



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร

ประจำปีงบประมาณ พ.ศ. 2569



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



www.otpc.go.th



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
๑. บทนำ	๑
๒. วัตถุประสงค์	๑
๓. คำนิยาม	๑
หมวดที่ ๑ แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
ส่วนที่ ๑ การปฏิบัติเพื่อให้สอดคล้องกับตามประมวลแนวทางปฏิบัติ	๔
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
ส่วนที่ ๒ การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑๐
ส่วนที่ ๓ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑๐
ส่วนที่ ๔ แผนการรับมือภัยคุกคามทางไซเบอร์	๑๑
หมวดที่ ๒ แนวปฏิบัติสำหรับผู้ใช้งาน	
ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)	๑๒
ข้อ ๒ การบริหารจัดการสินทรัพย์	๑๒
ข้อ ๓ การบริหารจัดการบัญชีผู้ใช้งาน (User Account)	๑๓
ข้อ ๔ การบริหารจัดการความปลอดภัยเครือข่ายของ สทท.	๑๓
ข้อ ๕ การใช้งานอุปกรณ์คอมพิวเตอร์	๑๔
ข้อ ๖ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา	๑๔
ข้อ ๗ การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์	๑๕
ข้อ ๘ การใช้งานอินเทอร์เน็ต	๑๕
ข้อ ๙ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล	๑๖
ข้อ ๑๐ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	๑๖
ข้อ ๑๑ การบริหารจัดการข้อมูลองค์กร	๑๗
ข้อ ๑๒ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล	๑๘
ข้อ ๑๓ การใช้งานโปรแกรมรรถประโยชน์ (Use of System Utilities)	๑๘
ข้อ ๑๔ หน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	๑๙
หมวดที่ ๓ แนวปฏิบัติการจัดการด้านความมั่นคงปลอดภัย สำหรับผู้ดูแลระบบ	
ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)	๒๑
ข้อ ๒ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ	๒๑
ข้อ ๓ การกำหนดและควบคุมการเดินสายสัญญาณสื่อสาร และสายไฟฟ้า	๒๒
ข้อ ๔ การกำหนดการบำรุงรักษาระบบสารสนเทศ	๒๒
ข้อ ๕ การบริหารจัดการสินทรัพย์	๒๓
ข้อ ๖ การควบคุมการใช้งานระบบสารสนเทศและบริหารจัดการ อุปกรณ์คอมพิวเตอร์แบบพกพา	๒๔

สารบัญ (ต่อ)

เรื่อง	หน้า
ข้อ ๗ การควบคุมการใช้งานระบบสารสนเทศ	๒๔
ข้อ ๘ การบริหารจัดการความปลอดภัยเครือข่าย	๒๖
ข้อ ๙ การบริหารจัดการในการปฏิบัติงาน	๒๘
ข้อ ๑๐ การสำรองและกู้คืนข้อมูลสารสนเทศ	๒๙
ข้อ ๑๑ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล	๒๙
ข้อ ๑๒ การบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสำหรับการให้บริการคลาวด์	๒๙
ข้อ ๑๓ การบริหารจัดการค่าคอนฟิกูเรชัน (Configuration Management)	๓๐
ข้อ ๑๔ การบริหารจัดการการลบสารสนเทศ (Information Deletion Management)	๓๐
ข้อ ๑๕ การบริหารจัดการการปิดบัง/ซ่อนข้อมูล (Data Masking Management)	๓๑
ข้อ ๑๖ การป้องกันข้อมูลส่วนบุคคล/ข้อมูลที่มีความสำคัญรั่วไหล (Data Leakage Prevention)	๓๑
ข้อ ๑๗ การบริหารจัดการการติดตามกิจกรรมทางเทคโนโลยีสารสนเทศ (Monitoring Activities)	๓๒
ข้อ ๑๘ การบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก (Web Filtering)	๓๓
ข้อ ๑๙ การเขียนโค้ดอย่างมั่นคงปลอดภัย (Secure Coding)	๓๓
ข้อ ๒๐ การปฏิบัติตามกรอบประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์	๓๓
หมวดที่ ๔ แนวปฏิบัติสำหรับเจ้าของระบบ (System Owner)	
ข้อ ๑ การบริหารจัดการโครงการ/งานด้านเทคโนโลยีสารสนเทศ	๓๔
หมวดที่ ๕ แนวปฏิบัติสำหรับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการกำกับผู้ให้บริการภายนอก (System Acquisition, Development, Maintenance and Third Party Management)	
ข้อ ๑ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของ สนช.	๓๖
ข้อ ๒ การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลโดยผู้ให้บริการภายนอก	๓๘
ข้อ ๓ การประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการภายนอก	๓๘
ในขั้นตอนของการคัดเลือก (Due Diligence) และการบริหารจัดการสัญญา	
ข้อ ๔ การติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก	๓๙
ข้อ ๕ โปรแกรมคอมพิวเตอร์มาตรฐานสำหรับการใช้งานของ สนช.	๔๐

แนวปฏิบัติรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.

๑. บทนำ

เพื่อให้การใช้งานระบบสารสนเทศของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) มีประสิทธิภาพ มีความมั่นคงปลอดภัยทางไซเบอร์ และมีความน่าเชื่อถือ ตลอดจนเพื่อให้มีการกำหนด มาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรง ต่อระบบสารสนเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.)

๒. วัตถุประสงค์

เพื่อกำหนดทิศทางและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับระบบสารสนเทศ และข้อมูล ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล สอดคล้องกับกฎหมาย มาตรฐานระเบียบข้อบังคับที่เกี่ยวข้องที่ สนข. ต้องปฏิบัติตาม

๓. คำนิยาม

- ๓.๑ หน่วยงาน หมายถึง สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.)
- ๓.๒ หัวหน้าหน่วยงาน หมายถึง ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร
- ๓.๓ ผอ.สนข. หมายถึง ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร
- ๓.๔ ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างหน่วยงาน
- ๓.๕ ผู้บริหารด้านไอซีที หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)
- ๓.๖ ผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (HoIS) หมายถึง ผู้รับผิดชอบบริหารจัดการและกำกับดูแลความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
- ๓.๗ ศทท. หมายถึง ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
- ๓.๘ ผอ.ศทท. หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
- ๓.๙ ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่มีหน้าที่ดูแลระบบสารสนเทศของ ซึ่งหมายรวมถึง ระบบสารสนเทศที่หน่วยงานภายในได้มีการจัดทำขึ้น หรือบุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่เป็นผู้ดูแลระบบสารสนเทศ (System Administrator) ของ สนข.
- ๓.๑๐ เจ้าของระบบ (System Owner) หมายถึง เจ้าหน้าที่ของ สนข. ที่ได้รับมอบหมาย ให้จัดทำโครงการ/งานด้านเทคโนโลยีสารสนเทศที่มีระบบสารสนเทศ หรือแอปพลิเคชันตามภารกิจของ สนข. ซึ่งต้องปฏิบัติตามแนวปฏิบัตินี้
- ๓.๑๑ ผู้ให้บริการภายนอก หมายถึง องค์กร หรือ หน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานระบบ หรือทรัพย์สินสารสนเทศต่าง ๆ ของหน่วยงาน ตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัย และความลับของข้อมูล
- ๓.๑๒ ผู้ใช้งาน หมายถึง บุคลากรที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของหน่วยงาน
- ๓.๑๓ ระบบสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์แม่ข่าย เครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์ และระบบ หรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงโปรแกรมบริหารจัดการฐานข้อมูลโปรแกรมประยุกต์ ระบบปฏิบัติการ แอปพลิเคชัน และระบบงานต่าง ๆ ที่ใช้เทคโนโลยีสารสนเทศของหน่วยงาน

๓.๑๔ แพตช์ หมายถึง โปรแกรมที่ใช้ปรับปรุงซอฟต์แวร์ เพื่อเพิ่มเติมความสามารถ หรือปรับปรุงแก้ไขโปรแกรม ให้มีประสิทธิภาพมากยิ่งขึ้น รวมถึงการอุดช่องโหว่ที่อาจเกิดภัยคุกคามทางไซเบอร์ให้มีความมั่นคงปลอดภัยมากขึ้น

๓.๑๕ สินทรัพย์ หมายถึง เครื่องคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ อุปกรณ์ประกอบ ข้อมูลสารสนเทศและอุปกรณ์ ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศทั้งหมดที่ สนข. จัดหาไว้ใช้งาน

๓.๑๖ โปรแกรมมาตรฐาน หมายถึง โปรแกรมที่ สนข. กำหนดให้เป็นโปรแกรมมาตรฐานสำหรับใช้งาน ได้ตามปกติ

๓.๑๗ ห้องปฏิบัติการศูนย์คอมพิวเตอร์ หมายถึง พื้นที่ที่จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูล ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์สื่อสารต่าง ๆ ของ สนข. ไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศ สำหรับใช้ปฏิบัติงาน

๓.๑๘ การเข้ารหัสลับ (Encryption) หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบหนึ่ง ที่อ่านได้ (Plain text) ให้อยู่ในอีกรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมจนไม่สามารถอ่านได้ (Cipher text) เพื่อปกปิดข้อมูลให้เป็นความลับ

๓.๑๙ เครือข่าย หมายถึง โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งภายในและภายนอกองค์กร สามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสาร ภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสาร กับคอมพิวเตอร์ของอีกองค์กรหนึ่งได้

๓.๒๐ เทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN) หมายถึง การใช้การเข้ารหัสลับ ข้อมูล เช่น โดยผ่านทางซอฟต์แวร์หรือฮาร์ดแวร์อย่างใดอย่างหนึ่ง เพื่อให้การเชื่อมต่อโดยผ่านทางเครือข่าย ที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต เครือข่ายไร้สาย มีความมั่นคงปลอดภัย ทั้งนี้ เนื่องจากข้อมูลจะได้รับการเข้ารหัสลับ ก่อนที่จะมีการส่งผ่านไปบนอินเทอร์เน็ต หรือเครือข่ายไร้สายนั้น และเมื่อกล่าวถึง VPN จะหมายรวมถึง ระบบ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ หรือฮาร์ดแวร์ ที่ใช้ช่องทางที่มีการเข้ารหัสลับก่อนส่งข้อมูลออกไป

๓.๒๑ ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) หมายถึง ข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นบนระบบ ๆ หนึ่ง และได้ถูกบันทึกไว้ในระบบนั้น เช่น ความผิดพลาดในการทำงานของระบบ ทรัพยากรระบบไม่พอ ความพยายาม ในการบุกรุกระบบ ข้อมูลเหตุการณ์ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้มีการบันทึกและจัดเก็บไว้ เป็นต้น ซึ่งใช้เพื่อตรวจและติดตามการทำงานของระบบ เตือนว่า มีเหตุการณ์หนึ่งเกิดขึ้นแล้วในระบบ หรือดำเนินการเชิงป้องกันหรือแก้ไขตามความจำเป็น ซึ่งรวมถึงการใช้เป็นหลักฐาน ในการดำเนินการทางกฎหมาย เช่น กรณีการบุกรุกระบบ หรือกรณีการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล ซึ่งพาดพิงถึงผู้อื่นและทำให้ผู้อื่นเกิดความเสียหาย เป็นต้น

๓.๒๒ ทรัพย์สินทางปัญญา หมายถึง ผลงานใด ๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ เป็นทรัพย์สิน อีกชนิดหนึ่ง ที่นอกเหนือจากสิทธิบัตร และสิทธิบัตร ทั้งนี้ ประเภทของทรัพย์สินทางปัญญา ประกอบด้วยซึ่งได้รับความคุ้มครองตามกฎหมายว่าด้วยลิขสิทธิ์ (Copyright) กฎหมายว่าด้วยสิทธิบัตร (Patent) กฎหมายว่าด้วยเครื่องหมายการค้า (Trademark) กฎหมายว่าด้วยการคุ้มครองแบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit) กฎหมายว่าด้วยความลับทางการค้า (Trade Secrets) และกฎหมายว่าด้วยการคุ้มครอง สิ่งบ่งชี้ทางภูมิศาสตร์และกฎหมายทรัพย์สินทางปัญญาอื่น

๓.๒๓ ความเสี่ยง หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศ ของ สนข. เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลง แก้ไขซึ่งอาจทำให้ สนข. เกิดปัญหาและเสียชื่อเสียง

๓.๒๔ ระดับความเสี่ยงที่ยอมรับได้ หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าค่าที่ยอมรับได้จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์นั้น มีความมั่นคงปลอดภัย ด้านสารสนเทศเพียงพอ

๓.๒๕ แผนการลดความเสี่ยง หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงซึ่งผู้ประเมินความเสี่ยง ได้ประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ โดยผู้ประเมิน ความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อผู้บังคับบัญชาเพื่อพิจารณา

๓.๒๖ Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

๓.๒๗ Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

๓.๒๘ Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่สามารถยอมให้ การดำเนินงานของ สนข. หยุดชะงัก เพื่อรองรับการดำเนินงานอย่างต่อเนื่องของ สนข. และรองรับการเกิดเหตุการณ์ ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ เพื่อให้ระบบกลับมาทำงานได้ตามปกติให้เร็วที่สุด

หมวดที่ ๑

แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ การปฏิบัติเพื่อให้สอดคล้องกับตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
หน่วยงานต้องกำหนด จัดทำ และมอบหมายผู้รับผิดชอบในการนำกรอบมาตรฐานตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปประยุกต์ใช้งานดังนี้

- ๑) มาตรการกำกับดูแล กำหนดกลยุทธ์ นโยบายที่สอดคล้องกับเป้าหมายองค์กร (Govern)
- ๒) มาตรการระบุความเสี่ยงที่อาจเกิดขึ้นกับคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิต ร่างกายบุคคล (Identify)
- ๓) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)
- ๔) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- ๕) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- ๖) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)



รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เวอร์ชัน ๒.๐

ข้อ ๑ การกำกับดูแล กำหนดกลยุทธ์ นโยบายที่สอดคล้องกับเป้าหมายองค์กร (Govern)

- ๑.๑ การกำหนดบทบาทหน้าที่ ความรับผิดชอบ อำนาจและหน้าที่ ดำเนินการดังนี้
 - ๑.๑.๑ จัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่รับผิดชอบงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
 - ๑.๑.๒ กำหนดนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยให้แก่วระบบเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์
 - ๑.๑.๓ กำกับ ควบคุม ดูแลนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersrcurity) และสื่อสารนโยบายให้แก่บุคคลภายในหน่วยงานและภายนอกหน่วยงาน
 - ๑.๑.๔ กำหนดเกณฑ์ความปลอดภัยสำหรับคู่สัญญาและผู้ให้บริการภายนอก
- ๑.๒ กำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) และแนวทางการประเมินความเสี่ยงเพื่อให้ทุกฝ่ายเข้าใจตรงกัน
- ๑.๓ ทบทวนนโยบายด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง
- ๑.๔ จัดให้มีกระบวนการติดตาม ประเมิน และรายงานผล เพื่อสร้างความมั่นใจต่อการใช้นโยบาย

ข้อ ๒ การระบุความเสี่ยงที่อาจเกิดขึ้นกับคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิต ร่างการบุคคล (Identify)

๒.๑ การจัดการทรัพย์สิน (Asset Management) ดำเนินการดังนี้

๒.๑.๑ จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของระบบสารสนเทศที่สำคัญ และดูแลปรับปรุงทะเบียนให้เป็นปัจจุบัน

๒.๑.๒ ระบุขอบเขตเครือข่ายบริการสำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง และมีนัยสำคัญ (Direct and Significant Interface)

๒.๑.๓ ตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงทรัพย์สินใด ๆ ให้ปรับปรุงทะเบียนให้เป็นปัจจุบันด้วย

๒.๒ การประเมินความเสี่ยง และกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๒.๒.๑ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในแผนบริหารความเสี่ยง และจัดทำเป็นทะเบียนความเสี่ยง

๒.๒.๒ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๒.๒.๓ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งที่มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒.๔ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ การระบุโอกาสที่จะเกิดเหตุความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับของความเสี่ยงที่ยอมรับได้

๒.๒.๕ ต้องมีการประเมินและวิเคราะห์ความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญ

๒.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ดำเนินการ ดังนี้

๒.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลเจ้าของผลิตภัณฑ์ แหล่งข้อมูลอื่นที่น่าเชื่อถือ เช่น จากศูนย์ประสานการรักษาความปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ เป็นต้น

๒.๓.๒ ประเมินช่องโหว่บริการสำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญของ สนข.

๒.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

(๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๒.๓.๔ ประเมินช่องโหว่ของบริการสำคัญเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบเจาะระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ

กับบริการสำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงเปลี่ยนแปลงเทคโนโลยี

๒.๓.๕ การทดสอบเจาะระบบ (Penetration Testting) สำหรับบริการสำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศของหน่วยงานที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing)

๒.๓.๖ ตรวจสอบขอบเขตการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการสำคัญ โดยเฉพาะอย่างยิ่งทุกระบบของหน่วยงานที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing)

๒.๓.๗ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการสำคัญ ก่อนที่จะทำการทดสอบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น การเพิ่มโมดูล การปรับปรุงระบบ การปรับเวอร์ชัน หรือการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๒.๓.๘ การทดสอบเจาะระบบและการให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบการเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรองและได้รับประกาศนียบัตร (Accreditation and Certifications) ที่เป็นที่ยอมรับระดับสากล และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

๒.๓.๙ การทดสอบการเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การกำกับดูแลของ สนช.

๒.๓.๑๐ ติดตามปรับปรุง และแก้ไข ตามข้อกำหนดยุติการผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤต และระดับสูง

ทั้งนี้ ให้ ศทท. จัดให้มีการตรวจประเมินช่องโหว่ และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบสารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบ ต้องดำเนินการแก้ไขให้แล้วเสร็จโดยไม่ชักช้า หรือไม่เกินกว่า ๗ วันทำการ นับถัดจากวันที่ได้รับแจ้งจาก ศทท. พร้อมทั้งรายงานผลการแก้ไขกลับมายัง ศทท. เพื่อทราบและดำเนินการตรวจสอบผลการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบที่ไม่อาจปิดช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบที่อาจแก้ไขได้ พร้อมกำหนดมาตรการชดเชย หรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่นั้น หรือในกรณีที่มีความจำเป็นต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอให้ ผอ.ศทท. หรือผู้รับมอบหมายเป็นผู้พิจารณาและให้ความเห็นชอบ

๒.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ดำเนินการ ดังนี้

๒.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของการให้บริการที่สำคัญของ สนช.

๒.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังนี้

(๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการสำคัญตามความต้องการทางธุรกิจของ สนข. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(๔) สิทธิของ สนข. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Right to Audit)

๑.๔.๓ กำหนดกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

ข้อ ๓ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

๓.๑ การควบคุมการเข้าถึง (Access Control) ดำเนินการ ดังนี้

๓.๑.๑ การเข้าถึงบริการที่สำคัญของ สนข. ถูกจำกัดไว้ที่

(๑) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๓.๑.๒ ให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของ สนข. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๓.๑.๓ เก็บรักษาบันทึกการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้ เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๓.๑.๔ ตรวจสอบการเข้าถึงอินเทอร์เฟซ (Interface) บริการสำคัญ เช่น USB port Serial port เป็นต้น และการเข้าถึงทาง Logical โดยให้อยู่ในการกำกับดูแลของ ศทท.

๓.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ดำเนินการดังนี้

๓.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และเครือข่ายทั้งหมดของบริการสำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการสำคัญ

๓.๒.๒ มาตรการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการอย่างน้อย ดังนี้

(๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(๒) การแบ่งแยกหน้าที่ (Separation of Duties)

(๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(๔) การลบบัญชีที่ไม่ได้ใช้งาน

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

(๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(๗) การป้องกันไวรัส มัลแวร์

(๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ
อย่างทันต่อเหตุการณ์และเหมาะสม

๓.๒.๓ มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านการรักษาความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการสำคัญ

๓.๒.๔ ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

๓.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๓.๓ การเชื่อมต่อระยะไกล (Remote) ดำเนินการ ดังนี้

๓.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการสำคัญ ได้จัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติ
ดังต่อไปนี้

(๑) เปิดใช้งานการเชื่อมต่อระยะไกล หรือจากไซต์งานระยะไกล เมื่อจำเป็นเท่านั้น

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

(๓) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่าย เช่น HTTPS SSL หรือ SCP เป็นต้น

(๔) ไม่อนุญาตให้เชื่อมต่อจากระยะไกลจากการใช้คำสั่ง (Issuing System Command) ที่จะส่งผลกระทบต่อการดำเนินการบริการสำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(๕) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๓.๔ สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media) ดำเนินการดังนี้

๓.๔.๑ กำหนดมาตรการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนสื่อบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรายกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดให้แน่ใจไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๓.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูล
แบบถอดได้

๓.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ
มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่าง ๆ ที่ สนข. กำหนดให้กับบุคลากร ผู้ให้บริการภายนอก ผู้ใช้งาน
ที่เป็นหน่วยงานภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ และให้มีการทบทวนการสร้าง
ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และวิเคราะห์ภัยคุกคาม
ทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของ สนข.
โดยต้องมีการทบทวนกลไกและกระบวนการ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

ดำเนินการดังนี้

๕.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน
และปรับปรุง ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง
เพื่อให้การรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๕.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์
ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๕.๓ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

มีการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือ
กับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

ข้อ ๖ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๖.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) ดำเนินการ ดังนี้

๖.๑.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้
แน่ใจว่าบริการที่สำคัญของ สนข. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจาก
เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผน
ของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของ สนข. เช่น ความสอดคล้องกันของขอบเขต
คำนิยาม และการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD),
Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๖.๑.๒ การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) มีการกำหนดบริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Analysis : BIA)

๖.๑.๓ ให้ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ควรดำเนินการ ดังต่อไปนี้

๑. จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยจากผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง ซึ่งมีขอบเขตการตรวจสอบอย่างน้อย ดังนี้

๑.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๑.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุม หรือมาตรการที่ใช้ในการปกป้องภัยคุกคามทางไซเบอร์ของหน่วยงาน ตามหลักการบริหารความเสี่ยง

ส่วนที่ ๓ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ควรดำเนินการ ดังต่อไปนี้

๑. กำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และจัดทำขั้นตอนปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ตามหลักเกณฑ์ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ประกาศกำหนดและเป็นไปตามมาตรฐานสากล

๒.๑ การจัดการความเสี่ยง (Risk Treatment) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินภารกิจของ สนข. ให้สอดคล้องกับสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตาม และทบทวนความเสี่ยง

๒.๒ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๓ การวิเคราะห์และรายงานความเสี่ยง (Risk Analysis and Reporting) มีการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการที่เกี่ยวข้อง และต้องทบทวนขั้นตอนปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงข้อกฎหมายหรือข้อกำหนดที่เกี่ยวข้องอย่างมีนัยสำคัญ

ส่วนที่ ๔ แผนการรับมือภัยคุกคามทางไซเบอร์

ควรดำเนินการ ดังต่อไปนี้

๑. จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดแนวทางในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
๒. ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยนับตั้งแต่วันที่แผนได้ประกาศใช้งาน หรือวันที่มีการทบทวนแผนครั้งล่าสุด หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของ สนข. หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หมวด ๒ แนวปฏิบัติสำหรับผู้ใช้งาน

ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

- ๑.๑ ปฏิบัติตามมาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูลอย่างเคร่งครัด
- ๑.๒ ติดบัตรผู้ติดต่อให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ห้องปฏิบัติการศูนย์ข้อมูล
- ๑.๓ ทำการยืนยันตัวตนก่อนเข้าห้องปฏิบัติการศูนย์ข้อมูลทุกครั้ง
- ๑.๔ ลงชื่อบันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูลในสมุดลงชื่อให้ชัดเจนทุกครั้ง
- ๑.๕ ไม่นำอาหารและเครื่องดื่มเข้าไปภายในห้องปฏิบัติการศูนย์ข้อมูล
- ๑.๖ ไม่สูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเปลวเพลิงในบริเวณภายในห้องปฏิบัติการศูนย์ข้อมูล

ข้อ ๒ การบริหารจัดการสินทรัพย์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

- ๒.๑ ดูแลรักษาสินทรัพย์ที่ สนข. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของตนเอง
- ๒.๒ ห้ามทิ้งสินทรัพย์ของ สนข. ไว้โดยไม่มีผู้ดูแล ซึ่งรวมถึงการทิ้งไว้ในรถยนต์ ซึ่งสามารถมองเห็นได้จากภายนอก
- ๒.๓ ห้ามนำสินทรัพย์ของ สนข. ไปให้ผู้อื่นยืมไปใช้งาน เช่น เพื่อน พี่น้อง หรือญาติ
- ๒.๔ ใช้งานสินทรัพย์และระบบสารสนเทศต่าง ๆ ในการปฏิบัติงานของ สนข. เท่านั้น
- ๒.๕ แจ้ง ศทท. ก่อนดำเนินการเปลี่ยนจุดติดตั้ง หรือต้องการส่งซ่อมสินทรัพย์
- ๒.๖ ส่งคืนสินทรัพย์ให้เจ้าหน้าที่ผู้รับผิดชอบของ ศทท. เมื่อผู้ใช้งานต้องการยกเลิกสิทธิการครอบครองสินทรัพย์นั้น ๆ หรือพ้นสภาพการเป็นผู้ปฏิบัติงานของ สนข. แล้ว
- ๒.๗ ต้องดำเนินการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ส่วนตัวเมื่อนำมาใช้งานภายในเครือข่าย สนข. และให้เชื่อมต่อกับเครือข่ายของ สนข. ตามนโยบายที่กำหนดเท่านั้น
- ๒.๘ จัดวางสินทรัพย์ต่าง ๆ ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
- ๒.๙ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ที่จำเป็นต้องให้บริการตลอด ๒๔ ชั่วโมง
- ๒.๑๐ ให้ผู้บังคับบัญชา หรือ ผอ.ศทท. อนุมัติก่อนทุกครั้ง ในกรณีที่ต้องการนำคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ออกนอก สนข.
- ๒.๑๑ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่ ศทท. ได้ติดตั้งไว้ให้ใช้งาน
- ๒.๑๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานในการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง
- ๒.๑๓ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของ สนข. เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้น หรือเครือข่ายของ สนข. ได้
- ๒.๑๔ ต้องแจ้งผู้บังคับบัญชาทราบทันทีที่พบว่าสินทรัพย์เสียหาย สูญหาย หรือปรากฏว่ามีผู้อื่นเข้าถึงสินทรัพย์ดังกล่าว โดยที่ผู้ใช้งานมิได้อนุญาตเพื่อจัดการเหตุการณ์ ได้อย่างมีประสิทธิภาพ

ข้อ ๓ การบริหารจัดการบัญชีผู้ใช้งาน (User account) ให้ผู้ใช้งานปฏิบัติตามดังต่อไปนี้

