ประกาศสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน)
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๗

โดยที่เป็นการสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) เพื่อเป็นแนวทางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์และเพื่อให้การดำเนินงานตามวัตถุประสงค์ของสถาบันเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้องทางไซเบอร์ อีกทั้ง สร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสียทุกฝ่าย

อาศัยอำนาจตามความในมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) ผู้อำนวยการจึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๑ ตุลาคม พ.ศ. ๒๕๖๗

(นายจุลเทพ ขจรไชยกูล)
ผู้อำนวยการสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง

สถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน)
อาคารศูนย์บริหารทางพิเศษ กทพ. เลขที่ 111 ชั้น 10
ถนนริมคลองบางกะปิ แขวงบางกะปิ
เขตห้วยขวาง กรุงเทพมหานคร 10310

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ สถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) (สทร.)

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
สถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) (สทร.)

๑. บทนำ

๑.๑. วัตถุประสงค์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และไปในทิศทางเดียวกัน

สถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) (สทร.) จัดตั้งขึ้นเมื่อวันที่ ๑๔ กรกฎาคม ๒๕๖๔ โดยพระราชกฤษฎีกาจัดตั้งสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) พ.ศ. ๒๕๖๔ เพื่อทำหน้าที่ศึกษา วิจัย และพัฒนาเทคโนโลยีระบบราง รวมทั้งประเมินความต้องการด้านเทคโนโลยีระบบราง เพื่อใช้ในการวางยุทธศาสตร์ของประเทศ ตลอดจนบริหารจัดการงานวิจัย การพัฒนาเทคโนโลยีและบุคลากรที่เกี่ยวข้องกับระบบรางและระบบการขนส่งทางราง เพื่อนำไปสู่การใช้ประโยชน์และส่งเสริมอุตสาหกรรมในระบบการขนส่งทางราง

ในการดำเนินงานของ สทร. มีการใช้เทคโนโลยีสารสนเทศและการสื่อสารเป็นเครื่องมือสำคัญในการวิจัยและพัฒนา ตลอดจนการบริหารจัดการองค์กร ซึ่งรวมถึงโครงการสำคัญต่างๆ ด้วยความสำคัญของข้อมูลและระบบสารสนเทศที่ใช้ในการดำเนินงานวิจัยและพัฒนาเทคโนโลยีระบบราง การรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งจำเป็นอย่างยิ่งเพื่อปกป้องทรัพย์สินทางปัญญา ข้อมูลสำคัญ และความต่อเนื่องในการดำเนินงานของ สทร. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้จึงได้จัดทำขึ้นเพื่อเป็นแนวทางในการปฏิบัติสำหรับบุคลากร นักวิจัย และผู้เกี่ยวข้องทุกฝ่าย

๑.๒. การบังคับใช้

(๑) ผู้บริหาร บุคลากร นักวิจัย ผู้เกี่ยวข้องในการวิจัย และหน่วยงานทั้งหมดที่เกี่ยวข้องกับ สทร.

(๒) บุคคลภายนอกหน่วยงานที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของ สทร. รวมถึงผู้ร่วมวิจัย ที่ปรึกษา และผู้เชี่ยวชาญจากภายนอกที่เข้ามาร่วมงานวิจัยกับ สทร.

(๓) ระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหมดที่ใช้ในการดำเนินงานของ สทร. รวมถึงระบบที่ใช้ในโครงการวิจัยและพัฒนาเทคโนโลยีระบบรางต่างๆ

(๔) ข้อมูลและทรัพย์สินทางปัญญาทั้งหมดที่เกี่ยวข้องกับการวิจัยและพัฒนาเทคโนโลยีระบบราง

๒. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้:

(๑) ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคล ข้อมูลการวิจัย หรือข้อมูลที่เป็นกรรมสิทธิ์ของ สทร.

(๒) ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของ สทร. ต้องไม่มีการแก้ไข ดัดแปลง หรือถูกทำลายโดยผู้ที่ไม่ได้รับอนุญาต โดยเฉพาะอย่างยิ่งข้อมูลที่เกี่ยวข้องกับงานวิจัยและพัฒนาเทคโนโลยีระบบราง

(๓) ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้ เพื่อสนับสนุนการดำเนินงานวิจัยและพัฒนาอย่างต่อเนื่อง

(๔) ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ ทั้งในส่วนของบุคลากรประจำและผู้เกี่ยวข้องในการวิจัย

(๕) การพิสูจน์ตัวตน (Authentication)การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น รวมถึงการตรวจสอบตัวตนของนักวิจัยและผู้เกี่ยวข้องในการวิจัยที่เข้าถึงข้อมูลและระบบของ สทร.

(๖) การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต โดยคำนึงถึงระดับการเข้าถึงที่เหมาะสมสำหรับนักวิจัยและผู้เกี่ยวข้องในแต่ละโครงการ

(๗) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม ที่เกี่ยวข้องในการทำธุรกรรมหรือการดำเนินการใดๆ ในระบบไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการกระทำที่เกิดขึ้น การรักษาความมั่นคงปลอดภัยอย่างได้ผลจำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย:

(๗.๑) การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของผู้บริหาร บุคลากร ผู้เกี่ยวข้องกับโครงการของ สทร. และบุคคลภายนอกที่เกี่ยวข้องทุกคน

(๗.๒) การบริหารและการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

(๗.๓) การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้ผู้บริหาร บุคลากร นักวิจัย ผู้เกี่ยวข้องในโครงการและการวิจัย และบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่

และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

๓. หน้าที่และความรับผิดชอบ (Roles and Responsibilities)

๓.๑. หน้าที่ของผู้บังคับบัญชา

(๑) ชี้แจงให้ผู้บริหาร บุคลากร นักวิจัย และผู้เกี่ยวข้องในโครงการและการวิจัยทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของ สทร. ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม

(๓) พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาคและเป็นธรรม

(๔) สนับสนุนและส่งเสริมให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรและนักวิจัยอย่างสม่ำเสมอ

๓.๒. หน้าที่ของบุคลากร

(๑) ผู้บริหาร บุคลากร นักวิจัย ผู้เกี่ยวข้องในโครงการและการวิจัย และผู้ปฏิบัติงานทุกคนต้องปฏิบัติดังต่อไปนี้:

(๑.๑) ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของ สทร. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

(๑.๒) ให้ความร่วมมือกับ สทร. อย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของ สทร.

