ประกาศกรมบังคับคดี

เรื่อง นโยบายและแนวปฏิบัติการรักษาความปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๙

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมบังคับคดีจึงได้มีการทบทวนและจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีเป็นประจำทุกปี เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล กรมบังคับคดีจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี เพื่อเป็นเครื่องมือให้กับผู้ใช้งานระบบ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

กรมบังคับคดีจึงออกประกาศ เรื่อง นโยบายและแนวปฏิบัติการรักษาความปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๙ ปรากฏตามเอกสารแนบท้ายประกาศ เพื่อให้หน่วยงานและเจ้าหน้าที่ในสังกัดกรมบังคับคดีปฏิบัติตามแนวนโยบายและแนวปฏิบัตินี้

ประกาศ ณ วันที่ ๑๙ สิงหาคม พ.ศ. ๒๕๖๙

(นายเสกสรร สุขแสง)
อธิบดีกรมบังคับคดี

อรอุมา ตรวจ/ทาน
วิทวัฒน์ ร่าง/พิมพ์

นโยบายและแนวปฏิบัติการรักษาความปลอดภัยสารสนเทศ

Information Security Polices and Guidelines

รหัสเอกสาร LED-ICT-PC-01

Version : 00

ประวัติการปรับปรุงเอกสาร

(DOCUMENT VERSION HISTORY)

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	1 ต.ค. 2569	เอกสารเผยแพร่ฉบับแรก

การอนุมัติเอกสาร

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
นางสาวอรอุมา เก่งทางดี	นายพลัฐ หิรัญสมบัติ	นายเสกสรร สุขแสง
ผอ.ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	หัวหน้าผู้ตรวจราชการกรม ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง	อธิบดีกรมบังคับคดี
27 ก.ค. 2569		

สารบัญ

1. บทนำ

1.1. หลักการและเหตุผล

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการต่าง ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กรมบังคับคดีจึงได้มีการทบทวนและจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีเป็นประจำทุกปี เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล กรมบังคับคดีจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี เพื่อเป็นเครื่องมือให้กับผู้ใช้งานระบบ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

จากประกาศกรมบังคับคดี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี พ.ศ. ๒๕๖๗ ซึ่งจัดทำขึ้นตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายที่เกี่ยวข้อง เพื่อใช้เป็นกรอบแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีนั้น กรมบังคับคดีได้พิจารณาทบทวนและปรับปรุงแนวนโยบายและแนวปฏิบัติดังกล่าวให้มีความสอดคล้องกับมาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 เพื่อยกระดับระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นระบบ มีประสิทธิภาพ สามารถบริหารจัดการความเสี่ยงด้านสารสนเทศได้อย่างเหมาะสม และรองรับการดำเนินงานของหน่วยงานด้วยวิธีการทางอิเล็กทรอนิกส์ได้อย่างมั่นคงปลอดภัยและเชื่อถือได้

การปรับปรุงดังกล่าวมุ่งให้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีเป็นไปตามหลักการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ครอบคลุมการกำหนดบทบาทหน้าที่ ความรับผิดชอบ การประเมินและจัดการความเสี่ยง การควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการติดตาม ตรวจสอบ และปรับปรุงอย่างต่อเนื่องตามแนวทางของมาตรฐาน ISO/IEC 27001

ทั้งนี้ เพื่อให้หน่วยงานและเจ้าหน้าที่ในสังกัดกรมบังคับคดีใช้เป็นแนวทางในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นไปในทิศทางเดียวกัน มีมาตรฐานเป็นที่ยอมรับในระดับสากล และสนับสนุนภารกิจของกรมบังคับคดีอย่างมีประสิทธิภาพและยั่งยืน

1.2. หลักการและเหตุผล

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้น ในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศ อันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอ ในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้องครบสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้น ทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

กรมบังคับคดีจึงได้จัดทำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมบังคับคดีขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในกรมบังคับคดี และบุคลากรทุกคนในกรมบังคับคดีมีความรู้เข้าใจในนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี สามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

2. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี ฉบับนี้มีวัตถุประสงค์เพื่อ

2.1. ทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมบังคับคดี

2.2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดี ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

2.3. จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อ ความมั่นคงปลอดภัยของข้อมูลระบบสารสนเทศขององค์กร

2.4. เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของกรมบังคับคดี มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศกรมบังคับคดี และ ใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

3. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมบังคับคดี โดยบุคลากรที่เกี่ยวข้องทุกระดับมีหน้าที่ต้องปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวอย่างเคร่งครัด ภายใต้การกำกับ ดูแล สนับสนุน และติดตามการนำไปประยุกต์ใช้ของผู้บริหารของกรมบังคับคดี

ในกรณีที่ข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรือก่อให้เกิดความเสี่ยงหรืออันตรายแก่กรมบังคับคดี หรือบุคคลใด อันเนื่องมาจากความบกพร่อง การละเลย หรือการฝ่าฝืนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้ที่เกี่ยวข้องต้องรับผิดชอบตามหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ของตน ทั้งนี้ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และ ระเบียบ คำสั่ง หรือแนวปฏิบัติภายในของกรมบังคับคดี ที่เกี่ยวข้อง รวมถึงกระบวนการบริหารจัดการความเสี่ยงของหน่วยงาน

4. คำนิยาม

ลำดับ	คำนิยาม	ความหมาย
1.	กรมฯ /องค์กร	กรมบังคับคดี
2.	ผู้ใช้งาน	ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการ และผู้ใช้งานทั่วไปของกรมบังคับคดี
3.	บัญชีผู้ใช้งาน	บัญชีระบบซึ่งผู้ใช้งานและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี
4.	สิทธิ์ของผู้ใช้งาน	สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
5.	สินทรัพย์ หรือ ทรัพย์สิน	เครื่องคอมพิวเตอร์ อุปกรณ์ประกอบคอมพิวเตอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร
6.	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
7.	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องน่าแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความเชื่อถือ (reliability)
8.	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยอันหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
9.	ข้อมูลอิเล็กทรอนิกส์	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์
10.	นโยบาย	นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ลำดับ	คำนิยาม	ความหมาย
11.	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
12.	ผู้บริหาร	อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมบังคับคดี
13.	หน่วยงาน	กรมบังคับคดี รวมถึงหน่วยงานในสังกัดกรมบังคับคดี
14.	ผู้บริหารระดับสูงสุด	ผู้บริหารของหน่วยงานระดับสูงสุด (CEO) หรืออธิบดีกรมฯ รับผิดชอบเกี่ยวกับความเสี่ยงและความเสียหายอันเกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ
15.	ศูนย์ฯ / ศทส.	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Center : ICTC)
16.	ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
17.	ระบบสารสนเทศ	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายเข้ามาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริหารการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีส่วนประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น
18.	ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
19.	หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และการใช้ข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล
20.	จดหมายอิเล็กทรอนิกส์ (E-Mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP และ IMAP เป็นต้น
21.	สื่อบันทึกพกพา	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น
22.	ชื่อผู้ใช้ (Username)	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบงานคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

ลำดับ	คำนิยาม	ความหมาย
23.	รหัสผ่าน (Password)	ตัวอักษรหรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ
24.	การเข้ารหัส (Encryption)	การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้ได้ตามปกติ
25.	อุปกรณ์จัดเส้นทาง (Router)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
26.	การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
27.	SSID (Service Set Identifier)	บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบจะต้องตั้งค่า SSID เดียวกัน
28.	WPA (Wi-Fi Protected Access)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิม WEP
29.	MAC Address (Media Access Control Address)	หมายเลขเฉพาะที่ใช้อ้างอิงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด (Internet Card) โดยแต่ละการ์ดจะมีเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังตำแหน่งและปลายทางได้อย่างถูกต้อง
30.	SSL-VPN (Secure Socket Layer Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
31.	แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
32.	ระบบเครือข่ายแบบรวมศูนย์ (Active Directory)	ข้อมูลที่ถูกจัดเก็บในระบบเครือข่าย ผู้ที่สามารถเข้าใช้งานจะต้องผ่านกระบวนการพิสูจน์ตัวตนจากเครื่องแม่ข่าย
33.	Token	อุปกรณ์ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งาน ก่อนการเข้าใช้งาน
34.	Outsource	องค์กร หรือหน่วยงานภายนอกที่กรมบังคับคดีอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมบังคับคดี
35.	การเชื่อมโยงข้อมูล	การเชื่อมโยงข้อมูลจากฐานข้อมูลหนึ่ง ไปยังอีกฐานข้อมูลหนึ่งได้อย่างรวดเร็ว
36.	บันทึกข้อตกลง (Memorandum of Understanding : MOU)	เอกสารหรือหนังสือบันทึกข้อตกลง ความเข้าใจที่ตรงกัน หรือข้อตกลงที่จะร่วมมือระหว่างกัน โดยที่แต่ละฝ่ายอาจเป็นองค์กรหน่วยงานของรัฐ หน่วยงานหรือบริษัทเอกชน หรือระหว่างรัฐกับรัฐ
37.	DCIO	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมบังคับคดี (Department Chief Information Officer)

ลำดับ	คำนิยาม	ความหมาย
38.	ISMS	ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
39.	คณะกรรมการ ISMS	คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Steering Committee)
40.	คณะทำงาน ISMS	คณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)
41.	คณะผู้ตรวจสอบภายใน ISMS	คณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Audit)
42.	คณะนายทะเบียนเอกสาร (DCO)	คณะนายทะเบียนเอกสารบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Document Controllers)

5. ส่วนที่ 1 นโยบายการกำกับดูแลและการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Governance and Management Policy)

5.1. แนวนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

เพื่อกำหนดกรอบนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของกรมบังคับคดีให้เป็นไปในทิศทางเดียวกัน และใช้เป็นแนวทางในการกำกับดูแลและบริหารจัดการระบบสารสนเทศภายใต้ความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

คณะกรรมการความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ และคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นกรอบการบริหารจัดการระดับองค์กร เพื่อคุ้มครองข้อมูลและระบบสารสนเทศของกรมบังคับคดีให้มีความมั่นคงปลอดภัย สอดคล้องกับกฎหมาย ระเบียบราชการ และมาตรฐานสากล โดยมีแนวปฏิบัติดังนี้

5.1.1. เป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อกำหนดเป้าหมายการคุ้มครองสารสนเทศและระบบสารสนเทศของกรมบังคับคดีให้ชัดเจนและสามารถนำไปใช้กำหนดมาตรการควบคุมที่เหมาะสม โดยมุ่งหมายให้การบริหารจัดการสารสนเทศเป็นไปอย่างมั่นคงปลอดภัย

1) เพื่อธำรงไว้ซึ่ง ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสำคัญทางราชการที่อยู่ภายใต้ความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2) เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของกรมบังคับคดีเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และแนวปฏิบัติของทางราชการ รวมถึงมาตรฐานสากลที่เกี่ยวข้อง
3) เพื่อสนับสนุนการดำเนินภารกิจและการให้บริการของกรมบังคับคดีด้วยระบบสารสนเทศและเทคโนโลยีสารสนเทศที่มีความน่าเชื่อถือ ลดความเสี่ยงจากภัยคุกคามด้านสารสนเทศ และสามารถให้บริการได้อย่างต่อเนื่อง
4) เพื่อส่งเสริมให้บุคลากรของกรมบังคับคดีและผู้ที่เกี่ยวข้องมีความตระหนักรู้ มีความรับผิดชอบ และมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยสารสนเทศตามบทบาทและหน้าที่ของตน

5.1.2. ทิศทางการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

กรมบังคับคดีกำหนดทิศทางการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศเป็นไปอย่างมั่นคงปลอดภัย สอดคล้องกับบริบทความเสี่ยง และภารกิจขององค์กร โดยยึดหลักการบริหารจัดการบนฐานความเสี่ยง และการปรับปรุงอย่างต่อเนื่องภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

ทั้งนี้ ทิศทางการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของกรมบังคับคดี ให้เป็นไปตามแนวทางดังต่อไปนี้

1) ดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบนฐานความเสี่ยง (Risk-Based Approach) โดยพิจารณาภัยคุกคาม ช่องโหว่ และผลกระทบที่อาจเกิดขึ้นกับข้อมูลและระบบสารสนเทศของกรมบังคับคดีอย่างเหมาะสม
2) ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และแนวปฏิบัติของทางราชการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล และการให้บริการด้วยระบบอิเล็กทรอนิกส์อย่างเคร่งครัด
3) บูรณาการการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับภารกิจหลักการบริหารราชการ และการให้บริการประชาชนของกรมบังคับคดี เพื่อสนับสนุนการดำเนินงานด้วยระบบเทคโนโลยีสารสนเทศที่มีความน่าเชื่อถือและมีประสิทธิภาพ
4) ส่งเสริมให้มีการปรับปรุง พัฒนา และทบทวนมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถรองรับการเปลี่ยนแปลงด้านเทคโนโลยี สภาพแวดล้อมการปฏิบัติงาน และภัยคุกคามด้านสารสนเทศที่อาจเกิดขึ้น
5) กำหนดให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปในทิศทางเดียวกันทั่วทั้งองค์กร โดยมีการกำกับ ดูแล และประสานงานภายใต้ความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
6) ในกรณีที่ไม่สามารถปฏิบัติตามนโยบายที่ได้ประกาศไปแล้วได้ คณะกรรมการฯและคณะทำงานฯ ระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ มีสิทธิในการขอละเว้นการปฏิบัติตามนโยบายหรือข้อกำหนดนั้น ๆ โดยให้กำหนดมาตรการอื่นๆ มาทดแทน ทั้งนี้ ให้จัดทำเรื่องพร้อมเหตุผลและมาตรการทดแทน เสนอคณะทำงานเพื่อพิจารณาและให้ความเห็นชอบเป็นกรณีไป

5.1.3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมฯ อย่างเป็นระบบ สามารถระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศได้อย่างเหมาะสม อันเป็นการป้องกันและลดระดับความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

กรมฯ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีแนวทางในการดำเนินการอย่างน้อยดังต่อไปนี้

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับผู้ตรวจสอบภายใน (Internal Auditor) และผู้ดูแลระบบที่ได้รับมอบหมาย ทำหน้าที่รับผิดชอบในการดำเนินการ ประสานงาน และสนับสนุนการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติที่กำหนด
2) ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมฯ อย่างน้อยปีละ 1 ครั้ง
3) การตรวจสอบและประเมินความเสี่ยงให้ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน เพื่อให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องได้รับทราบระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของกรมฯ
4) ให้มีการทบทวนกระบวนการบริหารจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

5) ให้มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้มีความเหมาะสมและสอดคล้องกับบริบทของหน่วยงาน
6) การตรวจสอบและประเมินความเสี่ยงต้องมีการจัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะเพื่อใช้ในการปรับปรุงและพัฒนามาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

5.1.4. การเผยแพร่และทบทวน

การเผยแพร่และทบทวน นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมบังคับคดีต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) กรมบังคับคดี จัดพิมพ์เผยแพร่เพื่อให้บุคลากรกรมบังคับคดี บุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

5.2. บทบาทและความรับผิดชอบในการรักษาความปลอดภัยของสารสนเทศ (Information security roles and responsibilities)

เพื่อให้มั่นใจว่ามีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และมีการระบุบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม กรมฯ จึงกำหนดแนวทางในการปฏิบัติ ดังต่อไปนี้

1) ผู้บริหารระดับสูงของกรมบังคับคดีต้องกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้ชัดเจน สอดคล้องกับโครงสร้างการบริหารงานและภารกิจของหน่วยงาน
2) ผู้บริหารระดับสูงต้องมอบหมายหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ที่เกี่ยวข้อง และสื่อสารให้บุคลากรได้รับทราบอย่างทั่วถึง โดยการมอบหมายหน้าที่ต้องมีการแบ่งแยกอย่างชัดเจน เพื่อลดความเสี่ยงจากหน้าที่ที่อาจขัดแย้งกัน และเพื่อป้องกันการละเมิดหรือการใช้งานทรัพย์สินสารสนเทศโดยมิชอบ ทั้งโดยเจตนาและไม่เจตนา
3) กรมฯ ต้องจัดให้มีการแต่งตั้งคณะกรรมการ คณะทำงาน หรือเจ้าหน้าที่ที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ ตามโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ และให้มีการทบทวน ปรับปรุง หรือเปลี่ยนแปลงบทบาทหน้าที่ตามความเหมาะสม หรือเมื่อมีการเปลี่ยนแปลงภารกิจหรือโครงสร้างการบริหารของหน่วยงาน

5.3. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

เพื่อป้องกันและลดความเสี่ยงจากความผิดพลาด การทุจริต หรือการใช้อำนาจหน้าที่โดยมิชอบในการบริหารจัดการระบบสารสนเทศของกรมฯ กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ ต้องกำหนดการแบ่งแยกบทบาท หน้าที่ และความรับผิดชอบในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมและชัดเจน
2) การแบ่งแยกหน้าที่ต้องครอบคลุมงานที่เกี่ยวข้องกับการพัฒนา การกำหนดค่า การดูแลรักษาระบบ การอนุมัติ และการใช้งานระบบสารสนเทศ เพื่อลดโอกาสในการเปลี่ยนแปลงหรือใช้งานทรัพย์สินสารสนเทศโดยมิชอบ ทั้งโดยเจตนาและไม่เจตนา
3) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องสนับสนุนและติดตามให้มีการปฏิบัติตามการแบ่งแยกหน้าที่ พร้อมทั้งพิจารณาการตรวจสอบการปฏิบัติงานตามความเหมาะสม

5.4. ความรับผิดชอบในการบริหารจัดการ (Management responsibilities)

เพื่อให้การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ เป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับโครงสร้างการบริหารราชการ กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ผู้บริหารทุกระดับต้องกำกับ ดูแล และสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติที่กำหนด
2) ในกรณีโครงการด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะดำเนินการโดยกรมฯ หรือมีการว่าจ้างหน่วยงานภายนอก ต้องกำหนดข้อกำหนดและวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการเข้าถึงและการใช้ข้อมูลอย่างเหมาะสม
3) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำหน้าที่เป็นหน่วยงานหลักในการประสานงาน ติดตาม และให้คำแนะนำด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

5.5. รายชื่อผู้ติดต่อกับหน่วยงานด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับเรา (Contact with authorities)

เพื่อให้การประสานงาน การแจ้งเหตุ และการรายงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ เป็นไปอย่างถูกต้องและทันเวลา กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดผู้รับผิดชอบในการติดต่อประสานงานด้านความมั่นคงปลอดภัยสารสนเทศกับหน่วยงานภายนอกที่เกี่ยวข้อง
2) ต้องจัดทำและบำรุงรักษาบัญชีรายชื่อและข้อมูลการติดต่อของหน่วยงานกำกับดูแล หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง
3) ต้องมีการทบทวนข้อมูลการติดต่อให้มีความถูกต้องและเป็นปัจจุบัน เพื่อรองรับการประสานงานเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

5.6. การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)

เพื่อเสริมสร้างองค์ความรู้และติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศ กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ศูนย์เทคโนยีสารสนเทศและการสื่อสารอาจจัดให้มีการติดต่อหรือเข้าร่วมเครือข่าย กลุ่มผู้เชี่ยวชาญ หรือสมาคมด้านความมั่นคงปลอดภัยสารสนเทศตามความเหมาะสม
2) การติดต่อกับกลุ่มหรือเครือข่ายต้องมุ่งเน้นการแลกเปลี่ยนข้อมูล ข่าวสาร แนวปฏิบัติที่เหมาะสม และการติดตามภัยคุกคามหรือช่องโหว่ที่อาจเกิดขึ้น
3) ควรจัดทำบัญชีรายชื่อและข้อมูลการติดต่อของกลุ่มหรือเครือข่ายที่เกี่ยวข้อง และทบทวนข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ

5.7. การจัดการข่าวกรองด้านภัยคุกคามสารสนเทศ (Threat intelligence management)