- ๓.๑ เปลี่ยนรหัสผ่านทันทีหลังจากได้รับแจ้งจากผู้ดูแลระบบ
- ๓.๒ กำหนดรหัสผ่าน (Password) ตามหลักเกณฑ์ดังนี้
 - (๑) รหัสผ่านต้องประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และตัวอักขระพิเศษผสมกันไม่น้อยกว่า ๘ ตัว
 - (๒) ไม่ตั้งรหัสผ่านด้วยข้อมูลที่เกี่ยวข้องกับตนเอง เช่น ชื่อตนเองหรือครอบครัว ชื่อเล่น วัน เดือน ปีเกิด หรือทะเบียนรถยนต์
 - (๓) ไม่ตั้งรหัสผ่านด้วยคำศัพท์ที่มีอยู่ในพจนานุกรม
 - (๔) ควรเปลี่ยนรหัสผ่านทุก ๙๐ วัน และไม่ใช้รหัสผ่านที่เคยใช้งานซ้ำ ๓ ครั้งล่าสุด
- ๓.๓ เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่านในการเข้าระบบงานต่าง ๆ ของตนเองไว้เป็นความลับ ไม่เผยแพร่ ไม่แจกจ่าย และไม่ใช้ร่วมกับผู้อื่น หรือทำให้ผู้อื่นล่วงรู้ได้
- ๓.๔ รับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
- ๓.๕ ไม่จดหรือบันทึกบัญชีผู้ใช้งานไว้ในสถานที่ที่ง่ายต่อการคาดเดา หรือสังเกตเห็นของบุคคลอื่น
- ๓.๖ ควรปิดการใช้งาน (Lock) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์
- ๓.๗ เปลี่ยนรหัสผ่านทันทีเมื่อคาดว่าจะมีการลวงรู้รหัสผ่านจากบุคคลอื่น
- ๓.๘ ไม่ใช้รหัสผ่านซึ่งได้เคยใช้มาแล้ว (Password History) อย่างน้อย ๓ รหัสผ่านที่เคยใช้งานล่าสุด
- ๓.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านโดยอัตโนมัติ
- ๓.๑๐ ควรกำหนดจำนวนการใส่รหัสผ่านผิด หากเกินกำหนดให้ระบบจะปิดกั้นการเข้าถึงเป็นเวลา ๑๕ นาที หรือเป็นลำดับไป โดยให้แจ้งผู้ดูแลระบบทันทีหากไม่สามารถใช้งานบัญชีผู้ใช้งานได้
- ๓.๑๑ กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจออัตโนมัติหากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกัน ๑๕ นาที โดยให้ป้อนชื่อผู้ใช้งาน และรหัสผ่านอีกครั้งก่อนเข้าใช้งาน
- ๓.๑๒ หากพบเหตุที่สงสัยว่าถูกผู้อื่นนำรหัสผ่านไปใช้ให้ผู้ใช้งานระบบสารสนเทศดำเนินการเปลี่ยนรหัสผ่าน และแจ้งต่อผู้รับผิดชอบระบบสารสนเทศในทันที

ข้อ ๔ การบริหารจัดการความปลอดภัยเครือข่ายของ สนข. ให้ผู้ใช้งานปฏิบัติตามดังต่อไปนี้

- ๔.๑ ต้องใช้บริการสารสนเทศผ่านระบบเครือข่ายตามที่ สนข. กำหนดไว้เท่านั้น
- ๔.๒ ลงทะเบียนคำขอใช้งาน หรือต้องได้รับอนุญาตจากผู้บังคับบัญชา หรือ ผอ.ศทท. ก่อนการเข้าถึงเครือข่ายภายใน สนข.
- ๔.๓ การใช้งานระบบเครือข่ายอินเทอร์เน็ตผ่านเครือข่ายอินเทอร์เน็ตจากภายนอก สนข. ผู้ใช้งานต้องเชื่อมต่อด้วยเทคโนโลยีเครือข่ายตามที่ สนข. กำหนด
- ๔.๔ ห้ามกระทำการใด ๆ ที่ส่งผลกระทบต่อ ชะลอ ชัดขวาง หรือรบกวนการส่งผ่านข้อมูลการดำเนินงานของ สนข. ในระบบเครือข่ายของ สนข. จนไม่สามารถทำงานตามปกติได้

ข้อ ๕ การใช้งานอุปกรณ์คอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๕.๑ อุปกรณ์คอมพิวเตอร์ที่ สนข. จัดไว้ให้ ถือเป็นสินทรัพย์ของ สนข. และมีวัตถุประสงค์เพื่อใช้ในการดำเนินงานของ สนข. เท่านั้น

๕.๒ ผู้ใช้งานมีหน้าที่ดูแลรักษาอุปกรณ์คอมพิวเตอร์โดยจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้ในสถานที่เสี่ยงต่อการสูญหาย และหลีกเลี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่อาจมีผลกระทบต่อความเสียหายของอุปกรณ์

๕.๓ ผู้ใช้งานต้องรับผิดชอบในการป้องกันการสูญหายของข้อมูล ในกรณีที่อุปกรณ์คอมพิวเตอร์สูญหาย หรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาโดยเร็ว

๕.๔ ผู้ใช้งานต้องดูแลรักษาข้อมูลของ สนข. ที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ให้สอดคล้องตามหลักการบริหารจัดการข้อมูลองค์กร

๕.๕ เมื่อผู้ใช้งานพ้นสภาพการเป็นเจ้าหน้าที่ของ สนข. แล้วต้องส่งอุปกรณ์ คอมพิวเตอร์ และอุปกรณ์เสริมทั้งหมดที่ สนข. จัดไว้ให้ใช้งานคืนต่อ ศทท.

๕.๖ การยืม การคืน หรือส่งซ่อมคอมพิวเตอร์และอุปกรณ์ที่ สนข. จัดไว้ให้ใช้งานให้เป็นไปตามขั้นตอน ปฏิบัติที่กำหนด

๕.๗ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบใด ๆ ของคอมพิวเตอร์ของ สนข. โดยไม่ได้รับอนุญาต

๕.๘ การใช้คอมพิวเตอร์ที่ สนข. จัดไว้ให้ใช้งานในการเข้าถึงระบบสารสนเทศ ของ สนข. ผู้ใช้งานต้องทำยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อน เข้าถึงระบบสารสนเทศของ สนข.

๕.๙ เพื่อป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ เช่น การใช้บัญชีผู้ใช้งานและรหัสผ่าน เทคโนโลยีไบโอเมตริก (Biometric) หรือพินโค้ด (PIN code) เป็นต้น

๕.๑๐ ก่อนการใช้งานกับสื่อบันทึกข้อมูลต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์ โดยใช้โปรแกรมป้องกันไวรัสคอมพิวเตอร์

๕.๑๑ ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์ และอุปกรณ์

๕.๑๒ ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

๕.๑๓ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากที่สูง เป็นต้น

ข้อ ๖ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๖.๑ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของ สนข. หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือนำไปให้ผู้อื่นใช้งาน

๖.๒ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา หากมีการตรวจสอบพบความผิดฐานละเมิดทรัพย์สินทางปัญญา สนข. จะถือว่าเป็นความผิดส่วนบุคคล

๖.๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของ สนข. เพิ่มเติม ก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๖.๔ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของทรัพย์สินทางปัญญาต่าง ๆ

๖.๕ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์สำเร็จรูปที่ สนข. จัดหามาให้ใช้งาน เว้นแต่ สนข. ได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๖.๖ ไม่นำผลงานของผู้อื่นหรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการ “คัดลอก” หรือ “ดัดแปลง” ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หากเกิดกรณีการละเมิดทรัพย์สินทางปัญญา สนข. จะถือว่าเป็นความผิดส่วนบุคคล

ข้อ ๗ การป้องกันโปรแกรมประสงค์ร้ายหรือมัลแวร์ ให้ผู้ใช้งานปฏิบัติตามดังต่อไปนี้

๗.๑ ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือมาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

๗.๒ การนำอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เช่น Thumb drive และ Data Storage มาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ สนข.ให้นำอุปกรณ์มาลงทะเบียนที่ ศทท. และขออนุญาตใช้งานเป็นรายการกรณีไป โดยก่อนการใช้งานขอให้ตรวจสอบหาโปรแกรมประสงค์ร้ายหรือมัลแวร์ก่อนทุกครั้ง

๗.๓ ตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมล (e-mail) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนเปิดใช้งาน

๗.๔ ตรวจสอบฐานข้อมูลไวรัสของโปรแกรมป้องกันไวรัส กรณีไม่ปรับปรุงให้เป็นปัจจุบัน ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบโดยทันที

๗.๕ ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่ สนข. ได้ติดตั้งไว้

๗.๖ ระมัดระวังการเข้าเว็บไซต์ที่มีความเสี่ยงเนื่องจากการเปิดไฟล์หรือเข้าเว็บไซต์อาจได้รับไวรัสจากไฟล์หรือเข้าเว็บไซต์เหล่านั้นได้

ข้อ ๘ การใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติตามดังต่อไปนี้

๘.๑ ปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ อย่างเคร่งครัด

๘.๒ ไม่ใช้งานอินเทอร์เน็ตของ สนข. เพื่อหาประโยชน์ในเชิงธุรกิจ ส่วนตัวและการเข้าสู่เว็บไซต์ที่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาที่เป็นการหมิ่นหรือละเมิดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่กระทบต่อความมั่นคง หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๘.๓ ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับของ สนข. โดยไม่ได้รับอนุญาต

๘.๔ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สนข. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๘.๕ ไม่เสนอความคิดเห็น หรือใช้ข้อความยั่วให้ร้ายบุคคลอื่น หรือข้อมูลที่ผิดกฎหมายในการใช้งานกระดานสนทนา (Webboard)

๘.๖ ไม่ใช้งานโปรแกรมเพียร์ทูเพียร์ (Peer to Peer) ผ่านเครือข่าย สนข.

๘.๗ ไม่ใช้โปรแกรมประเภทบริการส่งข้อความทันที (Instant Messaging : IM) เช่น Line Skype หรือ Messenger (Facebook) เป็นต้น นอกเหนือจากการใช้ปฏิบัติงานผ่านเครือข่าย สนข.

๘.๘ ไม่เข้าเว็บไซต์เครือข่ายสังคม (Social network) เช่น Facebook Twitter หรือ Game online เป็นต้น นอกเหนือจากการใช้ปฏิบัติงานผ่านเครือข่าย สนข.

๘.๙ ไม่ใช้งานสตรีมมิ่งมีเดีย (Streaming media) นอกเหนือจากการใช้ปฏิบัติงานผ่านระบบเครือข่ายของ สนข.

๘.๑๐ ต้องปิดเว็บเบราว์เซอร์ (Web Browser) เมื่อสิ้นสุดการใช้งานเพื่อป้องกันบุคคลอื่นเข้าใช้งานโดยไม่ได้รับอนุญาต

ข้อ ๙ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๙.๑ การปฏิบัติงานที่เกี่ยวข้องกับ สนข. ให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์หรืออีเมล (e-mail Address) ของ สนข. (.....@otp.go.th) ที่ผู้ดูแลระบบกำหนดให้เท่านั้น หากมีการตรวจสอบพบความผิด อันเกิดจากการใช้บัญชีจดหมายอิเล็กทรอนิกส์ส่วนตัว สนข. จะถือว่าเป็นความผิดส่วนบุคคล

๙.๒ ระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์หรืออีเมลเพื่อไม่ให้เกิดความเสียหาย ต่อ สนข. ละเมิดทรัพย์สินทางปัญญา ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือกระทบ ต่อความมั่นคงปลอดภัยไซเบอร์ รวมทั้งไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ ในเชิงธุรกิจ

๙.๓ ห้ามเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลของผู้อื่นโดยไม่ได้รับอนุญาต

๙.๔ ห้ามปลอมแปลงจดหมายอิเล็กทรอนิกส์หรืออีเมล

๙.๕ ใช้คำพูดที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล

๙.๖ สำรองข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลอย่างสม่ำเสมอ

๙.๗ ออกจากระบบ (Log out) ทุกครั้งเมื่อไม่ใช้งานระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๙.๘ ตรวจสอบเอกสารที่แนบมาจากจดหมายอิเล็กทรอนิกส์หรืออีเมลก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัส

๙.๙ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือมีลักษณะ สแปมเมล (Spam mail) เช่น การหลอกลวง การขายสินค้า หรือการสมัครสมาชิก เป็นต้น

๙.๑๐ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นอีเมลลูกโซ่ (Chain e-mail/Letter)

๙.๑๑ ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์หรืออีเมล (Inbox) ของตนเองทุกวันและควรลบ จดหมายอิเล็กทรอนิกส์หรืออีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ระบบจดหมายอิเล็กทรอนิกส์ หรืออีเมล

๙.๑๒ ในกรณีตรวจพบอีเมลหลอกลวง (Phishing Mail) ห้ามเปิดอ่าน ห้ามคลิกลิงก์ และห้ามเปิด ไฟล์แนบโดยเด็ดขาด รวมถึงให้แจ้งต่อ ศทท. ในทันที

ข้อ ๑๐ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๐.๑ กรณีจำเป็นต้องใช้การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของ สนข. ผู้รับผิดชอบต้องแสดงตัวตน ตำแหน่งหน้าที่ และสังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๑๐.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอ เกี่ยวกับการกิจของ สนข. ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๑๐.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของ สนข. ผ่านเครือข่ายสังคม ออนไลน์ (Social network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑๐.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่างต้องชี้แจงด้วยเหตุผล กรณี การโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่อง ที่เกี่ยวข้องต่อไป

๑๐.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจาก สนข. และต้องแสดง ข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑๐.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และแจ้งให้ ศทท. หรือผู้บังคับบัญชาทราบโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๐.๗ ต้องมีความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่เสมอ และต้องรับผิดชอบต่อหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับ สนข. จากการใช้งานเครือข่ายสังคมออนไลน์ (Social network)

๑๐.๘ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่ สนข. ได้กำหนดไว้เท่านั้น

ข้อ ๑๑ การบริหารจัดการข้อมูลองค์กร ให้ผู้ใช้งานปฏิบัติตามต่อไปนี้

การจัดหมวดหมู่และจัดระดับชั้นความลับของข้อมูล สนข. ควรมีกำหนดและการประกาศแนวทางการจัดทำบัญชีข้อมูลภาครัฐ โดยหลักเกณฑ์การพิจารณาการเปิดเผยหรือไม่เปิดเผยข้อมูล จะพิจารณาตามกฎหมายหรือระเบียบที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และระเบียบว่าด้วยการรักษาความลับ ของทางราชการ พ.ศ. ๒๕๔๔ รวมถึงระเบียบ ประกาศ หรือหลักเกณฑ์ของ สนข. เกี่ยวกับเอกสารลับ โดยมีการจำแนกหมวดหมู่ ดังนี้

๑. ข้อมูลส่วนบุคคล (Privacy Data)
๒. ข้อมูลความมั่นคง (National Security Data)
๓. ข้อมูลความลับทางราชการ (Confidential Government Data)
๔. ข้อมูลสาธารณะ (Public Data)

สำหรับการแบ่งระดับชั้นความลับ สามารถแบ่งเป็น ๔ ระดับ ดังนี้

ระดับข้อมูลเปิดเผยได้ (Public) หมายถึง สารสนเทศที่เปิดเผยสู่สาธารณะชน โดยบุคคลที่มีหน้าที่หรือได้รับมอบอำนาจให้ดำเนินการเผยแพร่ได้ โดยสารสนเทศที่เปิดเผยดังกล่าวได้ถูกพิจารณาแล้วว่าเมื่อมอบให้บุคคลอื่นแล้วจะไม่ก่อให้เกิดความเสียหายต่อองค์กร

ระดับข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลหรือสารสนเทศเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่งการดำเนินการและบริหารจัดการข้อมูลส่วนบุคคลจะต้องสอดคล้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของ สนข.