(๑.๓) แจ้งให้ สทร. ทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุก โจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อ สทร.

(๑.๔) ตระหนักถึงความสำคัญของการรักษาความลับของข้อมูลวิจัยและทรัพย์สินทางปัญญาของ สทร.

(๑.๕) เข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่ สทร. จัดขึ้นอย่าสม่ำเสมอ

(๒) ผู้บริหาร บุคลากร ผู้เกี่ยวข้องกับโครงกรของ สทร. และผู้ปฏิบัติงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้:

(๒.๑) ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

(๒.๒) ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน

(๒.๓) ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

(๒.๔) ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่ สทร. กำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของ สทร. เป็นความลับส่วนตัว ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น

(๒.๕) ต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนด หรือเมื่อเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่านและรหัสอื่นใดด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัสที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือห้ามตั้งรหัสซ้ำกันในทุกระบบที่มีสิทธิใช้งาน

(๒.๖) ต้องระมัดระวังในการใช้งานและเก็บรักษาอุปกรณ์พกพา เช่น โน้ตบุ๊ก แท็ปเล็ต หรือสมาร์ทโฟนที่ใช้ในการทำงานหรือเข้าถึงข้อมูลของ สทร

(๓) ผู้เกี่ยวข้องกับโครงการของ สทร. มีหน้าที่เพิ่มเติม ดังนี้:

(๓.๑) ต้องรักษาความลับของข้อมูลโครงการ งานวิจัย ผลการทดลอง และทรัพย์สินทางปัญญาที่เกิดจากการวิจัยและพัฒนาเทคโนโลยีระบบราง

(๓.๒) ต้องใช้ระบบคอมพิวเตอร์และซอฟต์แวร์ที่ สทร. จัดเตรียมไว้สำหรับงานวิจัยเท่านั้น ห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาตหรือไม่มีลิขสิทธิ์ถูกต้อง

(๓.๓) ต้องรายงานความก้าวหน้าของโครงการและการใช้ทรัพยากรด้านไอทีต่อผู้บังคับบัญชาตามระยะเวลาที่กำหนด

(๔) ต้องระมัดระวังในการแบ่งปันข้อมูลวิจัยกับบุคคลภายนอก โดยต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

(๕) ผู้บริหาร บุคลากร นักวิจัย ผู้ปฏิบัติงาน และผู้เกี่ยวข้องในการดำเนินโครงการที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สทร.

๔. การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

๔.๑. วัตถุประสงค์

เพื่อแสดงถึงการยอมรับความเสี่ยงและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดย สทร. ใช้วิธีการที่สอดคล้องกันในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management) รวมถึงมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลซึ่งสอดคล้องกับกระบวนการในการระบุและประเมินความเสี่ยง (Risk Identification and Assessment)

๔.๒. การระบุและประเมินความเสี่ยง (Risk Identification and Assessment)

(๑) สทร. ต้องดำเนินการระบุและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ โดยครอบคลุมทั้งระบบเทคโนโลยีสารสนเทศ ข้อมูลวิจัย และทรัพย์สินทางปัญญาที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีระบบราง

(๒) การประเมินความเสี่ยงต้องพิจารณาถึงผลกระทบที่อาจเกิดขึ้นต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบ

(๓) ต้องมีการจัดทำแผนบริหารจัดการความเสี่ยงที่ระบุมาตรการควบคุมที่เหมาะสมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๓. การลดความเสี่ยง (Risk Mitigation)

(๑) สทร. ต้องดำเนินมาตรการควบคุมที่เหมาะสมเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจรวมถึง:

(๑.๑) การติดตั้งและปรับปรุงระบบป้องกันการบุกรุก (Firewall) และระบบตรวจจับและป้องกันการบุกรุก (IPS/IDS) ให้ทันสมัยอยู่เสมอ

(๑.๒) การเข้ารหัสข้อมูลสำคัญและข้อมูลวิจัยที่มีความอ่อนไหว

(๑.๓) การจัดทำระบบสำรองข้อมูลและแผนกู้คืนระบบในกรณีเกิดเหตุฉุกเฉิน

(๑.๔) การควบคุมการเข้าถึงระบบและข้อมูลตามหลักการ "need-to-know" และ "least privilege"

(๑.๕) การฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรและนักวิจัยอย่างสม่ำเสมอ

(๑.๖) การตรวจสอบและประเมินความปลอดภัยของระบบและแอปพลิเคชันที่ใช้ในการวิจัยและพัฒนาเทคโนโลยีระบบรางอย่างสม่ำเสมอ

(๒) สทร. ต้องจัดทำแผนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Response Plan) และทำการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

(๓) ต้องมีการติดตามและประเมินประสิทธิภาพของมาตรการควบคุมที่นำมาใช้อย่างสม่ำเสมอ และปรับปรุงให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป

๔.๔. การยอมรับความเสี่ยง (Risk Acceptance)

(๑) ในกรณีที่มีความเสี่ยงที่ไม่สามารถลดหรือควบคุมได้อย่างเหมาะสม สทร. อาจพิจารณายอมรับความเสี่ยงนั้น โดยต้องมีกระบวนการพิจารณาและอนุมัติการยอมรับความเสี่ยงอย่างเป็นทางการ

(๒) การยอมรับความเสี่ยงต้องได้รับการอนุมัติจากผู้บริหารระดับสูงของ สทร. และต้องมีการบันทึกเหตุผลและมาตรการบรรเทาผลกระทบที่อาจเกิดขึ้น

(๓) ต้องมีการทบทวนการยอมรับความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมการทำงานหรือเทคโนโลยี

๕. การบริหารจัดการระบบ (System Management)

