กรมทรัพย์สินทางปัญญา

นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

1. บทนำ

นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมทรัพย์สินทางปัญญา ใช้แนวทางและกระบวนการโดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รายละเอียดบางส่วนจากนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 เพื่อใช้เป็นกรอบและแนวทางการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพย์สินทางปัญญา เพื่อปกป้องทรัพย์สินสารสนเทศ โครงสร้างพื้นฐาน รวมถึงการสร้างความมั่นใจในการดำเนินงานตามภารกิจของกรมทรัพย์สินทางปัญญาอย่างต่อเนื่องและปลอดภัย

2. วัตถุประสงค์

2.1 เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพย์สินทางปัญญา

2.2 เพื่อสร้างความรู้ความเข้าใจให้ผู้บริหาร บุคลากร และผู้ใช้งานปฏิบัติตามนโยบาย มาตรฐานกรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำรวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

2.3 เพื่อให้ผู้บริหาร บุคลากร ผู้ใช้งาน และผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของ กรมทรัพย์สินทางปัญญา ให้สามารถใช้งานระบบคอมพิวเตอร์ของกรมทรัพย์สินทางปัญญาได้อย่างถูกต้องและเหมาะสม

2.4 เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา โดนบุก รุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อภารกิจ และการดำเนินงานของกรมทรัพย์สินทางปัญญา

3. ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพย์สินทางปัญญาทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของกรมทรัพย์สินทางปัญญา ซึ่งครอบคลุมถึง

3.1 ผู้บริหาร บุคลากร และผู้ใช้งาน และหน่วยงานทั้งหมดที่เกี่ยวข้องกับกรมทรัพย์สินทางปัญญา

3.2 บุคคลภายนอกหน่วยงานที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา

4. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ ดังต่อไปนี้

4.1 ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของกรมทรัพย์สินทางปัญญา

4.2 ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของกรมทรัพย์สินทางปัญญา ต้องไม่มี การแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

4.3 ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึง ข้อมูล และบริการได้อย่างรวดเร็วและเชื่อถือได้

4.4 ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ

4.5 การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบ คอมพิวเตอร์ และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

4.6 การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบ คอมพิวเตอร์ และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการ พื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

4.7 การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้องอันประกอบไปด้วย

4.7.1 การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของผู้บริหาร บุคลากร ผู้ใช้งาน และบุคคลภายนอกที่เกี่ยวข้องทุกคน

4.7.2 การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

4.7.3 การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้ผู้บริหาร บุคลากร ผู้ใช้บริการ และบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมี ประสิทธิผล

5. คำนิยาม

“ศูนย์คอมพิวเตอร์ (Data Center)” หมายความว่า สถานที่สำหรับจัดวางเครื่องคอมพิวเตอร์แม่ข่าย (Computer Server) และอุปกรณ์เครือข่าย (Network Equipment) และจัดเก็บข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา ซึ่งประกอบด้วยศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง

“ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer: DCIO)” หมายความว่า อธิบดีหรือผู้บริหารระดับสูงที่ได้รับการแต่งตั้งจากอธิบดีกรมทรัพย์สินทางปัญญาให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพย์สินทางปัญญา

“ระบบสารสนเทศ” หมายความว่า ระบบงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างระบบสารสนเทศ เพื่อนำมาใช้ประโยชน์ในการวางแผน การบริหารจัดการ และการสนับสนุนการให้บริการของกรมทรัพย์สินทางปัญญา

“ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างตามหน่วยงานบุคคลภายนอก และผู้ให้บริการภายนอก ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และเข้าถึงข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้พัฒนาระบบ” หมายความว่า ผู้ที่มีหน้าที่และความรับผิดชอบในการพัฒนาและดูแลระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้ดูแลระบบ” หมายความว่า ผู้ที่มีหน้าที่และความรับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ฐานข้อมูล หรือจดหมายอิเล็กทรอนิกส์ (E-mail) ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาเพื่อการบริหารจัดการระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมทรัพย์สินทางปัญญา