ระดับใช้ภายในเท่านั้น (Internal Use Only หรือ Internal Use) หมายถึง สารสนเทศทั่วไปที่ใช้สื่อสารกันภายในเท่านั้น

ระดับลับ (Confidential) หมายถึง สารสนเทศที่ถูกพิจารณาแล้วว่ามีสำคัญ และหากรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่จะทำให้เกิดความเสียหายต่อความมั่นคงและผลประโยชน์ของรั้อย่างร้ายแรง ซึ่งสามารถแบ่งระดับชั้นความลับได้เป็นลับ ลับมาก และลับที่สุด ซึ่งตัวอย่างหมวดหมู่ข้อมูลที่จะจัดอยู่ในระดับลับขึ้นไป เช่น หมวดหมู่ข้อมูลความลับของทางราชการ และหมวดหมู่ข้อมูลความมั่นคง เป็นต้น

๑๑.๑ ระดับการเข้าถึงข้อมูล

- (ก) การเข้าถึงเพื่อการอ่าน (Read)
- (ข) การเข้าถึงเพื่อการเขียน (Write)
- (ค) การเข้าถึงเพื่อการแก้ไข (Edit)
- (ง) การเข้าถึงเพื่อการลบ (Delete)

ซึ่งผู้ใช้งานต้องได้รับการจัดสรรระดับการเข้าถึงให้สอดคล้องกับรายการข้อมูลที่เปิดเผยหรือไม่สามารถเปิดเผยได้ รวมถึงระดับชั้นความลับของข้อมูล หน้าที่และความรับผิดชอบของเจ้าหน้าที่ผู้ปฏิบัติงาน และสอดคล้องตามหลักการเท่าที่จำเป็นในการใช้งานเท่านั้น

๑๑.๒ รมัควะวังในการนำสือบ้นทักข้อมูลให้ผู้อื่นใช้งาน

๑๑.๓ คุแลร้กษาควลบของข้อมูลลั บ โดยหากข้อมูลอยู่ในรูปแบบบิเล็ทรอนิกส์จะต้งมืการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ หรือพิจารณาใช้มาตรการการเข้ารหัสลับ (Encryption) โดยจะต้องใช้เทคโนโลยีที่ สนข. พิจารณาแล้ว หรืออย่างน้อยจะต้องเป็นเทคโนโลยีที่ได้รับการยอมรับและเป็นที่รู้จักในระดับสากล

๑๑.๔ ไม่นำข้อมูลไปเปิดเผยกับบุคคลซึ่งไม่มีความเกี่ยวข้องกับการปฏิบัติหน้าที่เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาแล้ว

๑๑.๕ กำหนดประเภท ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับข้อมูลสารสนเทศแต่ละชนิดอย่างเหมาะสม

๑๑.๖ เวลาที่ได้เข้าถึง สามารถเข้าถึงข้อมูลได้ตลอดเวลา (๒๔ ชั่วโมง ๗ วัน) หรือตามภารกิจและความจำเป็นของผู้ใช้งานที่ได้รับมอบหมาย โดยผ่านระบบยืนยันตัวตน และในกรณีผู้ใช้งานไม่ใช้งานระบบสารสนเทศเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานจะต้องทำการ Login ระบบและพิสูจน์ตัวตนเพื่อเข้าใช้งานก่อนเข้าใช้ระบบสารสนเทศอีกครั้ง

๑๑.๗ ช่องทางการเข้าถึง ต้องจำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งานเท่านั้น โดย สนข. กำหนดจำนวนช่องทางที่สามารถเข้าถึง ดังนี้

(ก) ช่องทางที่สามารถเข้าถึงระบบสารสนเทศได้โดยผ่านเครือข่ายทางไกลจากภายนอก (VPN)

(ข) ช่องทางที่สามารถเข้าถึงระบบสารสนเทศได้จากระบบเครือข่ายภายใน สนข.

(ค) ช่องทางการรับ - ส่งข้อมูลสำคัญโดยผ่านระบบเครือข่ายสาธารณะ โดยช่องทางและข้อมูลสำคัญดังกล่าว ต้องได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL/TLS หรือ XML Encryption

ข้อ ๑๒ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล ที่ครอบคลุมขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง ช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก วิธีการเข้ารหัสลับข้อมูล (Cryptographic Algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) โดยอย่างน้อยต้องมีกระบวนการที่มีความรัดกุมปลอดภัยที่ครอบคลุมตั้งแต่การสร้างและติดตั้ง การจัดเก็บ การยกเลิกและทำลายกุญแจเข้ารหัสข้อมูล

ข้อ ๑๓ การใช้งานโปรแกรมรรถประโยชน์ (Use of System Utilities) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๓.๑ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่ สนข. ไม่อนุญาตให้ใช้งาน และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ สนข. จะถือว่าเป็นความผิดส่วนบุคคล

๑๓.๒ หากต้องการใช้งานโปรแกรมอรรถประโยชน์ที่ไม่อนุญาต เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานไม่ปลอดภัย ต้องได้รับความเห็นชอบที่เป็นลายลักษณ์อักษรจาก ผอ.ศทท. หรือผู้ที่ได้รับมอบหมาย ให้เป็นผู้พิจารณาอนุญาต

๑๓.๓ กำหนดให้มีการถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศของ สนข. ที่ไม่จำเป็นออกจากระบบเมื่อไม่จำเป็นต้องใช้งาน

ข้อ ๑๔ หน้าที่และความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๑๔.๑ ศึกษานโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายการคุ้มครองข้อมูลส่วนบุคคล แนวปฏิบัติและขั้นตอนปฏิบัติต่าง ๆ ที่ สนข. ประกาศกำหนดและปฏิบัติ ตามอย่างเคร่งครัด ในกรณีที่ฝ่าฝืนนโยบายและแนวปฏิบัติเหล่านี้ อาจนำมาซึ่งความรับผิดทางวินัย โทษทางปกครอง หรือความรับผิดทางอาญาได้ ทั้งนี้ หากเกิดการกระทำ ความผิดให้มีการตรวจสอบเพื่อดำเนินการทางวินัยต่อไป

๑๔.๒ ป้องกันการเข้าถึงอุปกรณ์ประมวลผลสารสนเทศทุกชนิด เช่น เครื่องคอมพิวเตอร์พีซี โน้ตบุ๊ก ที่ตนได้รับอนุญาตให้ใช้งาน โดยการกำหนดบัญชีผู้ใช้งานและรหัสผ่านหรือวิธีการอื่น ตามความสามารถของอุปกรณ์ เช่น การใช้รหัสผ่าน การใช้ PIN Code เป็นต้น

๑๔.๓ ไม่อนุญาตให้ใช้ USB port ในการเชื่อมต่อกับเครื่องคอมพิวเตอร์ของ สนข. และทำการถ่ายโอนข้อมูลการใช้งาน USB port ที่มีความเสี่ยง ซึ่ง สนข. มีความจำเป็นต้องควบคุมอย่างเคร่งครัด หากมีความจำเป็นต้องใช้งาน ผู้ใช้จะต้องได้รับอนุญาตจาก ศทท. แล้วเท่านั้น

๑๔.๔ ไม่อนุญาตให้นำข้อมูลส่วนบุคคลที่ สนข. ประมวลผลไปจัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์ หรือสื่อบันทึกข้อมูลส่วนบุคคล

๑๔.๕ ดูแลรับผิดชอบบัญชีผู้ใช้งานและรหัสผ่าน ไม่อนุญาตให้ผู้อื่นนำไปใช้งาน และเก็บข้อมูลรหัสผ่านหรือข้อมูลที่ใช้ในการพิสูจน์ตัวตนไว้เป็นความลับ

๑๔.๖ ไม่เข้าถึงข้อมูลสารสนเทศและระบบที่ตนไม่ได้รับอนุญาต

๑๔.๗ ดูแลรักษาข้อมูลสารสนเทศ และข้อมูลส่วนบุคคลให้สอดคล้องตามระดับชั้นความลับ ตลอดจนทั้งวงจรชีวิตของข้อมูลสารสนเทศ และข้อมูลส่วนบุคคลนั้น ตั้งแต่การสร้าง สำเนา แจกจ่าย ถ่ายโอน ไปจนกระทั่งลบทำลาย หรือการเก็บรวบรวม ใช้ เผยแพร่ ไปจนกระทั่งลบทำลาย

๑๔.๘ ไม่ส่งข้อมูลลับ สารสนเทศลับ และข้อมูลส่วนบุคคลผ่านอีเมล อินเทอร์เน็ต หรือช่องทางสื่อสารอื่น ๆ ด้วยวิธีการที่ไม่ปลอดภัย ในกรณีที่มีความจำเป็นต้องใช้มาตรการในการเข้ารหัส เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๑๔.๙ ไม่แอบดูข้อมูลลับบนเครื่องคอมพิวเตอร์ของผู้อื่น และระมัดระวังการพิมพ์เอกสารที่มีชั้นความลับ

๑๔.๑๐ ไม่จัดเก็บเอกสารที่มีข้อมูลลับไว้นานเกินความจำเป็น และดำเนินการทำลายด้วยวิธีการที่เหมาะสม เช่น ทำลายด้วยเครื่องทำลายเอกสาร เป็นต้น

๑๔.๑๑ ไม่ปล่อยหน้าจอคอมพิวเตอร์ค้างไว้ เมื่อไม่มีการใช้งาน และล็อกหน้าจอก่อนออกไปจากหน้าจอ หรือตั้งค่า Screen Saver ตามระยะเวลาที่กำหนดหรือตามระดับความสำคัญของข้อมูลที่กำลังใช้งาน

๑๔.๑๒ แจ้งผู้บังคับบัญชา หรือแจ้ง ศทท. เกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่ สนข. กำหนดทันที เมื่อพบเหตุต้องสงสัยว่าอาจจะเป็นการละเมิดความมั่นคงปลอดภัยสารสนเทศ หรือการละเมิดข้อมูลส่วนบุคคล

๑๔.๑๓ มีความตระหนักในการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศต่าง ๆ ของ สนข. อาทิ เครือข่ายคอมพิวเตอร์ที่ให้บริการ เครื่องคอมพิวเตอร์พีซี โน้ตบุ๊ก โดยทรัพยากรสารสนเทศของ สนข. มีไว้เพื่อใช้ในการปฏิบัติงานเท่านั้น และ สนข. โดย ศทท. มีสิทธิในการติดตามตรวจสอบการใช้งานที่ไม่เหมาะสม และระงับหรือปิดกั้นการเข้าใช้งานเครือข่ายสารสนเทศของ สนข. ได้ตามความเหมาะสม

๑๔.๑๔ กรณีที่ ศทท. ตรวจสอบพบบัญชีผู้ใช้งานใดที่ถูกครอบครอง โดยผู้ไม่ประสงค์ดี (Compromised) บัญชีผู้ใช้งานนั้นจะถูกยกเลิกหรืองดใช้งานชั่วคราวตามแต่กรณี และ ศทท. จะแจ้งวิธีปฏิบัติต่าง ๆ และการคืนสิทธิให้เมื่อดำเนินการระงับเหตุเรียบร้อยแล้ว

หมวด ๓

แนวปฏิบัติการบริหารจัดการด้านความมั่นคงปลอดภัย สำหรับผู้ดูแลระบบ

ข้อ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑.๑ กำหนดมาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูลของ สนข. เพื่อดูแลรักษาความปลอดภัย โดยบุคคลไม่มีสิทธิในการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูล ต้องการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูล ต้องแจ้งต่อ ศทท. ทราบ เป็นลายลักษณ์อักษร หรือต้องมีเจ้าหน้าที่ ศทท. กำกับดูแลตลอดระยะเวลาที่อยู่ในห้องปฏิบัติการศูนย์ข้อมูล

๑.๒ พิจารณานุมัติและกำหนดสิทธิการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูลให้เป็นไปตามภารกิจของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชา หรือ ผอ.ศทท. เท่านั้น