๕.๑. การจัดการสินทรัพย์ (Asset Management)

(๑) บัญชีทรัพย์สินและความเป็นเจ้าของ (Inventory and Ownership)

(๑.๑) สทร. ต้องจัดทำและรักษาบัญชีทรัพย์สินที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงอุปกรณ์ที่ใช้ในการวิจัยและพัฒนาเทคโนโลยีระบบราง

(๑.๒) ทรัพย์สินแต่ละรายการต้องมีการระบุเจ้าของหรือผู้รับผิดชอบอย่างชัดเจน

(๑.๓) ต้องมีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีการเปลี่ยนแปลง เพิ่มเติม หรือยกเลิกการใช้งานทรัพย์สิน

(๒) การจัดชั้นความลับและการควบคุม (Security Classification and Handling)

(๒.๑) ข้อมูลและทรัพย์สินสารสนเทศของ สทร. ต้องได้รับการจัดชั้นความลับตามระดับความสำคัญและความอ่อนไหว

(๒.๒) การจัดชั้นความลับอาจแบ่งเป็น: ลับที่สุด ลับมาก ลับ และทั่วไป

(๒.๓) ต้องมีการกำหนดแนวทางการจัดการและควบคุมข้อมูลตามระดับชั้นความลับ รวมถึงการเข้าถึง การจัดเก็บ การส่งต่อ และการทำลายข้อมูล

(๒.๔) ข้อมูลโครงการ งานวิจัยและทรัพย์สินทางปัญญาที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีระบบรางต้องได้รับการพิจารณาจัดชั้นความลับอย่างรอบคอบ

๕.๒. การบริหารจัดการซอฟต์แวร์ (Software Management)

(๑) การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์ (Software Licensing)

(๑.๑) สทร. ต้องใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

(๑.๒) ต้องมีการจัดทำทะเบียนซอฟต์แวร์ที่ใช้งานในองค์กร รวมถึงรายละเอียดลิขสิทธิ์และจำนวนสิทธิการใช้งาน

(๑.๓) ต้องมีการตรวจสอบการใช้งานซอฟต์แวร์อย่างสม่ำเสมอเพื่อให้มั่นใจว่าเป็นไปตามข้อกำหนดของลิขสิทธิ์

(๑.๔) การติดตั้งซอฟต์แวร์ใหม่หรือการปรับปรุงซอฟต์แวร์ต้องได้รับการอนุมัติและดำเนินการโดยเจ้าหน้าที่ไอทีที่ได้รับมอบหมายเท่านั้น

(๑.๕) ซอฟต์แวร์ที่ใช้ในการวิจัยและพัฒนาเทคโนโลยีระบบรางต้องได้รับการพิจารณาเป็นพิเศษ โดยคำนึงถึงความปลอดภัยและความเหมาะสมในการใช้งาน

๖. การบริหารจัดการหน่วยงานและบุคลากร (Human Resource Management)

๖.๑. ก่อนการจ้างงาน (Prior to Employment)

(๑) การคัดเลือกบุคลากร

(๑.๑) สทร. ต้องมีกระบวนการคัดเลือกบุคลากร นักวิจัย และผู้เกี่ยวข้องในการปฏิบัติงานโครงการต่างๆ ที่รัดกุม โดยคำนึงถึงความสำคัญของตำแหน่งงานและการเข้าถึงข้อมูลสำคัญ

(๑.๒) ต้องมีการตรวจสอบประวัติและคุณสมบัติของผู้สมัครอย่างละเอียด โดยเฉพาะสำหรับตำแหน่งที่เกี่ยวข้องกับการวิจัยและพัฒนาเทคโนโลยีระบบราง

(๑.๓) การตรวจสอบประวัติต้องเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

(๒) ข้อตกลงและเงื่อนไขการจ้างงาน

(๒.๑) สัญญาจ้างงานหรือข้อตกลงกับบุคลากร นักวิจัย และที่ปรึกษาต้องระบุหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน

(๒.๒) ต้องมีการลงนามในข้อตกลงการรักษาความลับ (Non-Disclosure Agreement) สำหรับผู้ที่จะเข้าถึงข้อมูลสำคัญหรือความลับทางการวิจัย

(๒.๓) ต้องแจ้งให้บุคลากรทราบถึงบทลงโทษหากมีการละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์

๖.๒. ระหว่างการจ้างงาน (During Employment)

(๑) ความรับผิดชอบของผู้บริหาร

(๑.๑) ผู้บริหารต้องกำกับดูแลให้บุคลากรของสถาบันฯ ปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

(๑.๒) ต้องสื่อสารและให้คำแนะนำเกี่ยวกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรอย่างสม่ำเสมอ

(๒) การสร้างความตระหนักและการฝึกอบรม

(๒.๑) สทร. ต้องจัดให้มีโปรแกรมการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรและนักวิจัยทุกระดับ

(๒.๒) ต้องจัดการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับบทบาทและความรับผิดชอบของแต่ละตำแหน่งงาน

(๒.๓) ต้องมีการอัปเดตเนื้อหาการฝึกอบรมให้ทันสมัยและสอดคล้องกับภัยคุกคามใหม่ๆ ที่อาจส่งผลกระทบต่อการวิจัยและพัฒนาเทคโนโลยีระบบราง

(๒.๔) ต้องมีการประเมินผลการฝึกอบรมและความเข้าใจของบุคลากรอย่างสม่ำเสมอ

(๓) กระบวนการทางวินัย

(๓.๑) ต้องมีกระบวนการทางวินัยที่ชัดเจนสำหรับการละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์

(๓.๒) การดำเนินการทางวินัยต้องเป็นไปอย่างเป็นธรรมและสอดคล้องกับระดับความรุนแรงของการละเมิด

(๓.๓) ต้องมีการบันทึกและรายงานเหตุการณ์ละเมิดนโยบายเพื่อใช้ในการปรับปรุงมาตรการรักษาความปลอดภัยในอนาคต

๖.๓. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment)