เพื่อสนับสนุนการป้องกัน ตรวจจับ และลดผลกระทบจากภัยคุกคามด้านสารสนเทศต่อระบบสารสนเทศและข้อมูลขององค์กร กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องรวบรวม วิเคราะห์ และประเมินข่าวกรองด้านภัยคุกคามที่เกี่ยวข้องกับระบบสารสนเทศของกรมฯ
2) การวิเคราะห์ข่าวกรองต้องพิจารณาความน่าเชื่อถือของแหล่งข้อมูล โอกาสเกิดเหตุ และผลกระทบต่อภารกิจของกรมฯ

3) ผลการวิเคราะห์ข่าวกรองต้องนำไปใช้ในการปรับปรุงมาตรการป้องกัน การเฝ้าระวัง และการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

5.8. ความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการ (Information security in project management)

เพื่อให้โครงการด้านเทคโนโลยีสารสนเทศของกรมฯ มีการคำนึงถึงความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมในทุกระยะของการดำเนินโครงการ กรมฯ จึงกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องมีการประเมินและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตั้งแต่ระยะเริ่มต้นของโครงการและตลอดระยะเวลาการดำเนินโครงการ
2) ต้องบูรณาการข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไว้ในกระบวนการวางแผน การดำเนินการและการส่งมอบโครงการ
3) ต้องกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับโครงการให้ชัดเจน และให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารติดตามและให้คำแนะนำตามความเหมาะสม

5.9. บัญชีทรัพย์สินสารสนเทศและทรัพย์สินอื่นๆ ที่เกี่ยวข้อง (Inventory of information and other associated assets)

เพื่อให้การบริหารจัดการและคุ้มครองทรัพย์สินสารสนเทศของกรมฯ เป็นไปอย่างเหมาะสม กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำและบำรุงรักษาทะเบียนทรัพย์สินสารสนเทศและทรัพย์สินที่เกี่ยวข้องให้ครบถ้วน เป็นปัจจุบัน และตรวจสอบได้
2) ทรัพย์สินทุกประเภทต้องระบุเจ้าของทรัพย์สินหรือผู้ดูแลรับผิดชอบอย่างชัดเจน โดยระบุเป็นบุคคลหรือหน่วยงานตามโครงสร้างการบริหารของกรมฯ
3) ทะเบียนทรัพย์สินต้องระบุสาระสำคัญอย่างน้อย ได้แก่ ประเภททรัพย์สิน สถานที่ตั้ง/ระบบที่เกี่ยวข้อง ผู้รับผิดชอบ สถานะการใช้งาน และข้อกำหนดการคุ้มครองตามระดับความสำคัญ
4) ต้องทบทวนรายการทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีทรัพย์สินใหม่ การย้าย การปรับปรุง หรือการเปลี่ยนแปลงที่มีนัยสำคัญ
5) ต้องประเมินความเสี่ยงของทรัพย์สินเมื่อมีการเพิ่มทรัพย์สินใหม่หรือมีการเปลี่ยนแปลงสำคัญเพื่อกำหนดมาตรการควบคุมให้เหมาะสม
6) จัดทำบัญชีเครื่องคอมพิวเตอร์และระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่ายโดยระบุรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง ,ผู้ใช้งาน เท่านั้น
7) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริการจัดการช่องโหว่ของระบบเหล่านั้น และมีการบันทึกดังต่อไปนี้
   - ชื่อซอฟต์แวร์และเวอร์ชั่น (version) ที่ใช้งาน
   - สถานที่ที่ติดตั้ง
   - เครื่องที่ติดตั้ง
   - ผู้ผลิตซอฟต์แวร์

- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาของซอฟต์แวร์นั้นๆ

5.10. การใช้ทรัพย์สินสารสนเทศและทรัพย์สินอื่นๆที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)

เพื่อให้การใช้ทรัพย์สินสารสนเทศของกรมฯ เป็นไปอย่างถูกต้องและไม่ก่อให้เกิดความเสี่ยง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ข้อกำหนดทั่วไป

(1.1) ทรัพย์สินสารสนเทศต้องใช้เพื่อภารกิจของกรมฯ ตามอำนาจหน้าที่และวัตถุประสงค์ของงานเท่านั้น

(1.2) ผู้ใช้งานต้องใช้งานทรัพย์สินอย่างถูกต้องตามข้อกำหนดด้านความปลอดภัย และต้องไม่กระทำการที่ขัดต่อกฎหมาย ระเบียบ หรือคำสั่งของทางราชการ

(1.3) ผู้ใช้งานต้องดูแลทรัพย์สินและข้อมูลไม่ให้บุคคลที่ไม่มีสิทธิเข้าถึง รวมถึงต้องป้องกันการสูญหาย การชำรุด และการเปิดเผยข้อมูลโดยมิชอบ

(1.4) ห้ามติดตั้งซอฟต์แวร์หรือเชื่อมต่ออุปกรณ์ที่ไม่ผ่านการอนุญาต/การควบคุมของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หากมีความจำเป็นต้องดำเนินการ ต้องขออนุมัติตามระเบียบของกรมฯ

(1.5) การใช้งานอุปกรณ์ส่วนบุคคลเพื่อปฏิบัติงาน (ถ้ามี) ต้องเป็นไปตามหลักเกณฑ์และมาตรการควบคุมที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด

2) การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพาของกรมบังคับคดี

(2.1) เครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้จะต้องนำมาลงทะเบียนที่ศูนย์ก่อน ซึ่งจะมีการกำหนดชื่อเครื่อง เพื่อง่ายต่อการตรวจสอบ หากก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ของหน่วยงาน

(2.2) การตั้งชื่อเครื่องคอมพิวเตอร์แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เท่านั้น

(2.3) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(2.4) เจ้าหน้าที่ศูนย์มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แบบพกพา

(2.5) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหายและตรวจสอบ ซ่อมแซม หากเครื่องคอมพิวเตอร์แบบพกพาเกิดความเสียหายด้วยตนเอง

3) การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(3.1) ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว

(3.2) หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวติดชุดคำสั่งไม่พึงประสงค์ ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

4) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(4.1) การใช้งานสำหรับผู้ใช้งาน (User)

(1) เจ้าหน้าที่ในสังกัด หากต้องการติดต่อราชการหรือติดต่อกับบุคคลภายนอกให้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือของส่วนราชการที่กำหนดให้เท่านั้น ห้ามนำไปใช้ติดต่อในเรื่องส่วนตัว และห้ามติดต่องานราชการผ่านระบบจดหมายอิเล็กทรอนิกส์ของเว็บไซต์ผู้ให้บริการอื่น

(2) สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อ มีการเข้าสู่ระบบ ผู้ใช้ทุกคนจะต้องทำการเปลี่ยนรหัสผ่านใหม่ในทันที

(3) ห้ามผู้ใช้ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติของระบบจดหมายอิเล็กทรอนิกส์

(4) ผู้ใช้ต้องระมัดระวังการใช้งานจดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และมาแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

(5) ผู้ใช้ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ–ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(6) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน เพื่อการทำงานของหน่วยงานเท่านั้น

(7) หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น และทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(8) ผู้ใช้ต้องทำการตรวจเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำ การตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

(9) ผู้ใช้ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(10) ห้ามผู้ใช้ใช้ข้อความที่ไม่สุภาพหรือรับ–ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์ และ ต้องระบุชื่อผู้รับและหัวข้อให้ชัดเจน

(11) หลีกเลี่ยงการส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่านบัญชีผู้ใช้งาน หมายเลขบัตรประชาชน ผ่านจดหมายอิเล็กทรอนิกส์

(12) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(13) ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(14) ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(15) ผู้ใช้ต้องย้ายจดหมายอิเล็กทรอนิกส์ที่จำเป็นต้องนำมาใช้ในภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อป้องกันผู้อื่นแอบเข้าไปแอบอ่านจดหมายได้

(16) ไม่จัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

(17) การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน จะถือว่าผู้ที่เข้าใช้บริการรับทราบ ทำความเข้าใจและยอมรับนโยบายจดหมายอิเล็กทรอนิกส์ของหน่วยงานแล้ว

(4.2) แนวทางการควบคุมการใช้งานสำหรับผู้และระบบ (Administrator)

(1) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้

(2) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อให้ผู้ใช้รายใหม่พร้อมรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์

(3) จัดทำระบบการปกปิดการเข้ารหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏ หรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น 'X', 'O' ในการพิมพ์แต่ละตัวอักษร

(4) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง

(5) ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ และมีการ Logout ออกจากหน้าจอ เพื่อตัดการใช้งานของผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้

5) การใช้งานระบบอินเตอร์เน็ต (Internet)

(5.1) ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ได้จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามมิให้ผู้ใช้ ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น

(5.2) เครื่องคอมพิวเตอร์ส่วนบุคคล ก่อนทำการเชื่อมต่ออินเทอร์เน็ตจะต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์ฯ และต้องมีการติดตั้งโปรแกรมป้องกันไวรัสก่อนเสมอ

(5.3) เครื่องคอมพิวเตอร์แบบพกพาส่วนตัวไม่อนุญาตให้ใช้อินเทอร์เน็ต

(5.4) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องผ่านระบบตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนจะทำการรับส่งข้อมูลทุกครั้ง

(5.5) กำหนดให้หน้าแรกของ browser Internet เป็นหน้าเว็บIntranet

(5.6) ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของหน่วยงาน เพื่อหาผลประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

(5.7) ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่ก่อความเสียหายให้กับหน่วยงาน

(5.8) ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

(5.9) ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

(5.10) ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(5.11) ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

(5.12) ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(5.13) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความยั่วยุ เสียดสี ด่าทอ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

(5.14) ห้ามผู้ใช้งานใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ (Bandwidth) ทั้งจำนวนมาก หรือเป็นเวลานาน

(5.15) ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(5.16) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความยั่วยุ เสียดสี ด่าทอ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน และเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

(5.17) ห้ามผู้ใช้งานใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ทั้งจำนวนมาก หรือเป็นเวลานาน

6) การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (Conversion)

(6.1) ข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงต้องมีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิม ซึ่งนำมาจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยผู้จัดทำหรือแปลงจะต้องตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์นั้น มีความหมายและรูปแบบเหมือนกับเอกสารและข้อความเดิม

(6.2) ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงขึ้นด้วยวิธีการที่เชื่อถือได้ และมีการระบุตัวตนของผู้จัดทำหรือแปลงข้อมูลนั้นๆ

(6.3) ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงโดยมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับข้อมูลนั้น เว้นแต่การรับรองหรือบันทึกเพิ่มเติมซึ่งไม่มีผลต่อความหมายของข้อมูลอิเล็กทรอนิกส์

(6.4) ผู้จัดทำหรือแปลงข้อมูลอิเล็กทรอนิกส์จะต้องรับผิดชอบในข้อผิดพลาดหรือความเสียหายที่เกิดจากข้อมูลที่ตนเป็นผู้จัดทำหรือแปลงนั้น

7) การนำข้อมูลต่างๆ เผยแพร่ลงในเว็บไซต์ (Web Information)

(7.1) ข้อมูลที่จะนำมาลงจะต้องได้รับความเห็นชอบ อนุมัติหรือคำสั่งจากผู้บริหาร ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์ฯ

(7.2) ข้อมูลจะนำมาลงจะต้องเป็นข้อมูลที่ไม่ก่อให้เกิดความเสียหายต่อผู้อื่น และหน่วยงาน หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม

(7.3) ผู้มีหน้าที่ลงข้อมูลจะต้องได้รับอนุญาตจากผู้บริหาร ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์ และเป็นเจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมายเท่านั้น

(7.4) กรณีเจ้าหน้าที่ในหน่วยงานที่ไม่อยู่ในสังกัดของศูนย์ ผู้ดูแลระบบจะต้องกำหนดสิทธิ์การเข้าถึงการลงข้อมูลให้แก่เจ้าหน้าที่ดังกล่าว เพื่อไม่ให้เกิดความเสียหายกับข้อมูลอันใดที่ไม่อยู่ในความรับผิดชอบ

8) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

(8.1) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

(8.2) ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องไม่เปิดเผยข้อมูลสำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของหน่วยงาน

(8.3) ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

(8.4) หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

9) การเข้าสู่ระบบเครื่องคอมพิวเตอร์ให้ดำเนินการผ่านระบบบริหารจัดการบัญชีผู้ใช้งานแบบรวมศูนย์ (Active Directory: AD)โดยผู้ใช้งานต้องแสดงตัวตนด้วย ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) หรือใช้ ระบบยืนยันตัวตนดิจิทัล ThaID ตามที่หน่วยงานกำหนด

10) การใช้เทคโนโลยี Generative AI

(10.1) ผู้ใช้งานต้องใช้งานเทคโนโลยี Generative AI ผ่านเครื่องมือหรือแพลตฟอร์มที่กรมฯ ได้ให้ความเห็นชอบหรืออนุมัติไว้เท่านั้น และห้ามนำเครื่องมือ Generative AI อื่นใดที่ไม่ได้รับอนุญาตมาใช้งานในการปฏิบัติงานของกรมฯ ทั้งนี้ หากมีความจำเป็นต้องใช้งานเครื่องมือ Generative AI ที่อยู่นอกเหนือจากรายการที่กำหนด ให้เสนอขออนุมัติผ่านหน่วยงานต้นสังกัด และศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนดำเนินการใช้งาน

(10.2) ผู้ใช้งานต้องศึกษาทำความเข้าใจเกี่ยวกับเทคโนโลยี Generative AI แต่ละประเภท ทั้งในด้านข้อมูลพื้นฐาน ศักยภาพ ประโยชน์ ความเสี่ยง และข้อจำกัด เพื่อให้สามารถนำเทคโนโลยีดังกล่าวไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างเหมาะสม มีประสิทธิภาพ และสอดคล้องกับกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง

(10.3) ผู้ใช้งานต้องใช้เทคโนโลยี Generative AI ภายใต้หลักธรรมาภิบาล มีความเหมาะสม โปร่งใส คำนึงถึงความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ หรือคำสั่งของกรมฯ รวมถึงหลักเกณฑ์อื่นที่เกี่ยวข้องอย่างเคร่งครัด

(10.4) ผู้ใช้งานต้องตรวจสอบและกลั่นกรองเนื้อหาที่สร้างขึ้นจากเครื่องมือ Generative AI (Content Moderation) ให้มั่นใจว่ามีความถูกต้อง (Accuracy) ความน่าเชื่อถือ (Reliability) และไม่ละเมิดสิทธิหรือเสรีภาพของบุคคล ไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อภาพลักษณ์และชื่อเสียงของกรมฯ ทั้งนี้ เนื้อหาที่สร้างขึ้นต้องผ่านการพิจารณาและตรวจสอบก่อนนำไปใช้งานหรือเผยแพร่

(10.5) ห้ามใช้เทคโนโลยี Generative AI เพื่อสร้างข้อมูลอันเป็นเท็จ หรือสร้างเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล หน่วยงาน หรือสังคม ซึ่งอาจนำไปสู่ความเข้าใจผิด การบิดเบือนข้อมูล หรือก่อให้เกิดความขัดแย้งในสังคม

(10.6) ห้ามนำข้อมูลที่เป็นความลับของกรมฯ ไปใช้หรือเปิดเผยผ่านเครื่องมือ Generative AI รวมถึงข้อมูลภายใน เอกสารสำคัญ หรือข้อมูลใด ๆ ที่อาจส่งผลกระทบต่อการดำเนินงานของกรมฯ เช่น ทรัพย์สินทางปัญญา ความลับตามภารกิจของกรมฯ ข้อมูลทางการเงิน รหัสผ่าน เอกสารสัญญา เอกสารหรือหนังสือที่มีการกำหนดชั้นความลับ ข้อมูลเกี่ยวกับโครงการภายใน ซอร์สโค้ด (Source Code) หรือข้อมูลอื่นในลักษณะเดียวกัน

(10.7) ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูล หรือใช้ข้อมูลที่อาจเป็นการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้องผ่านการใช้งานเทคโนโลยี Generative AI

(10.8) ห้ามใช้เทคโนโลยี Generative AI เพื่อสร้าง ทำซ้ำ คัดลอก หรือดัดแปลงเนื้อหาที่เป็นการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของบุคคลหรือหน่วยงานอื่น โดยไม่ได้รับอนุญาตตามกฎหมาย

(10.9) ห้ามใช้เทคโนโลยี Generative AI เพื่อสร้างเนื้อหาที่ส่งเสริมการเลือกปฏิบัติ การเหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือสถานะทางสังคม ซึ่งอาจขัดต่อกฎหมาย หลักสิทธิมนุษยชน หรือศีลธรรมอันดีของสังคม

(10.10) ห้ามใช้เทคโนโลยี Generative AI ในการดำเนินการใด ๆ ที่อาจเข้าข่ายเป็นการกระทำความผิดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หรือหลักเกณฑ์ที่เกี่ยวข้อง ไม่ว่าทางตรงหรือทางอ้อม

5.11. การคืนทรัพย์สิน (Return of assets)

เพื่อป้องกันการสูญหายหรือการนำทรัพย์สินสารสนเทศไปใช้งานโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) เมื่อมีการโอน ย้าย เปลี่ยนหน้าที่ สิ้นสุดการปฏิบัติงาน สิ้นสุดสัญญา หรือสิ้นสุดสิทธิการใช้งาน ผู้ครอบครองต้องส่งคืนทรัพย์สินให้ครบถ้วนภายในระยะเวลาที่กำหนด
2) ก่อนส่งคืนทรัพย์สิน ต้องดำเนินการส่งคืน ลบ ทำลาย หรือโอนย้ายข้อมูลของราชการตามระเบียบและชั้นความลับของกรมฯ
3) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องดำเนินการเพิกถอนสิทธิการเข้าถึงที่เกี่ยวข้องและปิดบัญชีผู้ใช้งานตามกระบวนการที่กำหนด
4) การส่งคืนต้องมีหลักฐานการส่งมอบ/ตรวจรับเพื่อรองรับการตรวจสอบย้อนหลัง

5.12. ชั้นความลับของสารสนเทศ (Classification of information)

เพื่อให้การบริหารจัดการสารสนเทศของกรมฯ เป็นไปอย่างเป็นระบบ เหมาะสมกับลักษณะและความสำคัญของข้อมูล และสามารถกำหนดมาตรการคุ้มครองสารสนเทศให้สอดคล้องกับระดับความเสี่ยงที่เหมาะสม กรมฯ จึงกำหนดหลักเกณฑ์การจำแนกประเภท ระดับความสำคัญ และชั้นความลับของสารสนเทศ และกำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ ต้องกำหนดเกณฑ์การจำแนกชั้นความลับของสารสนเทศ และสื่อสารให้ผู้เกี่ยวข้องรับทราบและปฏิบัติตาม
2) กรมฯ จัดแบ่งประเภทของข้อมูลออกเป็นประเภทต่าง ๆ เพื่อให้การบริหารจัดการและการกำหนดมาตรการควบคุมเป็นไปอย่างเหมาะสม ดังนี้

- ข้อมูลสารสนเทศทางการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และแผนงาน คำรับรองการปฏิบัติราชการ ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงิน และบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลการตรวจสอบบุคคลล้มละลาย ข้อมูลการตรวจฟื้นฟูกิจการของลูกหนี้ ข้อมูลประกาศขายทอดตลาด และข้อมูลอื่นที่เกี่ยวข้องกับการให้บริการประชาชน