๑.๓ ต้องทำการยืนยันตัวตนก่อนเข้าห้องปฏิบัติการศูนย์ข้อมูลทุกครั้งเพื่อป้องกันการเข้า-ออกโดยไม่ได้รับอนุญาต

๑.๔ ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ของผู้ใช้งาน และบุคคลภายนอก (Visitors) ทุกครั้ง

๑.๕ ควบคุมให้ผู้เข้า-ออกติดบัตรผู้มาติดต่อให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ห้องปฏิบัติการศูนย์ข้อมูล

๑.๖ ตรวจสอบการเข้าถึงสถานที่ที่มีระบบสารสนเทศที่สำคัญติดตั้งอยู่อย่างต่อเนื่อง รวมถึงจัดให้มีอุปกรณ์หรือเครื่องมือแจ้งเตือน เพื่อตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาตหรือพฤติกรรมที่น่าสงสัย

๑.๗ ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงานในห้องปฏิบัติการศูนย์ข้อมูลจนกระทั่งเสร็จสิ้นภารกิจและออกจากห้องปฏิบัติการศูนย์ข้อมูล เพื่อป้องกันการสูญหายของสินทรัพย์หรือ ป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๑.๘ แยกพื้นที่ในการส่งมอบสินทรัพย์ เพื่อตรวจสอบให้เสร็จเรียบร้อยก่อนนำเข้าไปติดตั้งหรือใช้งานภายในห้องปฏิบัติการศูนย์ข้อมูล

๑.๙ ประชาสัมพันธ์มาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูล แก่ผู้ใช้งาน และบุคคลภายนอก (Visitors)

๑.๑๐ ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในห้องปฏิบัติการศูนย์ข้อมูล

๑.๑๑ ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงไฟในบริเวณภายในห้องปฏิบัติการศูนย์ข้อมูล

๑.๑๒ ต้องทำการยกเลิก เพิกถอน หรือเปลี่ยนแปลงการอนุญาตการเข้า-ออกห้องปฏิบัติการศูนย์ข้อมูลของผู้ใช้งานเมื่อผู้นั้นพ้นสภาพการเป็นเจ้าหน้าที่ของ สนข.

๑.๑๓ ทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญภายในห้องปฏิบัติการศูนย์ข้อมูลอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๒.๑ จัดวางระบบสารสนเทศที่มีความสำคัญในพื้นที่ที่มีความมั่นคงและปลอดภัย เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงพอร์ตของระบบที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๒.๒ แยกจัดเก็บระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ที่สำคัญไว้ในพื้นที่ความปลอดภัยสูง แยกต่างหาก

๒.๓ ต้องควบคุมและป้องกันการใช้งานพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ที่การเข้าถึงทางกายภาพและทางเครือข่าย โดยต้องมีการขออนุญาตเข้าถึงพอร์ตดังกล่าวอย่างเป็นทางการเป็นลายลักษณ์อักษร และมีการบันทึกการใช้งานทุกครั้ง รวมถึงมีการตรวจสอบบันทึกการใช้งาน อย่างสม่ำเสมอเป็นประจำ หรืออย่างน้อยทุก ๓ เดือน

ข้อ ๓ การกำหนดและควบคุมการเดินสายสัญญาณสื่อสาร และสายไฟฟ้า ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ๓.๑ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้เป็นไปด้วยความเรียบร้อยและปลอดภัย
- ๓.๒ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณ
- ๓.๓ ทำแผนผังการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้ครบถ้วนและถูกต้อง
- ๓.๔ ปิดประตูตู้ Rack สำหรับติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณสื่อสารให้สนิทรวมถึงการล็อกประตูเพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง
- ๓.๕ จัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารและบนอุปกรณ์เพื่อป้องกันการปฏิบัติงานผิดพลาด
- ๓.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อความปลอดภัยและตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๔ การกำหนดการบำรุงรักษาระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ๔.๑ จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ
- ๔.๒ กำหนดเงื่อนไขของการให้บริการในสัญญาการบำรุงรักษาให้ชัดเจนเพื่อให้ผู้รับจ้างต้องติดต่อกลับ และเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม
- ๔.๓ ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายของระบบสารสนเทศ
- ๔.๔ บำรุงรักษาระบบสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ในสัญญาการบำรุงรักษา
- ๔.๕ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่คุณผลิตแนะนำ
- ๔.๖ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง
- ๔.๗ บันทึกปัญหาและข้อบกพร่องที่พบและรายงานให้ ผอ.ศทท. ทราบ
- ๔.๘ ควบคุม และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาการจ้างเหมาบำรุงรักษา
- ๔.๙ กำหนดสิทธิของผู้ให้บริการภายนอกในการเข้าถึงพื้นที่ อุปกรณ์ และข้อมูลที่สำคัญ
- ๔.๑๐ การบริหารจัดการช่องโหว่ทางเทคนิคภายหลังจากการติดตั้งและใช้งานระบบสารสนเทศ
 - ๔.๑๐.๑ จัดให้มีผู้รับผิดชอบในการติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) เป็นต้น

๔.๑๐.๒ ดำเนินการประเมินระดับความรุนแรงของช่องโหว่ที่มีการประกาศ และวิเคราะห์ ประเมินผลกระทบในกรณีที่ช่องโหว่นั้นเกิดกับระบบสารสนเทศในความดูแลและวางแผนในการปรับปรุงแก้ไข ช่องโหว่ดังกล่าวโดยเร็วที่สุด โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤต และระดับสูง

๔.๑๐.๓ ดำเนินการปรับปรุงและแก้ไขช่องโหว่ตามขั้นตอนปฏิบัติการบริหารจัดการ การเปลี่ยนแปลงที่ สนข. กำหนด และแจ้งผลการปรับปรุงแก้ไขกลับมายัง ศทท. เพื่อทราบและตรวจสอบผล การปรับปรุงแก้ไข

ข้อ ๕ การบริหารจัดการสินทรัพย์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๕.๑ บันทึกและตรวจสอบสินทรัพย์ เพื่อเก็บเป็นหลักฐานในการตรวจสอบความถูกต้อง และป้องกันการสูญหาย

๕.๒ กำหนดมาตรการหรือขั้นตอนการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่าย หรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ ให้ผู้ดูแลระบบดำเนินการตาม มาตรการทำลายข้อมูล และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่เหมาะสมกับระดับชั้นความลับของข้อมูล ที่ สนข. ได้กำหนด หมายความว่ารวมถึงสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่อยู่ในอุปกรณ์ที่ สนข. ใช้งานด้วย เพื่อลดความเสี่ยงของการรั่วไหลของข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามมาตรการ ดังนี้

๕.๒.๑ ผู้ดูแลระบบต้องตรวจสอบประเภทของข้อมูลบนสื่อบันทึกข้อมูลและคัดแยก สื่อบันทึกข้อมูล ออกตามหมวดหมู่หรือประเภทตามระดับชั้นความลับ

๕.๒.๒ ข้อมูลลับ ข้อมูลลับมาก ข้อมูลลับที่สุด หรือข้อมูลส่วนบุคคล ซึ่งอยู่บนกระดาด หรือวัสดุชั่วคราว ต้องดำเนินการทำลายกระดาดหรือวัสดุชั่วคราวนั้นตามนโยบายการเก็บรักษา และการลบ ทำลายข้อมูลส่วนบุคคล (Data Retention and Disposal Policy) ที่ สนข. กำหนด รวมถึงขั้นตอนปฏิบัติที่เกี่ยวข้อง

๕.๒.๓ ข้อมูลสารสนเทศที่อยู่บนเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ จะต้องทำการลบ หรือเขียนทับข้อมูลที่มีความสำคัญในสื่อบันทึกข้อมูลด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก ด้วยวิธีการทำลายแยกตามประเภทของสื่อบันทึกข้อมูล ได้แก่

- Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- กระดาด ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสารหรือทำลายตาม ขั้นตอนปฏิบัติของ สนข.
- แผ่น CD/DVD ใช้วิธีการหั่นด้วยเครื่องหั่นทำลายเอกสาร
- เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
- ฮาร์ดดิสก์ ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการเขียนทับ ให้ไม่สามารถนำข้อมูลกลับมาใช้ได้ อีก ตามมาตรฐาน การทำลายข้อมูลบนสื่อบันทึกข้อมูลอ้างอิงตามมาตรฐาน NIST ๘๐๐-๘๘ Revision ๑ แนวทางการลบทำลายข้อมูล บนสื่อบันทึกข้อมูล (Guideline for Media Sanitization)

๕.๒.๔ ในการทำลายสื่อบันทึกข้อมูล ผู้ดูแลระบบพิจารณาทำลายสื่อบันทึกข้อมูล ด้วยวิธีการทำลายแยกประเภทตามสื่อบันทึกข้อมูลและใช้วิธีการทำลายตามขั้นตอนปฏิบัติของ สนข.

๕.๓ กรณีที่สินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซม นอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญ ต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ ๖ การควบคุมการใช้งานระบบสารสนเทศและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพาให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๖.๑ ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัว หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของ สนข. ที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อบริษัทเครือข่ายภายในและเข้าถึงระบบสารสนเทศของ สนข. แจ้งขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพาที่ ศทท. และปฏิบัติตามขั้นตอนปฏิบัติที่ ศทท. กำหนดเพื่อป้องกันการเข้าถึงระบบสารสนเทศ ด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

๖.๒ ต้องกำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วยบัญชีผู้ใช้งานและรหัสผ่าน หรือเทคโนโลยีไบโอเมตริก (Biometric) หรือพินโค้ด (PIN code) เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาของตน

๖.๓ ต้องดูแลรักษาข้อมูลองค์กรในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องตามข้อกำหนดการบริหารจัดการข้อมูล

๖.๔ ต้องแจ้งผู้บังคับบัญชาและ ผอ.ศทท. ทันทีที่พบว่าอุปกรณ์คอมพิวเตอร์เสียหาย สูญหาย หรือเปลี่ยนเครื่องใหม่ เพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๗ การควบคุมการใช้งานระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

เป็นการควบคุมบุคคลที่ใช้งานระบบสารสนเทศ รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น โดยให้ผู้ดูแลระบบปฏิบัติ ดังต่อไปนี้

๗.๑ กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศตามการแบ่งระดับชั้นและสิทธิการเข้าถึง ดังนี้

๑) ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูล

๒) ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๓) ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูล และรายงานข้อมูลตามความต้องการของ สนข.

๔) ระดับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่ สนข. มอบให้เท่านั้น

๗.๒ ดำเนินการทบทวนและปรับปรุงการใช้งานระบบสารสนเทศให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย โดยผู้ดูแลระบบต้องจัดให้มีการสำรวจ ตรวจสอบ หรือประเมินผลการใช้งานระบบสารสนเทศ รวมทั้งมีการรวบรวมและรายงานปัญหาและข้อเสนอแนะการใช้งานระบบสารสนเทศต่อ สนข. อย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการทบทวน และปรับปรุงการใช้งานระบบสารสนเทศให้เหมาะสมกับภาระงานในปัจจุบัน

๗.๓ การอนุมัติและกำหนดระดับสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาแล้วเท่านั้น

๗.๔ กำหนดการเข้าถึงด้วยบัญชีผู้ใช้งานแยกเป็นรายบุคคลตามภารกิจ หรือแนวปฏิบัติของแต่ละหน่วยงานภายในที่ผู้ใช้งานปฏิบัติงาน

๗.๕ จัดเก็บข้อมูลการลงทะเบียนสำหรับสร้างบัญชีผู้ใช้งานไว้เพื่อการตรวจสอบในภายหลัง

๗.๖ กำหนดให้ทำการยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศ

๗.๗ กำหนดระยะเวลาการออกจากระบบสารสนเทศโดยอัตโนมัติเมื่อไม่มีการใช้งานเกิน ๓๐ นาที หรือตามความสำคัญของข้อมูลระบบสารสนเทศ

๗.๘ กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศที่สำคัญของ สนข. ตามภารกิจ และความจำเป็นของผู้ใช้งาน

๗.๙ กำหนดให้เครื่องคอมพิวเตอร์ที่จัดหาโดย สนข. พักหน้าจอ (Screen saver) โดยอัตโนมัติ หากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกัน ๑๕ นาที

๗.๑๐ จำกัดระยะเวลาในการเชื่อมต่อ (Limitation of Connection Time) ระบบสารสนเทศ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง ดังนี้

๗.๑๐.๑ กำหนดให้มีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานไม่เกิน ๘ ชั่วโมง หรือตั้งแต่เวลา ๘.๓๐ - ๑๖.๓๐ น. สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูงของ สนข.

