่อบันทึกข้อมูลภายนอก เช่น แฟลชไดรฟ์ และอุปกรณ์จัดเก็บข้อมูลอื่น เป็นต้น ด้วยโปรแกรมป้องกันภัยคุกคามก่อนใช้งานกับอุปกรณ์ขององค์กร และอุปกรณ์ขององค์กรต้องติดตั้งและเปิดใช้งานระบบป้องกันภัยคุกคาม เช่น EDR/Next-Gen Antivirus ตลอดเวลา เป็นต้น โดยผู้ใช้งาน ห้ามปิด หยุดการทำงาน หรือแก้ไขการตั้งค่าของระบบดังกล่าว เว้นแต่ผู้ดูแลระบบอนุญาตและดำเนินการตามขั้นตอนที่องค์กรกำหนด

๑๖๔.๒ ผู้ใช้งานต้องตรวจสอบเอกสารที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือแฟ้มข้อมูลที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๑๖๔.๓ ผู้ใช้งานต้องตรวจจับชุดคำสั่งไม่ประสงค์ดีบนแฟ้มข้อมูลคอมพิวเตอร์ที่จะสร้างความเสียหาย ทำลาย หรือแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น จนกระทั่งไม่สามารถใช้ปฏิบัติงานได้ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๖๕ การสำรองข้อมูลและการกู้คืน

๑๖๕.๑ ผู้ใช้งานต้องสำรองข้อมูลสำคัญลงบนระบบจัดเก็บข้อมูลกลาง (Centralized Storage/Cloud) ที่องค์กรจัดเตรียมไว้ให้ เพื่อความปลอดภัยและการบริหารจัดการข้อมูลในภาพรวม

๑๖๕.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๖๕.๓ ผู้ใช้งานต้องประเมินความเสี่ยงของข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ เพื่อมิให้เกิดความเสียหายต่อการดำเนินงานขององค์กร

๑๖๕.๔ แผ่นสื่อสำรอง...

๑๖๕.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก ต้องทำลายด้วยวิธีที่ปลอดภัยตามที่องค์กรกำหนดไว้เป็นอย่างน้อย เช่น การย่อยทำลาย หรือใช้ซอฟต์แวร์ลบข้อมูลถาวร เป็นต้น

ข้อ ๑๖๖ การใช้งานเครือข่ายสังคมออนไลน์ มีดังนี้

๑๖๖.๑ ผู้ใช้งานสามารถใช้งานเครือข่ายสังคมออนไลน์ที่ได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อใช้ประโยชน์ในการปฏิบัติงานราชการ

๑๖๖.๒ ผู้ใช้งานไม่สามารถติดตั้งโปรแกรมหรืออุปกรณ์ใช้งานเครือข่ายสังคมออนไลน์ใด ๆ ในระบบเครือข่ายขององค์กร ยกเว้น โปรแกรมประเภทเครือข่ายสังคมออนไลน์ที่ได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ในการปฏิบัติงานราชการ

๑๖๖.๓ ผู้ใช้งานที่มีความต้องการหรือมีความจำเป็นที่ต้องการใช้โปรแกรมหรือเว็บไซต์เครือข่ายสังคมออนไลน์เพื่อปฏิบัติงานราชการ ต้องขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์โมบายส่วนบุคคล (Mobile-BYOD)

ข้อ ๑๖๗ ผู้ดูแลระบบต้องกำหนดและควบคุมการตั้งค่าคอมพิวเตอร์ขององค์กร ได้แก่ การตั้งชื่อเครื่อง (Computer Name) การเข้าร่วมโดเมน (Domain) การกำหนดไอพีแอดเดรสและค่าพารามิเตอร์เครือข่าย รวมถึงการเชื่อมต่อเข้าสู่เครือข่ายภายในองค์กรตามมาตรฐานที่องค์กรกำหนด ดังนี้

๑๖๗.๑ การตั้งชื่อเครื่องต้องประกอบด้วย ชื่อย่อ กอง/สำนัก/กลุ่มขึ้นตรง เป็น อักษรภาษาอังกฤษ ตามด้วยเครื่องหมาย “-” หมายเลขไอพีแอดเดรสประจำเครือข่าย ตามด้วยเครื่องหมาย “-” และตามด้วย สามดิจิตสุดท้ายของหมายเลขไอพีแอดเดรส

๑๖๗.๒ การใช้หมายเลขไอพีแอดเดรส รุ่น ๔ (IPV๔) แบบ Private Network

รายการ	ช่วงของ IP Address
สงวนไว้สำหรับศูนย์เทคโนโลยีสารสนเทศ	๑๙๒.๑๖๘.X.๑-๕๐
เครื่องคอมพิวเตอร์ลูกข่าย (PC)	๑๙๒.๑๖๘.X.๕๑-๑๕๐
เครื่องคอมพิวเตอร์ลูกข่าย (Notebook)	๑๙๒.๑๖๘.X.๑๕๑-๒๐๐
เครื่องพิมพ์คอมพิวเตอร์และอุปกรณ์อื่น ๆ	๑๙๒.๑๖๘.X.๒๐๑-๒๓๐
เครื่องคอมพิวเตอร์ สำหรับผู้มาติดต่อ/ประสานงาน	๑๙๒.๑๖๘.X.๒๓๑-๒๕๔

ข้อ ๑๖๘ แนวทางปฏิบัติการใช้งานทั่วไป

๑๖๘.๑ เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ใช้งานเท่านั้น

๑๖๘.๒ โปรแกรมที่จะติดตั้งลงบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่องค์กรจัดซื้อลิขสิทธิมาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมไปติดตั้งบนเครื่องส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๖๘.๓ ไม่อนุญาตให้ผู้ใช้งาน ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมหรือระบบปฏิบัติการด้วยตนเอง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๑๖๘.๔ การเคลื่อนย้าย...

๑๖๘.๔ การเคลื่อนย้ายหรือส่งเครื่องไปตรวจซ่อมต้องกระทำโดยเจ้าหน้าที่ขององค์กรหรือผู้รับจ้างที่ทำสัญญากับองค์กรเท่านั้น โดยคอมพิวเตอร์แบบพกพาต้องบรรจุในกระเป๋าเฉพาะเพื่อป้องกันการกระทบกระเทือน

๑๖๘.๕ ผู้ใช้งาน มีหน้าที่รับผิดชอบดูแลรักษาความปลอดภัยของเครื่องที่ตนได้รับมอบหมาย และต้องระวังป้องกันเครื่องสูญหาย โดยเฉพาะเมื่อนำไปใช้งานนอกสถานที่ ห้ามวางทิ้งไว้ในที่สาธารณะหรือในยานพาหนะโดยไม่มีผู้ดูแล

๑๖๘.๖ ปิดเครื่องคอมพิวเตอร์เมื่อเสร็จสิ้นการใช้งานประจำวัน และให้ตั้งค่าพักหน้าจอ (Screen Saver) เพื่อล็อกหน้าจออัตโนมัติ เมื่อไม่ได้ใช้งานเกิน ๓๐ นาที

ข้อ ๑๖๙ การป้องกันจากโปรแกรมไม่ประสงค์ดี (Malware) บนเครื่องคอมพิวเตอร์แบบพกพา

๑๖๙.๑ เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งและเปิดใช้งานโปรแกรมป้องกันภัยคุกคาม (Antivirus/EDR) ที่องค์กรกำหนด และต้องอัปเดตฐานข้อมูลให้เป็นปัจจุบันอยู่เสมอ

๑๖๙.๒ ผู้ใช้งาน ต้องตรวจสอบหาไวรัสก่อนใช้งานสื่อบันทึกพกพา เช่น Flash Drive External Hard Disk เป็นต้น และตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตทุกครั้ง

๑๖๙.๓ ผู้ใช้งาน ต้องไม่ปิดการทำงานของโปรแกรมป้องกันไวรัส และหากตรวจพบพฤติกรรมผิดปกติของระบบ ต้องรีบแจ้งผู้ดูแลระบบทันที

ข้อ ๑๗๐ การควบคุมการเข้าถึงและรหัสผ่านบนเครื่องคอมพิวเตอร์แบบพกพา

๑๗๐.๑ ผู้ใช้งานต้องกำหนดบัญชีผู้ใช้งาน (User Account) และรหัสผ่านในการเข้าสู่ระบบตามมาตรฐานที่องค์กรกำหนด โดยห้ามบันทึกรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือจดไว้ในที่เปิดเผย

๑๗๐.๒ การเข้าใช้งานจากระยะไกล (Remote Access) ต้องผ่านการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) ตามที่องค์กรกำหนด

๑๗๐.๓ สำหรับคอมพิวเตอร์แบบพกพา ต้องมีการเข้ารหัสข้อมูลในฮาร์ดดิสก์ (Disk Encryption) เพื่อป้องกันการรั่วไหลของข้อมูลในกรณีเครื่องสูญหายหรือถูกโจรกรรม

ข้อ ๑๗๑ ผู้ดูแลระบบต้องจัดให้มีระบบการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control : NAC) สำหรับควบคุมเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่ายขององค์กร

ข้อ ๑๗๒ ผู้ดูแลระบบหรือผู้ประสานงานจะทำการยกเลิกการเชื่อมต่อทันที โดยไม่แจ้งให้ผู้ใช้งานทราบก่อนล่วงหน้า เมื่อตรวจพบว่าผู้ใช้งานใช้งานผิดจากวัตถุประสงค์ตามที่แจ้งไว้หรือมีพฤติการณ์เสี่ยงต่อความปลอดภัยระบบสารสนเทศขององค์กร

ข้อ ๑๗๓ การสำรองข้อมูลและการกู้คืนบนเครื่องคอมพิวเตอร์แบบพกพา

๑๗๓.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลสำคัญไว้บนระบบจัดเก็บข้อมูลส่วนกลาง (Network Drive) หรือระบบคลาวด์ขององค์กรเป็นหลัก เพื่อความปลอดภัยและความต่อเนื่องในการปฏิบัติงาน

๑๗๓.๒ กรณีสำรองข้อมูลบนสื่อบันทึกภายนอก ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหล และต้องทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑๗๓.๓ สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ต้องถูกทำลายไม่ให้สามารถนำไปใช้งานหรือกู้คืนข้อมูลได้อีก โดยต้องดำเนินการตามวิธีการที่ศูนย์เทคโนโลยีสารสนเทศกำหนด

ข้อ ๑๗๔ มาตรการ...

ข้อ ๑๗๔ มาตรการควบคุมการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์แบบพกพา

๑๗๔.๑ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวมาเชื่อมต่อกับระบบเครือข่ายขององค์กร เว้นแต่จะได้รับการตรวจสอบและอนุญาตจากผู้ดูแลระบบผ่านระบบควบคุมการเข้าถึงเครือข่าย (NAC)

๑๗๔.๒ ผู้ดูแลระบบมีสิทธิยกเลิกการเชื่อมต่อทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากตรวจพบว่ามีการใช้งานผิดวัตถุประสงค์ หรือมีพฤติการณ์ที่เสี่ยงต่อความปลอดภัยของระบบสารสนเทศองค์กร

ส่วนที่ ๑๖ การตรวจจับการบุกรุก

ข้อ ๑๗๕ องค์กรกำหนดให้มีการติดตั้งและใช้งานระบบตรวจจับและหรือป้องกันการบุกรุกเครือข่าย (IDS/IPS) เพื่อเฝ้าระวัง ตรวจสอบ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อสินทรัพย์ ระบบสารสนเทศ และข้อมูลขององค์กร นโยบายนี้กำหนดหลักเกณฑ์การดำเนินงานด้าน IDS/IPS รวมถึงบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องในการติดตั้ง กำหนดค่า เฝ้าระวัง ตอบสนอง และทบทวนการทำงานของระบบ

ข้อ ๑๗๖ นโยบายการตรวจจับการบุกรุกนี้ ครอบคลุมเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย (Hosts) ทุกเครื่องในเครือข่ายขององค์กร รวมถึงระบบเครือข่ายและช่องทางการรับส่งข้อมูลทั้งหมด ไม่จำกัดเฉพาะเส้นทางผ่านอินเทอร์เน็ต

ข้อ ๑๗๗ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจากระบบตรวจจับการบุกรุก

ข้อ ๑๗๘ ระบบทั้งหมดในเขตเครือข่ายกันชน (Demilitarized Zone: DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนติดตั้งและเปิดให้บริการ

ข้อ ๑๗๙ ต้องบันทึกผลการตรวจสอบโฮสต์ (Host) และระบบเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านระบบตรวจจับการบุกรุก

ข้อ ๑๘๐ ต้องตรวจสอบและอัพเดตแพตช์ (Patch/Signature) ของระบบตรวจจับการบุกรุกเป็นประจำ

ข้อ ๑๘๑ ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

ข้อ ๑๘๒ ระบบตรวจจับการบุกรุก จะทำงานภายใต้กฎควบคุมพื้นฐานของอุปกรณ์ป้องกันเครือข่ายที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๘๓ ต้องตรวจสอบข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบตรวจจับการบุกรุก (host-based IDS) เป็นประจำทุกวัน

ข้อ ๑๘๔ จะต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบทันทีที่ตรวจพบ

ข้อ ๑๘๕ จะต้อง...

ข้อ ๑๘๕ จะต้องรายงานพฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทราบภายใน ๑ ชั่วโมงหลังจากตรวจพบ

ข้อ ๑๘๖ ต้องเก็บบันทึกข้อมูลการตรวจสอบการบุกรุกทั้งหมดไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๘๗ องค์กรต้องจัดให้มีระบบตรวจจับการบุกรุกที่สามารถตรวจพบ รายงาน และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเหมาะสม เพื่อลดความเสียหาย กำจัดซอฟต์แวร์ที่ไม่พึงประสงค์ ป้องกันการเกิดเหตุซ้ำ และดำเนินการตามแผนที่กำหนดไว้

ข้อ ๑๘๘ หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันท่วงที กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่ายและให้แก้ไขเครื่องนั้นทันที

ข้อ ๑๘๙ องค์กรมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องแจ้งแก่ผู้ใช้งานทราบล่วงหน้า

ข้อ ๑๙๐ ผู้ที่ถูกตรวจพบว่ามีพฤติการณ์ละเมิดนโยบายด้านความมั่นคงปลอดภัยขององค์กร หรือพยายามเข้าถึงหรือโจมตีระบบสารสนเทศโดยมิชอบ ให้ระงับการใช้งานเครือข่ายทันที และหากการกระทำดังกล่าวเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือก่อให้เกิดความเสียหายต่อข้อมูลหรือสินทรัพย์ขององค์กร ให้ดำเนินการตามกฎหมายที่เกี่ยวข้อง

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๙๑ ปรับปรุงระบบปฏิบัติการ (Operating System Update) ผู้ดูแลระบบต้องติดตั้งและปรับปรุงระบบปฏิบัติการของเครื่องแม่ข่ายและอุปกรณ์ระบบให้เป็นไปตามมาตรฐานขององค์กรอย่างน้อยต้องดำเนินการ ดังนี้

๑๙๑.๑ ตรวจสอบความพร้อมของเครื่องและความถูกต้องของรุ่นระบบปฏิบัติการก่อนติดตั้ง และห้ามใช้งานระบบปฏิบัติการที่หมดระยะเวลาการสนับสนุนจากผู้ผลิต

๑๙๑.๒ ติดตั้งแพตช์ความปลอดภัยและแก้ไขช่องโหว่ที่เกี่ยวข้องก่อนเปิดใช้งานระบบ และดำเนินการติดตั้งแพตช์อย่างต่อเนื่องตามรอบเวลาที่องค์กรกำหนด

๑๙๑.๓ กำหนดค่าความปลอดภัยของระบบปฏิบัติการให้เป็นไปตามมาตรฐานความปลอดภัยขององค์กร (Security Baseline) และปิดบริการหรือพอร์ตที่ไม่จำเป็นต่อการใช้งาน

๑๙๑.๔ กำหนดชื่อเครื่อง (Computer Name) และกำหนดค่าเครือข่าย เช่น หมายเลขไอพี (IP Address) และค่าพารามิเตอร์ที่จำเป็นให้ถูกต้องตามมาตรฐานขององค์กร

๑๙๑.๕ จำกัดการใช้งานบัญชีสิทธิพิเศษ และกำหนดการเข้าถึงสิทธิของผู้ดูแลระบบตามหลักการอนุญาตเท่าที่จำเป็น (Least Privilege)

๑๙๑.๖ ติดตั้งและเปิดใช้งานโปรแกรมป้องกันไวรัส (Antivirus) และปรับปรุงฐานข้อมูลไวรัส (Virus Definition) ให้เป็นปัจจุบัน รวมถึงกำหนดค่าการตรวจสอบ การตรวจจับ และการปรับปรุงโปรแกรมตามที่องค์กรกำหนด

ข้อ ๑๙๒ ผู้ดูแล...

ข้อ ๑๙๒ ผู้ดูแลระบบต้องกำหนดและควบคุมบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบให้เหมาะสมและมีความมั่นคงปลอดภัย โดยอย่างน้อยต้องดำเนินการ ดังนี้

๑๙๒.๑ แยกบัญชีผู้ดูแลระบบ (Administrator) ออกจากบัญชีใช้งานทั่วไป และกำหนดสิทธิการใช้งานเท่าที่จำเป็น (Least Privilege)

๑๙๒.๒ จัดทำและปรับปรุงทะเบียนบัญชีผู้ใช้งานและสิทธิการเข้าถึง พร้อมทั้งยกเลิกสิทธิทันทีเมื่อหมดความจำเป็นหรือเมื่อผู้ใช้งานพ้นสภาพ

๑๙๒.๓ ทบทวนสิทธิการเข้าถึงระบบเป็นประจำอย่างน้อยทุก ๓ เดือน หรือเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ

ข้อ ๑๙๓ ปรับปรุงการรักษาความปลอดภัย Anti-Virus (System Security & Antivirus Update) ผู้ดูแลระบบต้องจัดให้เครื่องแม่ข่ายและเครื่องลูกข่ายมีมาตรการป้องกันและเฝ้าระวังภัยคุกคามโดยอย่างน้อยต้องดำเนินการ ดังนี้

๑๙๓.๑ ติดตั้งและเปิดใช้งานโปรแกรมป้องกันภัยคุกคาม เช่น ระบบตรวจจับและตอบสนองภัยคุกคามบนเครื่องปลายทาง (Endpoint Detection and Response: EDR) และโปรแกรมป้องกันไวรัส (Antivirus) และปรับปรุงฐานข้อมูล ลายมือชื่อหรือลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ และรายการป้องกันโดยอัตโนมัติหรือเป็นประจำตามที่องค์กรกำหนด เป็นต้น

๑๙๓.๒ กำหนดให้มีการสแกนตรวจหาโปรแกรมประสงค์ร้ายตามรอบเวลาและจัดให้มีการเฝ้าระวังเหตุผิดปกติพร้อมแนวทางตอบสนอง

๑๙๓.๓ ห้ามผู้ใช้งานปิด หยุดการทำงาน หรือแก้ไขการตั้งค่าระบบป้องกันภัยคุกคาม เว้นแต่ผู้ดูแลระบบอนุญาตและดำเนินการตามขั้นตอนที่องค์กรกำหนด

ข้อ ๑๙๔ ติดตั้งหรือปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation) ผู้ดูแลระบบต้องติดตั้งและกำหนดค่าระบบจัดการฐานข้อมูลให้ปลอดภัยและสอดคล้องกับข้อกำหนดของระบบโดยอย่างน้อยต้องดำเนินการ ดังนี้

๑๙๔.๑ กำหนดผู้บริหารระบบฐานข้อมูล (Database Administrator: DBA) บัญชีผู้ใช้งาน และสิทธิการใช้งานตามบทบาทหน้าที่ และบันทึกไว้เป็นหลักฐาน

๑๙๔.๒ กำหนดค่าความปลอดภัยของฐานข้อมูล และปรับปรุงแพตช์หรือการตั้งค่าที่เกี่ยวข้องเป็นประจำตามที่องค์กรกำหนด

๑๙๔.๓ จัดให้มีการบันทึกเหตุการณ์สำคัญของฐานข้อมูลตามที่องค์กรกำหนด และกำหนดมาตรการป้องกันการเข้าถึงโดยมิชอบ

ข้อ ๑๙๕ การติดตั้งระบบสารสนเทศ การกำหนดค่า และการควบคุมการเปลี่ยนแปลง (Application/Service Deployment & Change Control) โดยผู้ดูแลระบบต้องติดตั้งและกำหนดค่าระบบสารสนเทศหรือบริการให้ปลอดภัยก่อนเปิดใช้งาน และต้องควบคุมการเปลี่ยนแปลงอย่างเหมาะสม โดยดำเนินการอย่างน้อย ดังต่อไปนี้

๑๙๕.๑ ติดตั้งโปรแกรมระบบสารสนเทศตามรุ่นที่องค์กรอนุมัติ และกำหนดค่าโปรแกรมหรือบริการ (Services) ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง รวมทั้ง ปิดบริการที่ไม่จำเป็น

๑๙๕.๒ ตรวจสอบและแก้ไขช่องโหว่ที่เกี่ยวข้องก่อนเปิดใช้งานจริง และจัดให้มีมาตรการติดตามการแก้ไขไฟล์หรือส่วนประกอบสำคัญของระบบ (File Integrity Monitoring) ตามที่องค์กรกำหนด

๑๙๕.๓ กำหนด...