3) กรมฯ จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น 3 ระดับ เพื่อสะท้อนระดับผลกระทบที่อาจเกิดขึ้นจากการเข้าถึง การเปิดเผย หรือการสูญหายของข้อมูล ดังนี้
   - ข้อมูลที่มีระดับความสำคัญมากที่สุด
   - ข้อมูลที่มีระดับความสำคัญปานกลาง
   - ข้อมูลที่มีระดับความสำคัญน้อย
4) กรมฯ กำหนดชั้นความลับของสารสนเทศ เพื่อใช้เป็นแนวทางในการควบคุมการเข้าถึง การใช้งาน การเปิดเผย และการปกป้องข้อมูล ไว้ 5 ระดับ ดังนี้
   - ข้อมูลลับที่สุด (Top Secret) หมายถึง ข้อมูลหรือสารสนเทศที่หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อกรมฯ
   - ข้อมูลลับมาก (Secret) หมายถึง ข้อมูลหรือสารสนเทศที่หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงต่อกรมฯ
   - ข้อมูลลับ (Confidential) หมายถึง ข้อมูลหรือสารสนเทศที่หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายต่อการดำเนินงานหรือภาพลักษณ์ของกรมฯ
   - ข้อมูลใช้ภายใน (Internal Use Only) หมายถึง ข้อมูลหรือสารสนเทศที่ใช้สำหรับการปฏิบัติงานภายในกรมฯ ซึ่งไม่ประสงค์ให้เผยแพร่สู่ภายนอก แต่หากเปิดเผยจะก่อให้เกิดผลกระทบในระดับจำกัด
   - ข้อมูลทั่วไป (Public) หมายถึง ข้อมูลหรือสารสนเทศที่สามารถเปิดเผยหรือเผยแพร่ให้บุคคลทั่วไปเข้าถึงได้ โดยไม่ก่อให้เกิดความเสียหายต่อกรมฯ
5) หน่วยงานเจ้าของข้อมูลต้องจำแนกชั้นความลับของข้อมูลภายใต้ความรับผิดชอบ และกำหนดมาตรการควบคุมให้สอดคล้องกับระดับความลับ
6) กำหนดให้ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบ การรักษาความลับทางราชการ พ.ศ.2544 และให้เป็นไปตามนโยบายการเข้ารหัสข้อมูล (Use of Cryptography) ที่กรมฯ กำหนด
7) ต้องกำหนดแนวทางการจัดเก็บ การเข้าถึง การส่งต่อ การสำรอง และการทำลายข้อมูล ให้สอดคล้องกับชั้นความลับ
8) การเปิดเผยหรือส่งต่อข้อมูลให้บุคคลภายนอกต้องได้รับอนุมัติและกำหนดเงื่อนไขการคุ้มครองตามระเบียบของกรมฯ

5.13. การบ่งชี้สารสนเทศ (Labelling of information)

เพื่อให้การใช้งานและการจัดการสารสนเทศเป็นไปอย่างถูกต้องตามชั้นความลับ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องบ่งชี้ชั้นความลับหรือข้อความกำกับที่เหมาะสมบนเอกสาร ไฟล์ข้อมูล สื่อบันทึก และผลลัพธ์จากระบบ ตามเกณฑ์ของกรมฯ

2) ต้องกำหนดรูปแบบการบ่งชี้ให้สอดคล้องกับสื่อและช่องทางจัดเก็บ รวมถึงกรณีเอกสารอิเล็กทรอนิกส์และเอกสารกระดาษ
3) ต้องอบรมหรือสื่อสารให้ผู้เกี่ยวข้องเข้าใจการบ่งชี้และข้อปฏิบัติที่สัมพันธ์กับชั้นความลับ
4) กรณีจำเป็นที่ไม่สามารถบ่งชี้ได้ครบถ้วน ต้องมีมาตรการคุ้มครองทดแทนที่เหมาะสมและได้รับอนุมัติจากผู้รับผิดชอบ

5.14. การถ่ายโอนสารสนเทศ (Information transfer)

เพื่อป้องกันการรั่วไหล การเข้าถึง หรือการดัดแปลงข้อมูลโดยมิชอบระหว่างการถ่ายโอน กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดหลักเกณฑ์และช่องทางการถ่ายโอนให้สอดคล้องกับชั้นความลับของข้อมูล และประเภทสื่อที่ใช้ถ่ายโอน
2) ต้องใช้ช่องทางที่มีความมั่นคงปลอดภัยและผ่านการอนุญาต เช่น ช่องทางราชการหรือช่องทางที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด
3) ต้องกำหนดมาตรการคุ้มครอง เช่น การเข้ารหัส การยืนยันตัวตน การกำหนดผู้รับที่ชัดเจน และการควบคุมสิทธิการเข้าถึง
4) ต้องมีการบันทึกหรือหลักฐานการส่งมอบเมื่อเหมาะสม เพื่อรองรับการตรวจสอบย้อนหลัง
5) การถ่ายโอนให้หน่วยงานภายนอกต้องกำหนดเงื่อนไขการรักษาความลับ/การไม่เปิดเผยข้อมูล และเป็นไปตามกฎหมายและระเบียบของกรมฯ

5.15. การควบคุมการเข้าถึง (Access controls)

เพื่อให้การเข้าถึงสารสนเทศและระบบสารสนเทศเป็นไปตามความจำเป็นของหน้าที่ และเพื่อให้ผู้รับผิดชอบและผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และ บุคคล ภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนด โดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับผู้ดูแลระบบที่ได้รับมอบหมาย มีหน้าที่รับผิดชอบในการกำหนด ควบคุม ดูแล และติดตามการเข้าถึงและการใช้งานระบบสารสนเทศของกรมฯ ให้เป็นไปตามนโยบายและแนวปฏิบัติที่กำหนด
2) จัดทำบัญชีทรัพย์สิน ซึ่งจะจำแนกกลุ่มทรัพยากรของระบบและการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน
3) ต้องควบคุมการเข้าถึงตามหลักสิทธิขั้นต่ำ (least privilege) และความจำเป็นในการปฏิบัติงาน (need-to-know)
4) ต้องมีการลงทะเบียน อนุมัติ ปรับเปลี่ยน ระงับ และยกเลิกบัญชีผู้ใช้งานอย่างเป็นทางการ
5) ต้องกำหนดให้ผู้ใช้งานมีบัญชีเฉพาะบุคคลและไม่ซ้ำกับผู้อื่น ยกเว้นกรณีจำเป็นต้องใช้บัญชีร่วม ต้องมีทะเบียนบัญชีร่วมและมาตรการควบคุมเพิ่มเติม
6) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้
    (1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
        - อ่านอย่างเดียว สำหรับ กลุ่มผู้บริหาร
        - สร้างข้อมูล สำหรับ กลุ่มผู้ดูแลระบบ

- ป้อนข้อมูล สำหรับ กลุ่มหัวหน้างานและกลุ่มผู้ปฏิบัติงาน
- อนุมัติ สำหรับ กลุ่มผู้บริหาร
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(3) ผู้ใช้งานที่ต้องเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้อง

- ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตและกำหนดสิทธิการใช้งานเบื้องต้นจากผู้บังคับบัญชาก่อน
- ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
- สำหรับรหัสการใช้งานจะแจ้ง โดยการใส่ซองปิดผนึกส่งไปยังผู้ขออนุญาตใช้งานสารสนเทศ
- กรณีตรวจสอบสิทธิการใช้งานแล้ว บุคคลดังกล่าวไม่มีสิทธิการใช้งานจะแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร

7) กรมฯ กำหนดช่องทางในการเข้าถึงระบบสารสนเทศตามความจำเป็นและความเหมาะสม เพื่อให้สามารถควบคุม ตรวจสอบ และรักษาความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างมีประสิทธิภาพ โดย

- การเข้าถึงผ่านระบบเครือข่ายภายในแบบใช้สาย (Wired LAN) และเครือข่ายไร้สาย (Wireless LAN) ต้องมีการบันทึกข้อมูลการใช้งาน (Log) เพื่อสามารถตรวจสอบย้อนหลังได้
- การเข้าถึงผ่านระบบเครือข่ายอินเทอร์เน็ตหรือหน้าเว็บ ต้องมีการตรวจสอบและควบคุมสิทธิการเข้าใช้งานตามระดับสิทธิที่ได้รับอนุญาต

8) ต้องทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ โอน ย้าย หรือสิ้นสุดการปฏิบัติงาน

9) สิทธิของผู้ให้บริการภายนอกต้องจำกัดตามขอบเขตงาน ระยะเวลา และต้องเพิกถอนเมื่อสิ้นสุดการปฏิบัติงานหรือสิ้นสุดสัญญา

10) มีการประชาสัมพันธ์เผยแพร่เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness)

11) การป้องกันอุปกรณ์ในขณะไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(1) มีการกำหนดข้อปฏิบัติให้ป้องกันคอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(3) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(4) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(5) ตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

12) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง เพื่อให้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ 3 ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น
13) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย
14) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

5.16. การบริหารจัดการอัตลักษณ์ (Identity management)

เพื่อให้การจัดการบัญชีผู้ใช้งานมีความถูกต้อง ครบถ้วน และตรวจสอบได้ตลอดวงจรชีวิต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องจัดให้ผู้ใช้งานระบบสารสนเทศแต่ละรายมี ข้อมูลประจำตัวสำหรับการเข้าใช้งานระบบเป็นการเฉพาะ เพื่อให้สามารถระบุและตรวจสอบความรับผิดชอบต่อการใช้งานระบบได้อย่างชัดเจน
2) กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้
   (1) จัดแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม
   (2) เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
   (3) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
   (4) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น
   (5) มีการตรวจสอบและมอบสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
   (6) จัดทำเอกสารแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
   (7) มีการทำบันทึกและจัดเก็บข้อมูลการอนุมัติเข้าใช้ระบบสารสนเทศ
   (8) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
   (9) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดจากการจ้าง เป็นต้น
   (10) กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้
      - ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน
      - หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน
      - สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card, Finger scan
   (11) ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนด

ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน เพื่อให้เข้าสู่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

3) การจัดทำ การแก้ไข การระงับ และการยกเลิก ข้อมูลประจำตัวและบัญชีผู้ใช้งานระบบ ต้องดำเนินการตามขั้นตอนที่กำหนด และให้สอดคล้องกับสถานะการปฏิบัติงาน บทบาท และหน้าที่ความรับผิดชอบของผู้ใช้งาน
4) กรณีมีความจำเป็นต้องใช้ บัญชีผู้ใช้งานร่วม ต้องได้รับอนุมัติจากผู้มีอำนาจ มีการกำหนดผู้รับผิดชอบในการควบคุมการใช้งาน และต้องสามารถตรวจสอบการใช้งานย้อนหลังได้
5) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องจัดให้มี ทะเบียนบัญชีผู้ใช้งานพิเศษและบัญชีผู้ดูแลระบบ (Privileged Account and Administrator Account Register) พร้อมกำหนดมาตรการควบคุมการกำกับดูแล และการทบทวนการใช้งานตามความเหมาะสม
6) ทุกเครื่องที่อยู่ในระบบเครือข่ายจะต้องเข้าสู่ระบบเครือข่ายแบบรวมศูนย์ (Active Directory: AD)
7) กำหนดให้ผู้ดูแลระบบระบบเครือข่ายแบบรวมศูนย์ (Active Directory: AD) มีหน้าที่ในการกำหนด Policy ต่าง ๆ และกำหนดสิทธิ์ของผู้ใช้งานโดยผ่านความเห็นชอบจากผู้บริหาร, ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการศูนย์
8) กำหนดให้มีการบันทึกการทำงานของระบบเครือข่ายแบบรวมศูนย์ (Active Directory: AD) บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งานอินเทอร์เน็ตหรืออีเมล์ เป็นต้น

5.17. การพิสูจน์ตัวตน (Authentication information)

เพื่อยืนยันตัวตนของผู้ใช้งานก่อนการเข้าถึงระบบอย่างเหมาะสมกับระดับความเสี่ยง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้
   (1) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
   (2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา โดยให้มีความแตกต่างและหลากหลาย
   (3) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีที่ปลอดภัย
   (4) โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานต้องตอบกลับทันทีหลังจากได้รับรหัสผ่าน
   (5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้ยากต่อการคาดเดา
   (6) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว
   (7) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน
   (8) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่
   (9) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2) ต้องกำหนดวิธีพิสูจน์ตัวตนตามระดับความเสี่ยงและความสำคัญของระบบ เช่น รหัสผ่านที่รัดกุม การยืนยันหลายปัจจัย (MFA) หรือวิธีอื่นที่เหมาะสม
3) มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password User) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้
   (1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
   (2) ต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา
   (3) ต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ตัวปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
   (4) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือกลุ่มเหมือนกัน
   (5) ไม่ตั้งรหัสผ่านจากอักขระที่เรียง หรือกลุ่มเหมือนกัน
   (6) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
   (7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
   (8) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
   (9) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านนส่วนบุคคล (Save Password)
   (10) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
   (11) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้
   (12) ทำการเปลี่ยนแปลงโดยทันที
   (13) ต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาทุกๆ 90 วัน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
   (14) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานต่างๆ ที่ตนใช้งาน
   (15) หลีกเลี่ยงการใช้รหัสผ่านเดิมเมื่อเปลี่ยนรหัสผ่านใหม่
   (16) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป
4) ข้อมูลพิสูจน์ตัวตนต้องเก็บรักษาเป็นความลับและห้ามเปิดเผยแก่บุคคลอื่น รวมถึงต้องมีมาตรการป้องกันการถูกขโมยหรือถูกใช้งานโดยมิชอบ
5) การมอบหมายหรือรีเซ็ตข้อมูลพิสูจน์ตัวตนต้องผ่านการยืนยันตัวตนและการอนุมัติตามระเบียบของกรมฯ
6) กรณีมีความจำเป็นต้องมอบข้อมูลพิสูจน์ตัวตนเพื่อการปฏิบัติงาน ต้องกำหนดระยะเวลา บันทึกเหตุผลและยุติการใช้งานเมื่อครบกำหนด
7) การยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่นอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้
   - ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง
   - ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานจริง เช่น การใช้รหัสผ่าน (Password)
   - จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย 1 วิธี

- การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และให้มีการตรวจสอบผู้ใช้งานด้วย VPN

5.18. การบริหารจัดการสิทธิการเข้าถึง (Access rights)

เพื่อให้การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของกรมฯ เป็นไปอย่างเหมาะสม สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ (Business Requirement for access control) บทบาทหน้าที่ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ รวมทั้งเพื่อให้การให้สิทธิ การเปลี่ยนแปลง และการเพิกถอนสิทธิการเข้าถึงเป็นไปอย่างเป็นระบบ สามารถตรวจสอบได้ และลดความเสี่ยงจากการเข้าถึงโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุม และจัดกัดสิทธิ์เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้
   (1) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
      - ขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาต เบื้องต้นจากผู้บังคับบัญชาก่อน
      - ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
      - สำหรับรหัสการใช้งาน ผู้ดูแลระบบจะแจ้งให้ผู้ขออนุญาตใช้งานสารสนเทศทราบผ่านช่องทางที่แยกจากช่องทางการแจ้งชื่อบัญชีผู้ใช้งาน และกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านในครั้งแรกที่เข้าสู่ระบบ
2) กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานให้สอดคล้องกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้งานระบบสารสนเทศของหน่วยงาน
3) ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ
4) ผู้ดูแลระบบ จะต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง
5) กรมฯ กำหนดให้มีการจัดแบ่งระดับชั้นการเข้าถึงระบบสารสนเทศ โดยผู้ดูแลระบบเป็นผู้บริหารจัดการสิทธิของผู้ใช้งานให้สอดคล้องกับบทบาท หน้าที่ และความจำเป็นในการปฏิบัติงาน ดังต่อไปนี้
   (1) ระดับชั้นสำหรับผู้บริหาร ได้แก่
      - ผู้บริหารระดับสูง (อธิบดี, รองอธิบดี, ผู้บริหารเทคโนโลยีระดับสูง (DCIO) เป็นต้น)
      - ผู้บริหารระดับกลาง (ผู้อำนวยการ,ชำนาญการพิเศษ,ผู้เชี่ยวชาญ,ผู้ตรวจสอบ)
   (2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป ได้แก่
      - ระดับชำนาญการ
      - ระดับปฏิบัติการ (เจ้าหน้าที่ทั่วไป)
      - บุคลากรจากภายนอกที่ปฏิบัติงานในลักษณะจ้างเหมาบริการ (Outsource)
      - บุคคลภายนอก (ประชาชนทั่วไป หรืออื่นๆ)
   (3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

- ผู้ดูแลระบบ
- ผู้ที่ได้รับมอบหมาย (มีกำหนดเวลาในการใช้งาน)

6) การมอบหมายสิทธิ การให้สิทธิต้องได้รับอนุมัติจากผู้มีอำนาจและหน่วยงานเจ้าของระบบหรือเจ้าของข้อมูลตามที่กำหนด และต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง
7) ต้องมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน เก็บรักษาหลักฐานการอนุมัติและการดำเนินการเพื่อรองรับการตรวจสอบย้อนหลัง ดังนี้
   - มีการจัดเก็บเอกสารการร้องขอและการกำหนดสิทธิเป็นลายลักษณ์อักษร
   - ในฐานข้อมูลมีการเก็บวัน/เดือน/ปีและรหัสของผู้ดูแลระบบที่เข้ามาดำเนินการกำหนดสิทธิ
8) ต้องกำหนดระดับสิทธิให้สอดคล้องกับบทบาทหน้าที่และชั้นความลับของข้อมูล
9) การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business requirement for access control) จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจดังนี้
   - กลุ่มผู้บริหาร ได้แก่ อธิบดี, รองอธิบดี, ผู้ตรวจราชการ, ผู้เชี่ยวชาญ และผู้อำนวยการสำนัก/กอง/สาขา
   - กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
   - กลุ่มผู้ใช้งานทั่วไปเป็นบุคคลากรของหน่วยงาน
   - กลุ่มที่ปรึกษาหรือผู้ว่าจ้างที่มีระยะสัญญาจ้างกับหน่วยงาน
   - ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว
10) กรมฯ กำหนดช่วงเวลาในการเข้าถึงระบบสารสนเทศ เพื่อให้การใช้งานเป็นไปอย่างเหมาะสมและสามารถควบคุมความเสี่ยงได้ โดยแบ่งเป็น
    - ช่วงเวลาราชการ ได้แก่ วันจันทร์ถึงวันศุกร์ เวลา 08:30 – 16:30 น.
    - ช่วงเวลานอกราชการ ให้สามารถเข้าถึงได้เฉพาะกรณีที่ได้รับอนุญาตเป็นการเฉพาะ และอยู่ภายใต้การควบคุมและการพิจารณาของผู้มีอำนาจตามที่กำหนด
11) หน่วยงานต้นสังกัดของผู้ใช้งานต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำหนดสิทธิ์ตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิ์ต่างๆ ในการเข้าใช้ระบบสารสนเทศเมื่อผู้ใช้งานโยกย้าย ลาออก ย้าย สิ้นสุดการปฏิบัติงาน หรือหมดความจำเป็นเป็นต้น
12) ผู้ดูแลระบบต้องเพิกถอนหรือปรับสิทธิเมื่อผู้ใช้งานเปลี่ยนบทบาท โอน ย้าย สิ้นสุดการปฏิบัติงาน หรือหมดความจำเป็น
13) ผู้ดูแลระบบต้องดำเนินการทบทวนสิทธิและบัญชีผู้ใช้งานตามรอบระยะเวลาที่กำหนด และดำเนินการปรับปรุงหรือแก้ไขเมื่อพบว่าสิทธิการเข้าถึงไม่เหมาะสม ทั้งนี้ ต้องมีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบเพื่อให้การกำหนดสิทธิการเข้าถึงสอดคล้องกับภารกิจและการปฏิบัติงานที่เปลี่ยนแปลงไป เช่น กรณีมีการเปลี่ยนแปลงตำแหน่งงาน การย้ายหน่วยงาน หรือการสิ้นสุดการจ้างงานภายในกรมฯ เป็นต้น
14) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights) ต้องมีการระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง เป็นต้น โดยมี แนวปฏิบัติดังนี้
    (1) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่

ละบุคคล

(2) ส่งตรงรายชื่อนั้นกับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

(3) ผู้บังคับบัญชาของหน่วยงานดำเนินการแก้ไขข้อมูลสิทธิต่างๆ ให้ถูกต้องตามจริงและแจ้งกลับผู้ดูแลระบบ

(4) สำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน 7 วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วันหลังจากได้รับแจ้งจากหน่วยงาน

15) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างน้อยปีละ 1 ครั้ง

5.19. ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

เพื่อควบคุมและลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดจากการใช้บริการหรือการว่าจ้างหน่วยงานภายนอก กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอกให้เหมาะสมกับขอบเขตงาน ประเภทข้อมูล และระดับความเสี่ยง
2) ต้องพิจารณาความพร้อม ความน่าเชื่อถือ และความสามารถของผู้ให้บริการภายนอกก่อนการจัดจ้างหรืออนุญาตให้เข้าถึงระบบหรือข้อมูล
3) ผู้ให้บริการภายนอกต้องปฏิบัติตามนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ ตามที่กำหนด
4) ต้องมีการติดตามและประเมินผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอกตามระยะเวลาที่เหมาะสม
5) กำหนดให้ผู้อำนวยการศูนย์ เป็นผู้อนุมัติสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยผู้ให้บริการภายนอก (Outsource) จะต้องจัดทำเอกสารขออนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงานเป็นลายลักษณ์อักษร โดยจะต้องมีรายละเอียดประกอบในเอกสารอย่างน้อย ดังนี้
   - เหตุผลในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
   - ระยะเวลาในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
   - คำยินยอมจากเจ้าหน้าที่ของหน่วยงานที่รับผิดชอบในการนำผู้ให้บริการภายนอก (Outsource) เข้ามาปฏิบัติงานภายในศูนย์ฯ หรือสำนักงาน
6) ผู้ให้บริการภายนอก (Outsource) ที่มาปฏิบัติงานให้กับหน่วยงาน ไม่ว่าจะปฏิบัติงานภายใน หรือภายนอกหน่วยงาน จะต้องลงนามในสัญญาจ้างเรื่องการไม่เปิดเผยข้อมูลของสำนักงาน โดยจะต้องจัดทำสัญญาจ้างให้เสร็จสิ้นก่อนการกำหนดสิทธิ์ให้ผู้ให้บริการภายนอก (Outsource) นั้น เข้าถึงระบบเทคโนโลยีสารสนเทศ
7) เจ้าหน้าที่ของหน่วยงานซึ่งเป็นเจ้าของโครงการที่มีการเข้าถึงข้อมูลโดยผู้ให้บริการภายนอก (Outsource) จะต้องกำหนดสิทธิ์การเข้าถึงให้เฉพาะบุคคลที่จำเป็นเท่านั้น

8) สำหรับการปฏิบัติงานในโครงการใหญ่ ผู้ดูแลระบบจะต้องควบคุมให้ผู้ให้บริการภายนอก (Outsource) รักษาความมั่นคงปลอดภัย ทั้งทางด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาให้ระบบพร้อมให้บริการอยู่เสมอ (Availability)
9) ควรกำหนดให้ผู้ให้บริการภายนอก (Outsource) จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสาร
10) ที่เกี่ยวข้องในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน รวมทั้งให้มีการปรับปรุงอย่างสม่ำเสมอ เพื่อใช้ในการควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก (Outsource) ให้เป็นไปตามขอบเขตที่ได้กำหนดไว้
11) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
12) มอบหมายเจ้าหน้าที่ หรือผู้ดูแลระบบเจ้าหน้าที่ในการควบคุม ดูแล ตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก (Outsource)
13) การขอเข้ามาดำเนินการลงในสมุดบันทึก “การเข้า–ออกห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร”
14) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานจะต้องควบคุมดูแลอย่างรัดกุม และได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย
15) เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน
16) เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมอ

5.20. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing information security within supplier agreements)

เพื่อให้ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศได้รับการบังคับใช้ตามสัญญาหรือข้อตกลง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) สัญญาหรือข้อตกลงกับผู้ให้บริการภายนอกต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน ครอบคลุมการเข้าถึง การจัดเก็บ การใช้ การส่งต่อ และการทำลายข้อมูล
2) ต้องกำหนดหน้าที่ ความรับผิดชอบ และมาตรการรองรับกรณีเกิดเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศ
3) ต้องกำหนดเงื่อนไขการรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล และสิทธิในการตรวจสอบตามอำนาจของกรมฯ
4) เมื่อสิ้นสุดสัญญาหรือข้อตกลง ต้องกำหนดวิธีการเพิกถอนสิทธิและการจัดการข้อมูลของกรมฯ ให้แล้วเสร็จตามที่กำหนด

5.21. ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Managing information security in the ICT supply chain)

เพื่อบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตลอดห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับผู้ให้บริการ คู่ค้า และผู้รับจ้างช่วงตามความเหมาะสม
2) ผู้ให้บริการต้องแจ้งข้อมูลการใช้ผู้รับจ้างช่วงที่เกี่ยวข้องกับระบบหรือข้อมูลของกรมฯ ตามเงื่อนไขที่กำหนด
3) ต้องมีการติดตาม ทบทวน และประเมินผลการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงผู้ให้บริการภายนอกและผู้รับจ้างช่วงอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการให้บริการเป็นไปตามข้อกำหนดและมีประสิทธิภาพ
4) กรณีมีการเปลี่ยนแปลงผู้ให้บริการหรือรูปแบบการให้บริการ ต้องประเมินความเสี่ยงก่อนดำเนินการ

5.22. การติดตาม ทบทวน และการเปลี่ยนแปลง ของบริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)

เพื่อให้บริการจากผู้ให้บริการภายนอกเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องมีการติดตามและทบทวนผลการให้บริการของผู้ให้บริการภายนอกตามข้อตกลงและระดับความเสี่ยง
2) การเปลี่ยนแปลงบริการที่กระทบระบบหรือข้อมูลของกรมฯ ต้องผ่านกระบวนการบริหารการเปลี่ยนแปลงและการประเมินความเสี่ยง
3) ต้องสื่อสารข้อกำหนดหรือมาตรการที่ปรับปรุงให้ผู้ให้บริการภายนอกรับทราบและปฏิบัติตาม

5.23. การรักษาความปลอดภัยของมูลสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

เพื่อให้การใช้บริการคลาวด์ของกรมฯ มีความมั่นคงปลอดภัยและเป็นไปตามระเบียบของทางราชการ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การใช้บริการคลาวด์ต้องผ่านการประเมินความเสี่ยงและการอนุมัติตามขั้นตอนที่กำหนด
2) ต้องกำหนดมาตรการควบคุมการเข้าถึง การจัดเก็บ และการส่งต่อข้อมูลบนระบบคลาวด์ให้เหมาะสม
3) ต้องจัดทำทะเบียนทรัพย์สินและข้อมูลที่อยู่บนบริการคลาวด์ให้เป็นปัจจุบัน
4) ต้องมีมาตรการสำรองข้อมูล การกู้คืน และการตอบสนองต่อเหตุผิดปกติ
5) การยุติหรือเปลี่ยนผู้ให้บริการคลาวด์ต้องมีแผนการโอนย้ายและการทำลายข้อมูลอย่างเหมาะสม

5.24. การวางแผนและการเตรียมการบริหารจัดการอุบัติการณ์ด้านการรักษาความปลอดภัยสารสนเทศ (Information security incident management planning and preparation)

เพื่อให้สามารถรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเป็นระบบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดขั้นตอน ช่องทาง และผู้รับผิดชอบในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
2) ต้องจัดเตรียมบุคลากร เครื่องมือ และแนวทางปฏิบัติสำหรับการเฝ้าระวังและตอบสนองต่อเหตุการณ์
3) ผู้พบเห็นหรือผู้ให้บริการภายนอกต้องแจ้งเหตุให้ผู้รับผิดชอบทราบทันทีตามขั้นตอนที่กำหนด

5.25. การประเมินและการตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)

เพื่อให้การตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างเหมาะสมและทันเวลา กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการประเมินระดับความรุนแรงและผลกระทบของเหตุการณ์ตามหลักเกณฑ์ที่กำหนดไว้อย่างเป็นระบบและเหมาะสม
2) จัดลำดับความสำคัญของเหตุการณ์ พร้อมกำหนดแนวทางและมาตรการในการจัดการให้สอดคล้องกับระดับความเสี่ยงที่ประเมินได้
3) ดำเนินการแจ้งหน่วยงานหรือผู้ที่เกี่ยวข้องโดยทันที เพื่อให้สามารถควบคุม แก้ไข และบรรเทาผลกระทบของเหตุการณ์ได้อย่างมีประสิทธิภาพ

5.26. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

เพื่อจำกัดผลกระทบและลดความเสียหายของเหตุการณ์ที่อาจเกิดขึ้น กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการตอบสนองต่อเหตุการณ์อย่างรวดเร็ว เป็นระบบ และเป็นไปตามขั้นตอนที่กำหนดไว้อย่างเคร่งครัด
2) ดำเนินการประเมินขอบเขตและระดับความรุนแรงของเหตุการณ์ พร้อมทั้งรายงานต่อผู้มีอำนาจตามลำดับสายการบังคับบัญชา
3) ต้องมีการบันทึกเหตุการณ์ การตัดสินใจ และการดำเนินการที่เกี่ยวข้องอย่างครบถ้วน เพื่อรองรับการตรวจสอบและใช้เป็นข้อมูลในการปรับปรุงมาตรการในอนาคต

5.27. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

เพื่อปรับปรุงและพัฒนามาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ดำเนินการวิเคราะห์หาสาเหตุของเหตุการณ์อย่างเป็นระบบ พร้อมทั้งจัดทำสรุปบทเรียนที่ได้รับเพื่อใช้เป็นแนวทางในการป้องกันเหตุซ้ำ
2) บันทึกข้อมูลที่เกี่ยวข้องกับเหตุการณ์ ช่องโหว่ที่ตรวจพบ และแนวทางการแก้ไขอย่างครบถ้วน เพื่อสนับสนุนการบริหารความเสี่ยงอย่างมีประสิทธิภาพ
3) กำหนดให้นำผลการเรียนรู้และข้อค้นพบที่ได้ไปใช้ในการปรับปรุงมาตรการควบคุม และแนวปฏิบัติที่เกี่ยวข้องให้มีความเหมาะสมและทันต่อสถานการณ์

5.28. การเก็บรวบรวมหลักฐาน (Collection of evidence)

เพื่อสนับสนุนการตรวจสอบ การสอบสวน และการดำเนินการตามกฎหมาย กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการรวบรวมและจัดเก็บพยานหลักฐานที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างถูกต้อง ครบถ้วน และเป็นไปตามหลักวิชาการ
2) ต้องรักษาความถูกต้อง ความครบถ้วน และความน่าเชื่อถือของพยานหลักฐานตลอดระยะเวลาการจัดเก็บ เพื่อให้สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ
3) การใช้พยานหลักฐานต้องเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้องอย่างเคร่งครัด

5.29. การรักษาความปลอดภัยสารสนเทศระหว่างที่เกิดการหยุดชะงัก (Information security during disruption)

เพื่อคุ้มครองสารสนเทศในช่วงสถานการณ์ฉุกเฉินหรือการหยุดชะงักของระบบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) บูรณาการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้ในแผนการดำเนินงานด้านความต่อเนื่องของกรมฯ อย่างเหมาะสมและสอดคล้องกับบริบทขององค์กร
2) ต้องกำหนดขั้นตอนและแนวทางในการควบคุมเหตุการณ์ รวมถึงการฟื้นฟูระบบให้สามารถกลับสู่สภาพการให้บริการตามปกติได้อย่างมีประสิทธิภาพ
3) ต้องมีการทดสอบ ทบทวน และปรับปรุงแผนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถนำไปใช้งานได้จริงเมื่อเกิดสถานการณ์ฉุกเฉิน

5.30. ความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

เพื่อสนับสนุนการดำเนินภารกิจของกรมฯ ให้สามารถดำเนินต่อไปได้อย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการประเมินความพร้อมและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อรองรับการให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ
2) ต้องดำเนินการทดสอบและทบทวนแผนความต่อเนื่องอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนมีความเหมาะสมและสามารถนำไปใช้งานได้จริง
3) ต้องสื่อสารบทบาท หน้าที่ และขั้นตอนการปฏิบัติให้แก่ผู้ที่เกี่ยวข้องได้รับทราบอย่างชัดเจน เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องและสอดคล้องกัน
4) ต้องมีการจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้
    - มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องไว้อย่างชัดเจน
    - มีการประเมินความเสี่ยงสำหรับระบบสารสนเทศที่มีความสำคัญ พร้อมกำหนดมาตรการในการลดความเสี่ยงที่อาจเกิดขึ้น เช่น เหตุการณ์ไฟฟ้าดับเป็นเวลานาน อัคคีภัย หรือแผ่นดินไหว
    - มีการกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศอย่างเป็นระบบและเหมาะสม
    - มีการกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูล รวมถึงการทดสอบการกู้คืนข้อมูลจากระบบสำรองอย่างสม่ำเสมอ

- มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ผู้ให้บริการฮาร์ดแวร์ และซอฟต์แวร์ เพื่อรองรับกรณีเกิดเหตุฉุกเฉิน
- มีการดำเนินการสร้างความตระหนักและให้ความรู้แก่เจ้าหน้าที่ที่เกี่ยวข้องเกี่ยวกับขั้นตอนการปฏิบัติและแนวทางการดำเนินการเมื่อเกิดเหตุเร่งด่วน

5.31. ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา (Legal, statutory, regulatory and contractual requirements)

เพื่อให้การดำเนินงานด้านสารสนเทศเป็นไปตามกฎหมายและระเบียบของทางราชการ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการรวบรวมและทบทวนข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้องอย่างครบถ้วนและเป็นปัจจุบัน
2) ต้องสื่อสารข้อกำหนดที่เกี่ยวข้องให้แก่ผู้มีส่วนเกี่ยวข้องได้รับทราบอย่างทั่วถึง และกำกับดูแลให้มีการปฏิบัติตามอย่างเคร่งครัด
3) ต้องมีการติดตาม ตรวจสอบ และดำเนินการแก้ไขในกรณีที่พบความไม่สอดคล้อง เพื่อให้การดำเนินงานเป็นไปตามข้อกำหนดที่เกี่ยวข้องอย่างต่อเนื่อง

5.32. สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

เพื่อคุ้มครองสิทธิในทรัพย์สินทางปัญญาของกรมฯ และผู้อื่น กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การใช้ซอฟต์แวร์และผลงานที่มีลิขสิทธิ์ต้องเป็นไปตามกฎหมาย ระเบียบ และเงื่อนไขการใช้งานที่เกี่ยวข้องอย่างเคร่งครัด
2) ห้ามดำเนินการคัดลอก ดัดแปลง เผยแพร่ หรือใช้ประโยชน์จากผลงานที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์
3) ผลงาน ระบบสารสนเทศ หรือซอฟต์แวร์ที่จัดทำขึ้นภายใต้ภารกิจหรือสัญญาของกรมฯ ให้ถือเป็นทรัพย์สินทางปัญญาของกรมฯ เว้นแต่จะมีการกำหนดเป็นอย่างอื่นไว้เป็นลายลักษณ์อักษร

5.33. การป้องกันข้อมูล (Protection of records)

เพื่อคุ้มครองข้อมูลและบันทึกสารสนเทศจากการสูญหาย การทำลาย หรือการเข้าถึงโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กำหนดแนวทางในการจัดเก็บ การสำรอง และการทำลายข้อมูลให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้องอย่างเหมาะสม
2) จัดให้มีการควบคุมการเข้าถึงข้อมูลให้สอดคล้องกับบทบาทหน้าที่และระดับชั้นความลับของข้อมูล
3) กำหนดและดำเนินมาตรการคุ้มครองข้อมูล บันทึก ที่มีความสำคัญเพิ่มเติมตามระดับความเสี่ยงและความเหมาะสมของข้อมูล

5.34. ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of PII)

เพื่อคุ้มครองสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล กรมฯ กำหนดแนวทางในการปฏิบัติไว้ดังต่อไปนี้

1) บุคลากรของกรมฯ ผู้ปฏิบัติงานที่เกี่ยวข้อง รวมถึงผู้ให้บริการภายนอก ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด
2) บุคลากรของกรมฯ ผู้ปฏิบัติงานที่เกี่ยวข้อง รวมถึงผู้ให้บริการภายนอก ต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของกรมฯ ที่ประกาศใช้อย่างเคร่งครัด และติดตามการเปลี่ยนแปลงหรือการปรับปรุงนโยบายดังกล่าวอย่างต่อเนื่อง
3) ต้องกำหนดและดำเนินมาตรการควบคุม รวมถึงการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับระดับความเสี่ยงของข้อมูล
4) ผู้ให้บริการภายนอกต้องปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดไว้ในสัญญาอย่างเคร่งครัด

5.35. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

เพื่อประเมินความเหมาะสมและประสิทธิผลของมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) จัดให้มีการทบทวนโดยหน่วยงานหรือบุคคลที่มีความเป็นอิสระ เพื่อให้การประเมินมีความโปร่งใสและเป็นกลาง เช่น การทบทวนด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ด้านเทคนิค อาทิ การตรวจสอบระบบโดยผู้เชี่ยวชาญ (Technical Assessment) การทดสอบเจาะระบบ (Penetration Testing) หรือการประเมินช่องโหว่ (Vulnerability Assessment) รวมถึงด้านการปฏิบัติงานที่เกี่ยวข้อง
2) ต้องดำเนินการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มั่นใจว่าการดำเนินงานยังคงมีความเหมาะสมและสอดคล้องกับข้อกำหนด
3) ต้องรายงานผลการทบทวนต่อผู้บริหารอย่างเป็นทางการ พร้อมทั้งติดตามการดำเนินการแก้ไขข้อบกพร่องให้แล้วเสร็จอย่างมีประสิทธิภาพ

5.36. ความสอดคล้องกับนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with policies, rules and standards for information security)

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามนโยบายและมาตรฐานที่กำหนด กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ดำเนินการตรวจติดตามความสอดคล้องกับนโยบาย ระเบียบ และมาตรการที่กำหนดไว้อย่างสม่ำเสมอ
2) ดำเนินการแก้ไข ปรับปรุง และกำหนดมาตรการป้องกันอย่างเหมาะสม เมื่อพบกรณีไม่ปฏิบัติตามข้อกำหนด
3) การพิจารณาดำเนินมาตรการทางวินัยให้เป็นไปตามระเบียบของทางราชการที่เกี่ยวข้องอย่างเคร่งครัด

5.37. เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

เพื่อให้การปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างเป็นระบบ สม่ำเสมอ และตรวจสอบได้ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) คณะทำงาน หรือ หน่วยงานที่เกี่ยวข้องต้องจัดทำเอกสารขั้นตอนการปฏิบัติงานสำหรับกิจกรรมที่เกี่ยวข้องกับสารสนเทศและระบบสารสนเทศ โดยเฉพาะในกรณีดังต่อไปนี้
   - เมื่อกิจกรรมต้องดำเนินการในลักษณะเดียวกันโดยบุคลากรหลายราย
   - เมื่อกิจกรรมมีความถี่ในการปฏิบัติงานไม่สม่ำเสมอ หรือเกิดขึ้นเป็นครั้งคราว
   - เมื่อกิจกรรมเป็นกิจกรรมใหม่ หรือมีความเสี่ยงหากดำเนินการไม่ถูกต้อง
   - เมื่อมีการส่งมอบงานให้แก่บุคลากรใหม่ บุคคลอื่น หรือหน่วยงานอื่น
2) เอกสารต้องระบุรายละเอียดที่สำคัญ ได้แก่ ผู้รับผิดชอบ ขั้นตอนการปฏิบัติ มาตรการควบคุม และช่องทางการประสานงานอย่างชัดเจน
3) ต้องมีการทบทวนและปรับปรุงเอกสารให้เป็นปัจจุบันตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
4) ต้องจัดทำคู่มือการใช้งานระบบสารสนเทศ และเผยแพร่ให้ผู้ใช้งานสามารถเข้าถึงได้ผ่านช่องทางที่เหมาะสม เช่น เว็บไซต์ของหน่วยงาน

6. ส่วนที่ 2 นโยบายการบริหารจัดการทรัพยากรบุคคลด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Human Resource Management Policy)