๗.๑๐.๒ กำหนดให้ระบบสารสนเทศที่มีการใช้งานในสถานที่สาธารณะหรือพื้นที่ภายนอก สนข. จำกัดช่วงระยะเวลาการเชื่อมต่ออย่างน้อยไม่เกิน ๘ ชั่วโมงต่อ ๑ ครั้งการเชื่อมต่อ

๗.๑๑ จำกัดและควบคุมการเข้าถึงฟังก์ชัน (Functions) ต่าง ๆ ในการใช้งานระบบสารสนเทศของผู้ใช้งานและผู้ดูแลระบบ

๗.๑๒ ระบบซึ่งวางไว้ต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ สนข. ต้องแยกเครือข่ายออกจากระบบอื่น ๆ ต้องมีการควบคุมสภาพแวดล้อมแยกเป็นสัดส่วน และต้องกำหนดสิทธิการใช้งานเฉพาะผู้ที่มีสิทธิเท่านั้น

๗.๑๓ จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุ และพิสูจน์ตัวตนผู้ใช้งานที่มีความมั่นคงปลอดภัย อย่างน้อยดังนี้

- ผู้ใช้งานต้องสามารถกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยตามการบริหารจัดการบัญชีผู้ใช้งาน (User Account) ด้วยตนเอง

- ระบบสารสนเทศที่สำคัญต้องมีการใช้งานปัจจัยหลายอย่างในการระบุและพิสูจน์ตัวตน (Multi-Factor Authentication : MFA)

- ต้องจำกัดจำนวนครั้งในการล็อกอินที่ผิดพลาดได้ เช่น ล็อกอินผิดพลาดได้ไม่เกิน ๓ ครั้ง และมีการหน่วงเวลาในการล็อกอินยาวขึ้น เมื่อมีการล็อกอินผิดพลาดเกินกว่า ๓ ครั้ง

- ไม่ใช้ฟังก์ชันช่วยเหลือใด ๆ ในระหว่างที่ทำการล็อกอินเข้าสู่ระบบ

- ระบบต้องมีการแสดงประวัติวันเวลาที่ล็อกอินเข้าใช้งานระบบย้อนหลังได้

รวมถึงต้องกำหนดให้มีการบริหารจัดการรหัสผ่านอย่างรัดกุม โดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ผู้ใช้งาน (User) ได้รับการส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

๗.๑๔ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อผู้นั้นพ้นสภาพการเป็นเจ้าหน้าที่ของ สนข. ภายในระยะเวลา ๑ วันทำการ หลังจากที่ได้รับแจ้งเป็นลายลักษณ์อักษร

๗.๑๕ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานกรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลง หลังจากได้รับแจ้งจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๗.๑๖ ดำเนินการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ เพื่อป้องกันการเข้าถึงระบบสารสนเทศ โดยไม่ได้รับอนุญาต

ข้อ ๘ การบริหารจัดการความปลอดภัยเครือข่าย ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ๘.๑ กำหนดวิธีปฏิบัติเกี่ยวกับการใช้งานเครือข่ายทั้งภายในและภายนอก สนข.
- ๘.๒ กำหนดขั้นตอนการขออนุญาตเพื่อเข้าถึงระบบสารสนเทศที่อยู่ภายในเครือข่ายของ สนข. โดยจัดให้มีมาตรการควบคุมการเชื่อมต่อระยะไกล (Remote Desktop Protocol : RDP) สำหรับผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่ต้องการเชื่อมต่อเข้ามายังเครื่องปลายทางภายใน สนข.
- ๘.๓ ควบคุมการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายของ สนข. ที่มีการเข้าใช้งาน โดยผู้ให้บริการภายนอกตามขั้นตอนปฏิบัติที่ สนข. กำหนด
- ๘.๔ กำหนดขั้นตอนการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งานภายนอก สนข. อย่างมั่นคงปลอดภัย เช่น การเชื่อมต่อระบบเครือข่ายด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN)
- ๘.๕ ต้องควบคุมการจัดเส้นทางบนเครือข่ายทั้งหมดของ สนข. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก รวมทั้งการเชื่อมต่อระหว่าง สนข. กับหน่วยงานภายนอก โดยต้องเชื่อมต่อผ่านอุปกรณ์ไฟร์วอลล์ และอุปกรณ์ป้องกันการบุกรุกเท่านั้น
- ๘.๖ ระบุบริการที่ สนข. อนุญาตให้ใช้งานหรือบริการผ่านระบบเครือข่ายของ สนข.
- ๘.๗ กำหนดให้มีการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศของ สนข.
- ๘.๘ จัดทำทะเบียนอุปกรณ์ที่ใช้งานในระบบเครือข่าย โดยอย่างน้อยประกอบด้วยข้อมูลหมายเลขประจำเครื่อง ยี่ห้อ แบบรุ่น หมายเลข MAC Address หมายเลข IP Address ที่มา ผู้รับผิดชอบ วันที่เริ่มติดตั้ง วันที่เลิกใช้งาน และเหตุผลที่เลิกใช้งาน
- ๘.๙ ใช้ข้อมูล MAC Address หรือ IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่าย เพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่ายของ สนข. และใช้วิธีการทางเทคนิคที่เหมาะสมในการควบคุมการเข้าถึงอุปกรณ์เครือข่ายเหล่านั้น
- ๘.๑๐ กำหนดให้เฉพาะเครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถบริหารจัดการระบบและอุปกรณ์เครือข่ายของ สนข.
- ๘.๑๑ ตรวจสอบและปิดพอร์ตบนระบบและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- ๘.๑๒ ป้องกันและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการอุปกรณ์ในระบบเครือข่ายทั้งจากภายในและภายนอก สนข.
- ๘.๑๓ จัดแบ่งเครือข่ายตามวัตถุประสงค์การใช้งาน บริการ หรือกลุ่มผู้ใช้งาน เช่น เครือข่ายสำหรับผู้ใช้งาน เครือข่ายสำหรับเครื่องแม่ข่าย หรือเครือข่ายสำหรับทดสอบทดลองระบบ เป็นต้น โดยแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย
- ๘.๑๔ ใช้วิธีการทางเทคนิคบนไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ จำกัดเส้นทางบนเครือข่ายที่ สนข. ไม่อนุญาตให้ใช้งาน เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะเส้นทางบนเครือข่ายที่อนุญาตเท่านั้น
- ๘.๑๕ กำหนดมาตรการป้องกันระบบสารสนเทศที่ต้องเชื่อมโยงกับระบบเครือข่ายสาธารณะอย่างมีประสิทธิภาพ

๘.๑๖ ต้องตรวจสอบและกำหนดเส้นทางเครือข่าย (Network Routing Control) ให้เหมาะสม โดยต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการสารสนเทศได้แก่ระบบอินเทอร์เน็ต และระบบอินทราเน็ต เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ เพื่อเข้าถึงระบบที่นอกเหนือจากที่ได้รับอนุญาตได้

๘.๑๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเกิดขึ้น

๘.๑๘ กำหนดมาตรการป้องกันข้อมูลที่ส่งผ่านทางเครือข่ายสาธารณะเพื่อรักษาความลับและความถูกต้องของข้อมูลที่สำคัญ

๘.๑๙ กำหนดเส้นทางบนเครือข่ายที่เหมาะสมเพื่อควบคุมการเชื่อมต่อ และการไหลเวียนของสารสนเทศบนเครือข่ายให้มีประสิทธิภาพ ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายใน สนข. และระหว่าง สนข. กับหน่วยงานภายนอก โดยการแลกเปลี่ยนสารสนเทศให้ปฏิบัติ ดังนี้

๘.๑๙.๑ ต้องควบคุมให้มีการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางที่ปลอดภัย ทั้งการแลกเปลี่ยนสื่อบันทึกข้อมูลทางกายภาพ และการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่าย โดยหากเป็นการแลกเปลี่ยนข้อมูลสารสนเทศผ่านระบบเครือข่ายต้องให้มีการเข้ารหัสข้อมูลอย่างเหมาะสม ระหว่างการสื่อสารแลกเปลี่ยน รวมถึงการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) หรือการทำธุรกรรมออนไลน์ (Online Transaction) เพื่อไม่ให้มีการรับ - ส่งข้อมูลที่ไม่สมบูรณ์ หรือมีการรั่วไหลของข้อมูล หรือมีการแก้ไขข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๘.๑๙.๒ เจ้าของข้อมูลต้องทำการตรวจสอบประเภทของข้อมูลสารสนเทศและลำดับชั้นความลับของข้อมูลสารสนเทศตามที่กำหนดไว้ในขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูลที่จะดำเนินการแลกเปลี่ยน เพื่อควบคุมการแลกเปลี่ยนให้เหมาะสม และป้องกันข้อมูลสำคัญจากการถูกเข้าถึงการเปลี่ยนแปลงแก้ไข การสำเนา และการทำลายโดยไม่ได้รับอนุญาต รวมทั้งการแจกจ่ายหรือส่งผิดตัวผู้รับ

๘.๒๐ ตรวจสอบการใช้งานระบบเครือข่ายด้วยระบบตรวจจับและป้องกันการบุกรุกของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติอย่างสม่ำเสมอ หรืออย่างน้อยเดือนละ ๑ ครั้ง

๘.๒๑ ทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละ ๑ ครั้ง หรือตามสถานการณ์ของภัยคุกคามทางไซเบอร์ในระบบเครือข่าย และนำผลที่ได้ไปปรับปรุงความมั่นคงปลอดภัยระบบเครือข่ายของ สนข. ให้มีความมั่นคงปลอดภัยมากขึ้นและทันต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน

๘.๒๒ ติดตาม ตรวจสอบ ดูแล และปรับปรุงเครือข่ายของ สนข. ให้มีความมั่นคงปลอดภัย และทันสมัยอยู่เสมอ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานระบบเครือข่ายให้รีบดำเนินการแก้ไข และแจ้งให้ ผอ.ศทท. และผู้บังคับบัญชาทราบทันที เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้น

๘.๒๓ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน ต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อผู้นั้นพ้นสภาพการเป็นเจ้าหน้าที่ของ สนข. โดยกำหนดให้ผู้ดูแลระบบยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานภายในระยะเวลา ๑ วันทำการ หลังจากที่ได้รับแจ้งเป็นลายลักษณ์อักษร

๘.๒๔ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งานกรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๘.๒๕ ดำเนินการทบทวนสิทธิการเข้าถึงเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอหรืออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

๘.๒๖ การติดตั้งและใช้งานเครือข่ายไร้สาย (Wi-Fi) ให้ดำเนินการดังนี้

๘.๒๖.๑ ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๘.๒๖.๒ ต้องกำหนดให้ผู้ใช้งานใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi-Fi) รวมถึงทำประกาศความเป็นส่วนตัวเจ้าของข้อมูลส่วนบุคคลทราบ

๘.๒๖.๓ ต้องกำหนดให้การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (Wi-Fi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิของเครือข่ายไร้สาย (Wi-Fi) เท่านั้น

ข้อ ๙ การบริหารจัดการในการปฏิบัติงาน ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๙.๑ ไม่นำข้อมูลสารสนเทศของ สนข. ไปเปิดเผยกับบุคคลซึ่งไม่ได้มีความเกี่ยวข้องกับ การปฏิบัติหน้าที่ เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาและ ผอ.ศทท. แล้ว

๙.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือเปิดเผยข้อมูลส่วนบุคคล ของผู้ใช้งาน

๙.๓ เก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เท่าที่จำเป็นตามที่กำหนดไว้ในกฎหมาย ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๙.๔ ตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดใน สนข. ให้ตรงกับเวลา อ้างอิงสากล

๙.๕ บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ในการตรวจสอบ อย่างสม่ำเสมอ

๙.๖ ตรวจสอบและดูแลสภาพแวดล้อมของห้องปฏิบัติการศูนย์ข้อมูล รวมทั้งระบบสนับสนุน การทำงานต่าง ๆ เพื่อป้องกันความเสียหายต่อระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ

๙.๗ จำกัดและควบคุมการใช้งานโปรแกรมมัลแวร์สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมมัลแวร์บางชนิดสามารถทำให้ผู้ใช้งานหลักเสี่ยงมาตรการป้องกัน ทางด้านความมั่นคงปลอดภัยด้านสารสนเทศของระบบได้ ดังนั้น เพื่อป้องกันการละเมิดหรือหลักเสี่ยงมาตรการ ความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรม มัลแวร์

(๒) กำหนดการอนุญาตใช้งานโปรแกรมมัลแวร์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมมัลแวร์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมมัลแวร์ที่ไม่จำเป็นออกจากเครื่อง คอมพิวเตอร์

ข้อ ๑๐ การสำรองและกู้คืนข้อมูลสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๐.๑ กำหนดขั้นตอนการสำรองและกู้คืนข้อมูลรวมถึงซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ โดยมี รายละเอียดอย่างน้อย ดังนี้

- (๑) กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องสำรองข้อมูลไว้
 - (๒) ชื่อระบบสารสนเทศ
 - (๓) ผู้รับผิดชอบในการสำรองข้อมูล
 - (๔) ประเภทข้อมูล เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้องกับข้อมูลล็อก (Logs) ข้อมูลบัญชีผู้ใช้งานในระบบ เป็นต้น
 - (๕) ความถี่ในการสำรองข้อมูล
 - (๖) วิธีการสำรองข้อมูล
 - (๗) สื่อที่ใช้บันทึก
- ๑๐.๒ สำรองข้อมูลตามขั้นตอนและความถี่ที่กำหนดไว้ในแต่ละระบบ
 - ๑๐.๓ ตรวจสอบผลสำเร็จของการสำรองข้อมูลทุกครั้ง
 - ๑๐.๔ เลือกใช้สื่อที่เหมาะสม โดยมีอายุจัดเก็บตามระยะเวลาที่กำหนด
 - ๑๐.๕ นำข้อมูลสำรองไปเก็บไว้ในสถานที่อย่างน้อย ๑ ชุด
 - ๑๐.๖ สุ่มข้อมูลสำรองมาทดสอบกู้คืนเพื่อตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลในกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง
 - ๑๐.๗ ทบทวนขั้นตอนการสำรองและกู้คืนข้อมูลและประเมินประสิทธิภาพการดำเนินการอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