(๑) ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

(๑.๑) ต้องมีกระบวนการที่ชัดเจนในการจัดการกับการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานของบุคลากร และผู้เกี่ยวข้อง

(๑.๒) ต้องมีการเพิกถอนสิทธิการเข้าถึงระบบและข้อมูลทันทีเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนตำแหน่งงาน

(๑.๓) ต้องมีการส่งคืนทรัพย์สินของ สทร. ทั้งหมด รวมถึงอุปกรณ์ เอกสาร และข้อมูลที่เกี่ยวข้องกับการวิจัยและพัฒนา

(๒) การรักษาความลับหลังสิ้นสุดการจ้างงาน

(๒.๑) ต้องมีการแจ้งเตือนบุคลากรที่ลาออกหรือสิ้นสุดสัญญาเกี่ยวกับหน้าที่ในการรักษาความลับของข้อมูล สทร. แม้หลังจากสิ้นสุดการจ้างงาน

(๒.๒) ต้องมีการทบทวนและปรับปรุงข้อตกลงการรักษาความลับให้ครอบคลุมระยะเวลาหลังสิ้นสุดการจ้างงาน โดยเฉพาะสำหรับผู้ที่เข้าถึงข้อมูลสำคัญหรืองานวิจัยที่มีความอ่อนไหว

(๓) การจัดการความรู้และการถ่ายทอดงาน

(๓.๑) ต้องมีกระบวนการในการจัดการความรู้และการถ่ายทอดงานก่อนที่บุคลากรหรือนักวิจัยจะออกจากองค์กร เพื่อให้มั่นใจว่าความรู้และข้อมูลสำคัญจะยังคงอยู่กับ สทร.

(๓.๒) ต้องมีการบันทึกและจัดเก็บข้อมูลโครงการอย่างเป็นระบบ เพื่อให้สามารถสืบค้นและใช้งานได้แม้เมื่อผู้รับผิดชอบหลักไม่อยู่แล้ว

๗. การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

๗.๑. การรักษาความมั่นคงปลอดภัยสถานที่ (Physical Security)

(๑) การป้องกันการเข้าถึงสถานที่โดยไม่ได้รับอนุญาต

(๑.๑) สทร. ต้องกำหนดพื้นที่ควบคุม (Secure Areas) สำหรับการดำเนินโครงการพัฒนาเทคโนโลยีระบบราง และจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๑.๒) ต้องมีระบบควบคุมการเข้าออกที่มีประสิทธิภาพ เช่น บัตรผ่าน ระบบสแกนลายนิ้วมือ หรือการตรวจสอบทางชีวมิติอื่นๆ

(๑.๓) ต้องมีการบันทึกและตรวจสอบการเข้าออกพื้นที่ควบคุมอย่างสม่ำเสมอ

(๑.๔) ต้องมีมาตรการรักษาความปลอดภัยเป็นพิเศษสำหรับห้องปฏิบัติการวิจัยและพื้นที่ที่มีอุปกรณ์หรือข้อมูลสำคัญ

(๒) การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม

(๒.๑) ต้องมีมาตรการป้องกันภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ และแผ่นดินไหว

(๒.๒) ต้องติดตั้งระบบดับเพลิงที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์และห้องปฏิบัติการวิจัย

(๒.๓) ต้องมีระบบสำรองไฟฟ้าสำหรับอุปกรณ์และระบบสำคัญ

(๒.๔) ต้องมีการตรวจสอบและบำรุงรักษาระบบรักษาความปลอดภัยทางกายภาพอย่างสม่ำเสมอ

๗.๒. การรักษาความมั่นคงปลอดภัยอุปกรณ์ (Equipment Security)

(๑) การป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต

(๑.๑) อุปกรณ์คอมพิวเตอร์และอุปกรณ์วิจัยที่สำคัญต้องติดตั้งในพื้นที่ที่มีการควบคุมการเข้าถึง

(๑.๒) ต้องมีการล็อคอุปกรณ์พกพา เช่น โน้ตบุ๊ก แท็บเล็ต เมื่อไม่ได้ใช้งาน

(๑.๓) ต้องมีนโยบายโต๊ะทำงานและหน้าจอสะอาด (Clean Desk and Clear Screen Policy) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) การป้องกันการสูญหายหรือเสียหายของอุปกรณ์

(๒.๑) ต้องมีการทำทะเบียนและติดป้ายระบุอุปกรณ์ทั้งหมดของ สทร

(๒.๒) ต้องมีการตรวจสอบและบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอตามคำแนะนำของผู้ผลิต

(๒.๓) ต้องมีมาตรการป้องกันการโจรกรรมอุปกรณ์ โดยเฉพาะอุปกรณ์ที่ใช้ในการดำเนินงานของสถาบันฯ

๘. การบริหารจัดการการสื่อสารและการดำเนินงาน (Communications and Operation Management)

๘.๑. การบริหารจัดการการสื่อสาร (Communications Management)

(๑) การปกป้องข้อมูลในระหว่างการส่งข้อมูล

(๑.๑) ต้องมีการเข้ารหัสข้อมูลสำคัญและข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของสถาบันฯ ในระหว่างการส่งผ่านเครือข่าย

(๑.๒) ต้องใช้ช่องทางการสื่อสารที่ปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลสำคัญหรือข้อมูลความลับของสถาบันฯ

(๑.๓) ต้องมีการตรวจสอบและยืนยันตัวตนของผู้รับปลายทางก่อนการส่งข้อมูลสำคัญหรือข้อมูลความลับของสถาบันฯ

(๒) การจัดการการสื่อสารกับบุคคลภายนอก

(๒.๑) ต้องมีข้อตกลงการรักษาความลับ (Non-Disclosure Agreement) กับบุคคลภายนอกที่เข้าถึงข้อมูลของ สทร.

(๒.๒) ต้องมีการควบคุมและตรวจสอบการเข้าถึงระบบเครือข่ายของ สทร. โดยบุคคลภายนอก และถูกจำกัดให้ดำเนินการได้เฉพาะเท่าที่จำเป็นเท่านั้นและต้องได้รับอนุญาตจาก สทร. ก่อน

(๒.๓) ต้องมีการกำหนดนโยบายและแนวปฏิบัติสำหรับการใช้สื่อสังคมออนไลน์ที่เกี่ยวข้องกับงานของ สทร.