กรมฯ กำหนดนโยบายการบริหารจัดการทรัพยากรบุคคลด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้บุคลากรทุกระดับมีความตระหนัก เข้าใจบทบาทหน้าที่ และปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ครอบคลุมตลอดวงจรการจ้างงาน ตั้งแต่ก่อนการจ้างงาน ระหว่างการปฏิบัติงาน จนถึงเมื่อสิ้นสุดหรือมีการเปลี่ยนแปลงการจ้างงาน

6.1. มาตรการก่อนการจ้างงาน (Screening)

เพื่อให้มั่นใจว่าบุคลากรที่ได้รับการคัดเลือกมีความเหมาะสมต่อการปฏิบัติงานที่เกี่ยวข้องกับสารสนเทศและระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กองบริหารทรัพยากรบุคคล มีหน้าที่ดำเนินการตรวจสอบคุณสมบัติ ประวัติ และความเหมาะสมของผู้สมัคร ตามระเบียบและหลักเกณฑ์ของทางราชการ
2) กรณีตำแหน่งงานที่เกี่ยวข้องกับสารสนเทศสำคัญหรือระบบที่มีความเสี่ยงสูง ให้ประสานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อพิจารณามาตรการเพิ่มเติมตามความเหมาะสม
3) การตรวจสอบต้องดำเนินการโดยคำนึงถึงกฎหมาย สิทธิ และความเป็นส่วนตัวของผู้สมัคร

6.2. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรให้ชัดเจนตั้งแต่เริ่มต้นการจ้างงาน และสร้างความเข้าใจร่วมกันในการปฏิบัติตามนโยบายและระเบียบของกรมฯ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กองบริหารทรัพยากรบุคคลร่วมกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้ข้อตกลงหรือเงื่อนไขการจ้างงานระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้ชัดเจน
2) บุคลากรต้องรับทราบและยินยอมปฏิบัติตามนโยบาย ระเบียบ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ
3) กองบริหารทรัพยากรบุคคล ต้องกำหนดมาตรการหรือบทลงโทษกรณีฝ่าฝืนนโยบายให้เป็นไปตามระเบียบของทางราชการ

6.3. การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

เพื่อเสริมสร้างความรู้ ความเข้าใจ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรทุกระดับ ให้สามารถปฏิบัติงานได้อย่างถูกต้อง ลดความเสี่ยงจากการกระทำโดยไม่เจตนา และสนับสนุนการรักษาความมั่นคงปลอดภัยสารสนเทศของกรมฯ อย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กองบริหารทรัพยากรบุคคล ร่วมกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดให้มีการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ (Security Awareness) แก่บุคลากรทุกระดับ รวมทั้งจัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

พร้อมทั้งดำเนินการติดตามและประเมินผลการฝึกอบรม ตลอดจนสำรวจและรวบรวมความต้องการของผู้ใช้งานอย่างสม่ำเสมอ เพื่อนำไปปรับปรุงและพัฒนาการดำเนินงานให้มีประสิทธิภาพยิ่งขึ้น

2) การให้ความรู้และการฝึกอบรมต้องสอดคล้องกับบทบาทหน้าที่ ระดับความรับผิดชอบ และความเสี่ยงของการปฏิบัติงานของบุคลากรแต่ละกลุ่ม
3) กรณีมีการเปลี่ยนแปลงนโยบาย มาตรการ เทคโนโลยี หรือพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่มีนัยสำคัญ ต้องพิจารณาจัดกิจกรรมเสริมสร้างความตระหนักหรือการฝึกอบรมเพิ่มเติมตามความเหมาะสม
4) ต้องมีการบันทึกและจัดเก็บข้อมูลการเข้าร่วมกิจกรรม การฝึกอบรม หรือการสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้เป็นหลักฐานในการติดตามและประเมินผล

6.4. กระบวนการทางวินัย (Disciplinary process)

เพื่อให้การบังคับใช้นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างมีประสิทธิภาพ เป็นธรรม และสอดคล้องกับระเบียบของทางราชการ เมื่อเกิดการฝ่าฝืนหรือไม่ปฏิบัติตามที่กำหนด กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการพิจารณาและบังคับใช้มาตรการทางวินัยตาม กฎหมาย ระเบียบ และหลักเกณฑ์ของกรมฯ โดยให้กองบริหารทรัพยากรบุคคลทำหน้าที่กำหนดแนวทาง หลักเกณฑ์ และบทลงโทษที่เกี่ยวข้อง รวมถึงประสานงานกับหน่วยงานที่มีอำนาจหน้าที่ตามระเบียบที่เกี่ยวข้อง หรือหน่วยงานที่มีหน้าที่รับผิดชอบ
2) การดำเนินการทางวินัยต้องเป็นไปอย่างเป็นธรรม โปร่งใส ได้สัดส่วนกับลักษณะการกระทำ และสามารถตรวจสอบได้
3) ต้องมีการบันทึกและจัดเก็บผลการดำเนินการทางวินัยไว้เป็นหลักฐาน เพื่อใช้ในการตรวจสอบ ติดตาม และอ้างอิงตามระเบียบของทางราชการ

6.5. มาตรการเมื่อสิ้นสุดและเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)

เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้นจากการเปลี่ยนแปลงสถานะการจ้างงาน และเพื่อให้การจัดการสิทธิการเข้าถึง ทรัพย์สิน และข้อมูลของกรมฯ เป็นไปอย่างเหมาะสมและทันเวลา กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กองบริหารทรัพยากรบุคคล ต้องแจ้งข้อมูลการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานแก่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยทันที
2) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องดำเนินการเพิกถอนหรือปรับปรุงสิทธิการเข้าถึงระบบและข้อมูลให้สอดคล้องกับสถานะการจ้างงาน
3) บุคลากรต้องคืนทรัพย์สินและข้อมูลของกรมให้แก่หน่วยงานต้นสังกัด และแจ้งผู้อำนวยการหน่วยงานนั้น ๆ

6.6. ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

เพื่อคุ้มครองข้อมูล สารสนเทศ และข้อมูลสำคัญของกรมฯ จากการเปิดเผย การนำไปใช้ หรือการเผยแพร่โดยมิชอบ ทั้งในระหว่างและภายหลังการปฏิบัติงาน กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กองบริหารทรัพยากรบุคคล ต้องดำเนินการให้บุคลากรและผู้เกี่ยวข้องจัดทำข้อตกลงการรักษาความลับตามที่กำหนด
2) ข้อผูกพันด้านการรักษาความลับให้มีผลบังคับใช้ทั้งระหว่างและภายหลังสิ้นสุดการจ้างงาน
3) การฝ่าฝืนข้อตกลงให้ดำเนินการตามกฎหมายและระเบียบที่เกี่ยวข้อง

6.7. การปฏิบัติงานจากระยะไกล (Remote working)

เพื่อกำหนดแนวทางและมาตรการควบคุมให้การปฏิบัติงานจากระยะไกลเป็นไปอย่างมั่นคงปลอดภัย ลดความเสี่ยงด้านสารสนเทศ และสนับสนุนการปฏิบัติงานของกรมฯ อย่างมีประสิทธิภาพ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) หน่วยงานต้นสังกัดพิจารณาและอนุญาตการปฏิบัติงานจากระยะไกลตามหลักเกณฑ์ที่กรมบังคับคดีกำหนด
2) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดมาตรการควบคุมด้านเทคนิคที่เหมาะสม
3) ผู้ปฏิบัติงานต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
4) ให้มีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน
5) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
6) การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียด ดังนี้
   - เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน
   - รายละเอียดและลักษณะของระบบงาน
   - ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก
   - รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน
   - ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน
7) ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับ ชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด
8) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากระยะไกล ต้องมีการลงบันทึกการเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านร่วมกับการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนการเข้าใช้งานทุกครั้ง

9) ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานโดยไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้
10) ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที
11) ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานจากภายนอกหน่วยงานแก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
12) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

6.8. การรายงานเหตุการณ์การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

เพื่อให้สามารถตรวจพบ แจ้งเตือน และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างทันท่วงที ลดผลกระทบที่อาจเกิดขึ้น และสนับสนุนการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ อย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) บุคลากรต้องรายงานเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัยสารสนเทศตามช่องทางที่กำหนด
2) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องติดตาม วิเคราะห์ และดำเนินการจัดการเหตุการณ์ตามขั้นตอนที่กำหนด

7. นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security Policy)

กรมฯ กำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม เพื่อคุ้มครองอาคาร สถานที่ อุปกรณ์ ระบบสารสนเทศ และทรัพย์สินที่เกี่ยวข้อง จากการเข้าถึง การใช้งาน หรือความเสียหายโดยมิชอบ รวมถึงลดความเสี่ยงจากภัยคุกคามด้านสิ่งแวดล้อม อันอาจส่งผลกระทบต่อความต่อเนื่องในการปฏิบัติภารกิจของกรมฯ

7.1. ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeters)

เพื่อกำหนดและควบคุมขอบเขตพื้นที่ทางกายภาพที่เกี่ยวข้องกับการปฏิบัติงาน ระบบสารสนเทศ และทรัพย์สินสำคัญของกรมฯ ให้มีความชัดเจน ลดความเสี่ยงจากการเข้าถึงหรือการกระทำโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดขอบเขตพื้นที่ทางกายภาพของอาคาร ห้องปฏิบัติงาน และพื้นที่ที่เกี่ยวข้องกับระบบสารสนเทศให้ชัดเจน
2) พื้นที่ที่มีความสำคัญหรือมีความเสี่ยงสูงต้องกำหนดมาตรการควบคุมเพิ่มเติมตามความเหมาะสม
3) ต้องทบทวนขอบเขตและมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมหรือการใช้งานพื้นที่
4) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงานพื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบสารสนเทศ หรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย

7.2. การควบคุมการเข้าออกทางกายภาพ (Physical entry)

เพื่อให้การเข้าออกอาคารและพื้นที่สำคัญของกรมฯ เป็นไปตามสิทธิและหน้าที่ของผู้เกี่ยวข้อง และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) บทบาทและความรับผิดชอบการควบคุมการเข้า–ออกห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
   - ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
     - อนุมัติสิทธิ์การเข้า–ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
     - อนุมัติกระบวนการควบคุมการเข้า–ออกของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
2) กระบวนการควบคุมการเข้า–ออกห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
   - ผู้ดูแลระบบ และเจ้าหน้าที่ มีแนวทางปฏิบัติดังนี้
     - ผู้ดูแลระบบ มีการจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนของห้องเซิร์ฟเวอร์ (Server) ห้องทำงาน ห้องอบรมคอมพิวเตอร์ เป็นต้น เพื่อสะดวกในการปฏิบัติงานและการควบคุมดูแลให้มีประสิทธิภาพยิ่งขึ้น

- ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องมีการกำหนดสิทธิ์บุคคลในการเข้า–ออก
- สิทธิ์ในการเข้า–ออกห้องต่างๆ ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยสิทธิ์ของเจ้าหน้าที่แต่ละคนจะขึ้นอยู่กับหน้าที่ที่ต้องปฏิบัติหรือได้รับคำสั่งเท่านั้น
- เจ้าหน้าที่ทุกคนต้องใช้ระบบ Face Scan ในการเข้า–ออกศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และห้องควบคุมระบบคอมพิวเตอร์
- ต้องจัดทำระบบเก็บบันทึกการเข้า–ออกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและห้องควบคุมระบบคอมพิวเตอร์

3) ต้องควบคุมการเข้าออกพื้นที่ตามบทบาทหน้าที่และระดับความรับผิดชอบ
4) บุคคลภายนอกต้องได้รับอนุญาตและอยู่ภายใต้การควบคุมดูแลระหว่างอยู่ในพื้นที่
5) พื้นที่สำคัญต้องมีมาตรการบันทึกหรือการตรวจสอบการเข้าออกตามความเหมาะสม
6) ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร
7) ในกรณีที่หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงานจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

7.3. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่างๆ (Securing offices, rooms and facilities)

เพื่อคุ้มครองสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกของกรมฯ จากการบุกรุก ความเสียหาย หรือการใช้งานโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องจัดให้สำนักงานและห้องปฏิบัติงานมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม สอดคล้องกับลักษณะการใช้งานและระดับความสำคัญของพื้นที่
2) ห้องที่ใช้จัดเก็บอุปกรณ์หรือข้อมูลที่มีความสำคัญต้องได้รับการควบคุมการเข้า–ออกเป็นกรณีพิเศษ โดยกำหนดมาตรการควบคุมอย่างเหมาะสม
3) ต้องกำหนดผู้รับผิดชอบในการดูแลและกำกับด้านความมั่นคงปลอดภัยของแต่ละพื้นที่อย่างชัดเจน

7.4. การติดตามตรวจสอบความปลอดภัยทางกายภาพ (Physical security monitoring)

เพื่อให้สามารถเฝ้าระวัง ตรวจพบ และติดตามเหตุผิดปกติด้านความมั่นคงปลอดภัยทางกายภาพได้อย่างเหมาะสม กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องมีการตรวจสอบและเฝ้าระวังพื้นที่สำคัญให้สอดคล้องกับระดับความเสี่ยงอย่างสม่ำเสมอ
2) การตรวจสอบและเฝ้าระวังอาจดำเนินการโดยใช้มาตรการด้านบุคลากรหรือเทคโนโลยีตามความเหมาะสม เช่น การจัดเจ้าหน้าที่รักษาความปลอดภัย การติดตั้งระบบกล้องวงจรปิด (CCTV) ระบบควบคุมการเข้า–ออก (Access Control) หรือระบบแจ้งเตือนภัย

3) นำผลการตรวจสอบและเฝ้าระวังมาวิเคราะห์และใช้ในการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น

7.5. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against physical and environmental threats)

เพื่อป้องกันและลดผลกระทบจากภัยคุกคามด้านสิ่งแวดล้อมที่อาจส่งผลต่อระบบสารสนเทศและการดำเนินภารกิจของกรมฯ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ดำเนินการประเมินความเสี่ยงจากภัยคุกคามด้านสิ่งแวดล้อมอย่างเหมาะสม เช่น อัคคีภัย น้ำท่วม ไฟฟ้าดับ แผ่นดินไหว หรือเหตุการณ์ทางธรรมชาติอื่น ๆ ที่อาจส่งผลกระทบต่อการดำเนินงาน
2) กำหนดมาตรการป้องกัน รวมถึงจัดทำแผนรองรับเหตุฉุกเฉิน เพื่อรองรับและลดผลกระทบจากเหตุการณ์ดังกล่าวอย่างมีประสิทธิภาพ
3) เชื่อมโยงมาตรการด้านสิ่งแวดล้อมเข้ากับแผนความต่อเนื่องของกรมฯ เพื่อให้สามารถรองรับและฟื้นฟูการดำเนินงานได้อย่างต่อเนื่อง เช่น การจัดให้มีแหล่งพลังงานสำรอง (Generator/UPS) การกำหนดสถานที่ปฏิบัติงานสำรอง (Alternate Site) การจัดเตรียมอุปกรณ์ทดแทน และการกำหนดขั้นตอนการกู้คืนระบบภายหลังเกิดเหตุการณ์ฉุกเฉิน

7.6. การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

เพื่อควบคุมการปฏิบัติงานในพื้นที่ที่มีความสำคัญหรือมีความเสี่ยงสูง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ดังต่อไปนี้

1) ผู้ปฏิบัติงานต้องได้รับอนุญาตก่อนเข้าปฏิบัติงานในพื้นที่ควบคุม โดยเป็นไปตามสิทธิ์และหน้าที่ที่ได้รับมอบหมาย
2) ต้องกำหนดแนวปฏิบัติในการนำอุปกรณ์หรือข้อมูลเข้า–ออกพื้นที่ควบคุมอย่างชัดเจน และมีการตรวจสอบตามความเหมาะสม
3) บุคคลภายนอกที่เข้ามาปฏิบัติงานหรือเข้าพื้นที่ต้องอยู่ภายใต้การควบคุมและการดูแลของผู้รับผิดชอบตลอดระยะเวลาที่อยู่ในพื้นที่ดังกล่าว

7.7. การจัดโต๊ะทำงานให้เป็นระเบียบเรียบร้อยและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)

เพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ตั้งใจจากเอกสารหรือหน้าจอคอมพิวเตอร์ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องจัดเก็บเอกสารและสื่อบันทึกข้อมูลให้อยู่ในสถานที่ที่เหมาะสมและปลอดภัยเมื่อไม่ใช้งาน เช่น การเก็บเอกสารในตู้ที่สามารถล็อกได้ การจัดเก็บสื่อบันทึกข้อมูลในพื้นที่ควบคุม หรือการจัดเก็บในระบบที่มีการควบคุมสิทธิ์การเข้าถึง
2) ต้องป้องกันไม่ให้ข้อมูลบนหน้าจอคอมพิวเตอร์หรืออุปกรณ์แสดงผลถูกมองเห็นโดยบุคคลที่ไม่เกี่ยวข้อง เช่น การตั้งค่าล็อกหน้าจออัตโนมัติ หรือการจัดวางอุปกรณ์ให้เหมาะสม
3) ต้องปฏิบัติตามแนวทางการใช้งานพื้นที่ทำงานที่กรมฯ กำหนดอย่างเคร่งครัด เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินสารสนเทศ

4) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสารสนเทศ เช่น เอกสารสื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(1) กำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ เช่น
- การจัดการบริเวณโดยรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่ปลอดภัย

(2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้
- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(3) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(4) มีการกำหนดขอบเขตการป้องกัน ดังนี้
- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันรหัสโทรสาร เมื่อไม่ได้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันมิให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องถ่ายสำเนาเอกสาร เครื่องแสกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(5) การควบคุมการใช้งาน
- ตรวจสอบรายชื่อผู้เข้าอาคาร
- ลงชื่อผู้ขอปฏิบัติงานนอกเวลาและเบิกกุญแจห้องที่ฝ่ายพัสดุ
- ใช้ AD ควบคุม Policy การใช้งาน

5) เมื่อมีการว่างเว้นจากการใช้งานระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(1) มีการกำหนดให้ล็อกหน้าจอคอมพิวเตอร์โดยอัตโนมัติเมื่อไม่มีการใช้งานภายในระยะเวลา 15 นาที หรือเป็นไปตามระยะเวลาที่กรมฯ กำหนด

(2) หลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ (Session Timeout) เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา เช่น 15 นาทีตามความ

เหมาะสม หรือเป็นไปตามระยะเวลาที่กรมฯ กำหนด เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(3) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(4) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามกำหนด

7.8. การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

เพื่อให้อุปกรณ์ได้รับการจัดวางและป้องกันอย่างเหมาะสม ลดความเสี่ยงจากความเสียหายหรือการเข้าถึงโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) จัดวางอุปกรณ์ในตำแหน่งที่เหมาะสม ปลอดภัย และสอดคล้องกับลักษณะการใช้งาน เช่น การจัดระเบียบสายสัญญาณให้เรียบร้อย การติดตั้งอุปกรณ์ในตู้ Rack หรือพื้นที่ควบคุม เพื่อลดความเสี่ยงจากความเสียหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
2) กำหนดมาตรการควบคุมเพื่อป้องกันการเคลื่อนย้าย การสูญหาย หรือการใช้งานอุปกรณ์โดยไม่ได้รับอนุญาตอย่างเหมาะสม
3) พิจารณาสภาพแวดล้อมที่อาจส่งผลกระทบต่ออุปกรณ์ เช่น อุณหภูมิ ความชื้น ฝุ่นละออง ไฟฟ้าสถิต ไฟฟ้าดับหรือไฟกระชาก และกำหนดมาตรการป้องกันที่เหมาะสม
4) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์
5) ไม่ปล่อยให้อุปกรณ์หรือทรัพย์สินของหน่วยงานอยู่โดยไม่มีผู้ดูแลในที่สาธารณะ เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
6) สร้างจิตสำนึกให้เจ้าหน้าที่รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

7.9. ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of assets off-premises)