ข้อ ๑๑ การบริหารจัดการการเข้ารหัสลับ (Encryption) ข้อมูล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ๑๑.๑ จัดทำและปฏิบัติตามขั้นตอนปฏิบัติการเข้ารหัสข้อมูลตามที่ สนข. กำหนดอย่างเคร่งครัด ซึ่งขั้นตอนปฏิบัติดังกล่าวต้องสอดคล้องตามระดับความสำคัญของข้อมูลตามที่ สนข. กำหนด
- ๑๑.๒ กำหนดหลักเกณฑ์เพื่อให้การดำเนินการเกี่ยวกับการเข้ารหัสข้อมูลให้เป็นไปในทิศทางเดียวกัน และสอดคล้องตามระดับความสำคัญของข้อมูล
- ๑๑.๓ จัดทำและปฏิบัติตามขั้นตอนปฏิบัติการบริหารจัดการกุญแจเข้ารหัสข้อมูล เพื่อให้มีกระบวนการที่รัดกุมตลอดช่วงเวลาการใช้งาน (Key Management Whole Life Cycle) โดยมีการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของกุญแจเพื่อเข้ารหัส การจัดเก็บ การใช้งาน และการยกเลิกการใช้งานกุญแจรหัส
- ๑๑.๔ มีการอนุญาตการเข้าถึงรหัสลับเฉพาะผู้ที่รับผิดชอบเท่านั้น เพื่อป้องกันการถูกแก้ไขหรือเปิดเผยรวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามขั้นตอนปฏิบัติดังกล่าวอย่างเคร่งครัด

ข้อ ๑๒ การบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ๑๒.๑ จัดทำและปฏิบัติตามขั้นตอนปฏิบัติการใช้บริการคลาวด์ ตั้งแต่กระบวนการก่อนเริ่มต้นใช้งาน การใช้งาน การบริหารจัดการและการยกเลิกใช้บริการคลาวด์ อย่างมั่นคงปลอดภัย
- ๑๒.๒ จัดทำและปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการใช้บริการคลาวด์
- ๑๒.๓ ก่อนดำเนินการคัดเลือกผู้ให้บริการคลาวด์ต้องประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการคลาวด์ (Due Diligence) การพิจารณาถึงการได้รับการรับรองตามมาตรฐานสากลรายงานผลการตรวจประเมินที่น่าเชื่อถือ (เช่น SOGs Report) วิธีการที่จะเปลี่ยนหรือยกเลิกการใช้บริการคลาวด์ แนวทางในการถอดถอนบริการออกจากผู้ให้บริการคลาวด์นั้น ๆ และกำหนดหลักเกณฑ์ในการคัดเลือกบริการคลาวด์ให้เหมาะสมกับขอบเขตการใช้งานของ สนข.

๑๒.๔ กำหนดบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการใช้การบริหารจัดการบริการคลาวด์ และการรักษาความมั่นคงปลอดภัยไว้อย่างชัดเจน

๑๒.๕ พิจารณาอย่างรอบคอบเกี่ยวกับกระบวนการและวิธีในการบริหารจัดการบริการคลาวด์ อย่างมั่นคงปลอดภัย เพื่อให้มั่นใจว่ามีการวางมาตรการรักษาความมั่นคงปลอดภัยระหว่าง สนข. กับผู้ให้บริการคลาวด์ อย่างเหมาะสม

๑๒.๖ กำหนดขั้นตอนปฏิบัติในการบริหารจัดการการเปลี่ยนแปลงระหว่าง สนข. กับผู้ให้บริการคลาวด์ รวมถึงเงื่อนไขการแจ้งล่วงหน้าสำหรับการดำเนินการเปลี่ยนแปลงเพื่อป้องกันการขาดสภาพความพร้อมใช้งาน

๑๒.๗ กำหนดผู้ประสานงาน และระยะเวลาในการติดต่อประสานงานไว้อย่างชัดเจน รวมถึง ขั้นตอนปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มั่นใจว่าเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้นจะได้รับการแจ้ง และบริหารจัดการภายในระยะเวลาที่กำหนด

๑๒.๘ ประเมินความเสี่ยง พิจารณาถึงกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล หรือสารสนเทศที่จะนำไปไว้บนคลาวด์ และวางมาตรการเพื่อบริหารจัดการความเสี่ยงต่อการปฏิบัติตามกฎหมาย การปกป้องข้อมูลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมรวมถึงติดตามการดำเนินมาตรการต่าง ๆ และทบทวนอย่างสม่ำเสมอ

ข้อ ๑๓ การบริหารจัดการค่าคอนฟิกูเรชัน (Configuration Management) ให้ผู้ดูแลระบบปฏิบัติ ดังต่อไปนี้

๑๓.๑ กำหนดกระบวนการและเครื่องมือในการบังคับใช้ให้ฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายของ สนข. ได้รับการกำหนดและปรับแต่งค่าตามที่ สนข. กำหนดไว้ให้ใช้งาน

๑๓.๒ ต้องจัดทำเทมเพลตมาตรฐานสำหรับการกำหนดค่าฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายที่มั่นคงปลอดภัย

๑๓.๓ ทบทวนเทมเพลตมาตรฐานเป็นระยะ ๆ และทำการอัปเดตเมื่อจำเป็นต้องแก้ไข หรือมีภัยคุกคาม หรือช่องโหว่ใหม่ หรือเมื่อมีการเริ่มต้นใช้งานซอฟต์แวร์หรือฮาร์ดแวร์เวอร์ชันใหม่

๑๓.๔ จัดให้มีการตรวจสอบการปรับแต่งค่าให้มีความสอดคล้องกับค่ามาตรฐานเป็นระยะ ๆ เพื่อลดความเสี่ยงในการเปิดจุดอ่อน หรือช่องโหว่ให้กับผู้ไม่ประสงค์ดี

ข้อ ๑๔ การบริหารจัดการการลบสารสนเทศ (Information Deletion Management) ให้ผู้ดูแลระบบ ปฏิบัติดังต่อไปนี้

๑๔.๑ ต้องไม่จัดเก็บสารสนเทศที่ละเอียดอ่อนไว้นานเกินกว่าที่จำเป็น เพื่อลดความเสี่ยงจากการถูกเปิดเผยที่ไม่พึงประสงค์

๑๔.๒ เมื่อต้องลบสารสนเทศออกจากระบบ แอปพลิเคชัน หรือบริการต่าง ๆ ต้องพิจารณา กำหนดวิธีการลบให้สอดคล้องตามข้อกำหนดทางธุรกิจและกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

๑๔.๓ บันทึกผลการลบสารสนเทศไว้เป็นหลักฐาน รวมถึงในกรณีที่เมื่อมีการใช้ผู้ให้บริการลบ สารสนเทศ ต้องจัดเก็บหลักฐานการลบสารสนเทศจากผู้ให้บริการเหล่านั้น รวมถึงในกรณีที่ใช้บริการคลาวด์ และกระบวนการลบสารสนเทศนั้นจะต้องสามารถสอบทวนได้

ข้อ ๑๕ การบริหารจัดการการปิดบัง/ซ่อนข้อมูล (Data Masking Management) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๕.๑ จัดทำขั้นตอนปฏิบัติที่เกี่ยวข้องกับการปิดบัง/ซ่อนข้อมูล พิจารณาประกาศใช้งาน คัดเลือก และจัดหาเครื่องมือหรือวิธีการทางเทคนิคที่เหมาะสมในการปิดบัง/ซ่อนข้อมูลสำหรับข้อมูลส่วนบุคคล เพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและเพื่อให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับและสัญญาที่เกี่ยวข้อง

๑๕.๒ พิจารณาหลักเกณฑ์ที่เหมาะสมสำหรับการใช้เทคนิค การปกปิด/ซ่อนการใช้นามแฝง หรือการปิดบังชื่อ (Pseudonymization) และการทำให้ไม่สามารถระบุตัวบุคคล ได้อีก (Anonymization) ในกรณีที่มีการใช้เทคนิคการทำให้ไม่สามารถระบุตัวบุคคลได้อีก (Anonymization) กับข้อมูลส่วนบุคคลที่ สนข. ถือครองอยู่เพื่อประมวลผลจะต้องมั่นใจว่าเทคนิควิธีดังกล่าวจะไม่สามารถระบุตัวบุคคลทั้งทางตรง และทางอ้อมขึ้นมาได้อีก ทั้งนี้ เทคนิควิธีเหล่านี้ให้สอดคล้องตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จะประกาศกำหนด

๑๕.๓ เมื่อมีกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคล ให้ผู้รับผิดชอบ กิจกรรมนั้น ๆ ประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และขอคำปรึกษา จากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และแจ้งต่อ ศทท. ในกรณีที่ต้องพิจารณาใช้มาตรการ ในการปิดบัง/ซ่อน ข้อมูลส่วนบุคคล (Data Masking) เพื่อเป็นการปกป้องข้อมูลส่วนบุคคลให้สอดคล้อง ตามกฎหมาย ระเบียบ ข้อบังคับและสัญญาที่เกี่ยวข้อง

ข้อ ๑๖ การป้องกันข้อมูลส่วนบุคคล/ข้อมูลที่มีความสำคัญรั่วไหล (Data Leakage Prevention) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๖.๑ พิจารณาจัดหาเครื่องมือหรือวิธีการทางเทคนิคเพื่อนำมาใช้เป็นมาตรการป้องกันข้อมูล รั่วไหลกับระบบเครือข่าย และอุปกรณ์ประมวลผลสารสนเทศอื่น ๆ ในการจัดเก็บ หรือถ่ายโอนข้อมูลส่วนบุคคล และข้อมูลที่มีความสำคัญ

๑๖.๒ แนวทางปฏิบัติในการป้องกันข้อมูลรั่วไหล ควรประกอบด้วย

(๑) ระบุและจัดหมวดหมู่ข้อมูลสารสนเทศ ตามระดับความสำคัญและความอ่อนไหว ของสารสนเทศ

(๒) กำหนดให้มีเทคนิคในการเฝ้าระวังติดตามช่องทางที่ข้อมูลสารสนเทศของ สนข. อาจรั่วไหล เช่น การส่งผ่านอีเมล การถ่ายโอนไฟล์ การจัดเก็บในสื่อบันทึกข้อมูลแบบเคลื่อนที่ได้ เป็นต้น

(๓) ดำเนินการเพื่อป้องกันสารสนเทศรั่วไหล เช่น การกักอีเมลที่มีข้อมูลที่มีความอ่อนไหว หรือความเสี่ยง เป็นต้น

๑๖.๓ ในกรณีที่ใช้เครื่องมือป้องกันข้อมูลรั่วไหล เครื่องมือนี้จะต้องสามารถ

(๑) ระบุและเฝ้าติดตามสารสนเทศที่อ่อนไหว ซึ่งเสี่ยงต่อการถูกเปิดเผยโดยไม่ได้รับอนุญาต

(๒) ตรวจสอบการเปิดเผยสารสนเทศที่อ่อนไหว

(๓) บล็อกการดำเนินการของผู้ใช้หรือการส่งผ่านเครือข่ายที่แสดงสารสนเทศที่อ่อนไหวได้

๑๖.๔ หากมีความจำเป็นต้องส่งออกสารสนเทศนั้นจะต้องมีการขออนุญาตการส่งออก และผู้อนุญาตต้องรับผิดชอบต่อความเสี่ยงดังกล่าว

๑๖.๕ จัดทำข้อกำหนดให้กับผู้ใช้งานเพิ่มเติมเกี่ยวกับการห้ามใช้โปรแกรมจับภาพหน้าจอ หรือการถ่ายภาพหน้าจอสำหรับสารสนเทศที่มีความอ่อนไหว รวมถึง สนข. ต้องจัดให้มีการสร้างความตระหนักรู้ ต่อการรั่วไหลของสารสนเทศในกรณีดังกล่าว

๑๖.๖ สำหรับข้อมูลที่ได้มีการสำรองไว้ ต้องมีมาตรการควบคุมอื่น ๆ เพิ่มเติม เช่น การเข้ารหัส การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำรองไว้นั้นได้รับการปกป้องอย่างเหมาะสม

ข้อ ๑๗ การบริหารจัดการการติดตามกิจกรรมทางเทคโนโลยีสารสนเทศ (Monitoring activities) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๗.๑ ควรเฝ้าติดตามเครือข่าย ระบบและแอปพลิเคชัน เพื่อหาพฤติกรรมที่ผิดปกติ และการดำเนินการที่เหมาะสมเพื่อประเมินอุบัติการณ์ (Event) และเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศ (Incident) ที่อาจเกิดขึ้น

๑๗.๒ ควรกำหนดขอบเขตและระดับการเฝ้าติดตามตามที่สอดคล้องตามข้อกำหนดทางธุรกิจ และการรักษาความปลอดภัยของสารสนเทศ รวมถึงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

๑๗.๓ จัดเก็บข้อมูลล็อก หรือบันทึกหลักฐานต่าง ๆ ไว้ตามระยะเวลาที่กำหนด

๑๗.๔ จัดทำขั้นตอนปฏิบัติในการจัดเก็บและเฝ้าระวังติดตามกิจกรรมของระบบแอปพลิเคชัน ระบบเครือข่าย และเพื่อกำหนดข้อมูลล็อกที่ต้องจัดเก็บ และรายละเอียดที่เกี่ยวข้อง

๑๗.๕ กำหนดเงื่อนไขในการแจ้งเตือน อาทิ ตำแหน่งการเข้าถึง ความถี่ในการเข้าถึง ช่วงเวลาปกติ และช่วงเวลาสูงสุด เป็นต้น และระบุลักษณะพฤติกรรมที่ผิดปกติ อาทิ

- (๑) ระบบหรือแอปพลิเคชันหยุดการทำงานโดยไม่ได้วางแผน
- (๒) กิจกรรมที่มักเกี่ยวข้องกับมัลแวร์หรือการรับส่งข้อมูลที่มาจากแหล่งไอพี หรือโดเมน เครือข่ายที่เป็นอันตราย เช่น คำสั่งควบคุมและสั่งการเซิร์ฟเวอร์ (Command & Control Server)
- (๓) ลักษณะการโจมตีที่ทราบ เช่น การปฏิเสธบริการและหน่วยความจำล้น (Buffer Overflow)