๘.๒. การบริหารจัดการการดำเนินงาน (Operation Management)

(๑) การดำเนินงานบนระบบคอมพิวเตอร์อย่างปลอดภัย

(๑.๑) ต้องมีขั้นตอนการปฏิบัติงานมาตรฐาน (Standard Operating Procedures) สำหรับการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย อีกทั้ง ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสมเพื่อรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศ

(๑.๒) ต้องมีการแบ่งแยกหน้าที่และความรับผิดชอบในการดูแลระบบเพื่อป้องกันการใช้งานในทางที่ผิด

(๑.๓) ต้องมีการบันทึกและตรวจสอบกิจกรรมการใช้งานระบบที่สำคัญอย่างสม่ำเสมอ

(๒) การป้องกันมัลแวร์และซอฟต์แวร์ไม่พึงประสงค์

(๒.๑) ต้องติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัสและมัลแวร์บนทุกเครื่องคอมพิวเตอร์และเซิร์ฟเวอร์

(๒.๒) ต้องมีการตรวจสอบและสแกนไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตหรือได้รับจากแหล่งภายนอก

(๒.๓) ต้องมีการให้ความรู้แก่บุคลากรและนักวิจัยเกี่ยวกับภัยคุกคามจากมัลแวร์และวิธีการป้องกัน

(๓) การสำรองและกู้คืนข้อมูล

(๓.๑) ต้องมีนโยบายและขั้นตอนการสำรองข้อมูลที่ชัดเจน โดยครอบคลุมทั้งข้อมูลระบบและข้อมูลวิจัย

(๓.๒) ต้องมีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าสามารถใช้งานได้จริงในกรณีฉุกเฉิน

(๓.๓) ต้องเก็บรักษาข้อมูลสำรองในสถานที่ที่ปลอดภัยและแยกจากระบบหลัก

(๔) การจัดการช่องโหว่ทางเทคนิค

(๔.๑) ต้องมีการประเมินและทดสอบช่องโหว่ของระบบและแอปพลิเคชันอย่างสม่ำเสมอ

(๔.๒) ต้องมีกระบวนการในการติดตามและปรับปรุงระบบให้ทันสมัยเพื่อแก้ไขช่องโหว่ที่พบ

(๔.๓) ต้องมีการจัดลำดับความสำคัญในการแก้ไขช่องโหว่ตามระดับความเสี่ยงและผลกระทบต่องานวิจัยและพัฒนา

(๕) การจัดการการเปลี่ยนแปลง

(๕.๑) ต้องมีกระบวนการควบคุมการเปลี่ยนแปลงระบบ แอปพลิเคชัน และโครงสร้างพื้นฐานด้านไอที

(๕.๒) การเปลี่ยนแปลงที่สำคัญต้องได้รับการอนุมัติจากผู้มีอำนาจและผ่านการทดสอบก่อนนำไปใช้งานจริง

(๕.๓) ต้องมีแผนรองรับในกรณีที่การเปลี่ยนแปลงส่งผลกระทบไม่พึงประสงค์ต่อระบบหรืองานวิจัย

๙. การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

๙.๑. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๑) การลงทะเบียนและยกเลิกสิทธิผู้ใช้งาน

(๑.๑) ต้องมีขั้นตอนที่เป็นทางการในการลงทะเบียนและยกเลิกสิทธิผู้ใช้งานระบบและบริการต่างๆ

(๑.๒) การให้สิทธิการเข้าถึงต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบ

(๑.๓) ต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง โดยทบทวนตามความจำเป็นหรือตามหน้าที่ความรับผิดชอบของผู้ใช้งาน นอกจากนี้ สิทธิการเข้าถึงหรือใช้งานระบบสารสนเทศต้องถูกเพิกถอนทันทีเมื่อผู้ใช้งานไม่มีความจำเป็นต้องมีการเข้าถึงหรือใช้งานระบบสารสนเทศดังกล่าวอีกต่อไป ทั้งนี้ ถือเป็นความรับผิดชอบของผู้ใช้งานและผู้บังคับบัญชาที่ต้องแจ้งให้ผู้ดูแลระบบทราบโดยไม่ชักช้าว่าผู้ใช้งานนั้นสิ้นสิทธิการเข้าถึงหรือใช้งานระบบสารสนเทศแล้ว

(๒) การจัดการสิทธิพิเศษ

(๒.๑) ต้องจำกัดและควบคุมการใช้งานบัญชีผู้ใช้ที่มีสิทธิพิเศษ (Privileged Accounts) อย่างเข้มงวด

(๒.๒) การใช้งานบัญชีที่มีสิทธิพิเศษต้องได้รับการอนุมัติและมีการบันทึกการใช้งานอย่างละเอียด

(๒.๓) ต้องมีการเปลี่ยนรหัสผ่านของบัญชีที่มีสิทธิพิเศษอย่างสม่ำเสมอ และทันทีเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบ

๙.๒. การบริหารจัดการรหัสผ่าน (Password Management)

(๑) นโยบายรหัสผ่าน

(๑.๑) ต้องกำหนดนโยบายรหัสผ่านที่รัดกุม เช่น ความยาวขั้นต่ำ ความซับซ้อน และอายุการใช้งาน

(๑.๒) ห้ามใช้รหัสผ่านเริ่มต้น (Default Password) ที่มาจากผู้ผลิตหรือผู้ให้บริการ

(๑.๓) ต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่าอาจถูกล่วงรู้หรือเปิดเผย

(๒) การจัดการรหัสผ่าน

(๒.๑) ห้ามเปิดเผยรหัสผ่านให้ผู้อื่นทราบ รวมถึงเจ้าหน้าที่เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบ

(๒.๒) ควรใช้ระบบจัดการรหัสผ่าน (Password Manager) ที่ได้รับการรับรองสำหรับการจัดเก็บรหัสผ่านที่ซับซ้อน