๑๙๕.๓ กำหนดบัญชีผู้ใช้และสิทธิการเข้าถึงฐานข้อมูลหรือระบบสารสนเทศตามหลักการอนุญาตเท่าที่จำเป็น และจัดทำทะเบียนกำกับบัญชีผู้ใช้งานดังกล่าว

๑๙๕.๔ กำหนดหลักเกณฑ์การสำรองข้อมูลและการทดสอบกู้คืน (Restore Test) ตามรอบเวลาที่องค์กรกำหนด เก็บหลักฐานผลการทดสอบ และปรับปรุงหลักเกณฑ์และแนวทางการสำรองข้อมูลให้เหมาะสม

๑๙๕.๕ บันทึกข้อกำหนดการติดตั้ง การกำหนดค่า (Configuration) และการเปลี่ยนแปลงที่สำคัญของระบบทุกครั้ง เพื่อใช้ในการตรวจสอบย้อนหลัง

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Management)

ข้อ ๑๙๖ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) และระยะเวลาการเก็บรักษา องค์กรต้องจัดให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ในสื่อจัดเก็บที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และตรวจสอบย้อนกลับได้ โดยต้องสามารถระบุตัวบุคคลที่เข้าถึงข้อมูลดังกล่าวได้ รวมทั้งต้องกำหนดชั้นความลับและสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์ให้เหมาะสม ทั้งนี้ ให้เก็บรักษาข้อมูลไม่น้อยกว่า ๙๐ วัน หรือเป็นไปตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ข้อ ๑๙๗ การห้ามแก้ไขหรือลบข้อมูลจราจรคอมพิวเตอร์ ห้ามมิให้ผู้ใดแก้ไข เปลี่ยนแปลง ลบ ทำลาย ตัดทอน หรือกระทำการใด ๆ ที่ทำให้ข้อมูลจราจรคอมพิวเตอร์ (Log) ที่จัดเก็บไว้สูญเสียความครบถ้วนหรือความถูกต้อง เว้นแต่เป็นการดำเนินการตามอำนาจหน้าที่ที่ได้รับอนุญาตเป็นลายลักษณ์อักษร และต้องมีการบันทึกหลักฐานการดำเนินการเพื่อการตรวจสอบย้อนหลัง

ข้อ ๑๙๘ ประเภทของบันทึกและรายการเหตุการณ์ขั้นต่ำที่ต้องจัดเก็บ องค์กรต้องจัดให้มีการบันทึกเหตุการณ์และกิจกรรมการใช้งานของระบบอย่างเหมาะสม โดยอย่างน้อยต้องครอบคลุม

๑๙๘.๑ บันทึกการเข้าออกระบบและการพิสูจน์ตัวตน (Authentication Logs) เช่น การเข้าสู่ระบบสำเร็จหรือไม่สำเร็จ การล็อกบัญชี และเหตุการณ์ยืนยันตัวตนแบบหลายปัจจัย (MFA) เป็นต้น

๑๙๘.๒ บันทึกเหตุการณ์ของระบบงาน/แอปพลิเคชัน (Application Logs) ที่เกี่ยวข้องกับการใช้งาน การเปลี่ยนแปลงค่ากำหนด และข้อผิดพลาดสำคัญ

๑๙๘.๓ บันทึกจากระบบและอุปกรณ์รักษาความมั่นคงปลอดภัย (Security Logs) เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) หรือระบบที่เทียบเท่า เป็นต้น

ทั้งนี้ ต้องเก็บรักษาบันทึกดังกล่าวไม่น้อยกว่า ๙๐ วัน หรือเป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อกำหนดที่เกี่ยวข้อง

ข้อ ๑๙๙ มาตรการป้องกันการแก้ไขเปลี่ยนแปลงและการจำกัดสิทธิการเข้าถึงบันทึกองค์กรต้องจัดให้มีมาตรการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกดังกล่าวให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายตามบทบาทหน้าที่ ทั้งนี้ การเข้าถึงหรือเรียกดูข้อมูลจราจรคอมพิวเตอร์ต้องสามารถตรวจสอบย้อนกลับได้ และให้มีการบันทึกการเข้าถึงข้อมูลจราจรคอมพิวเตอร์ เพื่อการตรวจสอบย้อนหลัง

ข้อ ๒๐๐ การจัดเก็บบันทึกแบบรวมศูนย์ (Centralized Log Management) องค์กรควรจัดให้มีระบบจัดเก็บบันทึกแบบรวมศูนย์ เพื่อรวบรวม Log จากระบบสำคัญไว้ในจุดจัดเก็บกลางที่แยกจากระบบต้นทาง และกำหนดมาตรการคุ้มครองความถูกต้องแท้จริงของบันทึกตามความเหมาะสม

ข้อ ๒๐๑ การกำหนด...

ข้อ ๒๐๑ การกำหนดเวลาอ้างอิงของบันทึก (Time Synchronization) ระบบและอุปกรณ์ที่เกี่ยวข้องต้องกำหนดเวลาอ้างอิงให้ตรงกัน โดยใช้ระบบเทียบเวลามาตรฐาน เช่น NTP เป็นต้น เพื่อให้สามารถเชื่อมโยงเหตุการณ์และตรวจสอบย้อนหลังได้อย่างถูกต้อง

ข้อ ๒๐๒ การทบทวนบันทึกและการแจ้งเตือนเหตุผิดปกติ (Log Review & Alerting) องค์กรต้องกำหนดให้มีการทบทวนบันทึกและเฝ้าระวังเหตุผิดปกติของระบบตามระดับความสำคัญของระบบ รวมถึงกำหนดเงื่อนไขการแจ้งเตือนเหตุการณ์สำคัญ เช่น การพยายามเข้าสู่ระบบผิดพลาดจำนวนมาก การเปลี่ยนแปลงสิทธิ การแก้ไขค่ากำหนดสำคัญ หรือการตรวจพบภัยคุกคามระดับสูง เป็นต้น

ข้อ ๒๐๓ การคุ้มครองข้อมูลส่วนบุคคลในการจัดเก็บและใช้บันทึก (Privacy by Design for Logs) การจัดเก็บและใช้ข้อมูลจราจรคอมพิวเตอร์ต้องดำเนินการเท่าที่จำเป็นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัย จำกัดการเข้าถึงตามบทบาทหน้าที่ และจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและข้อกำหนดขององค์กร

ส่วนที่ ๑๙ สื่อบันทึกข้อมูลแบบถอดแยกได้ (Removable Media)

ข้อ ๒๐๔ การใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้กับอุปกรณ์ขององค์กร ให้ใช้ได้เฉพาะกรณีจำเป็นตามภารกิจ และต้องได้รับอนุญาตจากผู้บริหารตามสายงานและ/หรือผู้ดูแลระบบตามที่องค์กรกำหนด

ข้อ ๒๐๕ สื่อบันทึกข้อมูลแบบถอดแยกได้ที่ได้รับอนุญาต (ขึ้นทะเบียน) ระบุผู้รับผิดชอบ และควบคุมการนำเข้าและหรือนำออกข้อมูล ตามมาตรการขององค์กร และต้องเก็บรักษาในที่ปลอดภัยเมื่อไม่ใช้งาน

ข้อ ๒๐๖ ก่อนใช้งานสื่อบันทึกข้อมูลแบบถอดแยกได้ ต้องสแกนตรวจหาโปรแกรมประสงค์ร้ายด้วยระบบป้องกันภัยคุกคามที่ได้รับการปรับปรุงให้เป็นปัจจุบันเสมอ

ข้อ ๒๐๗ ห้ามใช้สื่อบันทึกข้อมูลแบบถอดแยกได้ที่ไม่สามารถระบุเจ้าของหรือแหล่งที่มาได้ และให้ส่งมอบสื่อบันทึกข้อมูลดังกล่าวแก่ผู้ดูแลระบบ เพื่อทำการตรวจสอบความมั่นคงปลอดภัย

ข้อ ๒๐๘ ห้ามเคลื่อนย้ายสื่อบันทึกข้อมูลออกนอกพื้นที่ทำงานหรือพื้นที่ที่องค์กรกำหนด เว้นแต่ได้รับอนุญาตและมีคำสั่งอย่างถูกต้อง

ข้อ ๒๐๙ กรณีสื่อบันทึกข้อมูลบรรจุข้อมูลสำคัญ ข้อมูลลับ ให้ใช้มาตรการเข้ารหัสและจำกัดสิทธิการเข้าถึงตามที่องค์กรกำหนด

ข้อ ๒๑๐ การทำลายข้อมูลในสื่อบันทึกข้อมูลแบบถอดแยกได้ให้ปฏิบัติตามแนวปฏิบัติการทำลายสื่อบันทึกข้อมูลขององค์กร โดยต้องมีผู้รับผิดชอบและมีหลักฐานการดำเนินการ

ส่วนที่ ๒๐ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรภายนอกหรือผู้รับจ้างภายนอก (Outsource)

ข้อ ๒๑๑ การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในขอบเขตงานและสัญญาจ้างผู้รับผิดชอบโครงการหรืองานที่มีการจ้างผู้รับจ้างภายนอกต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในขอบเขตงาน และสัญญาจ้างให้ชัดเจนโดยอย่างน้อยต้องกำหนดให้ผู้รับจ้างปฏิบัติตามมาตรการขององค์กร ได้แก่ การจำกัดสิทธิเท่าที่จำเป็น การพิสูจน์ตัวตน การบันทึกการใช้งาน (Log) การห้ามทดสอบบนระบบจริงสำหรับระบบสำคัญ และการติดตั้งใช้งานจริงต้องได้รับอนุมัติก่อน รวมถึงต้องรักษาความลับและสื่อสารข้อมูลเท่าที่จำเป็นและต้องจัดทำข้อตกลงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามแบบที่องค์กรกำหนด

ข้อ ๒๑๒ มาตรการ...

ข้อ ๒๑๒ มาตรการความปลอดภัยทางกายภาพ ณ สถานที่ปฏิบัติงานขององค์กร ก่อนอนุญาตให้ผู้รับจ้างเริ่มปฏิบัติงานภายในองค์กร ต้องจัดให้มีการกำหนดพื้นที่ปฏิบัติงานและสิทธิการเข้าถึงพื้นที่ตามระดับความสำคัญ รวมถึงกำหนดขั้นตอนการอนุญาตและเงื่อนไขการเข้าออกพื้นที่ตามที่องค์กรกำหนด

ข้อ ๒๑๓ มาตรการความมั่นคงปลอดภัยสำหรับการปฏิบัติงานจากระยะไกลของผู้รับจ้าง การปฏิบัติงานจากระยะไกลของผู้รับจ้างต้องเชื่อมต่อผ่านช่องทางที่องค์กรกำหนด และต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายก่อน โดยต้องมีการพิสูจน์ตัวตน การจำกัดสิทธิเท่าที่จำเป็น และการบันทึกการใช้งาน (Log) ตามที่องค์กรกำหนด

ข้อ ๒๑๔ ความปลอดภัยทางกายภาพของสถานที่ปฏิบัติงานจากระยะไกล ผู้รับผิดชอบโครงการต้องกำหนดมาตรการความปลอดภัยทางกายภาพสำหรับสถานที่ปฏิบัติงานจากระยะไกล เพื่อป้องกันการเข้าถึงอุปกรณ์หรือข้อมูลโดยไม่ได้รับอนุญาต และป้องกันการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

ข้อ ๒๑๕ มาตรการกำกับดูแลผู้รับจ้างระหว่างปฏิบัติงานภายในองค์กร กรณีผู้รับจ้างเข้าปฏิบัติงานภายในองค์กรต้องอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่ขององค์กรตลอดระยะเวลาการปฏิบัติงาน และต้องปฏิบัติตามมาตรการควบคุมผู้มาติดต่อขององค์กร เช่น การลงทะเบียนเข้าออก การติดบัตร และการตรวจสอบอุปกรณ์เข้าออกตามที่องค์กรกำหนด เป็นต้น

ส่วนที่ ๒๑ การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ

ข้อ ๒๑๖ การเปลี่ยนแปลงอุปกรณ์ระบบเครือข่ายและการสื่อสาร

๒๑๖.๑ ผู้รับผิดชอบงานหรือผู้ดำเนินการเปลี่ยนแปลงต้องจัดทำคำขอเปลี่ยนแปลง ระบุรายละเอียดรายการที่จะเปลี่ยนแปลง เหตุผล และผลกระทบเบื้องต้น พร้อมขออนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ ก่อนดำเนินการทุกครั้ง

๒๑๖.๒ ก่อนดำเนินการต้องวิเคราะห์ผลกระทบและความเสี่ยง กำหนดแผนการดำเนินงาน แผนทดสอบ และแผนย้อนกลับ (Rollback) ให้เหมาะสมกับระดับความสำคัญของระบบและบริการที่ได้รับผลกระทบ

๒๑๖.๓ ก่อนการเปลี่ยนแปลงต้องสำรองค่ากำหนด (Configuration) ที่เกี่ยวข้องและจัดเก็บค่ากำหนดก่อนและหลังการเปลี่ยนแปลง รวมถึงหลักฐานประกอบ เพื่อใช้ในการตรวจสอบย้อนหลัง

๒๑๖.๔ เมื่อดำเนินการแล้วเสร็จ ต้องทดสอบยืนยันผลการเปลี่ยนแปลง รายงานผลการดำเนินการและผลกระทบต่อผู้บังคับบัญชาหรือผู้มีอำนาจอนุมัติ และจัดเก็บบันทึกการเปลี่ยนแปลงเป็นหลักฐาน

ข้อ ๒๑๗ การควบคุมการเปลี่ยนแปลง (Change Control)

๒๑๗.๑ กรณีเหตุฉุกเฉินหรือมีความจำเป็นเร่งด่วนที่ต้องดำเนินการทันที ให้ดำเนินการตามแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP) และหรือแผนฉุกเฉินที่องค์กรกำหนด พร้อมบันทึกรายละเอียดการเปลี่ยนแปลงและรายงานผลภายหลังโดยเร็ว

๒๑๗.๒ กรณีการเปลี่ยนแปลงที่ทราบล่วงหน้า ให้ผู้รับผิดชอบแจ้งผู้ได้รับผลกระทบผ่านช่องทางที่องค์กรกำหนด และให้ผู้ดูแลระบบเตรียมมาตรการเฝ้าระวังและติดตามผลตามระดับความเสี่ยง

๒๑๗.๓ กรณีการเปลี่ยนแปลงที่มีผลกระทบสูง ให้จัดทำแผนรองรับการเปลี่ยนแปลง กำหนดช่วงเวลาดำเนินการที่เหมาะสม เช่น นอกช่วงเวลาการใช้งาน และจัดเตรียมแผนกู้คืนหรือแผนย้อนกลับกรณีเกิดปัญหา เป็นต้น

ข้อ ๒๑๘ การทบทวน...

ข้อ ๒๑๘ การทบทวนความเหมาะสมของสินทรัพย์และทรัพยากรด้านเทคโนโลยีสารสนเทศ

๒๑๘.๑ องค์กรต้องทบทวนความเพียงพอและความเหมาะสมของสินทรัพย์และทรัพยากรด้านเทคโนโลยีสารสนเทศเป็นประจำ ตามรอบเวลาที่กำหนด เพื่อให้รองรับภารกิจและความมั่นคงปลอดภัยของระบบสารสนเทศ

๒๑๘.๒ หน่วยงานที่ประสงค์ขอรับการสนับสนุนสินทรัพย์และทรัพยากรต้องยื่นคำขอระบุความจำเป็น ขอบเขตการใช้งาน และเหตุผลประกอบ ต่อหน่วยงานด้านเทคโนโลยีสารสนเทศ ตามแบบและขั้นตอนที่องค์กรกำหนด

๒๑๘.๓ ให้คณะกรรมการหรือคณะทำงานที่องค์กรแต่งตั้งพิจารณาคำขอตามรอบที่กำหนด และบันทึกผลการพิจารณาและมติไว้เป็นหลักฐาน

ส่วนที่ ๒๒ การเข้ารหัสข้อมูล มาตรการการเข้ารหัสข้อมูล

ข้อ ๒๑๙ นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

๒๑๙.๑ องค์กรกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลเพื่อคุ้มครองข้อมูลตามระดับชั้นความลับ กฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง โดยเฉพาะข้อมูลสำคัญและข้อมูลที่รับส่งผ่านเครือข่าย

๒๑๙.๒ การรับส่งข้อมูลระหว่างระบบต้องใช้การเข้ารหัสในระหว่างการส่งผ่าน (Encryption in Transit) โดยใช้มาตรฐาน TLS ตามที่องค์กรกำหนด และต้องกำหนดค่าความปลอดภัยให้เหมาะสม เช่น ปิดการใช้งานอัลกอริทึมหรือโปรโตคอลที่ไม่ปลอดภัย เป็นต้น

๒๑๙.๓ ข้อมูลที่จัดเก็บและมีความสำคัญตามที่องค์กรกำหนด ต้องใช้การเข้ารหัสในขณะจัดเก็บ (Encryption at Rest) และต้องควบคุมสิทธิการเข้าถึงอย่างเหมาะสม

๒๑๙.๔ ข้อมูลสำหรับการพิสูจน์ตัวตน เช่น ชื่อบัญชีผู้ใช้งานและรหัสลับ เป็นต้น ต้องได้รับการปกป้องด้วยการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒๑๙.๕ การจัดเก็บรหัสผ่านผู้ใช้งาน ต้องไม่จัดเก็บเป็นข้อความล้วนและต้องใช้วิธีแฮชรหัสผ่าน (Password Hashing) ที่เหมาะสมตามมาตรฐานที่องค์กรกำหนด เช่น Argon2 bcrypt PBKDF2 พร้อม salt และห้ามใช้ MD5 หรือ SHA-1 สำหรับรหัสผ่าน เป็นต้น

ข้อ ๒๒๐ มาตรฐานอัลกอริทึมและความยาวกุญแจ (Approved Algorithms & Key Length)

๒๒๐.๑ การเข้ารหัสแบบสมมาตรให้ใช้มาตรฐาน AES อย่างน้อย AES-128 หรือสูงกว่าตามที่องค์กรกำหนด

๒๒๐.๒ การเข้ารหัสแบบอสมมาตรให้ใช้มาตรฐานที่เป็นที่ยอมรับ เช่น RSA อย่างน้อย 2048 บิต หรือ ECC เช่น P-256 หรือสูงกว่าตามที่องค์กรกำหนด เป็นต้น

๒๒๐.๓ ให้ทบทวนมาตรฐานอัลกอริทึมและความยาวกุญแจ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีประกาศช่องโหว่/ข้อแนะนำด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ข้อ ๒๒๑ การบริหารจัดการกุญแจเข้ารหัส (Key Management)

๒๒๑.๑ องค์กรต้องจัดให้มีกระบวนการบริหารจัดการกุญแจตลอดวงจรชีวิต ได้แก่ การสร้าง การจัดเก็บ การใช้งาน การแจกจ่าย การหมุนเวียน/เปลี่ยนกุญแจ การเพิกถอน และการทำลายกุญแจอย่างปลอดภัย

๒๒๑.๒ กุญแจส่วนตัว (Private Key) และกุญแจที่มีความสำคัญ ต้องถูกจัดเก็บเป็นความลับและมีมาตรการป้องกันที่เหมาะสม เช่น KMS/HSM หรือกลไกที่องค์กรกำหนด และจำกัดสิทธิการเข้าถึงตามบทบาทหน้าที่ เป็นต้น

๒๒๑.๓ การส่งมอบ...

๒๒๑.๓ การส่งมอบกุญแจหรือข้อมูลลับที่เกี่ยวข้องต้องดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัย และต้องมีผู้รับผิดชอบกำกับดูแล

๒๒๑.๔ เมื่อทราบหรือสงสัยว่ากุญแจมีความเสี่ยงต่อการรั่วไหล ต้องเพิกถอนหรือเปลี่ยนกุญแจทันที พร้อมบันทึกเหตุผล วันที่ เวลา และผู้อนุมัติ

๒๒๑.๕ การกระทำใด ๆ ที่เกี่ยวข้องกับกุญแจต้องมีการบันทึกข้อมูลการดำเนินการ (Log) เพื่อการตรวจสอบย้อนหลัง

ส่วนที่ ๒๓ หลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย
(Secure System Engineering Principles)

องค์กรกำหนดให้การออกแบบ พัฒนา ปรับปรุง และติดตั้งระบบสารสนเทศ ต้องยึดหลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย โดยบูรณาการมาตรการด้านความมั่นคงปลอดภัยเป็นส่วนหนึ่งของวงจรการพัฒนาระบบสารสนเทศตั้งแต่ต้นจนสิ้นสุด และต้องดำเนินการอย่างน้อย ดังต่อไปนี้

ข้อ ๒๒๒ การสอดคล้องกับนโยบายและมาตรฐานขององค์กร โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติงาน และมาตรฐานด้านความมั่นคงปลอดภัยที่องค์กรกำหนด

ข้อ ๒๒๓ ความมั่นคงปลอดภัยตั้งแต่ขั้นกำหนดความต้องการ โดยต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยให้เป็นส่วนหนึ่งของข้อกำหนดระบบ (Requirements) ตั้งแต่เริ่มต้น และนำไปใช้ในการออกแบบระบบโดยรวม

ข้อ ๒๒๔ การบริหารการเปลี่ยนแปลงความต้องการ เมื่อมีการเปลี่ยนแปลงความต้องการของระบบ ต้องทบทวนและปรับมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

ข้อ ๒๒๕ ความเหมาะสมตามความเสี่ยงและความคุ้มค่า โดยมาตรการที่เลือกใช้ต้องเหมาะสมกับระดับความเสี่ยง วัตถุประสงค์ภารกิจ และผลกระทบต่อการใช้งาน โดยต้องลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ข้อ ๒๒๖ ความเรียบง่ายและลดความซับซ้อน โดยระบบต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็น ข้อผิดพลาด และพื้นผิวการโจมตี (Attack Surface)

ข้อ ๒๒๗ การป้องกันหลายชั้น ต้องออกแบบมาตรการด้านความมั่นคงปลอดภัยแบบหลายชั้น (Layered Security) ครอบคลุมทั้งด้านกายภาพและด้านตรรกะ ในระดับเครือข่าย ระบบปฏิบัติการฐานข้อมูล และแอปพลิเคชัน

ข้อ ๒๒๘ ปฏิเสธโดยปริยายและความสามารถในการฟื้นสภาพ โดยระบบต้องออกแบบให้ใช้หลักการปฏิเสธโดยปริยาย (Default Deny) เมื่อมาตรการล้มเหลวหรือถูกข้ามผ่าน และต้องมีความสามารถในการฟื้นสภาพ (Recoverability) ภายในระยะเวลาที่เหมาะสม

ข้อ ๒๒๙ คุ้มครองความลับ ความถูกต้อง และความพร้อมใช้ โดยต้องมีมาตรการคุ้มครองความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลทั้งระหว่างประมวลผล การรับและส่ง และการจัดเก็บข้อมูล

ข้อ ๒๓๐ การระบุตัวตนผู้ใช้งานแบบไม่ซ้ำกัน โดยผู้ใช้งานต้องมีบัญชีผู้ใช้งานเฉพาะบุคคลไม่ซ้ำกัน (Unique Identification) เพื่อให้ตรวจสอบย้อนกลับได้

ข้อ ๒๓๑ การออกแบบ...