“เจ้าของระบบงาน” หมายความว่า หน่วยงานที่มีหน้าที่และความรับผิดชอบในการควบคุมดูแลระบบสารสนเทศและอนุญาตให้เจ้าหน้าที่หรือบุคคลใด ๆ เข้าใช้งานระบบสารสนเทศดังกล่าวได้

“หน่วยงานภายนอก” หมายความว่า องค์กรหรือผู้มีส่วนได้ส่วนเสียที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงระบบสารสนเทศหรือข้อมูลของกรมทรัพย์สินทางปัญญา โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาข้อมูลไว้เป็นความลับ

“ผู้ให้บริการภายนอก” หมายความว่า องค์กรหรือบริษัทที่ให้บริการแก่กรมทรัพย์สินทางปัญญาในด้านต่าง ๆ เพื่อสนับสนุนการดำเนินการตามภารกิจของกรมทรัพย์สินทางปัญญา

“ทรัพย์สิน” หมายความว่า ทรัพย์สินหรือสิ่งอื่นใดอันมีมูลค่าหรือคุณค่าต่อกรมทรัพย์สินทางปัญญา

“อุปกรณ์สื่อสารพกพา (Mobile Device)” หมายความว่า โทรศัพท์มือถือสมาร์ทโฟน (Smartphone) หรือแท็บเล็ต (Tablet)

“โปรแกรมอรรถประโยชน์ (Utility Program)” หมายความว่า โปรแกรมจัดการงานพื้นฐานและบริการต่าง ๆ ซึ่งอำนวยความสะดวกให้กับผู้พัฒนาระบบและผู้ดูแลระบบในการดูแลระบบสารสนเทศของกรมทรัพย์สินทางปัญญา

“ระบบวิศวกรรมความมั่นคงปลอดภัย” หมายความว่า กรอบวิธีการออกแบบ การสร้าง และดำเนินการอย่างมั่นคงปลอดภัย

“ความมั่นคงปลอดภัยของสารสนเทศ (Information Security)” หมายความว่า การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของกรมทรัพย์สินทางปัญญาถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

6. หน้าที่และความรับผิดชอบ

6.1 หน้าที่ของผู้บังคับบัญชา ปฏิบัติดังต่อไปนี้

6.1.1 ชี้แจงให้ผู้บริหาร บุคลากร และผู้ใช้งานทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของสำนักงานการทะเบียนที่เกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์

6.1.2 ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม

6.1.3 พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาค และเป็นธรรม

6.2 หน้าที่ของผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้ใช้งาน ปฏิบัติดังต่อไปนี้

6.2.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของกรมทรัพย์สินทางปัญญาที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

6.2.2 ให้ความร่วมมือกับหน่วยงานอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของกรมทรัพย์สินทางปัญญา

6.2.3 แจ้งให้หน่วยงานทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุกโจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อหน่วยงาน

6.3 ผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้ใช้งานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ปฏิบัติดังต่อไปนี้

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

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

6.3.3 ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

6.3.4 ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่หน่วยงานกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของกรมทรัพย์สินทางปัญญาเป็นความลับส่วนตัว ผู้บริหาร บุคลากร และผู้ใช้งาน ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้ ผู้บริหาร บุคลากร และผู้ใช้งานต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อผู้บริหาร บุคลากร และผู้ใช้งานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่านและรหัสอื่นใดด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัสที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือห้ามตั้งรหัสซ้ำกันในทุกระบบที่มีสิทธิใช้งาน

6.3.5 ผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้ใช้งานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมทรัพย์สินทางปัญญา

7. องค์ประกอบของนโยบาย

องค์ประกอบของนโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy) ของกรมทรัพย์สินทางปัญญา แบ่งเป็น 10 หมวด ประกอบด้วย