(๒.๓) ควรใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับระบบที่สำคัญ

๙.๓. การควบคุมการเข้าถึง (Access Control)

(๑) การควบคุมการเข้าถึงเครือข่าย

(๑.๑) ต้องมีการแบ่งแยกเครือข่ายตามประเภทของการใช้งาน เช่น เครือข่ายภายในเครือข่ายสำหรับงานวิจัย และเครือข่ายสำหรับบุคคลภายนอก

(๑.๒) ต้องมีการควบคุมการเข้าถึงเครือข่ายผ่านระบบพิสูจน์ตัวตนที่น่าเชื่อถือ

(๑.๓) ต้องมีการเฝ้าระวังและตรวจสอบการเข้าถึงเครือข่ายอย่างสม่ำเสมอ

(๒) การควบคุมการเข้าถึงระบบปฏิบัติการ

(๒.๑) ต้องมีการล็อคหน้าจอเมื่อไม่ได้ใช้งานเกินระยะเวลาที่กำหนด

(๒.๒) ต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ

(๒.๓) ต้องมีการบันทึกประวัติการเข้าใช้งานระบบปฏิบัติการที่สำคัญ

(๓) การควบคุมการเข้าถึงแอปพลิเคชันและข้อมูล

(๓.๑) ต้องมีการกำหนดสิทธิการเข้าถึงแอปพลิเคชันและข้อมูลตามหลักการ "need-to-know" และ "least privilege"

(๓.๒) ต้องมีการแบ่งแยกหน้าที่และความรับผิดชอบในการเข้าถึงระบบและข้อมูลที่สำคัญ

(๓.๓) ต้องมีการทบทวนและปรับปรุงสิทธิการเข้าถึงเมื่อมีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ความรับผิดชอบ

๑๐. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

๑๐.๑.ข้อกำหนดการรักษาความมั่นคงปลอดภัยสำหรับระบบ (Security Requirements for Systems)

(๑) การวิเคราะห์และกำหนดข้อกำหนดด้านความมั่นคงปลอดภัย

(๑.๑) ต้องมีการวิเคราะห์และกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบใหม่หรือการปรับปรุงระบบเดิม

(๑.๒) ข้อกำหนดด้านความมั่นคงปลอดภัยต้องครอบคลุมทั้งด้านการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล

(๑.๓) ต้องคำนึงถึงความต้องการเฉพาะด้านความปลอดภัยสำหรับงานวิจัยและพัฒนาเทคโนโลยีระบบราง

(๒) การรักษาความมั่นคงปลอดภัยในการพัฒนาและสนับสนุนกระบวนการ

(๒.๑) ต้องมีการแยกสภาพแวดล้อมการพัฒนา การทดสอบ และการใช้งานจริงออกจากกัน

(๒.๒) ต้องมีการควบคุมการเข้าถึงซอร์สโค้ดและเครื่องมือพัฒนาอย่างเข้มงวด

(๒.๓) ต้องมีการตรวจสอบและทดสอบความมั่นคงปลอดภัยของระบบก่อนนำไปใช้งานจริง

๑๐.๒.การประมวลผลที่ถูกต้องในแอปพลิเคชัน (Correct Processing in Applications)

(๑) การตรวจสอบข้อมูลนำเข้า

(๑.๑) ต้องมีการตรวจสอบความถูกต้องของข้อมูลนำเข้าในแอปพลิเคชัน โดยเฉพาะข้อมูลที่เกี่ยวข้องกับการวิจัยและพัฒนา

(๑.๒) ต้องมีการป้องกันการโจมตีแบบ SQL Injection และ Cross-Site Scripting (XSS

(๒) การควบคุมการประมวลผลภายใน

(๒.๑) ต้องมีการตรวจสอบความถูกต้องของการประมวลผลข้อมูลในแอปพลิเคชัน

(๒.๒) ต้องมีการบันทึกการเปลี่ยนแปลงข้อมูลสำคัญและสามารถตรวจสอบย้อนหลังได้

(๓) การตรวจสอบข้อมูลส่งออก

(๓.๑) ต้องมีการตรวจสอบความถูกต้องของข้อมูลส่งออกจากแอปพลิเคชัน

(๓.๒) ต้องมีการป้องกันการรั่วไหลของข้อมูลสำคัญหรือข้อมูลส่วนบุคคลในรายงานหรือผลลัพธ์ของแอปพลิเคชัน

๑๐.๓.การควบคุมการเข้ารหัส (Cryptographic Controls)

(๑) นโยบายการใช้การควบคุมการเข้ารหัส

(๑.๑) ต้องมีการกำหนดนโยบายการใช้งานการเข้ารหัสข้อมูลสำหรับข้อมูลสำคัญและข้อมูลวิจัย

(๑.๒) ต้องใช้อัลกอริทึมการเข้ารหัสที่เป็นมาตรฐานและได้รับการยอมรับในระดับสากล

(๒) การจัดการกุญแจ

(๒.๑) ต้องมีกระบวนการจัดการกุญแจเข้ารหัสที่ปลอดภัยตลอดวงจรชีวิตของกุญแจ

(๒.๒) ต้องมีการแยกหน้าที่ในการจัดการกุญแจเพื่อป้องกันการใช้งานในทางที่ผิด

๑๐.๔.การรักษาความมั่นคงปลอดภัยของไฟล์ระบบ (Security of System Files)

(๑) การควบคุมซอฟต์แวร์ในระบบปฏิบัติการ

(๑.๑) ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ในระบบปฏิบัติการ

(๑.๒) ต้องมีการอัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่มีความปลอดภัย

(๒) การป้องกันข้อมูลทดสอบระบบ

(๒.๑) ต้องมีการป้องกันข้อมูลที่ใช้ในการทดสอบระบบอย่างเข้มงวด

(๒.๒) ห้ามใช้ข้อมูลจริงในการทดสอบระบบ เว้นแต่มีมาตรการป้องกันที่เพียงพอ

๑๐.๕.การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes)