ข้อ ๒๓๑ การออกแบบโดยคิดจากมุมผู้โจมตี โดยต้องพิจารณาภัยคุกคามจากมุมมองของผู้ไม่ประสงค์ดี (Threat Modeling) และกำหนดมาตรการรองรับการใช้งานในสภาพแวดล้อมที่ไม่พึงประสงค์ เช่น ภาวะฉุกเฉินหรือภัยพิบัติ เป็นต้น

ข้อ ๒๓๒ สิทธิเท่าที่จำเป็น โดยต้องออกแบบสิทธิการใช้งานโดยยึดหลักสิทธิที่น้อยที่สุด (Least Privilege) ตามบทบาทหน้าที่และความจำเป็น

ข้อ ๒๓๓ การตรวจสอบและบันทึกเพื่อการตรวจสอบย้อนหลัง โดยต้องออกแบบให้มีระบบบันทึกและตรวจสอบการใช้งาน (Audit Mechanism) สำหรับฟังก์ชันสำคัญ เพื่อสนับสนุนการตรวจจับและการตรวจสอบเหตุผิดปกติ

ข้อ ๒๓๔ การแยกระบบทดสอบและระบบใช้งานจริง โดยระบบที่มีความสำคัญสูงต้องทดสอบบนระบบทดสอบให้แล้วเสร็จก่อนนำขึ้นระบบใช้งานจริง และการติดตั้งบนระบบใช้งานจริงต้องได้รับอนุญาตก่อน

ข้อ ๒๓๕ การควบคุมการเข้าถึงสำหรับผู้ใช้งานภายนอกหรือผู้รับจ้าง กรณีอนุญาตให้ผู้ใช้งานภายนอกเข้าถึงระบบ ต้องจำกัดสิทธิเท่าที่จำเป็น มีการพิสูจน์ตัวตน และบันทึกกิจกรรมการใช้งานเป็นแฟ้มบันทึกเหตุการณ์ (Log File)

ข้อ ๒๓๖ การปรับตั้งค่าความมั่นคงปลอดภัยของระบบ (System Hardening) ขั้นต่ำก่อนเปิดให้บริการ โดยที่ก่อนเปิดให้บริการเครื่องแม่ข่ายต้องปิดบริการที่ไม่จำเป็น ติดตั้งระบบเทียบเวลา (NTP) จำกัดการเข้าถึงบัญชีสิทธิพิเศษ และตรวจสอบหรือแก้ไขช่องโหว่พร้อมรายงานตามลำดับ

ส่วนที่ ๒๔ การนำระบบงานไปติดตั้งบนคลาวด์ (Cloud Computing)

ข้อ ๒๓๗ การวางแผนการนำระบบสารสนเทศไปติดตั้งบนคลาวด์

๒๓๗.๑ องค์กรต้องคัดเลือกผู้ให้บริการคลาวด์ที่มีความน่าเชื่อถือด้านความมั่นคงปลอดภัย และกำหนดเงื่อนไขด้านสัญญาหรือข้อตกลงบริการให้ครอบคลุมการคุ้มครองข้อมูล การแจ้งเหตุ การเข้าถึงแฟ้มบันทึกเหตุการณ์ และแผนยุติหรือย้ายบริการ (Exit Plan)

๒๓๗.๒ ก่อนนำระบบงานขึ้นคลาวด์ ต้องระบุระบบและข้อมูลที่จะนำขึ้นคลาวด์ กำหนดชั้นความลับและเจ้าของข้อมูล จัดทำบัญชีสินทรัพย์เทคโนโลยีสารสนเทศ ประเมินความเสี่ยง และกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยให้เหมาะสม รวมถึงพิจารณาประเด็นเขตอำนาจรัฐและกฎหมายที่เกี่ยวข้อง

๒๓๗.๓ ต้องจัดทำและรับรองเอกสารควบคุมการเชื่อมต่อระบบ (Interface Control Document: ICD) และกำหนดบทบาท/ความรับผิดชอบของผู้เกี่ยวข้อง รวมถึงกระบวนการอนุมัติก่อนดำเนินการ

ข้อ ๒๓๘ การวิเคราะห์และออกแบบความมั่นคงปลอดภัยทางเครือข่าย

๒๓๘.๑ ต้องจัดทำผังเครือข่ายและแบ่งแยกเครือข่ายตามระดับความสำคัญ โดยแยกสภาพแวดล้อมทดสอบออกจากสภาพแวดล้อมใช้งานจริงอย่างชัดเจน

๒๓๘.๒ ต้องกำหนดการไหลของข้อมูลและรายการที่อนุญาต ตามหลักการปฏิเสธโดยปริยาย (Default Deny) และใช้มาตรการควบคุมข้อมูลจราจรอย่างเหมาะสม เช่น ไฟร์วอลล์ (Firewall) ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) และระบบป้องกันภัยคุกคามบนเครื่อง เช่น EDR/Antivirus เป็นต้น

๒๓๘.๓ การเข้าถึงเพื่อการบริหารจัดการต้องผ่านช่องทางที่องค์กรกำหนด เช่น VPN ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) สำหรับบัญชีสิทธิพิเศษ และต้องกำหนดระบบเทียบเวลา (NTP) เพื่อความถูกต้องของบันทึกเหตุการณ์ เป็นต้น

ข้อ ๒๓๙ การวิเคราะห์...

ข้อ ๒๓๙ การวิเคราะห์และออกแบบระบบงานด้านความมั่นคงปลอดภัย

๒๓๙.๑ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยครอบคลุม การพิสูจน์ตัวตนและการกำหนดสิทธิ การลงทะเบียนหรือเพิกถอนสิทธิ การหมดเวลาใช้งาน การบันทึกเหตุการณ์ (Log) การคุ้มครองรหัสผ่าน การป้องกันข้อมูลสำคัญ การเข้ารหัสข้อมูล และการบริหารจัดการกุญแจ และการกู้คืนระบบสารสนเทศ

๒๓๙.๒ ต้องกำหนดมาตรการบริหารตัวตนและสิทธิ (IAM) ตามหลักการอนุญาตเท่าที่จำเป็น และกำหนดให้มีการทบทวนสิทธิเป็นระยะตามที่องค์กรกำหนด

ข้อ ๒๔๐ การทดสอบระบบ

๒๔๐.๑ ต้องทดสอบด้านความมั่นคงปลอดภัยให้ครอบคลุมตามข้อกำหนดที่กำหนดไว้ และต้องทดสอบบนสภาพแวดล้อมทดสอบที่แยกจากระบบใช้งานจริง

๒๔๐.๒ ก่อนนำข้อมูลไปใช้ทดสอบ ต้องดำเนินการปกปิดข้อมูล (Data Masking) ตามชั้นความลับและข้อกำหนดด้านข้อมูลส่วนบุคคล

๒๔๐.๓ ต้องทดสอบตามความเหมาะสม เช่น การทดสอบอินพุตผิดปกติ (Fuzzing) และการทดสอบและรับรองการใช้งาน (UAT) พร้อมจัดเก็บผลการทดสอบเป็นหลักฐาน เป็นต้น

ข้อ ๒๔๑ การติดตั้งระบบและการปฏิบัติการก่อนเปิดใช้งานจริง

๒๔๑.๑ ก่อนเปิดใช้งานจริง ต้องติดตั้งแพตช์ความปลอดภัย ปิดบริการที่ไม่จำเป็น จัดทำและใช้มาตรฐานพื้นฐานด้านความปลอดภัย (Security Baseline) ตรวจสอบและแก้ไขช่องโหว่ และจำกัดการเข้าถึงซอร์สโค้ดตามความจำเป็น

๒๔๑.๒ ต้องจัดให้มีมาตรการติดตามการเปลี่ยนแปลงไฟล์หรือส่วนประกอบสำคัญโดยไม่ได้รับอนุญาต (File Integrity Monitoring) และจัดทำแผนการบันทึกและวิเคราะห์แฟ้มบันทึกเหตุการณ์ (Log File) รวมถึงกำหนดการเฝ้าระวังและการแจ้งเตือนตามระดับความเสี่ยง

๒๔๑.๓ ต้องจัดทำและดำเนินการตามแผนสำรองข้อมูล แผนติดตามความพร้อมใช้ทรัพยากร และแผนกู้คืนระบบสารสนเทศ โดยต้องทดสอบแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง และจัดเก็บหลักฐานผลการทดสอบ

๒๔๑.๔ ต้องบันทึกและควบคุมการเปลี่ยนแปลงค่ากำหนดสำคัญของระบบสารสนเทศและโครงสร้างคลาวด์ เพื่อการตรวจสอบย้อนหลัง

ส่วนที่ ๒๕ การใช้คลาวด์ส่วนบุคคล (Private Cloud)

ข้อ ๒๔๒ องค์กรไม่อนุญาต ให้จัดเก็บ ส่งต่อ หรือแบ่งปันข้อมูลที่เกี่ยวข้องกับภารกิจขององค์กร หรือข้อมูลของทางราชการ ผ่านบริการคลาวด์สำหรับบุคคลทั่วไป เช่น Google Drive Dropbox หรือบริการในลักษณะเดียวกันไม่ว่ากรณีใด เป็นต้น

ข้อ ๒๔๓ การใช้บริการคลาวด์สำหรับบุคคลทั่วไปบนเครื่องคอมพิวเตอร์และเครือข่ายขององค์กร อนุญาตได้เฉพาะข้อมูลส่วนบุคคลของผู้ใช้งานที่ไม่เกี่ยวข้องกับงานตามภารกิจ และต้องไม่กระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

ส่วนที่ ๒๖ การใช้ระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลาง (ONCB Drive)

ข้อ ๒๔๔ หลักการและวัตถุประสงค์

๒๔๔.๑ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) ต้องจัดให้มีระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลางขององค์กร เพื่อสนับสนุนการปฏิบัติงาน

การแลกเปลี่ยนข้อมูล และการบริหารจัดการทรัพยากรสารสนเทศของหน่วยงานให้เกิดประสิทธิภาพ ความคุ้มค่า และความต่อเนื่องในการปฏิบัติภารกิจ

๒๔๔.๒ การใช้ระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลาง ต้องดำเนินการภายใต้หลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศของทางราชการ ซึ่งเป็นหลักการสำคัญที่แนวปฏิบัติ ONCB Drive ยึดไว้เป็นวัตถุประสงค์หลักของระบบ

๒๔๔.๓ นโยบายนี้มีวัตถุประสงค์อย่างน้อย ดังต่อไปนี้

๒๔๔.๓.๑ เพื่อกำหนดกรอบการใช้งานและการบริหารจัดการระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลางของสำนักงาน ป.ป.ส. ให้เป็นมาตรฐานเดียวกัน

๒๔๔.๓.๒ เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ป้องกันการเข้าถึงข้อมูลโดยมิชอบ การรั่วไหล การสูญหาย หรือการใช้ข้อมูลผิดวัตถุประสงค์

๒๔๔.๓.๓ เพื่อสนับสนุนการปฏิบัติงานตามพันธกิจของสำนักงาน ป.ป.ส. ให้สามารถเข้าถึง ใช้งาน แลกเปลี่ยน และบริหารจัดการข้อมูลร่วมกันได้อย่างมีประสิทธิภาพต่อเนื่อง

๒๔๔.๓.๔ เพื่อให้การใช้ทรัพยากรพื้นที่จัดเก็บข้อมูลส่วนกลางขององค์กรเป็นไปอย่างคุ้มค่า เหมาะสม และตรวจสอบได้

ข้อ ๒๔๕ ขอบเขตการบังคับใช้

๒๔๕.๑ นโยบายนี้ใช้บังคับกับเจ้าหน้าที่สำนักงาน ป.ป.ส. ผู้ใช้งานระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลางทุกคน รวมถึง ผู้ดูแลระบบ ผู้ดูแลข้อมูล และผู้มีหน้าที่เกี่ยวข้องกับการบริหารจัดการระบบดังกล่าว

๒๔๕.๒ นโยบายนี้ให้ใช้บังคับกับการจัดเก็บ รับส่ง แลกเปลี่ยน แบ่งปัน สำรอง กู้คืน ควบคุมสิทธิการเข้าถึง และการลบหรือทำลายข้อมูลสารสนเทศที่อยู่ในระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลางของสำนักงาน ป.ป.ส.

๒.๓ ข้อมูลที่อยู่ภายใต้นโยบายนี้ ครอบคลุมข้อมูลปฏิบัติการ ข้อมูลภายใน ข้อมูลส่วนบุคคล ข้อมูลที่มีชั้นความลับ และข้อมูลอื่นใดที่อยู่ในความรับผิดชอบของสำนักงาน ป.ป.ส.

ข้อ ๒๔๖ การกำกับดูแลและความรับผิดชอบ

๒๔๖.๑ เจ้าของข้อมูล ร่วมกับศูนย์เทคโนโลยีสารสนเทศ ต้องรับผิดชอบในการบริหารจัดการระบบ กำหนดมาตรฐานทางเทคนิค มาตรการรักษาความมั่นคงปลอดภัย การกำหนดสิทธิการเข้าถึง การสำรองข้อมูล การกู้คืนข้อมูล และการติดตามตรวจสอบการใช้งานระบบ

๒๔๖.๒ เจ้าของข้อมูล ต้องรับผิดชอบในการกำหนดประเภทข้อมูล ระดับชั้นความลับ สิทธิการเข้าถึง ระยะเวลาการเก็บรักษา และความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บอยู่ในระบบ

๒๔๖.๓ ผู้ใช้งานระบบ ต้องรับผิดชอบต่อข้อมูลที่อยู่ในความครอบครองหรือที่ตนเป็นผู้จัดเก็บ อัปโหลด แบ่งปัน หรือส่งต่อผ่านระบบ โดยต้องใช้ข้อมูลตามภารกิจและตามขอบเขตที่ได้รับอนุญาตเท่านั้น

๒๔๖.๔ ผู้ใช้งานต้องตระหนักว่าข้อมูลที่จัดเก็บในระบบเป็นทรัพย์สินของทางราชการ และต้องรักษาความลับ ความถูกต้องครบถ้วน และความปลอดภัยของข้อมูลดังกล่าวตลอดระยะเวลาการใช้งาน ซึ่งสอดคล้องกับแนวปฏิบัติในไฟล์แนบที่กำหนดให้เจ้าหน้าที่ตระหนักว่าข้อมูลใน ONCB Drive เป็นทรัพย์สินของทางราชการ

ข้อ ๒๔๗ ช่องทาง...

ข้อ ๒๔๗ ช่องทางและวิธีการใช้งานระบบ

๒๔๗.๑ การเข้าใช้งานระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลาง ให้กระทำผ่านช่องทางที่สำนักงาน ป.ป.ส. กำหนดเท่านั้น

๒๔๗.๒ องค์กรอาจกำหนดช่องทางการใช้งานได้หลายรูปแบบตามความเหมาะสม ได้แก่

๒๔๗.๒.๑ ระบบงานผ่านเว็บแอปพลิเคชัน

๒๔๗.๒.๒ โปรแกรมประยุกต์บนเครื่องคอมพิวเตอร์

๒๔๗.๒.๓ โปรแกรมประยุกต์บนอุปกรณ์เคลื่อนที่

ทั้งนี้ ให้เป็นไปตามแนวทางเดียวกับระบบ ONCB Drive ซึ่งกำหนดช่องทางการใช้งานไว้ ๓ ช่องทาง ได้แก่ Web Application, Desktop Sync Application และ Mobile Application

๒๔๗.๓ ห้ามผู้ใช้งานเชื่อมต่อระบบผ่านช่องทาง เครื่องมือ หรือบริการอื่นที่องค์กรไม่ได้อนุมัติ เว้นแต่ได้รับอนุญาตเป็นกรณีพิเศษจากหน่วยงานที่รับผิดชอบ

ข้อ ๒๔๘ การใช้พื้นที่จัดเก็บข้อมูลและการบริหารทรัพยากรส่วนกลาง

๒๔๘.๑ สำนักงาน ป.ป.ส. อาจกำหนดสัดส่วนหรือโควตาพื้นที่จัดเก็บข้อมูล สำหรับระดับหน่วยงาน ระดับส่วนงาน และระดับบุคคล ตามความเหมาะสมกับภารกิจและทรัพยากรส่วนกลางขององค์กร

๒๔๘.๒ ผู้ใช้งานต้องจัดเก็บเฉพาะข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานตามพันธกิจขององค์กรเท่านั้น และต้องบริหารจัดการข้อมูลในความรับผิดชอบให้เป็นระเบียบเรียบร้อย

๒๔๘.๓ ผู้ใช้งานต้องพิจารณาลบข้อมูลที่หมดความจำเป็น หรือดำเนินการตามรอบอายุข้อมูลที่องค์กรกำหนด เมื่อเสร็จสิ้นภารกิจหรือสิ้นสุดความจำเป็นในการใช้งาน เพื่อให้การใช้ทรัพยากรพื้นที่จัดเก็บข้อมูลส่วนกลางเกิดประสิทธิภาพและความคุ้มค่าสูงสุด

๒๔๘.๔ ห้ามใช้ระบบส่วนกลางเพื่อจัดเก็บข้อมูลส่วนตัว ข้อมูลที่ไม่เกี่ยวข้องกับราชการ หรือข้อมูลที่มีลักษณะเป็นภาระเกินสมควรต่อทรัพยากรขององค์กร

ข้อ ๒๔๙ การแบ่งปันและแลกเปลี่ยนข้อมูล

๒๔๙.๑ การแบ่งปันหรือแลกเปลี่ยนข้อมูลผ่านระบบ ต้องกระทำภายใต้หลักเท่าที่จำเป็นและเฉพาะเท่าที่เกี่ยวข้องกับการปฏิบัติงานตามหน้าที่และอำนาจของผู้ใช้งานหรือองค์กร

๒๔๙.๒ การแบ่งปันข้อมูลออกสู่ภายนอกองค์กรผ่านลิงก์สาธารณะ (Public Link) หรือเครื่องมือที่มีผลในลักษณะเดียวกัน ต้องมีมาตรการควบคุมความปลอดภัยอย่างเหมาะสม

๒๔๙.๓ กรณีมีการแบ่งปันข้อมูลผ่านลิงก์สาธารณะหรือช่องทางภายนอก ผู้ใช้งานต้องกำหนดรหัสผ่าน และกำหนดวันสิ้นสุดการเข้าถึงข้อมูลทุกครั้ง เพื่อควบคุมสิทธิและป้องกันการเข้าถึงข้อมูลโดยมิชอบ

๒๔๙.๔ ห้ามแบ่งปันข้อมูลที่มีชั้นความลับ หรือข้อมูลที่อาจส่งผลกระทบต่อทางราชการผ่านช่องทางสาธารณะ เว้นแต่ได้รับอนุมัติจากผู้บังคับบัญชาตามลำดับอำนาจ และมีมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติมตามที่องค์กรกำหนด

๒๔๙.๕ การแบ่งปันข้อมูลส่วนบุคคล ต้องดำเนินการโดยสอดคล้องกับวัตถุประสงค์ของทางราชการ และต้องไม่เปิดเผยแก่บุคคลภายนอก เว้นแต่มีฐานกฎหมายรองรับ หรือได้รับความยินยอมจากเจ้าของข้อมูลตามที่กฎหมายกำหนด

๒๔๙.๖ ผู้ใช้งานต้องตรวจสอบสิทธิการเข้าถึงข้อมูลที่ตนแบ่งปันอย่างสม่ำเสมอ และต้องยกเลิกสิทธิการเข้าถึงทันทีเมื่อสิ้นสุดความจำเป็นในการใช้งานร่วมกัน

ข้อ ๒๕๐ การคุ้มครอง...

ข้อ ๒๕๐ การคุ้มครองข้อมูลและการรักษาความมั่นคงปลอดภัย

๒๕๐.๑ ผู้ใช้งานต้องรักษาบัญชีผู้ใช้งานและรหัสผ่านไว้เป็นความลับส่วนบุคคล และห้ามยินยอมให้ผู้อื่นใช้บัญชีของตนในการเข้าถึงระบบโดยเด็ดขาด ตามหลักที่กำหนดไว้ในแนวปฏิบัติ ONCB Drive

๒๕๐.๒ กรณีเป็นข้อมูลที่มีชั้นความลับ ข้อมูลสำคัญ หรือข้อมูลอ่อนไหว ผู้ใช้งานต้องใช้มาตรการคุ้มครองเพิ่มเติม เช่น การเข้ารหัสข้อมูล การเข้ารหัสไฟล์ หรือวิธีการอื่นที่เหมาะสมก่อนจัดเก็บหรือแบ่งปันข้อมูลผ่านระบบ เป็นต้น

๒๕๐.๓ ผู้ใช้งานต้องหลีกเลี่ยงการเข้าใช้งานระบบผ่านอุปกรณ์สาธารณะ หรือเครือข่ายไร้สายสาธารณะที่ไม่มีมาตรการรักษาความปลอดภัยเพียงพอ เพื่อป้องกันความเสี่ยงจากการถูกดักรับข้อมูลหรือการเข้าถึงโดยมิชอบ

๒๕๐.๔ การกำหนดสิทธิการเข้าถึงระบบและข้อมูล ต้องเป็นไปตามบทบาทหน้าที่ และหลักการให้สิทธิเท่าที่จำเป็น

๒๕๐.๕ ระบบต้องสามารถบันทึกเหตุการณ์ที่สำคัญเกี่ยวกับการเข้าถึง การแบ่งปัน การแก้ไข และการลบข้อมูล เพื่อรองรับการตรวจสอบย้อนหลังตามที่องค์กรกำหนด

ข้อ ๒๕๑ การสำรองข้อมูล การกู้คืนข้อมูล และความต่อเนื่องในการปฏิบัติงาน

๒๕๑.๑ สำนักงาน ป.ป.ส. ต้องจัดให้มีมาตรการสำรองข้อมูลของระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลาง เพื่อสร้างความเชื่อมั่นในการปฏิบัติงานอย่างต่อเนื่อง และป้องกันความเสี่ยงจากการสูญหายของข้อมูลสารสนเทศ

๒๕๑.๒ การสำรองข้อมูลต้องดำเนินการตามรอบระยะเวลาที่องค์กรกำหนด โดยอย่างน้อยควรมีรอบการสำรองข้อมูลเป็นประจำสม่ำเสมอ

๒๕๑.๓ หากเกิดกรณีข้อมูลสูญหาย เสียหาย หรือไม่สามารถเข้าถึงได้จากความผิดพลาดในการใช้งานหรือระบบขัดข้อง ผู้ใช้งานต้องแจ้งหน่วยงานที่รับผิดชอบโดยเร็ว เพื่อดำเนินการกู้คืนข้อมูลตามกระบวนการที่องค์กรกำหนด

๒๕๑.๔ หน่วยงานเจ้าของข้อมูลและผู้ใช้งานต้องตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำคัญเป็นประจำ และต้องใช้ความระมัดระวังก่อนลบหรือทำลายข้อมูลทุกครั้ง

ข้อ ๒๕๒ การจัดการข้อมูลส่วนบุคคลและข้อมูลที่มีความอ่อนไหว

๒๕๒.๑ การจัดเก็บ ใช้ แบ่งปัน หรือแลกเปลี่ยนข้อมูลส่วนบุคคลผ่านระบบสารสนเทศต้องดำเนินการเท่าที่จำเป็นตามภารกิจ และต้องสอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

๒๕๒.๒ กรณีข้อมูลมีความอ่อนไหวสูง หรืออาจก่อให้เกิดผลกระทบต่อสิทธิของบุคคล ความมั่นคงของรัฐ ภารกิจด้านข่าวกรอง หรือการบังคับใช้กฎหมาย ต้องกำหนดมาตรการควบคุมเพิ่มเติมตามระดับความเสี่ยง

๒๕๒.๓ ห้ามนำข้อมูลที่มีชั้นความลับ หรือข้อมูลที่มีผลกระทบสูงต่อทางราชการไปใช้ในลักษณะที่ทำให้บุคคลภายนอกเข้าถึงได้ เว้นแต่ได้รับอนุญาตโดยชอบและมีมาตรการควบคุมเฉพาะกรณี

ข้อ ๒๕๓ การเฝ้าระวัง ตรวจสอบ และรายงานเหตุผิดปกติ

๒๕๓.๑ หน่วยงานที่รับผิดชอบต้องจัดให้มีการเฝ้าระวัง ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศ เพื่อป้องกัน ตรวจจับ และตอบสนองต่อเหตุผิดปกติหรือเหตุละเมิดความมั่นคงปลอดภัยของข้อมูล

๒๕๓.๒ ผู้ใช้งาน...