เพื่อคุ้มครองอุปกรณ์และทรัพย์สินของกรมฯ ที่นำไปใช้งานนอกสถานที่ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องได้รับอนุญาตจากผู้มีอำนาจก่อนนำอุปกรณ์ออกนอกสถานที่ของหน่วยงาน
2) ผู้ใช้งานต้องรับผิดชอบต่อความปลอดภัยของอุปกรณ์และข้อมูลที่อยู่ในความครอบครองตลอดระยะเวลาการใช้งาน
3) ต้องกำหนดมาตรการเพื่อลดความเสี่ยงจากการสูญหาย การชำรุดเสียหาย หรือการเข้าถึงข้อมูลโดยมิชอบอย่างเหมาะสม
4) ต้องกำหนดผู้มีอำนาจในการอนุมัติการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากหน่วยงานอย่างชัดเจน
5) ต้องกำหนดระยะเวลาในการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน พร้อมทั้งมีการติดตามและควบคุมการใช้งานตามระยะเวลาที่กำหนด
6) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

7) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

7.10. สื่อจัดเก็บข้อมูล (Storage media)

เพื่อควบคุมการจัดการสื่อจัดเก็บข้อมูลให้เหมาะสมกับระดับความสำคัญของข้อมูล กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องมีการควบคุมการใช้ การจัดเก็บ และการเคลื่อนย้ายสื่อบันทึกข้อมูลอย่างเหมาะสม เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
2) สื่อบันทึกข้อมูลที่มีความสำคัญต้องได้รับการคุ้มครองเป็นกรณีพิเศษ เช่น การเข้ารหัสข้อมูล (Encryption) การจัดเก็บในพื้นที่ควบคุม การจำกัดสิทธิ์การเข้าถึง หรือการติดป้ายกำกับระดับชั้นความลับ โดยกำหนดมาตรการป้องกันตามระดับความสำคัญของข้อมูล
3) การจัดการสื่อบันทึกข้อมูลต้องสอดคล้องกับนโยบายการจัดการข้อมูลตามชั้นความลับของสารสนเทศ (Classification of information) ของกรมฯ อย่างเคร่งครัด
4) ต้องจัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และมีการควบคุมอย่างเหมาะสม
5) ต้องมีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ โดยให้สิทธิ์เฉพาะผู้ที่เกี่ยวข้องหรือผู้เป็นเจ้าของระบบเท่านั้น
6) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น
7) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

7.11. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

เพื่อให้ระบบและอุปกรณ์สนับสนุนมีความพร้อมใช้งานและรองรับการดำเนินงานของกรมฯ อย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องจัดให้มีระบบสนับสนุนที่เหมาะสมและเพียงพอต่อการใช้งาน เพื่อรองรับการดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น ระบบไฟฟ้าสำรอง (UPS/Generator) ระบบปรับอากาศสำหรับห้องศูนย์ข้อมูล ระบบเครือข่ายสื่อสารสำรอง หรือระบบสำรองข้อมูล (Backup System)
2) ต้องดำเนินการบำรุงรักษา ตรวจสอบ และทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้ระบบมีความพร้อมใช้งานอยู่เสมอ
3) ต้องจัดทำแผนรองรับกรณีระบบสนับสนุนขัดข้อง เพื่อให้สามารถดำเนินการแก้ไขและฟื้นฟูระบบได้อย่างทันท่วงที
4) ต้องมีระบบรองรับสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้
    - เครื่องกำเนิดกระแสไฟฟ้าสำรอง
    - ระบบน้ำหรือเครื่องดับเพลิงระบบปรับอากาศและควบคุมความชื้น

5) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้สามารถมั่นใจได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
6) ต้องติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

7.12. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

เพื่อป้องกันความเสียหายหรือการดัดแปลงสายสัญญาณที่อาจส่งผลต่อระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องจัดวางและป้องกันสายสัญญาณให้มีความเหมาะสม ปลอดภัย และเป็นระเบียบ เพื่อลดความเสี่ยงจากความเสียหายหรือการถูกดัดแปลงโดยไม่ได้รับอนุญาต
2) ต้องจำกัดการเข้าถึงจุดเชื่อมต่อสายสัญญาณในพื้นที่สำคัญ โดยกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม
3) ต้องมีการตรวจสอบสภาพสายสัญญาณอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถใช้งานได้อย่างมีประสิทธิภาพและปลอดภัย
4) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้
5) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย
6) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
7) ทำป้ายชื่อสำหรับสายสัญญาณและอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
8) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง
9) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ให้มีการปิดใส่กุญแจ เพื่อป้องกันการเข้าถึงของบุคคลภายนอก
10) พิจารณาใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ
11) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณ โดยผู้ไม่ประสงค์ดี

7.13. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

เพื่อให้อุปกรณ์อยู่ในสภาพพร้อมใช้งานอย่างปลอดภัยและไม่กระทบต่อข้อมูล กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการบำรุงรักษาอุปกรณ์ตามแผนที่กำหนด และตามแนวทางหรือคำแนะนำที่เหมาะสม เพื่อให้ระบบสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ
2) การบำรุงรักษาต้องดำเนินการโดยไม่ก่อให้เกิดความเสี่ยงต่อข้อมูลหรือระบบสารสนเทศ และต้องมีมาตรการป้องกันผลกระทบที่อาจเกิดขึ้น
3) บุคคลภายนอกที่เข้าดำเนินการบำรุงรักษาต้องอยู่ภายใต้การควบคุมและการกำกับดูแลของผู้รับผิดชอบตลอดระยะเวลาการปฏิบัติงาน

4) ต้องกำหนดรอบระยะเวลาการบำรุงรักษาอุปกรณ์ให้สอดคล้องกับข้อกำหนดหรือคำแนะนำของผู้ผลิตอย่างเหมาะสม
5) ต้องปฏิบัติตามแนวทางและข้อกำหนดในการบำรุงรักษาอุปกรณ์ตามที่ผู้ผลิตกำหนดอย่างเคร่งครัด
6) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง
7) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
8) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน
9) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7.14. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure disposal or re-use of equipment)

เพื่อป้องกันการรั่วไหลของข้อมูลจากอุปกรณ์ที่เลิกใช้งานหรือถูกนำกลับมาใช้ใหม่ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถกู้คืนได้ก่อนการกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ เพื่อป้องกันการรั่วไหลของข้อมูล
2) ปฏิบัติตามขั้นตอนปฏิบัติงานด้านการจัดระดับชั้นความลับ การจัดทำป้ายกำกับ และการจัดการสื่อบันทึกข้อมูลที่กรมฯ กำหนดอย่างเคร่งครัด
3) การกำจัดอุปกรณ์ต้องเป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดของกรมฯ ที่เกี่ยวข้องอย่างถูกต้องครบถ้วน
4) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์ ดังนี้
    (1) ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลาย
    (2) ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DAT จะต้องทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป
5) กำหนดให้มีการทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว
6) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

8. ส่วนที่ 4 นโยบายการควบคุมและบริหารจัดการเทคโนโลยีสารสนเทศและระบบสารสนเทศ (Information Technology and Information System Controls Policy)

กรมฯ กำหนดนโยบายการควบคุมและบริหารจัดการเทคโนโลยีสารสนเทศและระบบสารสนเทศ เพื่อให้การบริหารจัดการ การใช้งาน และการดูแลรักษาสารสนเทศ ระบบสารสนเทศ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างมั่นคงปลอดภัย เหมาะสมกับภารกิจและบริบทของหน่วยงาน สามารถป้องกัน ลดความเสี่ยง และรองรับการปฏิบัติงานของกรมฯ ได้อย่างมีประสิทธิภาพและต่อเนื่อง

8.1. ความมั่นคงปลอดภัยสำหรับอุปกรณ์ปลายทางผู้ใช้งาน (User endpoint devices)

เพื่อคุ้มครองอุปกรณ์ปลายทางของผู้ใช้งานจากการเข้าถึง การใช้งาน หรือความเสียหายโดยมิชอบ และลดความเสี่ยงที่อาจส่งผลกระทบต่อสารสนเทศและระบบสารสนเทศของกรมฯ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ดังต่อไปนี้

1) ข้อกำหนดทั่วไปข้อกำหนดทั่วไปสำหรับการจัดการอุปกรณ์ผู้ใช้งาน

(1.1) อุปกรณ์ปลายทางต้องได้รับการกำหนดค่าความมั่นคงปลอดภัยตามมาตรฐานของกรมฯ

(1.2) ต้องมีมาตรการควบคุมการใช้งาน การติดตั้งซอฟต์แวร์ และการเชื่อมต่อเครือข่าย

(1.3) ต้องมีมาตรการป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(1.4) ไม่อนุญาตให้บุคลากรนำอุปกรณ์เคลื่อนที่หรือคอมพิวเตอร์แบบพกพาส่วนบุคคลมาใช้ในการปฏิบัติงานของกรมฯ เว้นแต่จะได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารตามหลักเกณฑ์ที่กำหนด

(1.5) อุปกรณ์ผู้ใช้งานทุกเครื่องต้องมีการปิดหรือจำกัดการใช้งานฟังก์ชันที่ไม่จำเป็นต่อการปฏิบัติงาน เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

(1.6) ต้องกำหนดให้มีการล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานตามระยะเวลาที่กำหนด (Idle Timeout)

(1.7) ต้องมีการยืนยันตัวตนของผู้ใช้งานทุกครั้งก่อนการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

(1.8) ผู้ใช้งานต้องใช้งานอุปกรณ์หรือทรัพย์สินด้านสารสนเทศอย่างถูกต้องเหมาะสมตามประเภทและคุณสมบัติที่ผู้ผลิตกำหนด และให้สอดคล้องกับนโยบาย ระเบียบ และกฎหมายที่เกี่ยวข้องของกรมฯ ทั้งนี้ ห้ามนำอุปกรณ์หรือทรัพย์สินดังกล่าวไปใช้ในกิจกรรมส่วนตัว หรือกิจกรรมที่อาจก่อให้เกิดการฝ่าฝืนนโยบาย ระเบียบ หรือกฎหมาย

2) การป้องกันข้อมูลและการเข้าถึงของอุปกรณ์คอมพิวเตอร์แบบพกพา

(2.1) อุปกรณ์คอมพิวเตอร์แบบพกพาต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งในด้านกายภาพและด้านเทคนิค

(2.2) ห้ามปรับเปลี่ยนหรือแก้ไขการตั้งค่าระบบ (Configuration) ที่อาจส่งผลกระทบต่อการทำงานของอุปกรณ์ หรือก่อให้เกิดความเสี่ยงต่อระบบสารสนเทศของกรมฯ

(2.3) ต้องติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (Anti-Malware) และปรับปรุงฐานข้อมูลภัยคุกคามให้เป็นปัจจุบันอย่างสม่ำเสมอ

(2.4) ต้องจัดให้มีการสำรองข้อมูลสารสนเทศที่จัดเก็บอยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพาไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรือพื้นที่จัดเก็บข้อมูลที่กรมฯ กำหนด

(2.5) ข้อมูลสารสนเทศที่สำรองไว้บนสื่อบันทึกพกพาต้องได้รับการคุ้มครองตามหลักเกณฑ์การจัดประเภทข้อมูล การบ่งชี้ข้อมูล และการจัดการข้อมูลของกรมฯ

(2.6) เมื่อสื่อบันทึกพกพาไม่มีความจำเป็นต้องใช้งาน ข้อมูลสารสนเทศต้องถูกลบหรือทำลายอย่างปลอดภัยตามมาตรฐานและวิธีการกำจัดสื่อที่กรมฯ กำหนด

(2.7) ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้งานหรือเข้าถึงอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ของสำนักงานที่ตนรับผิดชอบ เว้นแต่เป็นการดำเนินการเพื่อแก้ไขปัญหาทางเทคนิคโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย

3) การควบคุมอุปกรณ์นอกสถานที่

(3.1) ผู้ใช้งานต้องเพิ่มความระมัดระวังในการใช้งานอุปกรณ์นอกสถานที่ และต้องป้องกันไม่ให้บุคคลอื่นสามารถมองเห็นข้อมูลบนหน้าจอในที่สาธารณะ (Screen Privacy)

4) การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(4.1) เครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้จะต้องนำมาลงทะเบียนที่ศูนย์ก่อน ซึ่งจะมีการกำหนดชื่อเครื่อง เพื่อง่ายต่อการตรวจสอบ หากก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ของหน่วยงาน

(4.2) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(4.3) ไม่อนุญาตให้ ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(4.4) การตั้งชื่อเครื่องคอมพิวเตอร์จะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เท่านั้น

(4.5) ห้ามคัดลอกโปรแกรมต่างๆ ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานซึ่งมีลิขสิทธิ์ถูกต้องตามกฎหมาย นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(4.6) การเคลื่อนย้ายจุดติดตั้งหรือตรวจซ่อมคอมพิวเตอร์จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เท่านั้น

(4.7) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเครื่องไวรัสโดยโปรแกรมป้องกันไวรัส ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ใช้งานอยู่

(4.8) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอคอมพิวเตอร์หรือ Disk Drive

5) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(5.1) อุปกรณ์สื่อสารเคลื่อนที่ (mobile computing) ผู้ดูแลระบบต้องตรวจสอบและดำเนินการเปิดสิทธิการใช้งาน โดยเพิ่มค่า Mac Address ของอุปกรณ์สื่อสารดังกล่าว ในระบบควบคุมการใช้งาน และแจ้งกลับผู้ที่ขออนุญาตใช้งานทราบเป็นลายลักษณ์อักษร

(5.2) กำหนดให้มีการจัดเก็บ Mac Address พร้อมรายละเอียดผู้ใช้งาน โดยมีระบบรองรับในการตรวจสอบ

(5.3) กำหนดสิทธิ์การเข้าระบบว่าผู้สามารถเข้าถึงข้อมูลและระบบใดได้บ้าง เพียงใด

(5.4) ผู้มีสิทธิเข้าใช้งานได้จะต้องได้รับการอนุมัติหรืออนุญาตจาก DCIO

(5.5) ผู้ดูแลระบบด้านเครือข่ายมีหน้าที่ตรวจสอบการเข้าใช้งานและผู้บุกรุกที่พยายามเข้าใช้งานโดยไม่ได้รับอนุญาต และรายงาน DCIO ทราบ

(5.6) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลความลับด้วยอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

6) การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

(6.1) ผู้ใช้งานต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศโดยทันทีต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เช่น กรณีอุปกรณ์สูญหาย อุปกรณ์ถูกขโมย หรือพบการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต

8.2. การบริหารจัดการสิทธิการเข้าถึงสิทธิพิเศษ (Privileged access rights)

เพื่อควบคุมและลดความเสี่ยงจากการใช้สิทธิพิเศษที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การให้สิทธิพิเศษต้องได้รับการอนุมัติจากผู้มีอำนาจตามขั้นตอนที่กำหนดไว้อย่างชัดเจน
2) ต้องจำกัดการใช้สิทธิพิเศษให้เฉพาะเท่าที่จำเป็นต่อการปฏิบัติหน้าที่ เพื่อลดความเสี่ยงในการใช้งานโดยมิชอบ
3) ต้องมีการทบทวนและตรวจสอบการใช้สิทธิพิเศษอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานเป็นไปอย่างเหมาะสมและสอดคล้องกับข้อกำหนด

8.3. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

เพื่อให้การเข้าถึงสารสนเทศเป็นไปตามหลักความจำเป็นต่อการปฏิบัติหน้าที่ และลดความเสี่ยงจากการเข้าถึงข้อมูลโดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดสิทธิการเข้าถึงให้สอดคล้องกับบทบาทหน้าที่และระดับความรับผิดชอบของผู้ใช้งาน (Role-Based Access Control) อย่างเหมาะสม
2) ต้องควบคุมการเข้าถึงข้อมูลให้เป็นไปตามระดับความสำคัญและชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
3) ต้องมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้อง เพื่อให้สิทธิ์มีความถูกต้องและเป็นปัจจุบัน
4) กรมกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน ดังนี้
   - ระดับผู้บริหาร ดูข้อมูล/พิจารณาอนุมัติหรือรับทราบ (เฉพาะระบบที่อยู่ในความรับผิดชอบ)
   - ระดับผู้อำนวยการ ดูข้อมูล/แก้ไขข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)
   - ระดับหัวหน้างาน ดูข้อมูล/แก้ไขข้อมูล/ลบข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)
   - ระดับปฏิบัติงาน ดูข้อมูล/เพิ่มข้อมูล (เฉพาะระบบที่อยู่ในความรับผิดชอบ)

8.4. การควบคุมการเข้าถึงซอร์สโค้ด (Access to source code)

เพื่อป้องกันการเข้าถึง แก้ไข หรือเปิดเผยซอร์สโค้ดโดยมิชอบ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ซอร์สโค้ด (Source Code) ของระบบต้องได้รับการควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันการเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต
2) การเข้าถึงต้องได้รับการอนุมัติจากผู้มีอำนาจ และต้องสามารถตรวจสอบย้อนหลังได้ (Traceability)
3) ต้องมีการจัดเก็บและสำรองซอร์สโค้ดอย่างปลอดภัย โดยกำหนดมาตรการป้องกันการสูญหายหรือความเสียหายของข้อมูลอย่างเหมาะสม

8.5. การรักษาความมั่นคงปลอดภัยสำหรับการยืนยันตัวตน (Secure authentication)

เพื่อให้กระบวนการยืนยันตัวตนมีความมั่นคงปลอดภัย เหมาะสมกับระดับความเสี่ยง และป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องใช้กลไกการยืนยันตัวตนที่เหมาะสมกับลักษณะของระบบและระดับความสำคัญของข้อมูล เช่น การใช้รหัสผ่านที่มีความซับซ้อน หรือการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)
2) ต้องมีมาตรการป้องกันการเปิดเผยข้อมูลยืนยันตัวตน เช่น การจัดเก็บข้อมูลอย่างปลอดภัย และการไม่เปิดเผยรหัสผ่านหรือข้อมูลสำคัญแก่ผู้อื่น
3) ต้องกำหนดแนวทางและขั้นตอนในการจัดการกรณีข้อมูลยืนยันตัวตนถูกละเมิด เพื่อให้สามารถตอบสนองและลดผลกระทบได้อย่างทันท่วงที
4) กำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้
    - ต้องจัดไม่ให้ระบบระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
    - ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
    - จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน
    - จำกัดการเชื่อมต่อโดยตรงเข้าสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจก่อให้สร้างความเสียหายให้กับระบบได้

8.6. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

เพื่อให้ระบบสารสนเทศมีขีดความสามารถเพียงพอ รองรับการใช้งาน และสนับสนุนการดำเนินภารกิจของกรมฯ อย่างต่อเนื่อง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องดำเนินการประเมินและวางแผนขีดความสามารถของระบบให้สอดคล้องกับความต้องการใช้งานในปัจจุบันและแนวโน้มในอนาคตอย่างเหมาะสม เช่น การประเมินปริมาณผู้ใช้งาน (User Load) การวิเคราะห์แนวโน้มการใช้ทรัพยากรระบบ (CPU, Memory, Storage) การวางแผนขยายระบบล่วงหน้า (Capacity Planning) หรือการจัดเตรียมโครงสร้างพื้นฐานให้รองรับการเติบโตของระบบในอนาคต

2) ต้องมีการติดตาม ตรวจสอบ และวิเคราะห์การใช้งานทรัพยากรของระบบอย่างสม่ำเสมอ เพื่อให้สามารถบริหารจัดการได้อย่างมีประสิทธิภาพ เช่น การติดตามการใช้งาน CPU หน่วยความจำ (Memory) พื้นที่จัดเก็บข้อมูล (Storage) และปริมาณการใช้งานเครือข่าย (Network Traffic) รวมถึงการใช้เครื่องมือเฝ้าระวังระบบ (Monitoring Tools) เพื่อแจ้งเตือนเมื่อทรัพยากรมีแนวโน้มใช้งานเกินขีดความสามารถ
3) ต้องจัดเตรียมมาตรการรองรับกรณีที่ระบบมีภาระงานเพิ่มขึ้น เช่น การขยายทรัพยากรระบบ (Scaling) การจัดสรรทรัพยากรเพิ่มเติม หรือการปรับแต่งประสิทธิภาพของระบบอย่างเหมาะสม