(๑) กระบวนการควบคุมการเปลี่ยนแปลง

(๑.๑) ต้องมีกระบวนการควบคุมการเปลี่ยนแปลงระบบและซอฟต์แวร์อย่างเป็นทางการ

(๑.๒) การเปลี่ยนแปลงที่สำคัญต้องได้รับการอนุมัติจากผู้มีอำนาจและผ่านการทดสอบก่อนนำไปใช้งานจริง

(๒) การทบทวนทางเทคนิคหลังจากการเปลี่ยนแปลงแพลตฟอร์มปฏิบัติการ

(๒.๑) ต้องมีการทบทวนและทดสอบแอปพลิเคชันที่สำคัญหลังจากมีการเปลี่ยนแปลงแพลตฟอร์มปฏิบัติการ

(๒.๒) ต้องมั่นใจว่าการเปลี่ยนแปลงไม่ส่งผลกระทบต่อความปลอดภัยและการดำเนินงานขององค์กร

(๓) การจำกัดการเปลี่ยนแปลงต่อแพคเกจซอฟต์แวร์

(๓.๑) ต้องหลีกเลี่ยงการแก้ไขแพคเกจซอฟต์แวร์สำเร็จรูป

(๓.๒) หากจำเป็นต้องแก้ไข ต้องมีการควบคุมอย่างเข้มงวดและบันทึกการเปลี่ยนแปลงทั้งหมด

๑๐.๖.การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

(๑) การควบคุมช่องโหว่ทางเทคนิค

(๑.๑) ต้องมีการติดตามข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานอย่างสม่ำเสมอ

(๑.๒) ต้องมีการประเมินความเสี่ยงของช่องโหว่ที่พบและดำเนินการแก้ไขตามความเหมาะสม

(๒) การทดสอบเจาะระบบ

(๒.๑) ต้องมีการทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบที่สำคัญอย่างน้อยปีละ ๑ ครั้ง

(๒.๒) ผลการทดสอบต้องนำมาใช้ในการปรับปรุงความปลอดภัยของระบบ

๑๑. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

๑๑.๑.การบริหารจัดการเหตุการณ์และการตอบสนอง (Incident Management)

(๑) การรายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

(๑.๑) ต้องมีช่องทางและขั้นตอนที่ชัดเจนสำหรับการรายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

(๑.๒) บุคลากรทุกคนต้องรายงานเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยที่พบโดยเร็วที่สุด

(๒) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

(๒.๑) ต้องมีทีมตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Incident Response Team)

(๒.๒) ต้องมีแผนตอบสนองต่อเหตุการณ์ที่ครอบคลุมขั้นตอนการจัดการเหตุการณ์ต่างๆ

(๒.๓) ต้องมีการฝึกซ้อมแผนตอบสนองต่อเหตุการณ์อย่างน้อยปีละ ๑ ครั้ง

(๓) การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

(๓.๑) ต้องมีการวิเคราะห์สาเหตุของเหตุการณ์ที่เกิดขึ้นเพื่อป้องกันการเกิดซ้ำ

(๓.๒) ต้องนำบทเรียนที่ได้จากเหตุการณ์มาปรับปรุงมาตรการรักษาความปลอดภัย

๑๒. การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

๑๒.๑.การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Planning)

(๑) การพัฒนาและการนำแผนความต่อเนื่องไปปฏิบัติ

(๑.๑) สทร. ต้องพัฒนาและรักษาแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้มั่นใจว่าสามารถดำเนินงานวิจัยและพัฒนาได้อย่างต่อเนื่องในสถานการณ์ฉุกเฉิน

(๑.๒) แผนความต่อเนื่องต้องครอบคลุมการปกป้องข้อมูลวิจัย ทรัพย์สินทางปัญญา และระบบสำคัญที่ใช้ในการวิจัยและพัฒนาเทคโนโลยีระบบราง

(๑.๓) ต้องมีการระบุกระบวนการและทรัพยากรที่จำเป็นสำหรับการรักษาความต่อเนื่องของงานวิจัยและพัฒนา

(๒) การทดสอบและปรับปรุงแผนความต่อเนื่อง

(๒.๑) ต้องมีการทดสอบแผนความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าแผนสามารถนำไปปฏิบัติได้จริง

(๒.๒) ต้องมีการปรับปรุงแผนความต่อเนื่องให้ทันสมัยอยู่เสมอ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่สำคัญในองค์กรหรือสภาพแวดล้อมการทำงาน

๑๒.๒.การกู้คืนระบบและข้อมูล (System and Data Recovery)

(๑) การสำรองข้อมูลและการกู้คืน

(๑.๑) ต้องมีนโยบายและขั้นตอนการสำรองข้อมูลที่ชัดเจน โดยครอบคลุมทั้งข้อมูลวิจัย ผลงานวิจัย และข้อมูลสำคัญอื่นๆ

(๑.๒) ต้องมีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้อย่างมีประสิทธิภาพในกรณีฉุกเฉิน

(๑.๓) ต้องเก็บรักษาข้อมูลสำรองในสถานที่ที่ปลอดภัยและแยกจากระบบหลัก

(๒) การกู้คืนระบบสำคัญ

(๒.๑) ต้องมีแผนและขั้นตอนการกู้คืนระบบสำคัญที่ใช้ในการวิจัยและพัฒนา

(๒.๒) ต้องกำหนดลำดับความสำคัญของระบบที่ต้องกู้คืน โดยพิจารณาจากผลกระทบต่องานวิจัยและพัฒนา

(๒.๓) ต้องมีการทดสอบแผนการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

๑๒.๓.การรักษาความต่อเนื่องของงานวิจัยและพัฒนา

(๑) การป้องกันการสูญหายของข้อมูลวิจัย

(๑.๑) ต้องมีมาตรการป้องกันการสูญหายของข้อมูลวิจัยและผลงานวิจัยที่สำคัญ

(๑.๒) ต้องมีการจัดเก็บข้อมูลวิจัยในรูปแบบที่สามารถเข้าถึงและใช้งานได้แม้ในสถานการณ์ฉุกเฉิน