๒๕๓.๒ ผู้ใช้งานที่พบเหตุการณ์ผิดปกติ หรือมีเหตุอันควรเชื่อได้ว่ามีการเข้าถึงโดยมิชอบ ข้อมูลรั่วไหล ระบบผิดปกติ หรืออาจเกิดการละเมิดความมั่นคงปลอดภัยของข้อมูล ต้องรีบรายงานต่อหน่วยงานที่รับผิดชอบทันที

๒๕๓.๓ กรณีเป็นเหตุละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามกระบวนการจัดการเหตุละเมิดข้อมูลส่วนบุคคลขององค์กร และแนวปฏิบัติที่เกี่ยวข้อง

ข้อ ๒๕๔ การสร้างความตระหนักรู้และการใช้งาน

๒๕๔.๑ สำนักงาน ป.ป.ส. ต้องส่งเสริมให้ผู้ใช้งานมีความรู้ ความเข้าใจ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศในการใช้ระบบจัดเก็บข้อมูลปฏิบัติการ และแลกเปลี่ยนข้อมูลส่วนกลางอย่างต่อเนื่อง

๒๕๔.๒ ผู้ใช้งานทุกคนต้องปฏิบัติตามนโยบายนี้ แนวปฏิบัติ คู่มือการใช้งาน และมาตรการที่องค์กรกำหนดอย่างเคร่งครัด

๒๕๔.๓ การฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายนี้ ให้ดำเนินการตามระเบียบของทางราชการ ระเบียบวินัย มาตรการทางปกครอง หรือกฎหมายที่เกี่ยวข้อง แล้วแต่กรณี

ข้อ ๒๕๕ การทบทวนและปรับปรุงนโยบาย

๒๕๕.๑ ให้มีการทบทวนนโยบายนี้อย่างเหมาะสม หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี ความเสี่ยง หรือรูปแบบการใช้งานระบบอย่างมีนัยสำคัญ

๒๕๕.๒ การปรับปรุงนโยบายนี้ต้องคำนึงถึงผลการใช้งานจริง เหตุการณ์ความเสี่ยง ข้อเสนอแนะจากหน่วยงานผู้ใช้งาน และแนวทางการบริหารจัดการข้อมูลของสำนักงาน ป.ป.ส.

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล (Database & Backup)

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ บัญชีฐานข้อมูล การจำแนกชั้นข้อมูล และผู้รับผิดชอบ

๑.๑ ให้องค์กรจัดทำและทบทวนบัญชีฐานข้อมูล และบัญชีสินทรัพย์ และองค์ประกอบที่เกี่ยวข้อง อาทิ ระบบสารสนเทศ เจ้าของระบบ ที่ตั้ง การเชื่อมต่อ และผู้ดูแลระบบสารสนเทศ เป็นต้น อย่างสม่ำเสมอ

๑.๒ กำหนดเจ้าของข้อมูล และหรือเจ้าของระบบสารสนเทศ สำหรับฐานข้อมูลแต่ละรายการ เพื่อรับผิดชอบการอนุมัติการเข้าถึงและการใช้ข้อมูลตามภารกิจ

๑.๓ ให้จำแนกข้อมูลในฐานข้อมูลและบัญชีสินทรัพย์ตามชั้นความลับ และระดับการเข้าถึง ให้สอดคล้องกับนโยบายการจัดลำดับชั้นความลับและการควบคุมการเข้าถึงขององค์กร

ข้อ ๒ การกำหนดสิทธิและการอนุมัติการเข้าถึงฐานข้อมูล

๒.๑ ให้กำหนดสิทธิการเข้าถึงฐานข้อมูลตาม บทบาทหน้าที่ (Role-based) และหลักอนุญาตเท่าที่จำเป็น (Least Privilege) โดยอย่างน้อยครอบคลุมสิทธิอ่าน เพิ่มหรือบันทึก แก้ไข ลบ และไม่มีสิทธิ

๒.๒ การขอใช้ เปลี่ยนแปลง หรือยกเลิกสิทธิ ให้ทำเป็นลายลักษณ์อักษรหรือผ่านระบบสนับสนุนงานให้บริการสารสนเทศ หรือระบบสารสนเทศที่ตรวจสอบย้อนหลังได้ และต้องได้รับอนุมัติจากเจ้าของข้อมูล เจ้าของระบบ หรือผู้ได้รับมอบหมายตามระดับชั้นความลับ

๒.๓ ให้มีการทบทวนสิทธิการเข้าถึงฐานข้อมูล อย่างน้อยทุก ๓ เดือน หรือเมื่อมีการเปลี่ยนหน้าที่/ย้ายงาน/พ้นสภาพ และให้เพิกถอนสิทธิทันทีเมื่อหมดความจำเป็น

ข้อ ๓ การควบคุม...

ข้อ ๓ การควบคุมบัญชีสิทธิพิเศษและการแยกหน้าที่

๓.๑ ให้แยกบัญชีผู้ดูแลฐานข้อมูลหรือผู้ดูแลระบบ (Privileged Account) ออกจากบัญชีใช้งานทั่วไป และห้ามใช้บัญชีร่วมกัน

๓.๒ ให้จำกัดและควบคุมการใช้สิทธิพิเศษตามหลักจำเป็น พร้อมกำหนดมาตรการกำกับดูแลการปฏิบัติงานของผู้ดูแล เช่น การขออนุมัติล่วงหน้า การบันทึกกิจกรรม และการตรวจสอบภายหลัง เป็นต้น

๓.๓ ให้กำหนดการแยกหน้าที่อย่างเหมาะสมระหว่าง ผู้อนุมัติสิทธิ (Owner) ผู้ดำเนินการให้สิทธิ (Admin/DBA) และผู้ตรวจสอบ (Audit/InfoSec) เพื่อลดความเสี่ยงจากการใช้อำนาจโดยมิชอบ

ข้อ ๔ การบันทึกเหตุการณ์และการตรวจสอบการใช้งานฐานข้อมูล

๔.๑ ให้ระบบฐานข้อมูลและระบบงานที่เกี่ยวข้องจัดให้มีแฟ้มบันทึกเหตุการณ์ (Log) ที่เพียงพอสำหรับการตรวจสอบย้อนหลัง เช่น การเข้าสู่ระบบ การเปลี่ยนสิทธิ การเข้าถึงข้อมูลสำคัญ การแก้ไขหรือการลบข้อมูล และการกระทำของบัญชีสิทธิพิเศษ เป็นต้น

๔.๒ ให้จำกัดสิทธิการเข้าถึง Log เฉพาะผู้ได้รับมอบหมาย และต้องมีมาตรการป้องกันการแก้ไข หรือการทำลาย Log

๔.๓ ระยะเวลาการเก็บรักษา Log ให้เป็นไปตามนโยบายการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ขององค์กรและกฎหมายที่เกี่ยวข้อง โดยหลักควรไม่น้อยกว่าเกณฑ์ขั้นต่ำขององค์กร

ข้อ ๕ การใช้ฐานข้อมูลร่วมและการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก

๕.๑ การเปิดเผยและการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก ต้องดำเนินการเท่าที่จำเป็นตามภารกิจ ภายใต้ฐานอำนาจตามกฎหมายหรือข้อตกลง และต้องกำหนดผู้รับผิดชอบชัดเจน

๕.๒ ให้จัดทำข้อตกลงหรือบันทึกความเข้าใจ โดยระบุใจความอย่างน้อย ดังนี้

๕.๒.๑ ขอบเขตข้อมูลที่ทำการเปิดเผย หรือการแลกเปลี่ยน

๕.๒.๒ วัตถุประสงค์

๕.๒.๓ ผู้มีสิทธิเข้าถึง

๕.๒.๔ วิธีการรับส่งข้อมูลที่ปลอดภัย

๕.๒.๕ มาตรการรักษาความมั่นคงปลอดภัยตามหลัก CIA

๕.๒.๖ วิธีการเก็บรักษา และวิธีการทำลายข้อมูลเมื่อสิ้นสุดการใช้งาน

๕.๒.๗ ขั้นตอนการดำเนินการเมื่อเผชิญเหตุข้อมูลรั่วไหล

๕.๓ กรณีจำเป็นต้องทำสำเนาหรือนำข้อมูลออกนอกระบบสารสนเทศ หรือนอกเครือข่าย ให้ปฏิบัติตามแนวปฏิบัติขององค์กรเรื่องการทำสำเนา/การส่งออกข้อมูล และต้องได้รับอนุมัติตามระดับชั้นความลับ พร้อมห้ามส่งต่อให้ผู้ไม่มีสิทธิ

ส่วนที่ ๒ การสำรองข้อมูลและกู้คืน (Backup and Recovery)

ข้อ ๖ การกำหนดระบบสารสนเทศที่มีความสำคัญและการจัดลำดับความสำคัญ

๖.๑ ให้ศูนย์เทคโนโลยีสารสนเทศร่วมกับเจ้าของข้อมูล พิจารณาคัดเลือกระบบสารสนเทศที่มีความสำคัญต่อภารกิจขององค์กร และจัดลำดับความสำคัญจากมากไปน้อย เพื่อกำหนดมาตรการสำรองและกู้คืนให้เหมาะสม

๖.๒ การกำหนดระดับความสำคัญให้พิจารณาผลกระทบต่อภารกิจตามเกณฑ์ที่องค์กรกำหนด โดยอาจอ้างอิงระดับผลกระทบ ๐–๕ ตามแนวปฏิบัติของสำนักงาน ป.ป.ส.

ข้อ ๗ บทบาท...

ข้อ ๗ บทบาท หน้าที่ และความรับผิดชอบ

๗.๑ ให้กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจนอย่างน้อย ได้แก่ เจ้าของระบบ เจ้าของข้อมูล ผู้ดูแลระบบสำรองข้อมูล และผู้ประสานงานหน่วยงาน

๗.๒ การดำเนินการสำรองและการกู้คืน ต้องมีผู้รับผิดชอบหลักและผู้ทดแทน และต้องกำหนดการอนุมัติการกู้คืนตามระดับความสำคัญของระบบและข้อมูล

ข้อ ๘ บัญชีระบบสำคัญ แผนสำรอง/กู้คืน และแผนเตรียมความพร้อมกรณีฉุกเฉิน

๘.๑ ให้จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และกำหนดระบบที่ต้องมีการสำรองข้อมูล พร้อมระบุเป้าหมายการกู้คืนที่เหมาะสม เช่น RTO/RPO ตามระดับความสำคัญของระบบ เป็นต้น

๘.๒ ให้จัดทำและทบทวน “แผนเตรียมความพร้อมกรณีฉุกเฉิน” ที่ได้รับความเห็นชอบจากผู้บริหาร โดยอย่างน้อยต้องกำหนดชนิดภัยพิบัติ ประเมินความเสี่ยง และขั้นตอนรับมือ

ข้อ ๙ การสำรองข้อมูล (Backup)

๙.๑ ให้กำหนดประเภทข้อมูล รายการข้อมูลที่ต้องสำรอง และความถี่การสำรองให้เหมาะสมกับระดับความสำคัญของระบบ โดยข้อมูลที่มีความสำคัญสูงต้องมีความถี่การสำรองมากกว่า และควรมีการสำรองข้อมูลภายนอกองค์กร

๙.๒ ให้กำหนดชนิดการสำรอง เช่น สำรองทั้งหมด หรือสำรองเฉพาะส่วน ช่วงเวลาการสำรอง และสื่อจัดเก็บตามความเหมาะสม เป็นต้น

๙.๓ ต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล และต้องจัดทำบันทึกการสำรองข้อมูล ตรวจสอบความสำเร็จ แก้ไขเมื่อพบปัญหาและรายงานต่อผู้บังคับบัญชาตามลำดับ

๙.๔ ต้องควบคุมการเข้าถึงสถานที่ และสื่อที่ใช้จัดเก็บข้อมูลสำรองให้สอดคล้องกับระดับความสำคัญของระบบ และให้จัดเก็บข้อมูลสำรองในสถานที่ปลอดภัยแยกจากห้องระบบตามความเหมาะสม

๙.๕ ข้อมูลสำรองที่มีระดับความสำคัญสูงต้องเข้ารหัสข้อมูลสำรองด้วยวิธีที่เหมาะสม และจำกัดสิทธิการเข้าถึงเฉพาะผู้ได้รับมอบหมาย

๙.๖ ต้องกำหนดให้ข้อมูลสำรองอย่างน้อย ๑ ชุด มีมาตรการป้องกันการแก้ไขหรือลบโดยมิชอบ เพื่อรองรับความเสี่ยงด้านภัยคุกคามสมัยใหม่ และเพื่อให้สามารถกู้คืนได้เมื่อเกิดเหตุ

ข้อ ๑๐ แผนบริหารความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศ (Business Continuity Plan and Disaster Recovery)

๑๐.๑ องค์กรต้องจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อรองรับกรณีเหตุฉุกเฉินที่กระทบการให้บริการระบบสารสนเทศ โดยต้องกำหนดบทบาทผู้เกี่ยวข้อง การประเมินความเสี่ยง ขั้นตอนการกู้คืนระบบ การสำรองและการทดสอบกู้คืน และช่องทางติดต่อผู้ให้บริการภายนอก

๑๐.๒ แผนดังกล่าวต้องสอดคล้องกับภารกิจของสำนักงาน ป.ป.ส. และต้องมีแนวทางรองรับการปฏิบัติงานในกรณีไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามความจำเป็น

ข้อ ๑๑ การทบทวนแผนบริหารความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศ

๑๑.๑ ให้ทบทวนแผนสำรอง/กู้คืน และแผนบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศที่มีนัยสำคัญ หรือเมื่อเกิดเหตุการณ์จริง

ข้อ ๑๒ การกำหนด...

ข้อ ๑๒ การกำหนดผู้รับผิดชอบและการเตรียมความพร้อมบุคลากร

๑๒.๑ ให้กำหนดผู้รับผิดชอบดูแลระบบสารสนเทศ ระบบสำรอง และแผนความต่อเนื่อง รวมถึงการสื่อสารแจ้งเตือนและการประสานงานเมื่อเกิดเหตุ

๑๒.๒ ให้จัดให้มีการสร้างความตระหนักรู้ และการฝึกซ้อมสำหรับเจ้าหน้าที่ที่เกี่ยวข้องตามความเหมาะสม

ข้อ ๑๓ การทดสอบสภาพพร้อมใช้งานและการเก็บหลักฐาน

๑๓.๑ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง และจัดเก็บหลักฐานผลการทดสอบเพื่อการตรวจสอบย้อนหลัง

๑๓.๒ การทดสอบต้องครอบคลุมอย่างน้อยในเรื่องการกู้คืนข้อมูลและการดำเนินงานตามขั้นตอนที่กำหนด

ข้อ ๑๔ การประเมินความเพียงพอของระบบสำรองและความต่อเนื่อง ให้ศูนย์เทคโนโลยีสารสนเทศประเมินความเพียงพอของระบบสำรองข้อมูลและมาตรการความต่อเนื่องให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ของสำนักงาน ป.ป.ส. และเสนอแนวทางปรับปรุงต่อผู้บริหารตามรอบที่กำหนด

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยง (Audit & Risk Assessment)

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ข้อ ๑ องค์กรต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างเป็นระบบ เพื่อให้ทราบระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของระบบสารสนเทศ และเพื่อกำหนดมาตรการลดความเสี่ยงให้เหมาะสมกับภารกิจ โดยดำเนินการอย่างน้อยปีละ ๑ ครั้ง โดยศูนย์เทคโนโลยีสารสนเทศร่วมกับกลุ่มตรวจสอบภายใน หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

ข้อ ๒ ผู้ตรวจสอบและความเป็นเอกเทศ

๒.๑ ผู้ตรวจสอบอาจเป็นผู้ตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ หรือผู้ตรวจสอบอิสระจากภายนอก โดยให้เป็นไปตามที่องค์กรกำหนด

๒.๒ ผู้ตรวจสอบต้องมีความเป็นเอกเทศจากกิจกรรมหรือระบบที่จะตรวจสอบ และต้องไม่ตรวจสอบกิจกรรมหรือระบบที่ตนมีหน้าที่ดูแลหรือรับผิดชอบ

๒.๓ ก่อนเริ่มการตรวจสอบ ให้มีข้อตกลงร่วมกันในขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจสอบ

ข้อ ๓ กระบวนการประเมินความเสี่ยงและจัดลำดับความสำคัญ

๓.๑ ให้ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องกับแผนบริหารความเสี่ยงขององค์กร และพิจารณาความเสี่ยงสำคัญที่สัมพันธ์กับภารกิจ เช่น การเข้าถึงโดยมิชอบ การลักลอบใช้รหัสผ่าน เหตุขัดข้องของระบบสารสนเทศหรือระบบเครือข่าย และความเสี่ยงจากเครือข่ายไร้สาย เป็นต้น

๓.๒ ต้องกำหนดวิธีการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง เช่น เกณฑ์โอกาสเกิด ผลกระทบ และระดับความเสี่ยง เป็นต้น

๓.๓ ให้จัดลำดับความสำคัญของความเสี่ยงและกำหนดเจ้าของความเสี่ยงและผู้รับผิดชอบมาตรการสำหรับแต่ละรายการ เพื่อให้ติดตามผลได้จริง

ข้อ ๔ การกำหนด...

ข้อ ๔ การกำหนดมาตรการลดความเสี่ยงและการติดตามผล

๔.๑ ให้พิจารณาทางเลือกในการจัดการความเสี่ยง เช่น ลดความเสี่ยง หลีกเลี่ยง ถ่ายโอน ยอมรับ และประเมินข้อดีข้อเสียของมาตรการที่จะใช้ เป็นต้น

๔.๒ ให้จัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยง พร้อมข้อเสนอแนะและแผนการปรับปรุงแก้ไข โดยระบุผู้รับผิดชอบและกรอบเวลา

๔.๓ ให้ติดตามผลการแก้ไขจนแล้วเสร็จ และจัดเก็บหลักฐานประกอบ เพื่อการตรวจสอบย้อนหลัง

๔.๔ ให้รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง เสนอต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม และแจ้งผู้ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ข้อ ๕ มาตรการควบคุมการเข้าถึงข้อมูล เพื่อการตรวจสอบสมดุลระหว่างความปลอดภัยและความสะดวกต่อผู้ใช้งาน

๕.๑ ให้ผู้ตรวจสอบเข้าถึงข้อมูลที่จำเป็นต่อการตรวจสอบในลักษณะอ่านได้อย่างเดียวเป็นหลัก

๕.๒ กรณีจำเป็นต้องเข้าถึงในลักษณะอื่น ให้สร้างสำเนาข้อมูลสำหรับการตรวจสอบและให้ทำลายและลบสำเนาทันทีเมื่อสิ้นสุดการตรวจสอบ หรือจัดเก็บในแหล่งจัดเก็บที่มีข้อกำหนดการเข้าถึงตามที่องค์กรกำหนด

๕.๓ ให้มีวิธีการแบบปลอดภัยสำหรับการอนุญาตการเข้าถึงข้อมูลที่สามารถเขียนหรือบันทึกได้ และให้กำหนดขั้นตอนปฏิบัติและความรับผิดชอบให้ชัดเจน

๕.๔ ต้องมีวิธีการที่ปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจสอบและจำกัดสิทธิการเข้าถึงเฉพาะผู้ได้รับมอบหมาย

๕.๕ ต้องเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ และบันทึกข้อมูลเหตุการณ์ (Event Log) แสดงการเข้าถึง วันและเวลาในการเข้าถึง โดยเฉพาะระบบงานที่มีความสำคัญ

๕.๖ ให้แยกการติดตั้งเครื่องมือสำหรับการตรวจประเมินออกจากระบบให้บริการจริงหรือระบบพัฒนา และจัดเก็บหรือป้องกันเครื่องมือดังกล่าวจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อไม่กระทบการให้บริการและลดความเสี่ยงต่อระบบจริง

ข้อ ๖ การทบทวนเพิ่มเติมนอกเหนือรอบประจำปี

ให้ดำเนินการทบทวน และประเมินความเสี่ยงเพิ่มเติมเมื่อมีเหตุการณ์สำคัญ เช่น มีการเปลี่ยนแปลงระบบสารสนเทศที่มีนัยสำคัญ เกิดเหตุละเมิดความมั่นคงปลอดภัย หรือพบช่องโหว่หรือภัยคุกคามที่มีผลกระทบสูง เป็นต้น

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ

ข้อ ๗ องค์กรต้องระบุภัยคุกคามที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยตามหมวดที่ ๓ ส่วนที่ ๑ เพื่อนำไปใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยง การกำหนดมาตรการควบคุม และการจัดทำแผนรองรับเหตุฉุกเฉิน

ข้อ ๘ ศูนย์เทคโนโลยีสารสนเทศต้องทบทวนรายการภัยคุกคามและมาตรการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบหรือภัยคุกคามอย่างมีนัยสำคัญ โดยสอดคล้องกับแนวทางการตรวจสอบและประเมินความเสี่ยงขององค์กร

ข้อ ๙ ภัยด้านความ...