7.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

7.2 การบริหารจัดการระบบ (System Management)

7.3 การบริหารจัดการหน่วยงานและบุคลากร (Human Resource Management)

7.4 การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

7.5 การบริหารจัดการการสื่อสารและการดำเนินงาน (Communications and Operation Management)

7.6 การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

7.7 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

7.8 การบริหารจัดการเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

7.9 การจัดการความต่อเนื่องทางด้านงานจดทะเบียนทรัพย์สินทางปัญญา (Business Continuity Management)

7.10 กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

นโยบายที่ 1

การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
(Cyber Security Risk Management)

วัตถุประสงค์

เพื่อแสดงถึงการยอมรับความเสี่ยงและการลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยใช้วิธีการที่สอดคล้องกันในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management) รวมถึงมีมาตรการรักษาความมั่นคงปลอดภัย เพื่อปกป้องข้อมูลซึ่งสอดคล้องกับกระบวนการในการระบุและประเมินความเสี่ยง (Risk Identification and Assessment)

รายละเอียด

1.1 วิธีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management Methodology)
1.2 การจัดโครงสร้างองค์กร (Internal Organization)
1.3 การบริหารความเสี่ยงภายนอก (Risk Management with External Parties)

นโยบายที่ 2

การบริหารจัดการระบบ
(System Management)

วัตถุประสงค์

เพื่อให้มีมาตรการในการปกป้องทรัพย์สินของกรมทรัพย์สินทางปัญญาอย่างเหมาะสม

รายละเอียด

2.1 บัญชีทรัพย์สินและความเป็นเจ้าของ (Inventory and Ownership)
2.2 การจัดชั้นความลับและการควบคุม (Security Classification and Handling)
2.3 การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์ (Software Licensing)

นโยบายที่ 3

การบริหารจัดการหน่วยงานและบุคลากร
(Human Resource Management)

วัตถุประสงค์

เพื่อให้ผู้บริหาร บุคลากร ผู้ใช้งาน และบุคคลภายนอกที่ทำสัญญากับกรมทรัพย์สินทางปัญญาเข้าใจในหน้าที่ความรับผิดชอบของตนเอง รวมถึงตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน

รายละเอียด

3.1 ก่อนการจ้างงาน (Prior to Employment)

3.2 ระหว่างการจ้างงาน (During Employment)

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment)

นโยบายที่ 4

การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงสถานที่และอุปกรณ์โดยไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความเสียหายและ เกิดการแทรกแซงการทำงานต่อระบบคอมพิวเตอร์ของกรมทรัพย์สินทางปัญญา

รายละเอียด

4.1 การรักษาความมั่นคงปลอดภัยสถานที่ (Physical Security)

4.2 การรักษาความมั่นคงปลอดภัยอุปกรณ์ (Equipment Security)

นโยบายที่ 5

การบริหารจัดการการสื่อสารและการดำเนินงาน (Communications and Operation Management)

วัตถุประสงค์

5.1 เพื่อทำให้มั่นใจว่ามีการดำเนินงานบนระบบคอมพิวเตอร์อย่างปลอดภัย

5.2 เพื่อดำเนินการ (Implement) และรักษา (Maintain) ระดับความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม

5.3 เพื่อลดความเสี่ยงจากการล้มเหลวของระบบคอมพิวเตอร์

5.4 เพื่อปกป้องและรักษาความถูกต้องของข้อมูล ซอฟต์แวร์ และระบบคอมพิวเตอร์ให้มีสภาพพร้อมใช้งาน

5.5 เพื่อทำให้มั่นใจว่ามีการปกป้องข้อมูลในเครือข่าย รวมถึงการป้องกันโครงสร้างพื้นฐาน สนับสนุนอื่นๆ

5.6 เพื่อป้องกันการเปิดเผย การแก้ไข การลบ หรือการทำลายทรัพย์สินโดยไม่ได้รับอนุญาต รวมถึงการหยุดชะงักของกิจกรรมทางทางด้านงานทะเบียนทรัพย์สินทางปัญญา