(๒) การรักษาความต่อเนื่องของโครงการวิจัย

(๒.๑) ต้องมีแผนรองรับเพื่อให้โครงการวิจัยสำคัญสามารถดำเนินต่อไปได้ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน

(๒.๒) ต้องมีการกำหนดบุคลากรสำรองที่สามารถดำเนินงานวิจัยแทนได้ในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติงานได้

๑๒.๔.การปกป้องทรัพย์สินทางปัญญาในสถานการณ์ฉุกเฉิน

(๑) การรักษาความลับของทรัพย์สินทางปัญญา

(๑.๑) ต้องมีมาตรการพิเศษในการปกป้องทรัพย์สินทางปัญญาและความลับทางการค้าในสถานการณ์ฉุกเฉิน

(๑.๒) ต้องมีแผนการอพยพหรือทำลายเอกสารสำคัญที่เกี่ยวข้องกับทรัพย์สินทางปัญญาในกรณีที่จำเป็น

(๒) การรักษาความต่อเนื่องของการจดสิทธิบัตร

(๒.๑) ต้องมีแผนรองรับเพื่อให้กระบวนการจดสิทธิบัตรหรือการปกป้องทรัพย์สินทางปัญญาอื่นๆ สามารถดำเนินต่อไปได้แม้ในสถานการณ์ฉุกเฉิน

(๒.๒) ต้องมีการสำรองข้อมูลและเอกสารที่เกี่ยวข้องกับการจดสิทธิบัตรในสถานที่ที่ปลอดภัยและสามารถเข้าถึงได้ในกรณีฉุกเฉิน

๑๓. กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

๑๓.๑.การปฏิบัติตามกฎหมายและข้อบังคับ (Compliance)

(๑) การระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

(๑.๑) สทร. ต้องระบุและติดตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและการวิจัยพัฒนาเทคโนโลยีระบบราง

(๑.๒) ต้องมีการปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดทางกฎหมายที่เปลี่ยนแปลงไป

(๒) การปฏิบัติตามกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา

(๒.๑) ต้องมีนโยบายและแนวปฏิบัติที่ชัดเจนเกี่ยวกับการใช้ซอฟต์แวร์และทรัพย์สินทางปัญญาอื่นๆ อย่างถูกต้องตามกฎหมาย

(๒.๒) ต้องมีการตรวจสอบการใช้งานซอฟต์แวร์และทรัพย์สินทางปัญญาอื่นๆ อย่างสม่ำเสมอเพื่อให้มั่นใจว่าเป็นไปตามข้อกำหนดของลิขสิทธิ์

(๓) การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(๓.๑) ต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

(๓.๒) ต้องมีการฝึกอบรมบุคลากรเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑๓.๒.การพิจารณาการตรวจสอบระบบ (System Audit Considerations)

(๑) การวางแผนและการดำเนินการตรวจสอบ

(๑.๑) ต้องมีการวางแผนและดำเนินการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอเพื่อให้มั่นใจว่าเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัย

(๑.๒) การตรวจสอบต้องดำเนินการโดยผู้ตรวจสอบที่มีความเป็นอิสระและมีความเชี่ยวชาญ

(๒) การป้องกันเครื่องมือตรวจสอบ

(๒.๑) ต้องมีการควบคุมการเข้าถึงเครื่องมือตรวจสอบระบบเพื่อป้องกันการใช้งานโดยไม่ได้รับอนุญาตหรือการละเมิด

(๒.๒) เครื่องมือตรวจสอบต้องแยกออกจากระบบพัฒนาและระบบปฏิบัติการ

๑๔. การทบทวนและปรับปรุงนโยบาย

(๑) สทร. ต้องทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์นี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในองค์กรหรือสภาพแวดล้อมการทำงาน

(๒) การปรับปรุงนโยบายต้องได้รับการอนุมัติจากผู้บริหารระดับสูงของ สทร. ก่อนนำไปใช้งาน

(๓) ต้องมีการสื่อสารการเปลี่ยนแปลงของนโยบายให้กับบุคลากร นักวิจัย และผู้เกี่ยวข้องทุกคนทราบอย่างทั่วถึง

๑๕. บทสรุป

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ครอบคลุมประเด็นสำคัญทั้งหมดที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบสารสนเทศ ข้อมูล และทรัพย์สินทางปัญญาของสถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน) (สทร.) โดยมุ่งเน้นการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการปกป้องข้อมูลวิจัย ผลงานวิจัย และการรักษาความต่อเนื่องของงานวิจัยและพัฒนา ตลอดจนโครงการต่างๆ ของ สทร.

การปฏิบัติตามนโยบายนี้จะช่วยให้ สทร. สามารถบริหารงานของสถาบันในด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการดำเนินงานวิจัยและพัฒนาเทคโนโลยีระบบรางได้อย่างมีประสิทธิภาพและปลอดภัย ตลอดจนสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียทุกฝ่าย

๑๖. ภาคผนวก

๑๖.๑.คำนิยาม (Definitions)

(๑) ความมั่นคงปลอดภัยไซเบอร์: การปกป้องระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม และข้อมูลจากการโจมตีทางดิจิทัล การเข้าถึงโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง หรือการทำลาย

(๒) ทรัพย์สินทางปัญญา: ผลงานที่เกิดจากความคิดสร้างสรรค์ของมนุษย์ ซึ่งได้รับการคุ้มครองทางกฎหมาย เช่น สิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า และความลับทางการค้า

(๓) การรักษาความต่อเนื่องทางธุรกิจ: กระบวนการในการวางแผนและเตรียมการเพื่อให้องค์กรสามารถดำเนินงานต่อไปได้ในกรณีที่เกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติ

๑๖.๒.แนวทางการดำเนินงาน (Guidelines)

(๑) แนวทางการจัดการรหัสผ่าน

(๒) ขั้นตอนการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

(๓) แนวทางการจัดการข้อมูลส่วนบุคคล

๑๖.๓.ข้อกำหนดทางกฎหมาย (Legal Requirements)

(๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๓) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