ข้อ ๙ ประเภทภัยด้านความมั่นคงปลอดภัยของระบบสารสนเทศ แยกได้ ๔ ประเภท ดังนี้

๙.๑ ประเภทที่ ๑ ภัยจากปัจจัยด้านบุคคล (Human Factor) ครอบคลุมความผิดพลาดจากการใช้งาน (Human Error) การหลอกลวงทางสังคม (Social Engineering) และการกระทำโดยเจตนาหรือภัยคุกคามภายใน (Insider Threat) ที่อาจทำให้ข้อมูลรั่วไหล ระบบสารสนเทศหยุดชะงัก หรือเกิดการเข้าถึงโดยมิชอบ โดยกำหนดให้มีมาตรการขั้นต่ำ ดังต่อไปนี้

๙.๑.๑ องค์กรต้องจัดให้มีการสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยและสื่อสารแนวปฏิบัติให้ผู้ใช้งานรับทราบอย่างสม่ำเสมอ

๙.๑.๒ ผู้ใช้งานต้องปฏิบัติตามนโยบายและรายงานเหตุละเมิด หรือข้อสงสัยด้านความมั่นคงปลอดภัยตามช่องทางที่องค์กรกำหนดโดยเร็ว

๙.๑.๓ การเข้าถึงข้อมูลหรือระบบสารสนเทศให้ยึดหลักเท่าที่จำเป็นตามหน้าที่ และให้มีการทบทวนสิทธิตามรอบการบริหารจัดการการเข้าถึงขององค์กร

๙.๒ ประเภทที่ ๒ ภัยทางเทคนิคและไซเบอร์ (Technical/Cyber Threats) ครอบคลุมโปรแกรมประสงค์ร้าย เช่น ไวรัส หนอน โทรจัน สปายแวร์ การโจมตีผ่านเครือข่าย หรือช่องโหว่ เป็นต้น และเหตุการณ์ที่กระทบต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล โดยกำหนดให้มีมาตรการขั้นต่ำ ดังต่อไปนี้

๙.๒.๑ องค์กรต้องจัดให้มีซอฟต์แวร์ หรือระบบสารสนเทศ เพื่อป้องกันภัยคุกคามและกำหนดรอบการปรับปรุงให้อย่างน้อยเป็นประจำ เช่น รายสัปดาห์หรืออัตโนมัติ ตามที่องค์กรกำหนด เป็นต้น

๙.๒.๒ ให้มีการตรวจสอบบันทึกเหตุการณ์ (Log) และรายงานจากอุปกรณ์ความปลอดภัย เพื่อใช้ระบุความผิดปกติและแหล่งที่มาของภัยคุกคาม

๙.๒.๓ เมื่อพบเหตุที่มีผลกระทบรุนแรงหรือเสี่ยงลุกลาม องค์กรต้องมีอำนาจสั่ง ระงับ/แยกการเชื่อมต่อของเครื่องหรือเครือข่ายที่เกี่ยวข้องทันที และดำเนินการแก้ไขตามขั้นตอนที่กำหนด

๙.๒.๔ ก่อนใช้งานสื่อบันทึกพกพา ให้ตรวจสอบด้วยโปรแกรมป้องกันไวรัสหรือภัยคุกคามตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนด

๙.๓ ประเภทที่ ๓ ภัยด้านสถานที่ โครงสร้างพื้นฐาน และสภาพแวดล้อม โดยครอบคลุมไฟไหม้ ไฟฟ้าขัดข้อง ความร้อนหรือความชื้นผิดปกติ การเข้าถึงพื้นที่สำคัญโดยไม่ได้รับอนุญาต และเหตุที่กระทบห้องศูนย์คอมพิวเตอร์หรืออุปกรณ์เครือข่าย โดยกำหนดให้มีมาตรการขั้นต่ำ ดังนี้

๙.๓.๑ องค์กรต้องกำหนดพื้นที่สำคัญและควบคุมการเข้าออกเฉพาะผู้มีสิทธิได้รับอนุญาต กำหนดช่วงเวลา และจัดให้มีการบันทึกการเข้าออก รวมถึงมาตรการป้องกันการ “ตามเข้า” (tailgating)

๙.๓.๒ ให้จัดให้มีมาตรการรองรับไฟฟ้าขัดข้อง เหตุเพลิงไหม้และตรวจสอบความพร้อมของอุปกรณ์ตามรอบการบำรุงรักษาที่กำหนด รายละเอียดขั้นตอนให้อยู่ในแผนบริหารความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศและแผนฉุกเฉินขององค์กร

๙.๔ ประเภทที่ ๔ ภัยพิบัติและเหตุการณ์รุนแรง (Disaster) เช่น น้ำท่วม เหตุการณ์กระทบสถานที่ปฏิบัติงาน เป็นต้น โดยกำหนดให้มีมาตรการขั้นต่ำ ดังนี้

๙.๔.๑ องค์กรต้องมีแผนรองรับเหตุฉุกเฉินและภัยพิบัติ และการสำรองหรือกู้คืนที่สอดคล้องกับภารกิจ พร้อมทดสอบความพร้อมตามรอบที่กำหนด อย่างน้อยปีละ ๑ ครั้ง หรือตามความเสี่ยงที่เกิดขึ้น

๙.๔.๒ ขั้นตอนปฏิบัติการย้ายอุปกรณ์ การตัดระบบไฟ และการกู้คืน ให้กำหนดไว้ในแผนบริหารความต่อเนื่องและแผนกู้คืนระบบขององค์กร โดยแยกเป็นเอกสารปฏิบัติการ เพื่อไม่ให้ข้อความในนโยบายยาวและล้าสมัยง่าย

หมวดที่ ๔ การรักษา...

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

ข้อ ๑ นิยามพื้นที่ที่เกี่ยวข้องกับระบบสารสนเทศ ให้องค์กรกำหนดอาคารสถานที่ และพื้นที่ใช้งานระบบสารสนเทศ โดยครอบคลุมพื้นที่ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย พื้นที่จัดเก็บสื่อหรือข้อมูลพื้นที่ปฏิบัติงานของบุคลากรด้านเทคโนโลยีสารสนเทศ รวมถึงอุปกรณ์ที่ติดตั้งประจำจุดปฏิบัติงาน

ข้อ ๒ ห้องระบบคอมพิวเตอร์/ศูนย์ข้อมูล (Data Center) และพื้นที่ระบบสำคัญ

๒.๑ ให้กำหนดเป็น “พื้นที่ควบคุม/พื้นที่หวงห้าม” ตามระดับความสำคัญ และอนุญาตเฉพาะผู้มีหน้าที่และได้รับอนุญาตเท่านั้น

๒.๒ ภายนอกพื้นที่ไม่ควรแสดงรายละเอียดที่บ่งชี้ความสำคัญของระบบโดยไม่จำเป็น แต่ภายในเขตควบคุมต้องมีป้ายเตือน/ข้อห้ามตามเหมาะสม เช่น ห้ามเข้าโดยไม่ได้รับอนุญาต เป็นต้น

๒.๓ ต้องล็อกประตู/หน้าต่างเมื่อไม่มีผู้รับผิดชอบอยู่ และต้องห้ามการถ่ายภาพหรือบันทึกภาพภายในพื้นที่ควบคุม เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษร

๒.๔ ให้แยกอุปกรณ์องค์กรสำหรับบุคคลทั่วไป/ผู้มาติดต่อออกจากพื้นที่ควบคุม เพื่อลดความเสี่ยงการเข้าถึงโดยมิชอบ

ข้อ ๓ การแบ่งโซนและกำหนดระดับการควบคุมพื้นที่

๓.๑ ให้จำแนกพื้นที่ตามการใช้งานและความเสี่ยง เช่น พื้นที่ทำงานทั่วไป พื้นที่ผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบ พื้นที่จัดเก็บข้อมูล พื้นที่ครอบคลุมเครือข่ายไร้สาย เป็นต้น และจัดทำแผนผังพื้นที่เพื่อการบริหารจัดการ

๓.๒ การเผยแพร่แผนผังให้จำกัดเฉพาะผู้เกี่ยวข้องตามความจำเป็น

ข้อ ๔ การควบคุมการเข้าออกพื้นที่ (Physical Entry Control)

๔.๑ ต้องกำหนด “ผู้มีสิทธิ/ช่วงเวลา/เงื่อนไข” ในการเข้า–ออกพื้นที่ควบคุมให้ชัดเจน และบันทึกการเข้า–ออกทุกครั้งในพื้นที่สำคัญ

๔.๒ ห้ามเปิดประตูทิ้งไว้ และห้ามยินยอมให้บุคคลอื่น “ติดตามเข้า” โดยไม่ได้รับอนุญาต (ป้องกันการตามเข้า/tailgating)

๔.๓ ผู้มาติดต่อ/ผู้รับจ้างต้องลงทะเบียน แสดงตน ติดบัตรผู้มาติดต่อให้เห็นชัด และต้องมีผู้รับผิดชอบกำกับดูแลตลอดเวลาที่อยู่ในพื้นที่ควบคุม

๔.๔ เมื่อออกจากพื้นที่ควบคุม ต้องคืนบัตรผู้มาติดต่อ และให้ตรวจสอบการคืนบัตรหรือเอกสารอนุญาต รวมถึงตรวจสอบรายการอุปกรณ์ที่นำเข้า–ออกตามที่บันทึกไว้

๔.๕ ให้แยก “จุดรับ–ส่งสิ่งของ” ออกจากพื้นที่ประมวลผลสารสนเทศ และต้องตรวจสอบหรือแกะหีบห่อก่อนนำเข้าสู่พื้นที่ควบคุม

ข้อ ๕ ระบบและสาธารณูปโภคสนับสนุน (Supporting Utilities)

๕.๑ ต้องจัดให้มีระบบสนับสนุนที่จำเป็น เช่น UPS เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศ/ควบคุมความชื้น ระบบระบายอากาศ เป็นต้น ให้เพียงพอต่อการให้บริการ

๕.๒ ต้องทดสอบหรือตรวจสอบระบบสนับสนุนอย่างน้อยปีละ ๑ ครั้ง และมีระบบแจ้งเตือนเมื่อทำงานผิดปกติ

ข้อ ๖ ความมั่นคงปลอดภัยของการเดินสาย (Cabling Security)

๖.๑ ให้จัดการเดินสายให้ลดโอกาสถูกเข้าถึงหรือดักรับข้อมูล และจัดทำผังสายให้ถูกต้อง

๖.๒ ในพื้นที่ควบคุม ให้ติดป้ายระบุสายต้นทาง–ปลายทาง และจัดเก็บสายให้เป็นระเบียบเพื่อลดความเสี่ยงและสะดวกต่อการบำรุงรักษา

ข้อ ๗ การบำรุง...

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ต้องบำรุงรักษาตามคำแนะนำผู้ผลิต และบันทึกกิจกรรมการบำรุงรักษาไว้ตรวจสอบย้อนหลัง

๗.๒ การเข้าดำเนินงานของผู้ให้บริการภายนอกในพื้นที่ควบคุม ต้องอยู่ภายใต้การกำกับดูแล และเป็นไปตามเงื่อนไขการเข้า–ออกขององค์กร

ข้อ ๘ การนำสินทรัพย์ออกนอกสถานที่ (Removal of Property)

๘.๑ การนำอุปกรณ์/สื่อบันทึกข้อมูลออกนอกองค์กร ต้องได้รับอนุญาต และต้องมีบันทึกการนำออก–นำเข้า พร้อมผู้รับผิดชอบและระยะเวลา

๘.๒ หากเป็นสินทรัพย์ที่เกี่ยวข้องกับข้อมูลสำคัญ ให้ใช้มาตรการป้องกันเพิ่มเติมตามที่องค์กรกำหนด เช่น การเข้ารหัสหรือการควบคุมการเข้าถึง เป็นต้น

ข้อ ๙ ความปลอดภัยของอุปกรณ์นอกสถานที่ (Security of Equipment off-premises)

๙.๑ ผู้ครอบครองอุปกรณ์ต้องดูแลไม่ให้สูญหาย ถูกขโมยหรือถูกเข้าถึงโดยมิชอบ และห้ามวางทิ้งไว้โดยไม่มีผู้ดูแล

๙.๒ เมื่อพบเหตุผิดปกติหรือสงสัยการละเมิด ต้องแจ้งผู้บังคับบัญชาหรือหน่วยงานที่รับผิดชอบทันที

ข้อ ๑๐ การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal / Re-use)

๑๐.๑ ก่อนจำหน่าย โอน ยืม หรือส่งซ่อมอุปกรณ์ที่เคยจัดเก็บข้อมูลขององค์กร ต้องลบ/ทำลายข้อมูลให้เหมาะสมตามระดับความสำคัญ และต้องมีหลักฐานการดำเนินการ

๑๐.๒ การลบข้อมูลต้องใช้วิธีที่ป้องกันการกู้คืนโดยมิชอบ หรือใช้การทำลายสื่อเมื่อจำเป็น ตามระเบียบ/แนวปฏิบัติที่องค์กรกำหนด

หมวดที่ ๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย (Incident Response)

ข้อ ๑ การจัดการระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

๑.๑ ผู้ดูแลระบบต้องเฝ้าระวัง ตรวจสอบ และวิเคราะห์บันทึกเหตุการณ์และรายงานจากระบบอย่างสม่ำเสมอ โดยให้สอดคล้องกับระดับความเสี่ยง ความสำคัญของระบบ และความถี่ของกิจกรรมที่เกี่ยวข้อง และต้องดำเนินการตรวจสอบทันทีเมื่อมีการแจ้งเตือนระดับสูงหรือพบเหตุผิดปกติ ทั้งนี้ให้สอดคล้องกับรอบการเฝ้าสังเกตและตรวจสอบรายงานขององค์กร

๑.๒ รายการตรวจสอบอย่างน้อย ได้แก่

๑.๑.๑ ความถี่และประเภทของการโจมตี

๑.๑.๒ รูปแบบ/ลักษณะการโจมตี (ผิดปกติหรือคาดการณ์ได้)

๑.๑.๓ ระดับความรุนแรงของเหตุการณ์

๑.๑.๔ หมายเลขที่อยู่ไอพี (IP Address) ต้นทาง/ปลายทางที่เกี่ยวข้อง

๑.๓ เมื่อพบเหตุที่เข้าข่ายการโจมตีหรือการละเมิดความมั่นคงปลอดภัย ให้ดำเนินการตามหมวดที่ ๕ ข้อ ๒.๓ ทันที

ข้อ ๒ การจัดการระบบไฟร์วอลล์ (Firewall)

๒.๑ ผู้ดูแลระบบต้องตรวจสอบการทำงานและบันทึกเหตุการณ์ของไฟร์วอลล์อย่างน้อยเดือนละ ๑ ครั้ง และควรสรุปผลเพื่อใช้ติดตามแนวโน้มความเสี่ยง

๒.๒ รายการตรวจสอบอย่างน้อย ได้แก่

๒.๒.๑ ทราฟฟิก/แพ็กเก็ต (Packet) หรือการเชื่อมต่อที่ไฟร์วอลล์ปิดกั้น

๒.๒.๒ รูปแบบ...

๒.๒.๒ รูปแบบทราฟฟิกที่ถูกปิดกั้น (ผิดปกติ/ซ้ำ ๆ /มีแนวโน้มโจมตี)

๒.๒.๓ แหล่งที่มา (IP Address/เครือข่าย) ที่ถูกปิดกั้นมากที่สุด

๒.๓ เมื่อพบเหตุที่เข้าข่ายภัยคุกคามทางไซเบอร์หรือการละเมิดความมั่นคงปลอดภัยไซเบอร์ ผู้ดูแลระบบต้องดำเนินมาตรการจำกัดขอบเขตผลกระทบโดยทันทีเท่าที่จำเป็น เก็บรักษาหลักฐานที่เกี่ยวข้อง และรายงานตามโครงสร้างการรายงานเหตุที่สำนักงาน ป.ป.ส. กำหนด พร้อมดำเนินการสอบสวน แก้ไข กู้คืน และทบทวนหลังเกิดเหตุ

ข้อ ๓ การจัดการระบบป้องกันโปรแกรมประสงค์ร้าย (Malware Protection)

๓.๑ องค์กรต้องจัดหาและติดตั้งระบบหรือซอฟต์แวร์ป้องกันภัยคุกคามทางอินเทอร์เน็ตในเครื่องที่เกี่ยวข้อง และสำหรับเครื่องแม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องตั้งค่าให้มีการปรับปรุงฐานข้อมูลภัยคุกคามและซอฟต์แวร์ป้องกันมัลแวร์ให้เป็นปัจจุบันโดยอัตโนมัติ หรือโดยเร็วที่สุดเท่าที่ระบบรองรับ และสอดคล้องกับระดับความเสี่ยงของระบบ

๓.๒ ผู้ดูแลระบบต้องตรวจสอบ Log File และรายงาน โดยตรวจอย่างน้อย ได้แก่

๓.๒.๑ ประเภทภัยคุกคามที่ตรวจพบมากที่สุด

๓.๒.๒ แหล่งต้นทางและปลายทางของการส่ง

๓.๒.๓ กรณีตรวจพบว่ามีการส่งออก/แพร่กระจายจากภายในเครือข่ายขององค์กร

๓.๓ ต้องศึกษาวิธีแก้ไขเครื่องที่ตรวจพบภัยคุกคาม โดยเฉพาะกรณีที่พบการกระจายในเครือข่ายขององค์กร

๓.๔ เมื่อพบว่าเครื่องภายในติดมัลแวร์ หรือมีพฤติการณ์ส่งมัลแวร์ออกไปภายนอก ให้ระงับการเชื่อมต่อเครือข่ายของเครื่องนั้น และดำเนินการแก้ไขทันที

๓.๕ การใช้งานสื่อบันทึกข้อมูลแบบถอดได้ให้ใช้เฉพาะอุปกรณ์ที่ได้รับอนุญาตตามที่สำนักงาน ป.ป.ส. กำหนด และต้องตรวจสอบให้ปลอดจากมัลแวร์ก่อนเชื่อมต่อทุกครั้ง รวมทั้งต้องเข้ารหัสข้อมูลสำคัญหรือข้อมูลละเอียดอ่อนที่บันทึกอยู่ในสื่อนั้น

หมวดที่ ๖ การสร้างความตระหนัก (Awareness Training)

ข้อ ๑ ให้องค์กรทบทวนหรือปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ตามความเหมาะสมและความทันสมัย หรือตามรอบระยะเวลาที่องค์กรกำหนด และต้องทบทวนหรือปรับปรุงทันทีเมื่อมีเหตุหรือปัจจัยสำคัญ เช่น การเปลี่ยนแปลงกฎหมาย เทคโนโลยี ภัยคุกคาม โครงสร้างระบบ หรือเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่มีนัยสำคัญ เป็นต้น ทั้งนี้ ให้เผยแพร่ฉบับที่ปรับปรุงให้ผู้เกี่ยวข้องรับทราบ

ข้อ ๒ การฝึกอบรมและการสร้างความตระหนัก องค์กรต้องจัดให้มีการสื่อสาร อบรม หรือกิจกรรมสร้างความตระหนักเกี่ยวกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ใช้งานตามบทบาทหน้าที่และระดับความเสี่ยง โดยดำเนินการตามรอบระยะเวลาที่องค์กรกำหนด และเพิ่มเติมเมื่อผู้ใช้งานเริ่มปฏิบัติงาน เปลี่ยนบทบาท หรือเมื่อมีประเด็นความเสี่ยงหรือเกิดเหตุการณ์สำคัญ ทั้งนี้ อาจดำเนินการในรูปแบบการอบรม สื่อเรียนรู้ การประชุม หรือการสัมมนา และให้จัดเก็บหลักฐานการดำเนินการตามที่องค์กรกำหนด

ข้อ ๓ การกำกับติดตามและประเมินผลให้ศูนย์เทคโนโลยีสารสนเทศกำกับ ติดตาม และประเมินผลการสร้างความตระหนัก เช่น อัตราการการเข้าร่วม ความเข้าใจหรือความตระหนักรู้หลังอบรม หรือเหตุการณ์ที่เกิดจากความผิดพลาด รวมทั้ง สำรวจความต้องการของผู้ใช้งาน เพื่อนำไปปรับปรุงมาตรการหรือหลักสูตรให้เหมาะสม เป็นต้น

ข้อ ๔ ความตระหนัก...

ข้อ ๔ ความตระหนักเรื่องโปรแกรมไม่ประสงค์ดี องค์กรต้องให้ความรู้เกี่ยวกับโปรแกรมไม่ประสงค์ดีและภัยคุกคามที่พบบ่อย พร้อมกำหนดแนวทางหรือช่องทางแจ้งเหตุเมื่อพบเหตุการณ์ต้องสงสัย เพื่อให้ผู้ใช้งานป้องกันตนเองและลดความเสี่ยงขององค์กร

ข้อ ๕ ความตระหนักเรื่องเหตุการณ์และสถานการณ์ความมั่นคงปลอดภัย องค์กรต้องสื่อสารให้ผู้ใช้งานตระหนักถึงเหตุการณ์หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น และย้ำแนวทางปฏิบัติที่ถูกต้อง เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายได้อย่างถูกต้อง

ข้อ ๖ ผู้ใช้งานต้องปฏิบัติตามกฎหมายที่ใช้บังคับ ระเบียบขององค์กร และข้อตกลงที่เกี่ยวข้องอย่างเคร่งครัด หากฝ่าฝืนหรือประมาทเลินเล่อจนก่อให้เกิดความเสียหายหรือความเสี่ยงต่อความมั่นคงปลอดภัยของสารสนเทศ องค์กรอาจดำเนินการตามระเบียบ/วินัยและมาตรการที่เกี่ยวข้อง ทั้งนี้ให้ถือว่าผู้ใช้งานเป็นผู้รับผิดชอบต่อการกระทำแล้วแต่กรณี

หมวดที่ ๗ หน้าที่และความรับผิดชอบ (Roles & Responsibilities)

ข้อ ๑ ระดับนโยบาย (Policy Level) ได้แก่ ผู้บริหารสูงสุดขององค์กร (Chief Executive Officer: CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

หน้าที่และความรับผิดชอบ

๑.๑ กำหนดนโยบาย มาตรฐาน และกรอบการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงกำหนดตำแหน่งด้านความมั่นคงปลอดภัยและมอบหมายความรับผิดชอบให้เหมาะสม

๑.๒ กำกับดูแล ติดตาม และทบทวนภาพรวมนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรให้คงไว้และมีประสิทธิผล

๑.๓ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ให้เป็นไปตามหลักความรับผิดชอบของผู้บริหารระดับสูงสุดตามที่นโยบายกำหนด

ข้อ ๒ ระดับบริหาร (Management Level) ได้แก่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ผู้บังคับบัญชาตามโครงสร้างการบริหารขององค์กร และหรือผู้ควบคุมและผู้ประสานงานหรือผู้ที่ได้รับมอบหมาย (ภาคผนวก)

หน้าที่และความรับผิดชอบ

๒.๑ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติหน้าที่ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามนโยบาย มาตรฐาน และข้อกำหนดขององค์กร

๒.๒ อนุมัติหรือกำกับการควบคุมการเข้าถึงพื้นที่สำคัญ เช่น ศูนย์คอมพิวเตอร์สำรอง และกระบวนการควบคุมการเข้าออก ตามที่นโยบายกำหนด เป็นต้น

๒.๓ เมื่อพบการโจมตีหรือเหตุละเมิดความมั่นคงปลอดภัย ให้สั่งการหรือตัดสินใจดำเนินการแก้ไขตามลำดับขั้น และให้รายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) และผู้บริหารสูงสุดขององค์กร (Chief Executive Officer: CEO) ตามลำดับ

ข้อ ๓ ระดับปฏิบัติ (Operational Level) ได้แก่ ผู้ดูแลระบบ ผู้ประสานงาน และหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

หน้าที่และความรับผิดชอบ

๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร และรายงานเหตุการณ์ที่เกี่ยวข้องตามลำดับขั้น

๓.๒ ดูแลความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการอย่างน้อย ได้แก่ ปิดบริการที่ไม่ใช้งาน ติดตั้งระบบเทียบเวลา (NTP) และจำกัดการเข้าถึงบัญชีสิทธิพิเศษโดยตรง รวมถึงตรวจสอบ แก้ไข และรายงานเหตุหรือช่องโหว่ต่อผู้บังคับบัญชา

๓.๓ ดำเนินการสำรองและกู้คืนข้อมูลตามแผนและรอบเวลาที่องค์กรกำหนด โดยระบบที่มีความสำคัญสูงต้องเพิ่มความถี่การสำรอง และจัดเก็บสื่อสำรองนอกสถานที่หรือศูนย์คอมพิวเตอร์สำรองตามที่กำหนด

๓.๔ ระงับหรือปิดกั้นการเข้าถึงอินเทอร์เน็ตชั่วคราวสำหรับเครื่องคอมพิวเตอร์หรือผู้ใช้งานที่มีพฤติการณ์เสี่ยงต่อความปลอดภัยสารสนเทศ จนกว่าจะพิสูจน์ได้ว่าปลอดภัยหรือได้ดำเนินการแก้ไขตามนโยบายแล้ว

หมวดที่ ๘ การพัฒนาระบบสารสนเทศ

ข้อ ๑ หลักเกณฑ์และคุณลักษณะขั้นต่ำของการพัฒนาระบบสารสนเทศการพัฒนาระบบสารสนเทศขององค์กร ต้องกำหนดขั้นตอนการพิจารณา ทบทวน และอนุมัติการสร้าง การติดตั้ง และการใช้งาน โดยอย่างน้อยระบบต้องมีคุณลักษณะ ดังนี้

๑.๑ สอดคล้องกับสถาปัตยกรรมองค์กร (Enterprise Architecture: EA) หรือสถาปัตยกรรมระบบที่ศูนย์เทคโนโลยีสารสนเทศกำหนด

๑.๒ สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร และหลักการควบคุมการเข้าถึงตามบทบาทหน้าที่

๑.๓ สามารถทำงานร่วมกับระบบที่ยังใช้งานอยู่ได้อย่างเหมาะสม และไม่กระทบต่อความต่อเนื่องของภารกิจ

๑.๔ ต้องทดสอบระบบบนสภาพแวดล้อมทดสอบ (Test) ที่แยกจากสภาพแวดล้อมใช้งานจริง (Production) และมีความใกล้เคียงกับการใช้งานจริงตามสมควร โดยสำหรับระบบที่มีความสำคัญสูงห้ามทดสอบบนระบบจริง และก่อนนำขึ้นใช้งานจริงต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อน

๑.๕ ระบบสำคัญและองค์ประกอบสำคัญ เช่น ระบบบริการไดเรกทอรีขององค์กร ต้องดำเนินการทบทวนค่ากำหนดด้านความมั่นคงปลอดภัยตามมาตรฐานการปรับตั้งค่าความมั่นคงปลอดภัยของระบบ (Security Baseline) ที่องค์กรกำหนด เช่น CIS Benchmarks หรือมาตรฐานเทียบเท่า และต้องประเมินภัยคุกคามและช่องโหว่ก่อนเปิดใช้งาน เป็นต้น

๑.๖ การจัดหาครุภัณฑ์ ซอฟต์แวร์ หรือบริการที่ใช้ในโครงการ ให้ดำเนินการตามกฎหมายและระเบียบด้านพัสดุที่เกี่ยวข้อง โดยพิจารณาความคุ้มค่า ความจำเป็น และความเสี่ยงด้านความมั่นคงปลอดภัยประกอบ

๑.๗ ก่อนนำระบบขึ้นใช้งานจริง ต้องมีผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยารสนเทศ และแผนจัดการความเสี่ยงของโครงการที่ผ่านการพิจารณาตามที่องค์กรกำหนด และกรณีมีข้อมูลส่วนบุคคลต้องดำเนินการตามผลการคัดกรองหรือผลการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

ข้อ ๒ ขั้นตอนการเสนอและอนุมัติโครงการพัฒนาระบบสารสนเทศ การเสนอโครงการพัฒนาระบบสารสนเทศขององค์กร ให้ดำเนินการอย่างน้อย ดังนี้

๒.๑ เจ้าของโครงการทบทวนกระบวนงานและสำรวจความต้องการ พร้อมประเมินผลกระทบต่อภารกิจและความเสี่ยงเบื้องต้น

๒.๑.๑ เจ้าของ...