5.7 เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลที่มีการรับส่งภายในกรมทระย์สินทางปัญญาและบุคคลภายนอก

5.8 เพื่อเฝ้าระวังการประมวลผลข้อมูลที่ไม่ได้รับอนุญาตรายละเอียด

รายละเอียด

1. การบริหารจัดการการส่งมอบบริการของบุคคลภายนอก (External Party Service Delivery Management)

2. การบริหารจัดการปริมาณความจุของระบบ (Capacity Management)

3. การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection Against Malicious Software)
4. การสำรองและการกู้คืนข้อมูล (Back Up and Restoration)
5. การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)
6. การควบคุมสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media Handling)
7 การจัดการข้อมูลแบบคลาวด์ (Cloud Storage)
8. การรับส่งข้อมูล (Information Transfer)
9. การเฝ้าระวัง (Monitoring)
10. การบริหารจัดการแพทช์ (Patch Management)

นโยบายที่ 6

การบริหารจัดการการควบคุมการเข้าถึง
(Access Control Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการ เข้าถึง ระบบและบริการโดยไม่ได้รับอนุญาต

รายละเอียด

6.1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
6.2 การบริหารจัดการรหัสผ่าน (Password Management)
6.3 การควบคุมการเข้าถึง (Access Control)
6.4 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

นโยบายที่ 7

การจัดหา การพัฒนา และการบำรุงรักษาระบบ
(System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อให้การจัดหา การพัฒนา และการบำรุงรักษาระบบ คำนึงถึงความมั่นคงปลอดภัยเป็นองค์ประกอบสำคัญ

รายละเอียด

7.1 ข้อกำหนดการรักษาความมั่นคงปลอดภัยสำหรับระบบ (Security Requirements for Systems)
7.2 การประมวลผลบนแอปพลิเคชัน (Correct Processing in Applications)
7.3 การควบคุมการเข้ารหัส (Cryptographic Controls)
7.4 การรักษาความมั่นคงปลอดภัย System File (Security of System Files)
7.5 การรักษาความมั่นคงปลอดภัยในการพัฒนา และกระบวนการสนับสนุน (Security in Development

and Support Processes)

7.6 การบริหารจัดการช่องโหว่ (Vulnerability Management)

นโยบายที่ 8

การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

วัตถุประสงค์

เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น และทำให้มั่นใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงจุดอ่อนที่เกี่ยวข้องกับระบบได้รับการสื่อสารและสามารถดำเนินการแก้ไขได้ทันเวลา

รายละเอียด

8.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Management of Cyber Security Incident)

นโยบายที่ 9

การจัดการความต่อเนื่องทางด้านงานจดทะเบียนทรัพย์สินทางปัญญา (Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันกระบวนการทางด้านงานจดทะเบียนทรัพย์สินทางปัญญาที่สำคัญจากผลกระทบของความ ล้มเหลวที่สำคัญของระบบคอมพิวเตอร์หรือจากภัยพิบัติ

รายละเอียด

9.1 แผนการบริหารความต่อเนื่องการให้บริการของระบบ (Business Continuity Plan) ของกรมทรัพย์สินทางปัญญา

นโยบายที่ 10

กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับหรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคง

ปลอดภัยไซเบอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมาย ระเบียบข้อบังคับอื่นที่เกี่ยวข้องซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะได้ออกใช้บังคับต่อไปในภายหน้า

รายละเอียด

10.1 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ.2558 พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558 และพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 4) พ.ศ. 2561

10.2 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

10.3 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งแก้ไขเพิ่มเติมโดยระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ. 2561

10.4 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

10.5 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

10.6 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

10.7 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

10.8 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552

10.9 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

10.10 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

10.11 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559

10.12 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

10.13 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

10.14 นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

10.15 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562