8.7. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Protection against malware)

เพื่อป้องกัน ตรวจจับ และลดผลกระทบจากโปรแกรมไม่ประสงค์ดีที่อาจกระทบต่อสารสนเทศและระบบสารสนเทศของกรมฯ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องติดตั้งและใช้งานมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ที่เหมาะสมกับลักษณะของระบบและความเสี่ยงที่เกี่ยวข้อง
2) ต้องดำเนินการปรับปรุงฐานข้อมูลลายเซ็น (Signature) และกลไกการป้องกันให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้สามารถตรวจจับภัยคุกคามได้อย่างมีประสิทธิภาพ
3) ต้องกำหนดแนวทางและขั้นตอนในการตอบสนองเมื่อพบการติดโปรแกรมไม่ประสงค์ดี เพื่อให้สามารถควบคุม แก้ไข และลดผลกระทบได้อย่างทันท่วงที
4) เจ้าหน้าที่ศูนย์ฯ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์
5) การใช้ USB จะต้องได้รับการกำหนดสิทธิ์การใช้งานอย่างเหมาะสม และต้องผ่านการตรวจสอบและอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ ก่อนนำมาใช้งาน เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล
6) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานเสมอ
7) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
8) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

8.8. การบริหารจัดการของช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

เพื่อให้สามารถระบุ ประเมิน และจัดการช่องโหว่ทางเทคนิคอย่างเป็นระบบ ลดโอกาสและผลกระทบจากการถูกโจมตี กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องมีการติดตามและเฝ้าระวังข้อมูลช่องโหว่ที่เกี่ยวข้องกับระบบของกรมฯ จากแหล่งข้อมูลที่เชื่อถือได้อย่างสม่ำเสมอ
2) ต้องบันทึกข้อมูลช่องโหว่ที่ตรวจพบ รวมถึงติดตามผลการดำเนินการแก้ไขอย่างเป็นระบบและต่อเนื่อง
3) ต้องกำหนดให้มีการประเมินช่องโหว่ของระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

4) ต้องมีการติดตามและทบทวนผลการจัดการช่องโหว่อย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามาตรการที่ดำเนินการมีประสิทธิผลและสามารถลดความเสี่ยงได้อย่างเหมาะสม
5) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริการจัดการช่องโหว่ของระบบเหล่านั้น
6) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที
7) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้
   - มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
   - ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
   - กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น
8) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

8.9. การบริหารจัดการการกำหนดค่า (Configuration management)

เพื่อควบคุมการกำหนดค่าระบบสารสนเทศให้มีความมั่นคงปลอดภัยและสอดคล้องกับมาตรฐานที่กำหนด กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดมาตรฐานการตั้งค่าระบบที่ปลอดภัย (Secure Configuration Baseline) ให้สอดคล้องกับแนวปฏิบัติที่เหมาะสมและระดับความเสี่ยงของระบบ
2) การเปลี่ยนแปลงการกำหนดค่าระบบต้องได้รับการอนุมัติจากผู้มีอำนาจตามกระบวนการที่กำหนด และมีการควบคุมอย่างเหมาะสม
3) ต้องจัดเก็บและบันทึกข้อมูลการกำหนดค่าระบบในรูปแบบเอกสารสารสนเทศอย่างเป็นระบบ รวมถึงประวัติการเปลี่ยนแปลง เพื่อรองรับการตรวจสอบและการติดตามย้อนหลัง (Audit Trail)

8.10. การลบสารสนเทศ (Information deletion)

เพื่อให้การลบสารสนเทศเป็นไปอย่างถูกต้อง ปลอดภัย และไม่สามารถกู้คืนได้โดยมิชอบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดระยะเวลา (Retention) ในการจัดเก็บและการลบข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูล และกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง
2) ต้องใช้วิธีการลบหรือทำลายข้อมูลที่เหมาะสมกับประเภทของสื่อบันทึกข้อมูล เพื่อให้ไม่สามารถกู้คืนข้อมูลได้
3) ต้องมีการบันทึกและจัดเก็บหลักฐานการดำเนินการลบข้อมูลอย่างครบถ้วน เพื่อรองรับการตรวจสอบและการติดตามย้อนหลัง

8.11. การปิดบังข้อมูล (Data masking)

เพื่อป้องกันการเปิดเผยข้อมูลสำคัญโดยไม่จำเป็นในระหว่างการใช้งาน การทดสอบ หรือการแสดงผล กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กำหนดกรณีที่จำเป็นต้องใช้การปิดบังข้อมูลสำคัญหรือข้อมูลอ่อนไหว โดยใช้เทคนิคที่เหมาะสม เช่น การปกปิดข้อมูล (Data Masking), การทำข้อมูลให้ไม่สามารถระบุตัวบุคคลได้ (Data Anonymization) หรือ การแปลงข้อมูลให้ไม่สามารถระบุตัวบุคคลได้โดยใช้รหัสแทน (นามแฝง) (Pseudonymization)
2) การปิดบังข้อมูลต้องดำเนินการโดยไม่กระทบต่อความถูกต้อง ความครบถ้วน หรือการทำงานของระบบสารสนเทศ
3) มีการควบคุมการเข้าถึงข้อมูลต้นฉบับอย่างเหมาะสม โดยจำกัดสิทธิ์เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น

8.12. การป้องกันข้อมูลรั่วไหล (Data leakage prevention)

เพื่อป้องกัน ตรวจจับ และลดความเสี่ยงจากการรั่วไหลของข้อมูลสารสนเทศของกรมฯ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดมาตรการควบคุมการส่งออกหรือถ่ายโอนข้อมูลอย่างเหมาะสม เช่น การปิดการใช้งานอุปกรณ์ USB การจำกัดขนาดไฟล์ หรือการควบคุมช่องทางการรับ–ส่งข้อมูล
2) ต้องมีการเฝ้าระวังและตรวจสอบพฤติกรรมการใช้งานที่อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลอย่างสม่ำเสมอ
3) ผู้พบเห็นหรือผู้ตรวจพบความผิดปกติที่อาจก่อให้เกิดการรั่วไหลของข้อมูล (Data Leakage) เช่น การส่งข้อมูลไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์ การสูญหายของอุปกรณ์หรือสื่อบันทึกข้อมูล หรือพฤติกรรมการใช้งานที่ผิดปกติ ต้องดำเนินการแจ้งเหตุโดยทันที เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถตอบสนอง ตรวจสอบ และดำเนินการแก้ไขได้อย่างทันท่วงทีและเป็นระบบ อันจะช่วยป้องกัน ควบคุม และลดผลกระทบที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

8.13. การสำรองข้อมูล (Information backup)

เพื่อคุ้มครองสารสนเทศของกรมฯ จากการสูญหาย การเสียหาย หรือเหตุการณ์ไม่คาดคิด และเพื่อให้สามารถกู้คืนข้อมูลและระบบสารสนเทศได้อย่างทันท่วงที กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ กำหนดให้มีการสำรองข้อมูลสารสนเทศและระบบสารสนเทศที่สำคัญตามระดับความสำคัญของข้อมูล
2) การสำรองข้อมูลต้องจัดเก็บในสถานที่หรือระบบที่มีความมั่นคงปลอดภัย และแยกจากระบบงานหลักตามความเหมาะสม
3) ต้องมีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสามารถนำข้อมูลกลับมาใช้งานได้จริง
4) เจ้าหน้าที่ศูนย์ต้องรับผิดชอบในการสำรองข้อมูล และเก็บรักษาข้อมูล เมื่อผู้ใช้นำเครื่องคอมพิวเตอร์มาทำการตรวจสอบ ซ่อมแซม และหากทำการตรวจสอบ ซ่อมแซมจนเครื่องคอมพิวเตอร์สามารถใช้งานได้ตามปกติเป็นที่เรียบร้อยแล้ว จะต้องทำการคัดลอกย้ายข้อมูลกลับไปให้คงเดิม

5) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมภาวะฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

6) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดความถี่ให้มีการสำรองข้อมูลมากขึ้น โดยให้มีการสำรองข้อมูล ดังนี้
   - กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
   - กำหนดรูปแบบในการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น Data Backupหรือ System Backup
   - บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ข้อมูลที่สำรอง วัน/เวลาสำเร็จ/ไม่สำเร็จ เป็นต้น
   - ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ข้อมูลในฐานข้อมูล เป็นต้น
   - จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการเขียนชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงวันที่สำรองข้อมูลไว้อย่างชัดเจน
   - จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ซึ่งระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
   - ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
   - ทดสอบบันทึกข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
   - จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
   - ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

7) ต้องสื่อสารบทบาท หน้าที่ และขั้นตอนการปฏิบัติให้ผู้เกี่ยวข้องรับทราบ โดยผู้อำนวยการศูนย์รับผิดชอบ ดังนี้
   - วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการให้ผู้บังคับบัญชาระดับสูงทราบ
   - กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งาน การปฏิบัติงานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ
   - กำกับดูแล ตรวจสอบ การบำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติ
   - กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในหน่วยงาน
   - กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้
   - แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

- รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ
- กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก โดยไม่ได้รับอนุญาต

8) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง
9) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

8.14. สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Redundancy of information processing facilities)

เพื่อสนับสนุนความต่อเนื่องในการดำเนินภารกิจของกรมฯ และลดผลกระทบจากความขัดข้องของระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ ต้องจัดให้มีมาตรการรองรับกรณีระบบสารสนเทศที่มีความสำคัญต่อภารกิจหลักเกิดความขัดข้อง เช่น การจัดให้มีระบบสำรอง (Redundant System) ระบบสำรองข้อมูล (Backup System) หรือระบบสลับการทำงานอัตโนมัติ (Failover) รวมถึงการสำรองข้อมูลที่แยกจากพื้นที่ศูนย์ข้อมูลหลัก (Offsite Backup) เพื่อรองรับกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อศูนย์ข้อมูลหลัก เช่น อัคคีภัย น้ำท่วม หรือเหตุขัดข้องร้ายแรง
2) การจัดเตรียมระบบหรืออุปกรณ์สำรองต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความจำเป็นในการให้บริการอย่างเหมาะสม เช่น การจัดให้มีอุปกรณ์สำรอง (Spare Parts) ระบบไฟฟ้าสำรอง ระบบเครือข่ายสำรอง หรือการจัดเตรียมศูนย์ปฏิบัติงานสำรอง (Disaster Recovery Site)
3) ต้องมีการทบทวนและประเมินความเพียงพอของมาตรการด้านความพร้อมใช้งานอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถรองรับเหตุขัดข้องได้อย่างมีประสิทธิภาพ

8.15. การบันทึกข้อมูลล็อก (Logging)

เพื่อสนับสนุนการตรวจสอบ การติดตามเหตุการณ์ และการวิเคราะห์ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ระบบสารสนเทศที่สำคัญต้องมีการบันทึกกิจกรรมการใช้งานและเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
2) ข้อมูลบันทึกต้องได้รับการป้องกันจากการเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต
3) ต้องกำหนดระยะเวลาการจัดเก็บข้อมูลบันทึกให้เหมาะสมกับข้อกำหนดของทางราชการ
4) ต้องมีการบันทึกพฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้
   - ข้อมูลชื่อบัญชีผู้ใช้งาน
   - ข้อมูลวันเวลาที่เข้าระบบ
   - ข้อมูลวันเวลาที่ออกจากระบบ
   - ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
   - ข้อมูลการล็อกอิน (login) ทั้งที่สำเร็จและไม่สำเร็จ

- ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- ข้อมูลการเปลี่ยนคอนฟิกูเรชั่น (Configuration) ของระบบ
- ข้อมูลแสดงการใช้งานแอพพลิเคชั่น (Application)
- ข้อมูลการล็อกอิน (Login) ทั้งที่สำเร็จและไม่สำเร็จ
- ข้อมูลไอพีแอดเดรส (Ip-Address) ที่เข้าถึง
- ข้อมูลโปรโตคอล (Protocol) เครือข่ายที่ใช้
- ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
- ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

5) จัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง ชัดเจน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง
6) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย
7) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการเข้าใช้งานอินเทอร์เน็ตหรืออีเมล์ เป็นต้น
8) กำหนดระยะเวลาจัดเก็บ Log ไม่น้อยกว่า 90 วัน หรือเป็นไปตามข้อกำหนดทางกฎหมาย ระเบียบและนโยบายที่เกี่ยวข้อง

8.16. กิจกรรมการเฝ้าระวังติดตาม (Monitoring activities)

เพื่อให้สามารถตรวจพบความผิดปกติหรือเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างเหมาะสม กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ ควรพิจารณาจัดให้มีการเฝ้าระวังและติดตามการใช้งานระบบสารสนเทศอย่างเหมาะสมสอดคล้องกับลักษณะการใช้งานและระดับความเสี่ยง เช่น การตรวจสอบบันทึกเหตุการณ์ (Log Monitoring) การใช้ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) การเฝ้าระวังการใช้งานเครือข่าย การใช้เครื่องมือวิเคราะห์พฤติกรรมการใช้งาน (User Activity Monitoring) รวมถึงการดำเนินงานผ่านศูนย์เฝ้าระวังความมั่นคงปลอดภัย (Security Operations Center: SOC) หรือศูนย์ปฏิบัติการเครือข่าย (Network Operations Center: NOC) ตามความเหมาะสม
2) การเฝ้าระวังและติดตามต้องคำนึงถึงความจำเป็น ความเหมาะสม ระดับความเสี่ยง รวมถึงการคุ้มครองสิทธิส่วนบุคคลตามกฎหมายและนโยบายที่เกี่ยวข้อง
3) เหตุการณ์ผิดปกติที่ตรวจพบต้องได้รับการบันทึก รายงาน และดำเนินการตามกระบวนการจัดการเหตุการณ์ที่กำหนดไว้อย่างทันท่วงทีและเป็นระบบ

8.17. การตั้งนาฬิกาให้ถูกต้อง (Clock synchronization)

เพื่อให้ข้อมูลเวลาในระบบสารสนเทศมีความถูกต้องและสอดคล้องกัน อันเป็นประโยชน์ต่อการตรวจสอบและวิเคราะห์เหตุการณ์ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ระบบสารสนเทศของกรมฯ ต้องมีการตั้งค่าเวลาให้สอดคล้องกับแหล่งเวลาอ้างอิงที่เชื่อถือได้ เช่น มาตรฐานเวลาเครือข่าย (Network Time Protocol: NTP)

2) ควบคุมและดูแลการตั้งค่าเวลาอย่างเหมาะสม เพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

8.18. การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

เพื่อควบคุมการใช้เครื่องมือหรือโปรแกรมที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษต้องได้รับอนุญาตตามอำนาจหน้าที่
2) ต้องจำกัดการใช้งานเฉพาะผู้ที่มีความจำเป็นและมีความรับผิดชอบโดยตรง
3) ต้องสามารถตรวจสอบย้อนหลังการใช้งานได้
4) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป
5) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ
6) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้
7) กำหนดให้มีการถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ
8) ห้ามติดตั้งหรือใช้งานโปรแกรมละเมิดลิขสิทธิ์ หรือโปรแกรมที่มีนโยบายห้ามไม่ให้เข้าถึง หรือติดตั้งหรือใช้งาน

8.19. การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

เพื่อป้องกันความเสี่ยงจากการติดตั้งซอฟต์แวร์ที่ไม่เหมาะสมหรือไม่ได้รับอนุญาต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การติดตั้งหรือปรับปรุงซอฟต์แวร์บนระบบที่ใช้งานจริงต้องได้รับการอนุมัติจากผู้มีอำนาจ และต้องดำเนินการผ่านกระบวนการบริหารการเปลี่ยนแปลง (Change Management) ที่กำหนด
2) ต้องมีการทดสอบและประเมินผลกระทบก่อนนำไปใช้งานจริง เพื่อให้มั่นใจว่าไม่ส่งผลกระทบต่อระบบหรือการให้บริการ
3) ต้องมีการบันทึกการติดตั้งหรือการเปลี่ยนแปลง รวมถึงรายละเอียดที่เกี่ยวข้องไว้เป็นหลักฐานอย่างครบถ้วน เพื่อรองรับการตรวจสอบและการติดตามย้อนหลัง
4) ต้องไม่ติดตั้งซอร์สโค้ด คอมไพเลอร์ (Compiler) หรือเครื่องมือสำหรับพัฒนา แก้ไข หรือแปลงโปรแกรมให้สามารถทำงานได้ ไว้บนเครื่องแม่ข่ายที่ให้บริการระบบ เพื่อป้องกันความเสี่ยงจากการแก้ไขหรือเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต
5) การติดตั้ง การตั้งค่า และการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์หรือผู้ได้รับอนุญาตเท่านั้น

8.20. การรักษาความมั่นคงปลอดภัยของเครือข่าย (Networks security)

เพื่อปกป้องคุ้มครองเครือข่ายของกรมฯ จากการเข้าถึง การใช้งาน หรือการโจมตีโดยไม่ได้รับอนุญาต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ ต้องกำหนดมาตรการควบคุมและป้องกันด้านเครือข่ายให้สอดคล้องกับระดับความเสี่ยงและความสำคัญของระบบ

2) การเชื่อมต่อเครือข่ายต้องได้รับการควบคุม ตรวจสอบ และอนุญาตอย่างเหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
3) ต้องมีการทบทวนและประเมินความมั่นคงปลอดภัยของเครือข่ายเป็นระยะ เพื่อให้มั่นใจว่ามาตรการที่นำมาใช้ยังคงมีประสิทธิภาพและเหมาะสมกับสถานการณ์
4) ต้องมีการกำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address
5) กำหนดให้ใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้
6) จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวข้องกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย
7) แผนผังระบบเครือข่าย จะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผัง
8) ระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง
9) IP address ของระบบเครือข่ายภายในหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถเข้าถึงได้ เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าสู่ระบบเครือข่ายได้โดยง่าย
10) การป้องกันพอร์ต (Port) ที่ใช้งานสำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic And Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ
    - แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ
        - ตรวจสอบโปรโตคอล (Protocol) และพอร์ต (Port) ที่ใช้
        - ตรวจสอบว่ามีแอพพลิเคชั่นใดทำงานบนเครื่องเป้าหมาย
    - กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบเครือข่าย
        - ทำการปิดบริการ (Service) และพอร์ต (Port) ที่ไม่จำเป็น
        - ใช้เครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย
    - ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาที่จำเป็น
    - ต้องมีการมอบหมายบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน
11) การเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติ ดังนี้
    - จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย
    - ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)
    - การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น
    - ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย
    - มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย
    - ควบคุมมิให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานให้เชื่อมต่อผ่านอุปกรณ์ที่ป้องกันการบุกรุก เช่น Firewall เป็นต้น

12) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องแนวปฏิบัติการควบคุมการเข้าถึงหรืออุปกรณ์การประยุกต์ใช้งานตามภารกิจ ดังนี้
    - ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานหมายเลขเครือข่าย (IP address)
    - กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก
    - กำหนดมาตรการการบังคับใช้เส้นทางบนเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย
    - กำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น
13) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)
    - ผู้ดูแลแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้งานระบบเครือข่ายไร้สาย
    - ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
    - ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
    - ผู้ดูแลระบบเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่
    - ผู้ดูแลระบบต้องกำหนดค่าของการใช้งานให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น
    - ผู้ดูแลระบบต้องมีการแยก VLAN ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน
    - ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน
    - ผู้ดูแลระบบต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

8.21. ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

เพื่อให้บริการเครือข่ายที่ใช้สนับสนุนการปฏิบัติงานของกรมฯ มีความมั่นคงปลอดภัยและเชื่อถือได้ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ใช้บริการเครือข่ายต้องเป็นไปตามเงื่อนไข ข้อกำหนด และข้อตกลงการใช้งานที่กรมฯ กำหนดอย่างเคร่งครัด