๒.๑.๑ เจ้าของโครงการต้องจัดทำ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของโครงการ และกำหนดมาตรการลดความเสี่ยง (Risk Treatment) ร่วมกับศูนย์เทคโนโลยีสารสนเทศ เพื่อใช้ประกอบการอนุมัติโครงการ

๒.๑.๒ กรณีโครงการมีการประมวลผลข้อมูลส่วนบุคคล ให้ดำเนินการคัดกรองความจำเป็นในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และเมื่อเข้าเกณฑ์ความเสี่ยงสูงให้จัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และมาตรการคุ้มครองข้อมูลส่วนบุคคลก่อนเสนออนุมัติหรือก่อนเริ่มประมวลผลข้อมูลจริง

ทั้งนี้ การคัดกรองโครงการที่ต้องจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) อาจพิจารณาจากปัจจัย อาทิ ข้อมูลอ่อนไหว ข้อมูลด้านคดีหรือข่าวกรอง ปริมาณข้อมูล จำนวนมาก การเฝ้าติดตามอย่างเป็นระบบ การใช้เทคโนโลยีใหม่หรือเทคโนโลยีปัญญาประดิษฐ์ หรือการแลกเปลี่ยนข้อมูลข้ามหน่วยงานหรือใช้ผู้รับจ้างภายนอก เป็นต้น

๒.๒ จัดทำข้อเสนอโครงการ โดยให้ศูนย์เทคโนโลยีสารสนเทศร่วมพิจารณาด้านสถาปัตยกรรมระบบและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๓ เสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศพิจารณาให้ความเห็นหรืออนุมัติในส่วนที่เกี่ยวข้อง ก่อนดำเนินการจัดทำข้อกำหนดและการจัดหา

๒.๔ ดำเนินการจัดทำข้อกำหนดของโครงการและการจัดหาตามระเบียบพัสดุและข้อกำหนดภายในขององค์กร

ข้อ ๓ การควบคุมการพัฒนาระบบสารสนเทศที่จัดจ้างผู้รับจ้างภายนอก เมื่อองค์กรจัดจ้างผู้รับจ้างภายนอกพัฒนาหรือบำรุงรักษาระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๓.๑ เจ้าของโครงการและศูนย์เทคโนโลยีสารสนเทศชี้แจงแนวคิด ข้อกำหนด มาตรฐาน และกระบวนงานให้ผู้รับจ้างทราบอย่างชัดเจน

๓.๒ กำหนดบทบาท หน้าที่ ความรับผิดชอบ และช่องทางประสานงานของผู้เกี่ยวข้อง ไม่ว่าจะเป็นเจ้าของโครงการ ศูนย์เทคโนโลยีสารสนเทศ และผู้รับจ้างในโครงการนั้นให้ชัดเจน

๓.๓ กำหนดแผนงานและรอบการรายงานความก้าวหน้าเป็นระยะ เช่น รายสัปดาห์ รายปักษ์ เป็นต้น ทั้งนี้ ให้เป็นไปตามความเหมาะสมของโครงการ

๓.๔ กำหนดมาตรการควบคุมการเข้าถึงระบบสำหรับผู้ใช้งานภายนอก โดยอย่างน้อยต้องจำกัดสิทธิขั้นต่ำ วิธีการพิสูจน์ตัวตน และบันทึกกิจกรรมเป็นแฟ้มบันทึกเหตุการณ์ (Log File) รวมทั้งกำหนดให้หน่วยงานภายนอกลงนามในข้อตกลงไม่เปิดเผยข้อมูลตามที่นโยบายกำหนด

๓.๕ สำหรับระบบที่มีความสำคัญสูง ห้ามทดสอบบนระบบใช้งานจริง (Production) ต้องทดสอบบนระบบทดสอบ (Test) ให้แล้วเสร็จก่อน และก่อนติดตั้งขึ้นระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

ข้อ ๔ การทดสอบ การนำขึ้นใช้งานจริง และการตรวจรับ

๔.๑ ต้องทดสอบระบบตามข้อกำหนดที่กำหนดไว้ รวมถึงการทดสอบด้านความมั่นคงปลอดภัย บนสภาพแวดล้อมทดสอบที่แยกจากระบบใช้งานจริง และจัดเก็บผลการทดสอบเป็นหลักฐาน

๔.๒ การนำระบบขึ้นใช้งานจริงต้องได้รับอนุญาตจากผู้บริหารก่อน โดยเฉพาะระบบสารสนเทศที่มีความสำคัญสูง

๔.๓ การตรวจรับ...

๔.๓ การตรวจรับให้เป็นไปตามระเบียบพัสดุ โดยต้องมีเงื่อนไขการส่งมอบเอกสารที่จำเป็น เช่น คู่มือผู้ใช้งาน รายการค่ากำหนดที่สำคัญ หรือรายงานผลการทดสอบระบบสารสนเทศที่เกี่ยวข้อง เป็นต้น เพื่อสนับสนุนการดูแลต่อเนื่องตามที่นโยบายกำหนดให้มีคู่มือและเอกสารควบคุมงาน

๔.๔ การนำระบบขึ้นใช้งานจริงให้กระทำได้เมื่อ

๔.๔.๑ ได้ดำเนินการตามมาตรการจัดการความเสี่ยงที่กำหนดไว้แล้ว หรือ

๔.๔.๒ ได้รับการยอมรับความเสี่ยงตามลำดับอำนาจขององค์กร และกรณีข้อมูลส่วนบุคคลต้องดำเนินการตามผลการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) หรือมาตรการคุ้มครองข้อมูลส่วนบุคคลแล้ว

ข้อ ๕ เงื่อนไขการรับประกันและการสนับสนุนหลังตรวจรับ

๕.๑ ให้กำหนดระดับการให้บริการและเวลาการตอบสนองและการแก้ไข (Service Level Agreement: SLA) ตามความรุนแรงและผลกระทบต่อภารกิจ เพื่อสมดุลความปลอดภัยและความพร้อมใช้

๕.๒ ผู้รับจ้างต้องจัดให้มีผู้ประสานงานหรือทีมสนับสนุนตามที่กำหนดในสัญญาจ้าง และต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กรตลอดระยะเวลารับประกัน

หมวดที่ ๙ การจัดหาครุภัณฑ์คอมพิวเตอร์

ข้อ ๑ หลักการจัดหาและการปฏิบัติตามกฎหมาย

๑.๑ การจัดหาครุภัณฑ์คอมพิวเตอร์ ระบบสารสนเทศ ซอฟต์แวร์ และบริการดิจิทัลที่เกี่ยวข้องขององค์กร ต้องดำเนินการให้เป็นไปตามกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ระเบียบกระทรวงการคลังที่เกี่ยวข้อง แนวทางของกรมบัญชีกลาง หลักเกณฑ์การดำเนินการผ่านระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ตลอดจนประกาศหรือแนวปฏิบัติของกระทรวงยุติธรรมและขององค์กรที่เกี่ยวข้อง

๑.๒ องค์กรต้องจัดทำแผนการจัดซื้อจัดจ้างประจำปีและดำเนินการเผยแพร่ตามหลักเกณฑ์ที่กฎหมายและระเบียบกำหนด

๑.๓ การพิจารณาแนวทางจัดหาให้คำนึงถึงความจำเป็น ความคุ้มค่าในภาพรวม ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และความต่อเนื่องของภารกิจ โดยให้พิจารณาตามลำดับความเหมาะสม ดังนี้

๑.๓.๑ การใช้ครุภัณฑ์เดิมที่ยังอยู่ในสภาพพร้อมใช้งานหรือการโอนย้ายครุภัณฑ์ภายในองค์กร

๑.๓.๒ การใช้บริการหรือสัญญากลาง หรือบริการร่วมของภาครัฐ (ถ้ามี)

๑.๓.๓ การเช่า หรือเช่าซื้อ เมื่อเหมาะสมด้านงบประมาณและการดูแลรักษา

๑.๓.๔ การจัดซื้อ เมื่อมีเหตุผลความจำเป็นและมีความคุ้มค่าโดยเปรียบเทียบทางเลือกแล้ว

ข้อ ๒ การกำหนดความต้องการและคุณลักษณะเฉพาะ (TOR)

๒.๑ ให้หน่วยงานเจ้าของความต้องการจัดทำข้อกำหนดและคุณลักษณะเฉพาะของครุภัณฑ์ร่วมกับศูนย์เทคโนโลยีสารสนเทศ เพื่อให้สอดคล้องกับสถาปัตยกรรมองค์กร มาตรฐานความมั่นคงปลอดภัยสารสนเทศ และแนวทางการดูแลบำรุงรักษาและการบริหารจัดการภายหลังการใช้งาน

๒.๒ การกำหนด...

๒.๒ การกำหนดคุณลักษณะเฉพาะต้องยึดตามวัตถุประสงค์การใช้งาน สมรรถนะ และคุณภาพทางเทคนิค โดยต้องไม่กำหนดคุณลักษณะในลักษณะจำเพาะเจาะจงให้ใกล้เคียงเครื่องหมายการค้า รุ่น หรือผู้ประกอบการรายใดรายหนึ่ง เว้นแต่มีเหตุจำเป็นและเป็นไปตามหลักเกณฑ์ที่กฎหมายและระเบียบกำหนด

๒.๓ ข้อกำหนดหรือสัญญา ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขั้นต่ำให้เหมาะสมกับระดับความสำคัญของระบบข้อมูล และความเสี่ยงที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

๒.๓.๑ ระยะเวลาการสนับสนุนจากผู้ผลิตและการได้รับแพตช์ความปลอดภัย โดยต้องไม่จัดหารุ่นที่หมดระยะการสนับสนุน

๒.๓.๒ การตั้งค่าเริ่มต้นที่ปลอดภัย การปิดบริการหรือพอร์ตที่ไม่จำเป็น และการปรับแต่งค่าความมั่นคงปลอดภัยของระบบ (System Hardening) ตามความเหมาะสม

๒.๓.๓ ความสามารถด้านการบันทึกเหตุการณ์และการตรวจสอบย้อนกลับ

๒.๓.๔ การตรวจสอบช่องโหว่ (Vulnerability Assessment) ก่อนใช้งานจริงหรือก่อนส่งมอบ ในกรณีที่มีความเสี่ยงหรือมีความสำคัญต่อภารกิจ

๒.๓.๕ การเชื่อมต่อหรือรองรับการเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) หรือศูนย์เฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) ตามความเหมาะสม เป็นต้น

๒.๓.๖ การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบสำคัญหรือระบบที่เข้าถึงข้อมูลสำคัญ ตามความเหมาะสมของความเสี่ยง

๒.๓.๗ เงื่อนไขการเข้าถึงของผู้ให้บริการหรือคู่สัญญา โดยต้องได้รับอนุญาตจำกัดสิทธิเท่าที่จำเป็น และมีการบันทึกการเข้าถึง

๒.๓.๘ เงื่อนไขด้านการรับประกัน การซ่อมบำรุง และการสนับสนุนต่อเนื่องตามภารกิจขององค์กร

๒.๔ กรณีครุภัณฑ์หรือระบบที่จัดหามีการประมวลผล จัดเก็บ หรือเข้าถึงข้อมูลส่วนบุคคล หรือข้อมูลสำคัญขององค์กร ต้องกำหนดมาตรการให้สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง ดังนี้

๒.๔.๑ ต้องรองรับมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง

๒.๔.๒ ต้องสอดคล้องกับการจำแนกประเภทข้อมูลขององค์กร และระดับชั้นความลับของข้อมูล

๒.๔.๓ ต้องมีมาตรการป้องกันการรั่วไหลของข้อมูล เช่น การเข้ารหัสข้อมูล และการควบคุมสิทธิการเข้าถึง เป็นต้น

๒.๔.๔ กรณีมีการโอนย้าย เลิกใช้งาน หรือปลดระวางครุภัณฑ์หรือระบบสารสนเทศต้องดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถกู้คืนได้ตามมาตรฐานและแนวปฏิบัติขององค์กร

๒.๕ กรณีมีการจัดหาในรูปแบบบริการประมวลผลแบบกลุ่มคลาวด์ (Cloud Computing) บริการซอฟต์แวร์ (Software as a Service: SaaS) หรือบริการแบบบอกรับสมาชิก Subscription) ต้องกำหนดเงื่อนไขเพิ่มเติมตามความเหมาะสม ดังนี้

๒.๕.๑ การระบุสถานที่จัดเก็บข้อมูล (Data Location) หรือเงื่อนไขด้านการประมวลผลข้อมูลให้ชัดเจน

๒.๕.๒ การกำหนด...

๒.๕.๒ การกำหนดให้ผู้ให้บริการมีมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม เช่น ISO/IEC ๒๗๐๐๑ หรือมาตรฐานอื่นที่เทียบเท่า เป็นต้น

๒.๕.๓ การกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) และมาตรการคุ้มครองข้อมูลส่วนบุคคล

๒.๕.๔ การกำหนดสิทธิการเข้าถึงข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล และเงื่อนไขการส่งคืนหรือย้ายข้อมูลเมื่อสิ้นสุดสัญญา

ข้อ ๓ ขั้นตอนเสนออนุมัติและความโปร่งใส

๓.๑ การเสนอขอจัดหาให้จัดทำข้อเสนอประกอบด้วยเหตุผลความจำเป็น ขอบเขตการใช้งาน แผนการดูแลรักษาหรือบำรุงรักษา และการประเมินความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลตามความเหมาะสม

๓.๒ หน่วยงานผู้รับผิดชอบต้องจัดทำบันทึกรายงานผลการพิจารณา วิธีการ และขั้นตอนการดำเนินการให้เป็นระบบ เพื่อรองรับการตรวจสอบย้อนหลัง

๓.๓ ต้องรักษาความลับของข้อมูลข้อเสนอและข้อมูลทางเทคนิคของผู้ยื่นข้อเสนอ และห้ามเปิดเผยแก่ผู้ไม่มีหน้าที่เกี่ยวข้อง

๓.๔ ผู้มีหน้าที่ดำเนินการจัดซื้อจัดจ้างต้องหลีกเลี่ยงการขัดกันแห่งผลประโยชน์ และต้องไม่เป็นผู้มีส่วนได้เสียกับผู้ยื่นข้อเสนอหรือคู่สัญญา

๓.๕ ให้ดำเนินการจัดซื้อจัดจ้างผ่านช่องทางและระบบที่กฎหมายกำหนด ได้แก่ ระบบ e-GP และปฏิบัติตามหลักเกณฑ์การรายงานหรือการประกาศที่เกี่ยวข้องอย่างเคร่งครัด

ข้อ ๔ การตรวจรับ การติดตั้ง และการขึ้นทะเบียนสินทรัพย์

๔.๑ การตรวจรับครุภัณฑ์ให้เป็นไปตามกฎหมายและระเบียบพัสดุภาครัฐ โดยต้องตรวจสอบคุณลักษณะให้ครบถ้วนตามสัญญา และทดสอบการใช้งานจริงตามวัตถุประสงค์ รวมถึงการทดสอบความเสถียรตามความเหมาะสม

๔.๒ ก่อนนำครุภัณฑ์เข้าสู่การใช้งานจริง ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดค่าและตรวจสอบการตั้งค่าพื้นฐานด้านความปลอดภัยให้เป็นไปตามมาตรฐานขององค์กร

๔.๓ องค์กรต้องขึ้นทะเบียนสินทรัพย์ (Asset Register) กำหนดผู้รับผิดชอบสินทรัพย์ และจัดเก็บข้อมูลสำคัญประกอบการบริหารจัดการ อาทิ หมายเลขประจำเครื่อง สถานที่ติดตั้ง ผู้ถือครอง ระยะรับประกัน วันเริ่มใช้งาน และสถานะของสินทรัพย์ เป็นต้น

๔.๔ ให้จัดเก็บเอกสารส่งมอบที่จำเป็น เช่น รายการตั้งค่า การกำหนดสิทธิการเข้าถึง คู่มือการใช้งานหรือการดูแลรักษา และเงื่อนไขบริการหลังการส่งมอบ เพื่อรองรับการตรวจสอบย้อนหลังและการบำรุงรักษา เป็นต้น

๔.๕ องค์กรต้องบริหารจัดการวงจรชีวิตของครุภัณฑ์หรือระบบอย่างเหมาะสม ดังนี้

๔.๕.๑ กำหนดอายุการใช้งานและเกณฑ์การพิจารณาทดแทนที่เหมาะสม

๔.๕.๒ จัดทำแผนการบำรุงรักษาและแผนการทดแทนล่วงหน้า

๔.๕.๓ เมื่อสิ้นสุดการใช้งาน ต้องดำเนินการจำหน่าย โอนย้าย ทำลาย หรือปลดระวางตามระเบียบที่เกี่ยวข้อง พร้อมทั้งดำเนินการลบหรือทำลายข้อมูลอย่างปลอดภัยตามแนวปฏิบัติขององค์กร

ข้อ ๕ การรับประกัน...

ข้อ ๕ การรับประกันหรือการบำรุงรักษา และการเข้าถึงโดยคู่สัญญา

๕.๑ เงื่อนไขการให้บริการหลังส่งมอบ ให้กำหนดตามระดับความรุนแรงของเหตุขัดข้องและผลกระทบต่อภารกิจขององค์กร โดยระบุเวลาตอบสนองและเวลาแก้ไขให้ชัดเจนในสัญญา

๕.๒ การเข้าถึงระบบสารสนเทศหรือข้อมูลขององค์กรโดยคู่สัญญา ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง กำหนดขอบเขตสิทธิเท่าที่จำเป็น และต้องบันทึกการเข้าถึงเพื่อการตรวจสอบย้อนหลัง

๕.๓ บุคลากรของคู่สัญญาต้องปฏิบัติตามข้อกำหนดด้านความลับและความมั่นคงปลอดภัยขององค์กร และต้องลงนามในข้อตกลงไม่เปิดเผยข้อมูลตามแบบที่องค์กรกำหนดก่อนเข้าปฏิบัติงาน

๕.๔ เมื่อสิ้นสุดการรับประกัน หรือสิ้นสุดสัญญา หรือสิ้นสุดการใช้งาน ให้เพิกถอนสิทธิการเข้าถึงทั้งหมด คืนสินทรัพย์ และดำเนินการจัดการข้อมูล หรือสื่อบันทึกที่เกี่ยวข้องตามแนวปฏิบัติขององค์กร

๕.๕ องค์กรต้องบริหารความเสี่ยงของผู้รับจ้างหรือผู้ให้บริการภายนอกตามความเหมาะสม ดังนี้

๕.๕.๑ ประเมินความเสี่ยงของผู้รับจ้างหรือผู้ให้บริการภายนอกก่อนทำสัญญาในกรณีที่มีการเข้าถึงระบบสารสนเทศ ข้อมูลสำคัญ หรือข้อมูลส่วนบุคคล

๕.๕.๒ กรณีมีการประมวลผลข้อมูลส่วนบุคคลในนามขององค์กร ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) หรือเอกสารอื่นที่มีผลในทำนองเดียวกันตามที่กฎหมายกำหนด

๕.๕.๓ องค์กรอาจกำหนดสิทธิในการตรวจสอบหรือประเมินมาตรการด้านความมั่นคงปลอดภัยของผู้รับจ้างหรือผู้ให้บริการภายนอก ตามความเหมาะสมและตามเงื่อนไขที่กำหนดไว้ในสัญญา

ข้อ ๖ การกำกับดูแลและการตรวจสอบ

๖.๑ ให้องค์กรหรือหน่วยงานที่ได้รับมอบหมายดำเนินการตรวจสอบภายในด้านการจัดหาครุภัณฑ์คอมพิวเตอร์ ระบบสารสนเทศ และบริการดิจิทัลที่เกี่ยวข้องเป็นระยะตามความเหมาะสม

๖.๒ การดำเนินการตามหมวดนี้ต้องสามารถตรวจสอบย้อนหลังได้ทุกขั้นตอน โดยมีเอกสาร หลักฐาน และบันทึกเหตุการณ์ที่เกี่ยวข้องอย่างเพียงพอ

๖.๓ ให้องค์กรประเมินความสอดคล้องของการดำเนินการตามหมวดนี้กับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้องเป็นระยะ และปรับปรุงมาตรการให้เหมาะสมกับความเสี่ยงและบริบทขององค์กร

หมวดที่ ๑๐ การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI)

ส่วนที่ ๑ การใช้ความสามารถเทคโนโลยีปัญญาประดิษฐ์

ข้อ ๑ หลักการทั่วไป

๑.๑ การประยุกต์ใช้ปัญญาประดิษฐ์ขององค์กรต้องเป็นไปเพื่อสนับสนุนภารกิจของหน่วยงานอย่างเหมาะสม โปร่งใส ตรวจสอบได้ ปลอดภัย และสอดคล้องกับกฎหมาย ระเบียบ นโยบายองค์กร และหลักธรรมาภิบาลปัญญาประดิษฐ์ของประเทศไทย

๑.๒ การประยุกต์ใช้ปัญญาประดิษฐ์ ต้องคำนึงถึงอย่างน้อย ดังต่อไปนี้

๑.๒.๑ ความถูกต้อง ความน่าเชื่อถือ และความเหมาะสมของผลลัพธ์

๑.๒.๒ ความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

๑.๒.๓ ความเป็นธรรม...

๑.๒.๓ ความเป็นธรรม การลดอคติ และการหลีกเลี่ยงการเลือกปฏิบัติ

๑.๒.๔ ความโปร่งใส ความสามารถในการอธิบายผลลัพธ์ และการตรวจสอบย้อนหลัง

๑.๒.๕ การกำกับดูแลโดยมนุษย์ตามระดับความเสี่ยงของระบบ

๑.๓ ปัญญาประดิษฐ์เป็นเครื่องมือเพื่อสนับสนุนการปฏิบัติงานและการตัดสินใจของเจ้าหน้าที่ ไม่ใช่เพื่อทดแทนดุลยพินิจของมนุษย์ในเรื่องที่มีผลกระทบสำคัญ

ข้อ ๒ การจำแนกประเภทการใช้งานตามระดับความเสี่ยง

๒.๑ องค์กรกำหนดให้การใช้ปัญญาประดิษฐ์แบ่งเป็นอย่างน้อย ๓ ระดับ เพื่อกำหนดระดับการอนุมัติ มาตรการควบคุม และระดับการกำกับดูแลโดยมนุษย์ให้เหมาะสม ดังนี้

๒.๑.๑ ระดับความเสี่ยงต่ำ ได้แก่ การใช้เพื่อช่วยสรุปเนื้อหา จัดหมวดหมู่เอกสารที่ไม่เป็นข้อมูลจำกัดการเข้าถึง หรือช่วยค้นหาข้อมูลสาธารณะ โดยต้องไม่ใช้ข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กร

๒.๑.๒ ระดับความเสี่ยงปานกลาง ได้แก่ การใช้เพื่อวิเคราะห์แนวโน้ม สนับสนุนการวางแผน หรือช่วยคัดกรองข้อมูลที่มีความอ่อนไหวบางส่วน โดยต้องมีมาตรการคุ้มครองข้อมูลและการกำกับดูแลเพิ่มเติมตามที่องค์กรกำหนด

๒.๑.๓ ระดับความเสี่ยงสูง ได้แก่ การใช้กับข้อมูลจำกัดการเข้าถึง ข้อมูลลับ ข้อมูลด้านคดีหรือข่าวกรอง ข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวจำนวนมาก หรือกรณีที่ผลลัพธ์อาจมีผลกระทบอย่างมีนัยสำคัญต่อสิทธิของบุคคล ภารกิจขององค์กร หรือการบังคับใช้กฎหมาย โดยต้องใช้มาตรการควบคุมเข้มงวด ได้รับอนุมัติตามลำดับอำนาจ และมีการกำกับดูแลโดยมนุษย์อย่างใกล้ชิด

๒.๒ การกำหนดระดับความเสี่ยงต้องพิจารณาร่วมกันอย่างน้อยจากประเภทข้อมูล วัตถุประสงค์การใช้งาน ระดับการพึ่งพาผลลัพธ์ของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบุคคล องค์กร หรือสาธารณะ

ส่วนที่ ๒ เงื่อนไขก่อนเริ่มใช้งานและการใช้บริการจากภายนอก

ข้อ ๓ เงื่อนไขก่อนเริ่มใช้งานปัญญาประดิษฐ์

๓.๑ ก่อนเริ่มใช้งานปัญญาประดิษฐ์ ต้องกำหนดบทบาทและผู้รับผิดชอบอย่างชัดเจนอย่างน้อย ได้แก่

๓.๑.๑ เจ้าของระบบ (System Owner: SO)

๓.๑.๒ เจ้าของข้อมูล (Data Owner: DO)

๓.๑.๓ เจ้าของแบบจำลอง (Model Owner: MO) หรือผู้รับผิดชอบการใช้งานปัญญาประดิษฐ์ (AI Service Owner: AISO) แล้วแต่กรณี

๓.๒ ต้องพิจารณาความจำเป็น ความเหมาะสมของการใช้ปัญญาประดิษฐ์ (AI) และความพร้อมของข้อมูลให้สอดคล้องกับวัตถุประสงค์ของงานก่อนเริ่มใช้งาน

๓.๓ ต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของการใช้งานปัญญาประดิษฐ์ (AI) ให้สอดคล้องกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรและแนวทางที่องค์กรอ้างอิง

๓.๔ กรณีมีการเก็บ ใช้ เปิดเผย หรือประมวลผลข้อมูลส่วนบุคคล ต้องคัดกรองความจำเป็นในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) และเมื่อเข้าเกณฑ์ความเสี่ยงสูงให้จัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และกำหนดมาตรการคุ้มครองก่อนเริ่มประมวลผลข้อมูลจริง

๓.๕ ต้องกำหนด...

๓.๕ ต้องกำหนดมาตรการควบคุมขั้นต่ำอย่างน้อย ดังนี้

๓.๕.๑ การควบคุมการเข้าถึงตามบทบาทหน้าที่ และการกำหนดสิทธิเท่าที่จำเป็น

๓.๕.๒ การยืนยันตัวตนแบบหลายปัจจัยสำหรับบัญชีสิทธิพิเศษหรือการเข้าถึงจากภายนอก

๓.๕.๓ การจัดชั้นข้อมูลและการจำกัดการเปิดเผยข้อมูลตามระดับชั้นความลับ

๓.๕.๔ การจัดให้มีบันทึกเหตุการณ์เพื่อการตรวจสอบย้อนหลัง

๓.๕.๕ การคุ้มครองข้อมูลระหว่างส่งผ่านและขณะจัดเก็บตามมาตรฐานขององค์กร

ข้อ ๔ การจัดหาและการใช้บริการปัญญาประดิษฐ์จากภายนอก

๔.๑ การใช้บริการปัญญาประดิษฐ์จากภายนอก ต้องผ่านการพิจารณาความเสี่ยงของผู้ให้บริการอย่างน้อย ดังต่อไปนี้

๔.๑.๑ สถานที่จัดเก็บข้อมูล ระยะเวลาการเก็บรักษา และผู้มีสิทธิเข้าถึงข้อมูล

๔.๑.๒ นโยบายการนำข้อมูลขององค์กรไปใช้ฝึกต่อหรือปรับปรุงแบบจำลอง

๔.๑.๓ มาตรการป้องกันการรั่วไหลของข้อมูลและการแจ้งเหตุด้านความมั่นคงปลอดภัย

๔.๑.๔ ความเหมาะสมของสภาพแวดล้อมการให้บริการกับระดับชั้นและความอ่อนไหวของข้อมูล

๔.๒ สัญญาหรือข้อตกลงต้องกำหนดเงื่อนไขขั้นต่ำ ได้แก่ ความลับ สิทธิในข้อมูล การแจ้งเหตุรั่วไหล สิทธิการตรวจสอบ การยุติบริการ และการลบหรือทำลายข้อมูลเมื่อสิ้นสุดการให้บริการ

๔.๓ การเข้าถึงระบบหรือข้อมูลขององค์กรโดยผู้รับจ้างหรือผู้ให้บริการ ต้องจำกัดสิทธิเท่าที่จำเป็น ใช้การยืนยันตัวตนตามที่องค์กรกำหนด และต้องบันทึกการเข้าถึงเพื่อรองรับการตรวจสอบย้อนหลัง

๔.๔ กรณีเป็นข้อมูลอ่อนไหว ข้อมูลชั้นความลับ ข้อมูลคดี หรือข้อมูลด้านความมั่นคง ให้ใช้เฉพาะสภาพแวดล้อมที่องค์กรสามารถกำกับควบคุมได้อย่างเหมาะสมตามที่องค์กรกำหนด

ส่วนที่ ๓ การใช้ปัญญาประดิษฐ์เชิงสร้างสรรค์ที่ยอมรับได้

ข้อ ๕ หลักการทั่วไป

๕.๑ บุคลากรอาจใช้ปัญญาประดิษฐ์เชิงสร้างสรรค์เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานได้ เฉพาะกรณีที่ไม่ขัดต่อกฎหมาย ระเบียบ และนโยบายขององค์กร และต้องใช้เครื่องมือหรือบริการที่องค์กรรับรองหรืออนุมัติเท่านั้น

๕.๒ ผลลัพธ์จากปัญญาประดิษฐ์เชิงสร้างสรรค์ให้ถือเป็นร่างหรือข้อเสนอแนะ ผู้ใช้งานต้องตรวจสอบความถูกต้อง ความครบถ้วน และความเหมาะสมก่อนนำไปใช้ เผยแพร่ หรืออ้างอิงในนามองค์กร

ข้อ ๖ การใช้งานที่อนุญาต

๖.๑ อนุญาตให้ใช้เพื่อสนับสนุนงานภายใน โดยต้องไม่ป้อนข้อมูลลับหรือข้อมูลส่วนบุคคลขององค์กร เว้นแต่ได้รับอนุญาตและมีมาตรการคุ้มครองตามที่กำหนด

๖.๒ ตัวอย่างการใช้งานที่อนุญาต ได้แก่

๖.๒.๑ การร่างเอกสารหรือสรุปประเด็นจากข้อมูลสาธารณะ

๖.๒.๒ การจัดทำโครงร่างแนวปฏิบัติ รายการตรวจสอบ หรือแบบฟอร์มภายใน

๖.๒.๓ การอธิบาย...

๖.๒.๓ การอธิบายแนวคิดทางเทคนิคหรือรหัสโปรแกรม โดยไม่เปิดเผยข้อมูลลับ รหัสผ่าน กุญแจลับ หรือข้อมูลการเข้าถึงระบบ

๖.๒.๔ การแปลภาษาหรือปรับสำนวนเอกสารที่ไม่เป็นข้อมูลจำกัดการเข้าถึง

ข้อ ๗ การใช้งานที่ห้าม

ห้ามใช้ปัญญาประดิษฐ์เชิงสร้างสรรค์ในกรณีต่อไปนี้ เว้นแต่ได้รับอนุมัติเป็นกรณีพิเศษและใช้ระบบที่องค์กรควบคุมได้

๗.๑ การป้อนหรือนำเข้าข้อมูลลับ ข้อมูลจำกัดผู้รับรู้ ข้อมูลคดีหรือข่าวกรอง ข้อมูลแหล่งข่าว หรือข้อมูลที่อาจกระทบต่อความมั่นคงหรือภารกิจขององค์กร

๗.๒ การป้อนหรือนำเข้าข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวโดยไม่มีฐานกฎหมายและมาตรการคุ้มครองที่เหมาะสม รวมถึงการจัดทำ DPIA เมื่อเข้าเกณฑ์

๗.๓ การใช้เพื่อสร้างหรือเผยแพร่ข้อมูลอันเป็นเท็จ ปลอมแปลงเอกสาร ปลอมแปลงเสียงหรือภาพ หรือการกระทำที่อาจเข้าข่ายความผิดตามกฎหมาย

๗.๔ การใช้เพื่อหลีกเลี่ยงการตรวจสอบ หรือเพื่อสนับสนุนการกระทำที่เป็นการละเมิดความมั่นคงปลอดภัยไซเบอร์หรือฝ่าฝืนนโยบายขององค์กร

๗.๕ การส่งมอบผลลัพธ์ที่สร้างโดยปัญญาประดิษฐ์ให้หน่วยงานภายนอกในนามองค์กรโดยไม่มีการตรวจทานและอนุมัติตามกระบวนการขององค์กร

ข้อ ๘ ข้อกำหนดด้านการจัดการข้อมูลและความโปร่งใส

๘.๑ ให้ใช้หลักการใช้ข้อมูลเท่าที่จำเป็น โดยป้อนข้อมูลเฉพาะเท่าที่จำเป็นต่อวัตถุประสงค์ของงาน

๘.๒ หากจำเป็นต้องใช้ข้อมูลจริง ให้ดำเนินการตัดทอน ปกปิดข้อมูลระบุตัวบุคคล ทำข้อมูลให้ไม่สามารถระบุตัวบุคคลได้ หรือใช้ข้อมูลจำลองหรือข้อมูลสังเคราะห์แทนตามที่องค์กรกำหนด

๘.๓ ห้ามบันทึกหรือเปิดเผยรหัสผ่าน กุญแจลับ โทเคน หรือข้อมูลยืนยันตัวตนหรือข้อมูลเข้าถึงระบบในการใช้งานปัญญาประดิษฐ์ไม่ว่ากรณีใด

๘.๔ เอกสารที่มีสาระสำคัญซึ่งจัดทำโดยมีการใช้ปัญญาประดิษฐ์ช่วย ให้ระบุข้อความแสดงการใช้เครื่องมือดังกล่าวตามแบบที่องค์กรกำหนด

๘.๕ เมื่อใช้ข้อมูลจากแหล่งภายนอก ต้องตรวจสอบแหล่งที่มาและความถูกต้องก่อนนำไปใช้

ส่วนที่ ๔ การพัฒนา การทดสอบ การใช้งาน และการกำกับดูแลวงจรชีวิตระบบปัญญาประดิษฐ์

ข้อ ๙ การกำกับดูแลวงจรชีวิตระบบปัญญาประดิษฐ์ โดยองค์กรต้องกำกับดูแลการพัฒนา การทดสอบ การนำไปใช้งาน การติดตามผล การปรับปรุง และการยุติการใช้งานระบบปัญญาประดิษฐ์ตลอดวงจรชีวิต โดยครอบคลุมอย่างน้อย ดังนี้

๙.๑ การกำหนดวัตถุประสงค์และขอบเขตการใช้งาน

๙.๒ การพิจารณาความพร้อมของข้อมูลและการจัดชั้นข้อมูล

๙.๓ การออกแบบและพัฒนาระบบหรือแบบจำลอง

๙.๔ การทดสอบและประเมินผลก่อนใช้งาน

๙.๕ การพิจารณาความพร้อมและอนุมัติก่อนนำไปใช้งานจริง

๙.๖ การเฝ้าระวังหลังใช้งาน รวมถึงความคลาดเคลื่อนของแบบจำลองหรือข้อมูล

๙.๗ การทบทวน ปรับปรุง จำกัด ระงับ หรือยุติการใช้งานตามความเหมาะสม

ข้อ ๑๐ ข้อกำหนด...

ข้อ ๑๐ ข้อกำหนดก่อนฝึกและก่อนใช้งานแบบจำลองหรือระบบปัญญาประดิษฐ์ (AI)

๑๐.๑ ต้องจัดทำเอกสารขั้นต่ำ โดยครอบคลุมอย่างน้อยขอบเขตการใช้งาน แหล่งข้อมูล วิธีพัฒนา ตัวชี้วัดคุณภาพ ข้อจำกัด ความเสี่ยง และมาตรการลดความเสี่ยง

๑๐.๒ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และกรณีมีข้อมูลส่วนบุคคลให้คัดกรองหรือจัดทำ DPIA ตามเกณฑ์ที่องค์กรกำหนดก่อนใช้ข้อมูลจริง

๑๐.๓ ต้องกำหนดมาตรการกำกับดูแลข้อมูลอย่างชัดเจน ได้แก่ ความถูกต้องตามกฎหมายของแหล่งข้อมูล คุณภาพข้อมูล สิทธิการเข้าถึง ระยะเวลาการเก็บรักษา วิธีทำลายเมื่อหมดความจำเป็น และความสามารถในการตรวจสอบแหล่งที่มาและการเปลี่ยนแปลงของข้อมูลตามความเหมาะสม

ข้อ ๑๑ คุณภาพ ความเป็นธรรม การอธิบายผลลัพธ์ และการกำกับดูแลโดยมนุษย์

๑๑.๑ ต้องทดสอบความถูกต้อง ความเสถียร ความเหมาะสม และความน่าเชื่อถือของระบบหรือแบบจำลอง รวมทั้งประเมินอคติที่อาจส่งผลกระทบต่อบุคคลหรือกลุ่มบุคคล

๑๑.๒ สำหรับการใช้งานที่มีความเสี่ยงสูงหรือมีผลกระทบสูง ต้องจัดให้มีการอธิบายผลลัพธ์เท่าที่สามารถทำได้ และต้องมีการกำกับดูแลโดยมนุษย์ในระดับที่เหมาะสม

๑๑.๓ ระบบที่มีความเสี่ยงสูงต้องไม่ถูกใช้แทนดุลยพินิจของมนุษย์โดยสมบูรณ์ในเรื่องที่มีผลกระทบสำคัญต่อบุคคล องค์กร หรือสาธารณะ

๑๑.๔ ต้องมีกลไกให้เจ้าหน้าที่สามารถตรวจสอบ ควบคุม ระงับ หรือจำกัดการทำงานของระบบได้ในกรณีที่พบความผิดปกติ ความเสี่ยงที่เพิ่มขึ้น หรือผลกระทบที่ไม่เหมาะสม

๑๑.๕ ต้องมีการบันทึกหลักฐานการกำกับดูแลโดยมนุษย์ตามความเหมาะสม เพื่อรองรับการติดตามและตรวจสอบย้อนหลัง

ข้อ ๑๒ ความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง

๑๒.๑ ต้องป้องกันการเข้าถึงชุดข้อมูลฝึก แบบจำลอง พารามิเตอร์ และสภาพแวดล้อมการพัฒนาหรือใช้งานโดยมิชอบ และกำหนดสิทธิการเข้าถึงตามบทบาทหน้าที่

๑๒.๒ ต้องเฝ้าระวังความเสี่ยงด้านเทคนิคที่เกี่ยวข้อง เช่น การสอดแทรกข้อมูลฝึกการโจมตีด้วยข้อมูลป้อนเข้า การรั่วไหลจากการอนุมานของแบบจำลอง หรือความเสี่ยงทางไซเบอร์อื่นที่เกี่ยวข้อง เป็นต้น

๑๒.๓ ต้องมีการบันทึกเหตุการณ์และการเปลี่ยนแปลงสำคัญของระบบหรือแบบจำลอง เพื่อรองรับการตรวจสอบย้อนหลังตามระบบการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

ส่วนที่ ๕ การกำกับดูแล การตรวจประเมิน และการบังคับใช้

ข้อ ๑๓ การจัดทำทะเบียนและเอกสารกำกับดูแล

๑๓.๑ ให้จัดทำทะเบียนการใช้ปัญญาประดิษฐ์ โดยอย่างน้อยระบุเจ้าของระบบ เจ้าของข้อมูล ระดับความเสี่ยง เครื่องมือที่ได้รับอนุมัติ สถานะการอนุมัติ และข้อมูลอื่นที่จำเป็นต่อการกำกับดูแล

๑๓.๒ ระบบหรือโครงการปัญญาประดิษฐ์ (AI) ต้องมีเอกสาร หลักฐาน หรือแบบฟอร์มตามที่องค์กรกำหนด เพื่อรองรับการตรวจสอบย้อนหลัง การประเมินความเสี่ยง และการทบทวนการใช้งาน

ข้อ ๑๔ การตรวจประเมินและการทบทวน

๑๔.๑ ให้มีการตรวจประเมินการใช้ปัญญาประดิษฐ์อย่างน้อยปีละ ๑ ครั้ง

๑๔.๒ ต้องทบทวนเพิ่มเติมเมื่อเกิดเหตุละเมิด เหตุด้านความมั่นคงปลอดภัย การเปลี่ยนแปลงข้อมูลหรือวัตถุประสงค์การใช้งานที่มีนัยสำคัญ หรือเมื่อพบว่าระบบมีความเสี่ยงเพิ่มขึ้นหรือผลลัพธ์ไม่เหมาะสม

๑๔.๓ ผลการตรวจ...

๑๔.๓ ผลการตรวจประเมินและการทบทวนต้องนำไปใช้ในการปรับปรุงมาตรการควบคุม กระบวนการทำงาน หรือการจำกัด ระงับ หรือยุติการใช้งานระบบตามความเหมาะสม

ข้อ ๑๕ การบังคับใช้

๑๕.๑ ผู้ฝ่าฝืนหรือไม่ปฏิบัติตามหมวดนี้ ให้ดำเนินการตามระเบียบวินัย มาตรการขององค์กร และกฎหมายที่เกี่ยวข้อง

๑๕.๒ กรณีพบการใช้งานที่อาจก่อให้เกิดความเสี่ยงสูงเกินยอมรับได้ องค์กรอาจสั่งระงับ จำกัด หรือยุติการใช้งานระบบหรือบริการปัญญาประดิษฐ์ (AI) นั้นได้ทันทีตามความเหมาะสม

หมวดที่ ๑๑ การเชื่อมโยงและแลกเปลี่ยนข้อมูล

ข้อ ๑ หลักการทั่วไป

๑.๑ สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.) ต้องดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลอย่างเป็นระบบ มีมาตรฐาน ปลอดภัย โปร่งใส ตรวจสอบย้อนหลังได้ และสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

๑.๒ การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องสนับสนุนภารกิจของสำนักงาน ป.ป.ส. ในการป้องกัน ปราบปราม สืบสวน วิเคราะห์ และบูรณาการข้อมูลด้านยาเสพติด รวมทั้ง สนับสนุนบทบาทของสำนักงาน ป.ป.ส. ในการเป็นศูนย์กลางการเชื่อมโยงข้อมูลด้านยาเสพติดของประเทศ

๑.๓ การดำเนินการตามหมวดนี้ต้องคำนึงถึงอย่างน้อย ดังต่อไปนี้

๑.๓.๑ ความจำเป็นและความเหมาะสมตามภารกิจและอำนาจหน้าที่

๑.๓.๒ ความถูกต้อง ครบถ้วน ทันสมัย และคุณภาพของข้อมูล

๑.๓.๓ ความสามารถในการทำงานร่วมกันได้ของระบบและข้อมูล

๑.๓.๔ ความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

๑.๓.๕ การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่มีความอ่อนไหว

๑.๓.๖ ความสามารถในการตรวจสอบย้อนหลังและความรับผิดชอบต่อข้อมูล

๑.๔ การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องเป็นไปตามหลักการใช้ข้อมูลเท่าที่จำเป็น จำกัดตามวัตถุประสงค์ และกำหนดสิทธิการเข้าถึงตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน

ข้อ ๒ ขอบเขตการบังคับใช้

๒.๑ หมวดนี้ใช้บังคับกับการเชื่อมโยง การรับส่ง การแลกเปลี่ยน การเปิดเผย การใช้ร่วม การเข้าถึง หรือการประมวลผลข้อมูลของสำนักงาน ป.ป.ส. ไม่ว่าดำเนินการระหว่างหน่วยงานภายในหน่วยงาน ระหว่างสำนักงาน ป.ป.ส. กับหน่วยงานภายนอก หรือผ่านระบบหรือแพลตฟอร์มดิจิทัลใด

๒.๒ หมวดนี้ให้ใช้บังคับกับข้อมูลทุกรูปแบบที่เกี่ยวข้องกับภารกิจของสำนักงาน ป.ป.ส. รวมถึงข้อมูลสถิติ ข้อมูลเชิงปฏิบัติการ ข้อมูลข่าวกรอง ข้อมูลคดี ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว ข้อมูลที่มีชั้นความลับ และข้อมูลอื่นใดที่อยู่ในความครอบครองหรือความรับผิดชอบของสำนักงาน ป.ป.ส.