2) ต้องกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยระหว่างหน่วยงานภายในกรมฯ และหน่วยงานหรือผู้ให้บริการภายนอกที่เกี่ยวข้องให้ชัดเจน เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและสามารถตรวจสอบได้
3) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายให้ชัดเจนและรัดกุม เพื่อทำให้การควบคุม และป้องกันการบุกรุกเป็นไปอย่างมีประสิทธิภาพ
4) ผู้ดูแลระบบต้องมีวิธีในการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
5) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้เข้าถึงเท่านั้น ดังนี้
    - ควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
    - ควบคุมการเข้าถึงระบบเครือข่าย
    - ควบคุมการเข้าถึงระบบปฏิบัติการ
    - ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
6) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

8.22. การแบ่งแยกเครือข่าย (Segregation of networks)

เพื่อลดความเสี่ยงจากการแพร่กระจายของภัยคุกคามภายในเครือข่าย กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ระบบเครือข่ายต้องได้รับการแบ่งแยกตามระดับความสำคัญและลักษณะการใช้งานอย่างเหมาะสม พร้อมทั้งจัดทำแผนผังเครือข่าย (Network Diagram) ในรูปแบบเอกสารสารสนเทศที่เป็นปัจจุบัน เพื่อใช้ในการบริหารจัดการและการตรวจสอบ
2) การเชื่อมต่อระหว่างเครือข่ายต้องอยู่ภายใต้การควบคุมและการกำกับดูแลอย่างเหมาะสม เพื่อป้องกันการเข้าถึงหรือการเชื่อมต่อโดยไม่ได้รับอนุญาต
3) มีการกำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้
    - Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ต้องบูรณาการ
    - แบ่งแยกเครือข่าย สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็นโซน ดังนี้
        - Intranet Zone
        - Application Zone
        - Database Zone
        - Extranet Zone
        - DMZ Zone
        - HCI Zone
        - Banking Zone
        - Management Zone

4) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้
   (1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน
   (2) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้
      - ควบคุมการเข้าถึงอาคารหรือระบบ โดยจัดตั้งให้เป็นไปเพื่อให้ปลอดภัย
      - ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และพร้อมรับการใช้งานทันที เมื่อพบเหตุการณ์ผิดปกติ
   (3) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing And Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว โดยมีขั้นตอนการควบคุม ดังนี้
      - ผู้ที่ใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตเบื้องต้นจากผู้บังคับบัญชาก่อน
      - ผู้อำนวยการศูนย์พิจารณาอนุญาต เมื่อผ่านการพิจารณา ผู้อำนวยการศูนย์ส่งต่อให้ผู้ดูแลระบบตรวจสอบและดำเนินการกำหนดสิทธิการใช้งาน และแจ้งกลับผู้บังคับบัญชาของบุคคลดังกล่าวทราบเป็นลายลักษณ์อักษร
      - สำหรับการขอเข้าใช้งานระบบสารสนเทศจากกภายนอก (Teleworking) ต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รหัสการใช้งานจะแจ้งโดยการใส่ซองปิดผนึกกลับไปยังผู้ที่ขออนุญาตใช้งาน

8.23. การกรองเว็บ (Web filtering)

เพื่อป้องกันการเข้าถึงแหล่งข้อมูลที่ไม่เหมาะสมหรือเป็นภัยต่อความมั่นคงปลอดภัย กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กรมฯ อาจกำหนดมาตรการควบคุมและกรองการเข้าถึงเว็บไซต์ตามความจำเป็น เช่น การกำหนดรายการเว็บไซต์ที่อนุญาต (Whitelist) หรือไม่อนุญาต (Blacklist) การจำกัดการเข้าถึงเว็บไซต์ที่มีความเสี่ยง เช่น เว็บไซต์การพนัน เว็บไซต์สื่อลามก หรือเว็บไซต์ที่เป็นอันตราย รวมถึงการใช้ระบบกรองเนื้อหา (Web Filtering)
2) การกำหนดรายการเว็บไซต์ต้องคำนึงถึงภารกิจ ความจำเป็นในการปฏิบัติงาน และลักษณะการใช้งานของหน่วยงาน เพื่อไม่ให้กระทบต่อการดำเนินงาน
3) ให้มีการสร้างความตระหนักรู้แก่ผู้ใช้งานเกี่ยวกับความเสี่ยงจากการใช้งานอินเทอร์เน็ต และแนวทางการใช้งานอย่างปลอดภัย เช่น การหลีกเลี่ยงเว็บไซต์ที่ไม่น่าเชื่อถือ หรือมีเนื้อหาที่เป็นอันตราย

8.24. การเข้ารหัสข้อมูล (Use of cryptography)

เพื่อคุ้มครองข้อมูลจากการเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ข้อมูลที่มีความสำคัญหรือมีความอ่อนไหวต้องได้รับการเข้ารหัส (Encryption) ตามความเหมาะสม เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
2) การเลือกใช้วิธีการเข้ารหัสต้องคำนึงถึงระดับความเสี่ยงและข้อกำหนดของทางราชการ

3) ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล
4) การจัดเก็บ Username และ Password ของระบบสารสนเทศในฐานข้อมูลตามภารกิจหลัก จะต้องทำการเข้ารหัสด้วย SHA256 หรือดีกว่าใน Field ของ Password ก่อนบันทึกลงในฐานข้อมูล ทุกครั้ง
5) ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล Https สำหรับระบบ สารสนเทศ แบบ Web Application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่าง บราว์เซอร์และเว็บเซิร์ฟเวอร์
6) กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมสำหรับช่องทางดังต่อไปนี้
   - ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
   - เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย

8.25. วงจรการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development life cycle)

เพื่อให้การพัฒนาระบบสารสนเทศของกรมฯ คำนึงถึงความมั่นคงปลอดภัยตั้งแต่ระยะเริ่มต้นจนถึงการใช้งานจริง กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การพัฒนาระบบต้องบูรณาการข้อพิจารณาด้านความมั่นคงปลอดภัยสารสนเทศในทุกขั้นตอนของกระบวนการพัฒนา (Secure Software Development Life Cycle: Secure SDLC) อย่างเหมาะสม
2) ต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment) ก่อนนำระบบไปใช้งานจริง เพื่อให้มั่นใจว่าความเสี่ยงอยู่ในระดับที่ยอมรับได้ (Acceptable Risk)
3) ต้องจัดให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันก่อนหน้า (Previous Version) รวมถึงข้อมูลและเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเดิม เช่น ขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง เพื่อรองรับกรณีจำเป็นต้องย้อนกลับไปใช้งานเวอร์ชันเดิม (Rollback) โดยกำหนดระยะเวลาในการจัดเก็บอย่างเหมาะสม

8.26. ข้อกำหนดด้านการรักษาความปลอดภัยของแอปพลิเคชัน (Application security requirements)

เพื่อให้แอปพลิเคชันของกรมฯ มีความปลอดภัยและลดความเสี่ยงจากช่องโหว่ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application Security Requirements) ให้ชัดเจน และสอดคล้องกับความเสี่ยงของระบบ เช่น การควบคุมการเข้าถึง (Access Control) การยืนยันตัวตน (Authentication) การจัดการสิทธิ์ผู้ใช้งาน (Authorization) การปกป้องข้อมูลด้วยการเข้ารหัส (Encryption) และการป้องกันช่องโหว่ของแอปพลิเคชัน เช่น OWASP Top 10
2) ต้องดำเนินการทดสอบ ตรวจสอบ และแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัย (Security Testing) ก่อนเปิดใช้งานระบบ เพื่อให้มั่นใจว่าระบบมีความปลอดภัยเพียงพอ
3) ต้องมีการจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) เข้าใช้งานของผู้ใช้งานและบุคคลากรฝ่ายสนับสนุนการใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยดำเนินการดังนี้
   (1) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียน ผู้ใช้งาน และการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูล

(2) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

(3) ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยหน่วยงาน และต้องลงนามในสัญญารักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

(4) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(5) ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

8.27. หลักการสถาปัตยกรรมระบบและหลักการทางวิศวกรรมระบบที่ปลอดภัย (Secure system architecture and engineering principles)

เพื่อสนับสนุนการออกแบบระบบสารสนเทศที่มีความมั่นคงปลอดภัยในระยะยาว กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การออกแบบระบบต้องคำนึงถึงความมั่นคงปลอดภัยเป็นองค์ประกอบหลัก เช่น หลักการลดสิทธิ์ให้เหลือน้อยที่สุด (Least Privilege) การแบ่งแยกระบบ (Segregation/Segmentation) และการป้องกันหลายชั้น (Defense in Depth)
2) พิจารณาเลือกใช้แนวทางการออกแบบที่เหมาะสมกับภารกิจและระดับความเสี่ยง เช่น การออกแบบระบบแบบแยกส่วน (Modular Design) การใช้สถาปัตยกรรมแบบ Zero Trust หรือการใช้มาตรการรักษาความปลอดภัยตั้งแต่ขั้นตอนการออกแบบ (Security by Design)
3) ต้องมีการทบทวนและประเมินความมั่นคงปลอดภัยของสถาปัตยกรรมระบบอย่างสม่ำเสมอ รวมถึงการปรับปรุงให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป

8.28. การพัฒนาโปรแกรมอย่างปลอดภัย (Secure Coding)

เพื่อลดความเสี่ยงจากช่องโหว่ที่เกิดจากการเขียนโปรแกรม กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดแนวทางและมาตรฐานในการพัฒนาโปรแกรมให้มีความมั่นคงปลอดภัย โดยสอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง เช่น กฎหมายและมาตรฐานที่เกี่ยวข้องในการพัฒนาเว็บไซต์ มาตรฐานด้านความปลอดภัยของแอปพลิเคชัน และแนวทาง OWASP
2) มีการทบทวน ตรวจสอบ หรือทดสอบซอร์สโค้ด (Code Review / Security Testing) ตามความเหมาะสม เพื่อค้นหาและแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยก่อนนำไปใช้งาน
3) ต้องจัดเก็บซอร์สโค้ด (Source Code) และไลบรารี (Library) ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และมีการควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันการเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต
4) ต้องมีการควบคุมการใช้ไลบรารีหรือซอฟต์แวร์จากภายนอก (Third-party Components) โดยต้องตรวจสอบช่องโหว่และความน่าเชื่อถือก่อนนำมาใช้งาน

5) มีการควบคุมเวอร์ชันของซอร์สโค้ด (Version Control) และบันทึกประวัติการเปลี่ยนแปลงอย่างครบถ้วน เพื่อรองรับการติดตามย้อนหลัง

8.29. การทดสอบการรักษาความรักษาความปลอดภัยในการพัฒนาและการยอมรับ (Security testing in development and acceptance)

เพื่อให้มั่นใจว่าระบบสารสนเทศมีความพร้อมด้านความมั่นคงปลอดภัยก่อนนำไปใช้งาน กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) กำหนดเกณฑ์การยอมรับระบบด้านความมั่นคงปลอดภัย (Security Acceptance Criteria) และดำเนินการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศก่อนนำไปใช้งานจริง โดยครอบคลุมการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing: VA/PT) ก่อนขั้นตอนการนำขึ้นใช้งานจริง (Production Deployment: PD)
2) มีการทดสอบด้านความมั่นคงปลอดภัยของแอปพลิเคชัน เช่น Static Application Security Testing (SAST) หรือ Dynamic Application Security Testing (DAST) ตามความเหมาะสม
3) กำหนดให้มีการดำเนินการทดสอบการยอมรับระบบโดยผู้ใช้งาน (User Acceptance Testing: UAT) เพื่อยืนยันว่าระบบสารสนเทศสามารถรองรับความต้องการทางธุรกิจและมีความมั่นคงปลอดภัยเพียงพอก่อนนำไปใช้งานจริง โดยผลการทดสอบต้องได้รับการอนุมัติจากผู้มีอำนาจก่อนการนำระบบขึ้นใช้งานจริง (Production Deployment)
4) ผลการทดสอบต้องได้รับการวิเคราะห์ และนำไปใช้ในการปรับปรุง แก้ไข รวมถึงเสริมสร้างมาตรการควบคุมด้านความมั่นคงปลอดภัยของระบบอย่างเหมาะสม โดยต้องดำเนินการแก้ไขช่องโหว่ตามระดับความเสี่ยงที่กำหนดให้แล้วเสร็จก่อนการนำระบบขึ้นใช้งานจริง

8.30. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

เพื่อควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยจากการพัฒนาระบบโดยหน่วยงานภายนอก กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไว้ในข้อตกลงหรือสัญญากับผู้รับจ้างหรือผู้ให้บริการภายนอกอย่างชัดเจน
2) ต้องมีการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานของผู้รับจ้างหรือผู้ให้บริการภายนอกให้เป็นไปตามขอบเขตและข้อกำหนดที่กำหนดไว้อย่างต่อเนื่อง
3) ต้องมีการควบคุมและกำกับดูแลโครงการพัฒนาซอฟต์แวร์ที่ดำเนินการโดยผู้รับจ้างจากภายนอกอย่างเหมาะสม เพื่อให้เป็นไปตามมาตรฐานและข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนด
4) ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก
5) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น
6) ต้องกำหนดให้ผู้รับจ้างหรือผู้ให้บริการภายนอกลงนามในข้อตกลงการรักษาความลับ (Non-Disclosure Agreement: NDA) ก่อนเข้าถึงข้อมูลหรือระบบของกรมฯ

7) ต้องกำหนดและควบคุมสิทธิการเข้าถึงระบบของผู้รับจ้างหรือผู้ให้บริการภายนอก โดยให้สิทธิ์เท่าที่จำเป็น และมีการยกเลิกสิทธิ์เมื่อสิ้นสุดสัญญา
8) ต้องกำหนดให้มีการทดสอบ ตรวจรับ และยืนยันความถูกต้องของงาน (Acceptance) ก่อนการส่งมอบหรือใช้งานจริง
9) ต้องกำหนดให้ผู้รับจ้างหรือผู้ให้บริการภายนอกมีหน้าที่แจ้งเหตุด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องโดยทันที

8.31. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test and production environments)

เพื่อป้องกันความเสี่ยงจากการเปลี่ยนแปลงหรือการเข้าถึงระบบโดยไม่เหมาะสม กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ต้องแยกสภาพแวดล้อมของระบบออกจากกันอย่างชัดเจน เช่น สภาพแวดล้อมสำหรับการพัฒนา (Development) การทดสอบ (Testing) และการใช้งานจริง (Production) เพื่อป้องกันผลกระทบระหว่างกันและลดความเสี่ยงด้านความมั่นคงปลอดภัย
2) การเข้าถึงแต่ละสภาพแวดล้อมต้องได้รับการควบคุมตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) อย่างเหมาะสม เพื่อป้องกันการเข้าถึงหรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต เช่น การจำกัดสิทธิ์การเข้าถึงระบบ Production เฉพาะผู้ที่ได้รับมอบหมาย การแยกบัญชีผู้ใช้งานสำหรับแต่ละสภาพแวดล้อม และการกำหนดสิทธิ์การแก้ไขข้อมูลเฉพาะผู้มีหน้าที่เกี่ยวข้องเท่านั้น
3) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น
4) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ
5) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นดำเนินการพัฒนา

8.32. การบริหารจัดการการเปลี่ยนแปลง (Change management)

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศไม่ให้ส่งผลกระทบต่อความมั่นคงปลอดภัย กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การเปลี่ยนแปลงระบบต้องได้รับการอนุมัติตามกระบวนการที่กำหนด
2) ต้องประเมินผลกระทบด้านความมั่นคงปลอดภัยก่อนดำเนินการ
3) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ
4) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

5) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น
6) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ดำเนินหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน
7) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการอนุมัติให้ติดตั้งก่อนดำเนินการ

8.33. การทดสอบสารสนเทศ (Test information)

เพื่อป้องกันการนำข้อมูลจริงหรือข้อมูลอ่อนไหวไปใช้โดยไม่เหมาะสมในการทดสอบระบบ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) ข้อมูลที่ใช้ในการทดสอบต้องได้รับการควบคุมและคุ้มครองอย่างเหมาะสม สอดคล้องกับระดับความสำคัญและชั้นความลับของข้อมูล
2) ต้องหลีกเลี่ยงการใช้ข้อมูลจริง (Production Data) ในการทดสอบ เว้นแต่มีความจำเป็น โดยต้องได้รับอนุญาตจากผู้มีอำนาจ และมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม
3) กรณีมีความจำเป็นต้องใช้ข้อมูลจริง ต้องดำเนินการปกปิดหรือแปลงข้อมูล (Data Masking / Anonymization) ก่อนนำไปใช้ในการทดสอบ เพื่อป้องกันการระบุตัวบุคคลหรือข้อมูลสำคัญ
4) ต้องมีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบ โดยจำกัดสิทธิ์เฉพาะผู้ที่เกี่ยวข้องตามบทบาทหน้าที่
5) ต้องมีการลบหรือทำลายข้อมูลที่ใช้ในการทดสอบเมื่อสิ้นสุดการใช้งาน ตามแนวทางการจัดการข้อมูลหรือการจัดระดับชั้นความลับของกรมฯ เพื่อป้องกันการนำข้อมูลไปใช้โดยมิชอบ

8.34. การป้องกันระบบสารสนเทศระหว่างที่ทดสอบการตรวจประเมิน (Protection of information systems during audit testing)

เพื่อให้การตรวจประเมินระบบสารสนเทศไม่ก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัย กรมฯ มีมาตรการในการตรวจประเมินระบบสารสนเทศในการดำเนินการตรวจประเมินระบบสารสนเทศ กรมฯ กำหนดแนวทางในการปฏิบัติไว้ ดังต่อไปนี้

1) การตรวจประเมินต้องดำเนินการภายใต้การควบคุมและการกำกับดูแลอย่างเหมาะสม เพื่อป้องกันผลกระทบต่อระบบและข้อมูลสารสนเทศ เช่น การจัดทำแผนการตรวจประเมินล่วงหน้า การกำหนดช่วงเวลาการตรวจสอบให้ไม่กระทบต่อการให้บริการ การใช้บัญชีทดสอบแทนบัญชีจริง การสำรองข้อมูลก่อนดำเนินการตรวจสอบ และการมีผู้รับผิดชอบกำกับดูแลระหว่างการดำเนินการตรวจประเมิน
2) ต้องจำกัดขอบเขตการเข้าถึงระบบให้เฉพาะเท่าที่จำเป็นตามวัตถุประสงค์ของการตรวจประเมิน และสอดคล้องกับบทบาทหน้าที่ที่ได้รับมอบหมาย
3) มาตรการในการตรวจประเมินระบบสารสนเทศในการดำเนินการตรวจประเมินระบบสารสนเทศ ให้กำหนดมาตรการควบคุมอย่างน้อยดังต่อไปนี้
    - กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต่อการตรวจสอบในลักษณะอ่านอย่างเดียว (Read-only)

- กรณีมีความจำเป็นต้องเข้าถึงข้อมูลในส่วนอื่น ให้จัดทำสำเนาข้อมูลสำหรับการตรวจสอบโดยเฉพาะ และต้องดำเนินการทำลายหรือลบข้อมูลดังกล่าวทันทีเมื่อการตรวจสอบเสร็จสิ้น หรือจัดเก็บไว้โดยมีมาตรการป้องกันอย่างเหมาะสม
- ให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ
- ให้มีการเฝ้าระวังและบันทึกข้อมูลการเข้าถึงระบบของผู้ตรวจสอบ รวมถึงบันทึกข้อมูล Log ที่แสดงวันและเวลาการเข้าถึงระบบสารสนเทศที่สำคัญ
- ในกรณีที่มีการใช้เครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือดังกล่าวออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และต้องมีการจัดเก็บและป้องกันเครื่องมือจากการเข้าถึงโดยไม่ได้รับอนุญาต

9. เอกสารที่เกี่ยวข้อง

ลำดับ	รายการเอกสาร	รหัสเอกสาร
1	คำสั่งกรมบังคับคดี ที่ ๗๑๙ / ๒๕๖๘ เรื่อง แต่งตั้งคณะกรรมการความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Steering Committee) และคณะทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ คณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และคณะนายทะเบียนเอกสารบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	-