๒.๓ หมวดนี้ให้ใช้บังคับกับระบบสารสนเทศ ฐานข้อมูล บริการเชื่อมต่อระบบส่วนเชื่อมต่อโปรแกรมประยุกต์ (Application Programming Interface: API) บริการประมวลผลแบบคลาวด์ สื่อบันทึกข้อมูล และช่องทางดิจิทัลอื่นที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

ข้อ ๓ การกำกับดูแลและความรับผิดชอบ

๓.๑ ให้มีหน่วยงานหรือกลไกกำกับดูแลการเชื่อมโยงและแลกเปลี่ยนข้อมูลของสำนักงาน ป.ป.ส. ตามที่องค์กรกำหนด เพื่อทำหน้าที่กำหนดมาตรฐาน หลักเกณฑ์ กระบวนการอนุมัติ และติดตามประเมินผลการดำเนินงาน

๓.๒ ศูนย์เทคโน...

๓.๒ ศูนย์เทคโนโลยีสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมาย ต้องรับผิดชอบในการกำหนดมาตรฐานทางเทคนิค มาตรการรักษาความมั่นคงปลอดภัย การควบคุมการเข้าถึง การพิสูจน์ตัวตน การเข้ารหัส การบันทึกเหตุการณ์ การทดสอบ และการติดตามการใช้งานระบบเชื่อมโยงข้อมูล

๓.๓ หน่วยงานเจ้าของข้อมูล หรือเจ้าของภารกิจ ต้องรับผิดชอบในการกำหนดวัตถุประสงค์การใช้ข้อมูล ระดับชั้นข้อมูล เงื่อนไขการเปิดเผย ขอบเขตการใช้งาน ระยะเวลาการเก็บรักษา และข้อจำกัดในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๓.๔ หน่วยงานผู้ขอใช้หรือขอเชื่อมโยงข้อมูล ต้องรับผิดชอบในการใช้ข้อมูลตามขอบเขตที่ได้รับอนุญาต และต้องไม่ใช้ข้อมูลเกินกว่าวัตถุประสงค์ที่กำหนด หรือส่งต่อให้แก่บุคคลหรือหน่วยงานอื่นโดยไม่ได้รับอนุญาต

๓.๕ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กร ต้องให้คำปรึกษาและพิจารณาความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งความจำเป็นในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ก่อนดำเนินการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลที่มีความเสี่ยงสูง

ข้อ ๔ การจำแนกข้อมูลและระดับการควบคุม

๔.๑ สำนักงาน ป.ป.ส. ต้องจำแนกประเภทข้อมูลอย่างน้อย ดังนี้

๔.๑.๑ ข้อมูลสาธารณะ

๔.๑.๒ ข้อมูลใช้ภายใน

๔.๑.๓ ข้อมูลจำกัดการเข้าถึง

๔.๑.๔ ข้อมูลลับหรือข้อมูลที่มีชั้นความลับ

๔.๑.๕ ข้อมูลส่วนบุคคล

๔.๑.๖ ข้อมูลอ่อนไหว หรือข้อมูลที่หากเปิดเผยแล้วอาจกระทบต่อสิทธิของบุคคล ความมั่นคงของรัฐ ภารกิจด้านข่าวกรอง การสืบสวนสอบสวน หรือการบังคับใช้กฎหมาย

๔.๒ การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องกำหนดมาตรการควบคุมให้เหมาะสมกับประเภทข้อมูล ระดับความเสี่ยง และผลกระทบที่อาจเกิดขึ้น

๔.๓ กรณีข้อมูลชุดเดียวกันมีหลายสถานะหรือมีหลายระดับความอ่อนไหว ให้ใช้ระดับการคุ้มครองที่สูงกว่าเป็นเกณฑ์ในการกำหนดมาตรการควบคุม

๔.๔ การเชื่อมโยงข้อมูลข่าวกรอง ข้อมูลคดี ข้อมูลแหล่งข่าว ข้อมูลส่วนบุคคลอ่อนไหว หรือข้อมูลที่เกี่ยวข้องกับความมั่นคง ต้องอยู่ภายใต้การควบคุมเป็นกรณีพิเศษ และได้รับอนุมัติตามลำดับอำนาจที่องค์กรกำหนด

ข้อ ๕ หลักเกณฑ์การขอเชื่อมโยงและแลกเปลี่ยนข้อมูล

๕.๑ หน่วยงานที่ประสงค์จะเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับสำนักงาน ป.ป.ส. ต้องเสนอคำขออย่างเป็นทางการ โดยอย่างน้อยต้องระบุ ดังต่อไปนี้

๕.๑.๑ วัตถุประสงค์และความจำเป็น

๕.๑.๒ ฐานกฎหมายหรืออำนาจหน้าที่ที่เกี่ยวข้อง

๕.๑.๓ ประเภทและขอบเขตของข้อมูล

๕.๑.๔ หน่วยงานเจ้าของข้อมูลและหน่วยงานผู้รับข้อมูล

๕.๑.๕ วิธีการเชื่อมโยงและมาตรการรักษาความมั่นคงปลอดภัย

๕.๑.๖ ระยะเวลาการใช้และการเก็บรักษาข้อมูล

๕.๑.๗ ผู้รับผิดชอบและช่องทางการประสานงาน

๕.๒ ก่อนอนุมัติ...

๕.๒ ก่อนอนุมัติการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล ต้องมีการพิจารณาความเหมาะสมอย่างน้อย ดังต่อไปนี้

๕.๒.๑ ความจำเป็นตามภารกิจ

๕.๒.๒ ความพร้อมของระบบและข้อมูล

๕.๒.๓ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๕.๒.๔ ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

๕.๒.๕ ความสอดคล้องกับกฎหมาย ระเบียบ และนโยบายขององค์กร

๕.๒.๖ ความสามารถในการควบคุม ตรวจสอบ และยุติการเข้าถึง หรือเมื่อหมดความจำเป็น

๕.๓ การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก ต้องได้รับอนุมัติตามลำดับอำนาจขององค์กร และต้องมีเอกสารข้อตกลงหรือบันทึกความเข้าใจ หรือเอกสารอื่นที่มีผลผูกพันตามที่องค์กรกำหนด เป็นต้น

๕.๔ เอกสารข้อตกลงตามข้อ ๕.๓ ต้องกำหนดเรื่องสำคัญอย่างน้อย ได้แก่ วัตถุประสงค์ ชุดข้อมูล ขอบเขตการใช้งาน ระดับชั้นข้อมูล สิทธิและหน้าที่ของแต่ละฝ่าย มาตรการรักษาความมั่นคงปลอดภัย การแจ้งเหตุผิดปกติหรือเหตุละเมิดข้อมูล การตรวจสอบ การระงับการเชื่อมโยง และการคืน ลบ หรือทำลายข้อมูลเมื่อสิ้นสุดการใช้งาน เป็นต้น

ข้อ ๖ มาตรฐานข้อมูลและมาตรฐานทางเทคนิค

๖.๑ การออกแบบและพัฒนาการเชื่อมโยงและแลกเปลี่ยนข้อมูล ต้องยึดหลักการทำงานร่วมกันได้ของระบบสารสนเทศ และให้ใช้มาตรฐานข้อมูล มาตรฐานโครงสร้างข้อมูล มาตรฐานรหัสอ้างอิง และมาตรฐานทางเทคนิคที่ภาครัฐกำหนดหรือยอมรับ

๖.๒ การกำหนดโครงสร้างข้อมูล นิยามข้อมูล พจนานุกรมข้อมูล และรูปแบบข้อมูล ต้องทำให้เกิดความเข้าใจตรงกันระหว่างหน่วยงาน เพื่อให้ข้อมูลสามารถนำไปใช้ วิเคราะห์ และตรวจสอบร่วมกันได้อย่างถูกต้อง

๖.๓ การเชื่อมโยงข้อมูลใหม่ควรใช้ช่องทางหรือรูปแบบที่เป็นมาตรฐาน เปิดเผยได้ และสามารถทำงานร่วมกันได้ เช่น บริการเชื่อมต่อผ่านส่วนเชื่อมต่อโปรแกรมประยุกต์ (API) หรือรูปแบบข้อมูลมาตรฐานอื่นตามที่องค์กรกำหนด

๖.๔ ระบบเชื่อมโยงข้อมูลต้องกำหนดรายละเอียดทางเทคนิคอย่างเพียงพอ เช่น รูปแบบข้อมูล วิธีพิสูจน์ตัวตน วิธีอนุญาตให้เข้าถึง เวอร์ชันของบริการ ข้อจำกัดการเรียกใช้ และวิธีการติดตามตรวจสอบการใช้งาน

๖.๕ กรณีสำนักงาน ป.ป.ส. ทำหน้าที่เป็นศูนย์กลางการเชื่อมโยงข้อมูลด้านยาเสพติด ต้องกำหนดมาตรฐานข้อมูลกลาง รหัสอ้างอิงกลาง และหลักเกณฑ์การเชื่อมโยงข้อมูลร่วมกันระหว่างหน่วยงาน เพื่อให้ข้อมูลมีความสอดคล้องและใช้งานร่วมกันได้อย่างมีประสิทธิภาพ

ข้อ ๗ มาตรการรักษาความมั่นคงปลอดภัย

๗.๑ การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับระดับความเสี่ยงและความอ่อนไหวของข้อมูล อย่างน้อยดังต่อไปนี้

๗.๑.๑ การพิสูจน์ตัวตนและการกำหนดสิทธิการเข้าถึงตามบทบาทหน้าที่

๗.๑.๒ การใช้หลักการกำหนดสิทธิเท่าที่จำเป็น

๗.๑.๓ การบันทึก...

๗.๑.๓ การเข้ารหัสข้อมูลระหว่างส่งผ่านและตามความเหมาะสมขณะจัดเก็บ

๗.๑.๔ การบันทึกเหตุการณ์และการตรวจสอบย้อนหลัง

๗.๑.๕ การป้องกันการเข้าถึงโดยมิชอบ การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูล

๗.๑.๖ การเฝ้าระวังและตรวจจับเหตุผิดปกติด้านความมั่นคงปลอดภัย

๗.๒ การเข้าถึงข้อมูลสำคัญหรือข้อมูลที่เชื่อมโยงจากภายนอกเครือข่ายขององค์กร ต้องมีมาตรการควบคุมเพิ่มเติม เช่น การยืนยันตัวตนหลายปัจจัย การจำกัดเครือข่ายหรืออุปกรณ์ การอนุมัติเป็นรายกรณี หรือการใช้งานผ่านจุดเชื่อมต่อที่องค์กรควบคุมได้ เป็นต้น

๗.๓ ระบบต้นทางและระบบปลายทางต้องมีการทดสอบและรับรองความพร้อมด้านความมั่นคงปลอดภัยก่อนเปิดใช้งานจริง

๗.๔ กรณีใช้ผู้ให้บริการภายนอกหรือแพลตฟอร์มของบุคคลภายนอก ต้องประเมินความเสี่ยงของผู้ให้บริการ และกำหนดเงื่อนไขด้านความมั่นคงปลอดภัย การรักษาความลับ การแจ้งเหตุ และการควบคุมการเข้าถึงไว้ในสัญญาหรือข้อตกลงอย่างชัดเจน

ข้อ ๘ การคุ้มครองข้อมูลส่วนบุคคล

๘.๑ การเชื่อมโยงและแลกเปลี่ยนข้อมูลส่วนบุคคลต้องมีฐานกฎหมายรองรับอย่างชัดเจน และจำกัดการใช้ข้อมูลตามวัตถุประสงค์ที่กำหนด

๘.๒ ให้ใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อภารกิจ และต้องกำหนดมาตรการลดความเสี่ยงที่เหมาะสม เช่น การปกปิดข้อมูล การแทนค่าข้อมูล การทำข้อมูลให้ไม่สามารถระบุตัวบุคคลได้ หรือมาตรการอื่นตามความเหมาะสม เป็นต้น

๘.๓ กรณีการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลมีลักษณะที่อาจก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ต้องพิจารณาความจำเป็นในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลก่อนดำเนินการ

๘.๔ ห้ามใช้ข้อมูลส่วนบุคคลเกินขอบเขตที่ได้รับอนุญาต หรือใช้เพื่อวัตถุประสงค์อื่นที่ไม่สอดคล้องกับวัตถุประสงค์เดิม เว้นแต่มีฐานกฎหมายรองรับ

๘.๕ เมื่อสิ้นสุดความจำเป็นในการใช้ข้อมูล หรือสิ้นสุดสิทธิการเข้าถึงข้อมูลส่วนบุคคล ต้องดำเนินการคืน ลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลได้ตามหลักเกณฑ์ที่องค์กรกำหนด

ข้อ ๙ การเชื่อมโยงข้อมูลเพื่อสนับสนุนบทบาทศูนย์กลางข้อมูลด้านยาเสพติด

๙.๑ สำนักงาน ป.ป.ส. อาจจัดให้มีแพลตฟอร์มหรือศูนย์กลางสำหรับเชื่อมโยง บูรณาการและแลกเปลี่ยนข้อมูลด้านยาเสพติด เพื่อสนับสนุนการวิเคราะห์สถานการณ์ การบังคับใช้กฎหมาย การอำนวยการเชิงนโยบาย และการประสานความร่วมมือระหว่างหน่วยงาน

๙.๒ การดำเนินการตามข้อ ๙.๑ ต้องอยู่ภายใต้หลักธรรมาภิบาลข้อมูล การกำหนดเจ้าของข้อมูล ผู้ดูแลข้อมูล หลักเกณฑ์การเข้าถึง คุณภาพข้อมูล และการตรวจสอบแหล่งที่มาของข้อมูลอย่างชัดเจน

๙.๓ การนำข้อมูลจากหลายแหล่งมาเชื่อมโยงหรือประมวลผลร่วมกัน ต้องมีมาตรการควบคุมความถูกต้อง ความสอดคล้อง และความสามารถในการตรวจสอบแหล่งที่มาและการเปลี่ยนแปลงของข้อมูล

๙.๔ การใช้ข้อมูลที่ผ่านการเชื่อมโยงแล้วเพื่อการวิเคราะห์เชิงนโยบาย เชิงพื้นที่ เชิงเครือข่าย หรือเชิงปฏิบัติการ ต้องอยู่ภายใต้ขอบเขตวัตถุประสงค์ที่ชัดเจน และไม่กระทบต่อสิทธิของบุคคลหรือภารกิจของรัฐเกินความจำเป็น

๙.๕ การเปิดเผยข้อมูลเชิงสถิติหรือข้อมูลเพื่อประโยชน์สาธารณะ ต้องดำเนินการในลักษณะที่ไม่ก่อให้เกิดการระบุตัวบุคคล และต้องผ่านการพิจารณาตามหลักเกณฑ์ที่สำนักงานกำหนด

ข้อ ๑๐ การควบคุม

ข้อ ๑๐ การควบคุมคุณภาพข้อมูล

๑๐.๑ ข้อมูลที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนต้องผ่านการตรวจสอบความถูกต้อง ความครบถ้วน ความสอดคล้อง ความทันสมัย และความพร้อมใช้งานตามเกณฑ์ที่องค์กรกำหนด

๑๐.๒ ต้องมีการระบุแหล่งที่มา วันที่ปรับปรุงล่าสุด เจ้าของข้อมูล นิยามข้อมูล และข้อจำกัดในการใช้ข้อมูลอย่างเหมาะสม

๑๐.๓ หากตรวจพบว่าข้อมูลมีความผิดพลาด ไม่ครบถ้วน ไม่ทันสมัย หรือมีความเสี่ยงสูงต่อการนำไปใช้ผิดวัตถุประสงค์ ให้หน่วยงานเจ้าของข้อมูลหรือหน่วยงานที่เกี่ยวข้องดำเนินการแก้ไข ระงับ หรือจำกัดการเชื่อมโยงและแลกเปลี่ยนข้อมูลนั้นตามความเหมาะสม

ข้อ ๑๑ การทดสอบ การขึ้นใช้งาน และการควบคุมการเปลี่ยนแปลง

๑๑.๑ ก่อนเปิดใช้งานการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล ต้องมีการทดสอบอย่างน้อยในด้านความถูกต้องของข้อมูล ความเข้ากันได้ของระบบ ความมั่นคงปลอดภัย และความพร้อมใช้งาน

๑๑.๒ การเปลี่ยนแปลงโครงสร้างข้อมูล วิธีการเชื่อมต่อ สิทธิการเข้าถึง หรือองค์ประกอบสำคัญของระบบที่อาจกระทบต่อการเชื่อมโยงและแลกเปลี่ยนข้อมูล ต้องผ่านกระบวนการควบคุมการเปลี่ยนแปลง การทดสอบ และการอนุมัติตามที่องค์กรกำหนด

๑๑.๓ ต้องมีการรับรองความพร้อมก่อนขึ้นใช้งานจริง โดยหน่วยงานเจ้าของระบบ หน่วยงานเจ้าของข้อมูล และหน่วยงานด้านเทคโนโลยีสารสนเทศ หรือผู้มีอำนาจตามที่องค์กรกำหนด

ข้อ ๑๒ การติดตาม ตรวจสอบ และการทบทวน

๑๒.๑ ต้องมีการติดตามการใช้งาน การเรียกใช้ข้อมูล ปริมาณการแลกเปลี่ยนข้อมูล ความผิดปกติ และเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบเชื่อมโยงข้อมูลอย่างต่อเนื่อง

๑๒.๒ ต้องมีการตรวจสอบสิทธิการเข้าถึง การปฏิบัติตามเงื่อนไขการอนุมัติ และการใช้ข้อมูลให้สอดคล้องกับวัตถุประสงค์ที่กำหนดเป็นระยะ

๑๒.๓ ต้องสามารถตรวจสอบย้อนหลังได้ทุกขั้นตอน โดยมีเอกสาร หลักฐาน และบันทึกเหตุการณ์ที่เกี่ยวข้องอย่างเพียงพอ

๑๒.๔ ให้มีการทบทวนหมวดนี้และแนวปฏิบัติที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีกฎหมาย มาตรฐาน เทคโนโลยี หรือความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๑๓ การจัดการเหตุผิดปกติและเหตุละเมิดข้อมูล

๑๓.๑ เมื่อเกิดเหตุผิดปกติ เหตุรั่วไหล เหตุเข้าถึงโดยมิชอบ หรือเหตุที่อาจกระทบต่อความมั่นคงปลอดภัยของการเชื่อมโยงและแลกเปลี่ยนข้อมูล ต้องรายงานและตอบสนองเหตุการณ์ตามกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยขององค์กรโดยทันที

๑๓.๒ กรณีเป็นเหตุละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามกระบวนการที่องค์กรกำหนด และตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๑๓.๓ กรณีเหตุที่มีลักษณะเป็นภัยคุกคามทางไซเบอร์หรือกระทบต่อระบบสำคัญขององค์กร ต้องดำเนินการตามแผนรับมือภัยคุกคามทางไซเบอร์ และแนวทางการประสานงานที่เกี่ยวข้อง

๑๓.๔ ภายหลังเกิดเหตุ ต้องมีการวิเคราะห์สาเหตุ ทบทวนผลกระทบ และกำหนดมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ

ข้อ ๑๔ การบังคับใช้

๑๔.๑ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามหมวดนี้ ให้ดำเนินการตามระเบียบของทางราชการ ระเบียบวินัย มาตรการขององค์กร สัญญา หรือกฎหมายที่เกี่ยวข้อง แล้วแต่กรณี

ข้อ ๑๔.๒ องค์กร...

๑๔.๒ องค์กรอาจสั่งระงับ จำกัด หรือยุติการเชื่อมโยงและแลกเปลี่ยนข้อมูลใดได้ทันที หากพบว่ามีความเสี่ยงสูงเกินยอมรับได้ มีการใช้งานผิดวัตถุประสงค์ หรือมีเหตุอันควรเชื่อได้ว่าอาจก่อให้เกิดความเสียหายอย่างมีนัยสำคัญต่อบุคคล องค์กร หรือรัฐ

เอกสารอ้างอิง

๑. สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงาน ป.ป.ส.). (๒๕๖๓). นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๓ สำนักงาน ป.ป.ส.

๒. International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC). (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

๓. International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC). (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.

๔. International Organization for Standardization (ISO). (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.

๕. ราชกิจจานุเบกษา. (๒๕๖๐). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐.

๖. ราชกิจจานุเบกษา. (๒๕๖๒). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒.

๗. ราชกิจจานุเบกษา. (๒๕๖๒). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒.

๘. (หน่วยงานเผยแพร่: สำนักหอจดหมายเหตุแห่งชาติ). (๒๕๔๔). ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔.

๙. ราชกิจจานุเบกษา. (๒๕๖๔). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔.

๑๐. ราชกิจจานุเบกษา. (๒๕๖๐). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐.

๑๑. ราชกิจจานุเบกษา. (๒๕๖๒). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒.

๑๒. ราชกิจจานุเบกษา. (๒๕๖๒). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒.

๑๓. (หน่วยงานเผยแพร่: สำนักหอจดหมายเหตุแห่งชาติ). (๒๕๔๔). ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔.

๑๔. ราชกิจจานุเบกษา. (๒๕๖๔). ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔.

๑๕. National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.

๑๖. National...

๑๖. National Institute of Standards and Technology (NIST). (2025). NIST Special Publication 800-61 Revision 3: Computer Security Incident Handling Guide.

๑๗. Cloud Security Alliance (CSA). (2026). Cloud Controls Matrix (CCM) and CAIQ v4.1.

๑๘. Center for Internet Security (CIS). (2021). CIS Critical Security Controls v8 และ (2026). CIS Critical Security Controls v8.1.

๑๙. Open Web Application Security Project (OWASP). (ไม่ปรากฏปีในหน้าอ้างอิง). OWASP Application Security Verification Standard (ASVS).

๒๐. Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for media sanitization* (NIST Special Publication 800-88 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1

๒๑. สำนักงานคณะกรรมการอาหารและยา. (๒๕๖๘, ๒๙ กันยายน). นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ. (หมวด “นโยบายด้านเทคโนโลยีสารสนเทศ” บนเว็บไซต์สำนักงานคณะกรรมการอาหารและยา).