(๔) พฤติกรรมของระบบที่ผิดปกติ เช่น การบันทึกการกดแป้นพิมพ์ การเบี่ยงเบนในการใช้โปรโตคอลมาตรฐาน

(๕) สภาพคอขวดหรือปริมาณทราฟฟิกมากเกินไป ทำให้เกิดความล่าช้าของเครือข่าย

(๖) การเข้าถึงโดยไม่ได้รับอนุญาต

(๗) การสแกนแอปพลิเคชัน ระบบ และเครือข่ายโดยไม่ได้รับอนุญาต

(๘) ความพยายามในการเข้าถึงทรัพยากรที่มีการป้องกัน

(๙) ผู้ใช้งานที่ผิดปกติและพฤติกรรมของระบบที่คาดหวังก่อให้เกิดขึ้น

๑๗.๖ ต้องดำเนินการเฝ้าระวังติดตามอย่างต่อเนื่อง และเป็นปัจจุบัน หรือเป็นระยะ ๆ สอดคล้องตามอำนาจ หน้าที่ และการดำเนินงานของ สนข. และควรปรับปรุงให้สอดคล้องกับบริบทอย่างเหมาะสม

๑๗.๗ จัดให้มีการฝึกอบรมกับเจ้าหน้าที่ที่เกี่ยวข้อง โดยเจ้าหน้าที่ต้องตระหนักรู้ถึงความสำคัญ ของอุบัติการณ์และเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น และเมื่อมีความสงสัยว่าอาจจะเป็นเหตุการณ์ ด้านความมั่นคงปลอดภัย ต้องมีขั้นตอนปฏิบัติในการแจ้งผู้ที่เกี่ยวข้องให้ได้รับทราบและติดตาม แก้ไขเหตุ ที่เกิดขึ้นได้อย่างทันท่วงที

ข้อ ๑๘ การบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก (Web Filtering) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๘.๑ จัดให้มีเครื่องมือทางเทคนิคในการบริหารจัดการการเข้าถึงเว็บไซต์ภายนอก เช่น การดำเนินการบล็อกไอพี หรือโดเมนของเว็บไซต์ เป็นต้น เพื่อลดความเสี่ยงจากข้อมูลที่มุ่งร้ายอันเกิดจากการที่เจ้าหน้าที่ของ สนข. อาจเข้าถึงเว็บไซต์ที่มีลักษณะผิดกฎหมาย หรือมีมัลแวร์ หรืออาจแฝงด้วย ภัยอันตรายประเภทฟิชซิง มีการจำกัดการเข้าถึงเว็บไซต์ และแอปพลิเคชันที่ควรเข้าถึง (Whitelist) หรือไม่ควรเข้าถึง (Blacklist) อย่างเหมาะสม และควรทำการปรับปรุงรายการอย่างสม่ำเสมอ

๑๘.๒ กำหนดกฎระเบียบให้กับผู้ใช้งานได้ทราบถึงการใช้งานทรัพยากรออนไลน์อย่างปลอดภัย และเหมาะสม ก่อนที่จะดำเนินการควบคุมทางเทคนิค รวมถึงสื่อสารให้ผู้ใช้งานได้รับทราบ

๑๘.๓ จัดอบรมสร้างความตระหนักรู้ให้กับผู้ใช้งานเพื่อเสริมสร้างนิสัยในการใช้งานทรัพยากรออนไลน์อย่างปลอดภัยและเหมาะสม

ข้อ ๑๙ การเขียนโค้ดอย่างมั่นคงปลอดภัย (Secure Coding) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๙.๑ ปฏิบัติตามหลักการเขียนโค้ดอย่างมั่นคงปลอดภัย เพื่อช่วยลดช่องโหว่ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นในซอฟต์แวร์

๑๙.๒ สนับสนุนการนำหลักการเขียนโค้ดอย่างมั่นคงปลอดภัยให้สามารถประยุกต์ใช้งานทั่วทั้ง สนข. พร้อมทั้งให้คำแนะนำและช่วยกันดูแลให้มีการเขียนโค้ดอย่างมั่นคงปลอดภัยครอบคลุมทั้งซอฟต์แวร์จากบุคคลภายนอก และซอฟต์แวร์แบบโอเพ่นซอร์ส (Open Source)

๑๙.๓ ติดตามข่าวสารและคำแนะนำเกี่ยวกับช่องโหว่ของซอฟต์แวร์และนำมาปรับปรุงแก้ไขหลักการเขียนโค้ดอย่างต่อเนื่อง

ข้อ ๒๐ การปฏิบัติตามกรอบประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๒๐.๑ ปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หมวดที่ ๑)

๒๐.๒ ให้ความร่วมมือในการสนับสนุนและรับตรวจสำหรับการตรวจสอบตามแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ส่วนที่ ๒)

๒๐.๓ ดำเนินการอย่างเป็นรูปธรรมเพื่อให้สอดคล้องตามขั้นตอนปฏิบัติการประเมินความเสี่ยงที่กำหนด และจัดเก็บหลักฐานผลการประเมินความเสี่ยงเพื่อแสดงถึงการปฏิบัติอย่างสอดคล้องตามกฎหมาย (ส่วนที่ ๓)

๒๐.๔ ให้ความร่วมมือในการซักซ้อม และปฏิบัติตามบทบาทหน้าที่ที่ตนได้รับมอบหมายตามแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อให้เกิดประสิทธิภาพประสิทธิผลในการรับมือกับภัยคุกคามทางไซเบอร์อย่างสูงสุด

หมวด ๔ แนวปฏิบัติสำหรับเจ้าของระบบ (System Owner)

ข้อ ๑ การบริหารจัดการโครงการ/งานด้านเทคโนโลยีสารสนเทศ

เมื่อมี โครงการ/งาน ด้านเทคโนโลยีสารสนเทศ เจ้าของระบบต้องดำเนินการ ดังนี้

๑.๑ ประเมินและบริหารจัดการต่อความเสี่ยงด้านการรักษาความปลอดภัยของสารสนเทศ ข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยไซเบอร์ รวมถึงความเสี่ยงที่เกี่ยวข้องกับการทำโครงการ อาทิ ความเสี่ยงด้านการรักษาความปลอดภัยในด้านการสื่อสารภายในและภายนอก ทั้งนี้ต้องเริ่มตั้งแต่ระยะแรก และเป็นระยะ ๆ ตลอดวงจรชีวิตโครงการ

๑.๒ ประยุกต์ใช้ข้อกำหนดในการรักษาความมั่นคงปลอดภัย (Security Requirement) หลักการวิศวกรรมด้านความมั่นคงปลอดภัย (System Engineering Principle) ข้อกำหนดด้านการให้บริการคลาวด์ (Cloud Security Requirement) ข้อกำหนดด้านความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Privacy by Design by Default) ข้อกำหนดในการปฏิบัติตามสิทธิในทรัพย์สินทางปัญญา ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยและการปฏิบัติให้สอดคล้องตามกฎหมาย ก่อนเริ่มดำเนินการ

๑.๓ จัดทำสถาปัตยกรรมระบบเพื่อแสดงให้เห็นถึงองค์ประกอบของระบบส่วนที่เป็นการรักษาความมั่นคงปลอดภัยระบบ และการเชื่อมต่อกับเครือข่ายและระบบภายในของ สนข. และแจ้งต่อ ศทท.

๑.๔ จัดส่งรายงานผลการประเมินและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และแจ้งต่อ ศทท. เพื่อประเมินความเหมาะสมและเพียงพอของมาตรการด้านความมั่นคงปลอดภัยที่เจ้าของระบบได้วางไว้ พร้อมรับคำแนะนำเพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยของ สนข. เป็นไปอย่างมีประสิทธิภาพประสิทธิผล สูงสุด และสอดคล้องตามข้อกำหนดของกฎหมาย

๑.๕ กำหนดหน้าที่และความรับผิดชอบด้านการรักษาความปลอดภัยระหว่างเจ้าของระบบ ผู้ดูแลระบบ และผู้ให้บริการภายนอก และ ศทท. ให้ชัดเจน เพื่อป้องกันการปฏิเสธ ความรับผิดชอบในกรณีเกิดอุบัติเหตุหรือเหตุการณ์ด้านความมั่นคงปลอดภัย

๑.๖ กำกับดูแลให้ผู้ปฏิบัติงานในโครงการดำเนินการตามนโยบายและแนวปฏิบัตินี้ และเฝ้าระวังติดตามการดำเนินโครงการอย่างเป็นระยะ ๆ รวมทั้ง ต้องแจ้งปัญหาอุปสรรคที่พบในการปฏิบัติงาน หากไม่สามารถ ดำเนินการตามมาตรการที่จัดวางไว้ได้ จะต้องแจ้ง ศทท. เพื่อร่วมหาทางแก้ไขปัญหาก่อน

๑.๗ ทดสอบประสิทธิภาพของมาตรการต่าง ๆ ที่จัดให้มีในระบบแอปพลิเคชันนั้นก่อนส่งมอบงาน

๑.๘ ประสานงาน ศทท. เพื่อตรวจประเมินและแก้ไขด้านความมั่นคงปลอดภัยให้กับระบบแอปพลิเคชันก่อนนำออกสู่การให้บริการ ในกรณีที่ต้องการนำระบบแอปพลิเคชันไว้ที่ ศทท. ต้องดำเนินการตามขั้นตอนปฏิบัติที่ ศทท. กำหนด

๑.๙ ต้องมีการดูแลและปรับปรุงด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๑.๑๐ เมื่อ ศทท. ดำเนินการตรวจประเมินช่องโหว่ หรือทำการทดสอบเจาะระบบประจำปี และพบว่าระบบแอปพลิเคชัน ภายใต้การดูแลของเจ้าของระบบมีช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัย เจ้าของระบบจะต้องสั่งการให้มีการดำเนินการแก้ไขระบบ แอปพลิเคชัน โดยไม่ชักช้า หรือภายใน ๗ วันทำการ สำหรับช่องโหว่ในระดับวิกฤติและระดับสูง และต้องดำเนินการตามข้อกำหนดอื่น ๆ ที่เกี่ยวข้องในนโยบาย และแนวปฏิบัตินี้

๑.๑๑ เมื่อปิดโครงการ/งาน ควรมีการถอดบทเรียน (Lesson Learned) จากผู้ที่มีส่วนร่วมในโครงการ/งาน เพื่อรวบรวมจัดทำรายงานเสนอแนะการปรับปรุงการดำเนินโครงการ/งาน ไว้ใช้ในการปรับปรุงการบริหารโครงการ/งาน ต่อไป

หมวด ๕

แนวปฏิบัติสำหรับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการกำกับผู้ให้บริการภายนอก

(System Acquisition, Development, Maintenance and Third Party Management)

เพื่อกำหนดแนวทางในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการบริหารจัดการ ผู้ให้บริการ ภายนอก การทำสัญญาจ้าง การประเมินความเหมาะสม การติดตามและประเมินผลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกสามารถปฏิบัติงานให้ สนข. ได้ตามเป้าหมาย และเงื่อนไขที่กำหนด โดยไม่ก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จนส่งผลกระทบต่อการทำงาน และการให้บริการของ สนข. อย่างมีนัยสำคัญ

ข้อ ๑ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของ สนข. ผู้ที่ได้รับมอบหมายในการจัดหา พัฒนา และดูแลรักษาระบบ ต้องดำเนินการดังนี้

๑.๑ การจัดหาและพัฒนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศให้ประสานงานกับ ศทท. เพื่อพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายสารสนเทศของ สนข. ก่อนนำเสนอพิจารณาอนุมัติจัดหาหรือพัฒนาทุกครั้ง

๑.๒ การจัดหาและพัฒนาที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญยิ่งยวด และมีลักษณะที่เสี่ยงต่อความล้มเหลวในการให้บริการหากมีเพียงชุดเดียว ให้ผู้รับผิดชอบพิจารณาจัดหาอุปกรณ์สำรองไว้โดยขอความเห็นชอบจากผู้บังคับบัญชา

๑.๓ การพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย ให้คำนึงถึงเรื่องดังต่อไปนี้

- (๑) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา
- (๒) การตรวจสอบด้านคุณภาพ และความถูกต้องของระบบสารสนเทศ
- (๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์
- (๔) ข้อจำกัดในการเปิดเผยข้อมูลของ สนข.
- (๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง
- (๖) การทดสอบระบบสารสนเทศ

๑.๔ ไม่อนุญาตให้นำข้อมูลสำคัญของ สนข. เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูล ใช้ภายในเท่านั้นไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชา หรือได้รับความยินยอมโดยชัดแจ้ง หรือมีการแจ้งเจ้าของข้อมูลส่วนบุคคลตามแต่กรณีไว้ก่อนแล้ว

๑.๕ ต้องกำกับดูแลการออกแบบและพัฒนาระบบให้จัดทำและปฏิบัติตามหลักการวิศวกรรมด้านความมั่นคงปลอดภัย และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของ สนข.

๑.๖ ต้องกำกับดูแลการออกแบบและพัฒนาระบบ Website และ Web Application ให้สอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard : WSS) และมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ (Web Application Security Standard : WAS) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อให้ระบบมีความมั่นคงปลอดภัย

๑.๗ ดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบสารสนเทศจากภายนอก (Outsourced System Development) ให้เป็นไปตามขั้นตอนปฏิบัติการพัฒนาระบบสารสนเทศของ สนข.

๑.๘ ต้องทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงตามความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ สนข. ควรระมัดระวังข้อมูลรั่วไหล โดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบหากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

๑.๙ ต้องทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพการประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไข เปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๑.๑๐ กำหนดผู้รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน รวมถึงเพื่อประสานงานกับ ศทท. ก่อนที่จะนำระบบสารสนเทศที่พัฒนาติดตั้งขึ้นให้บริการ

๑.๑๑ ในระหว่างการพัฒนาสารสนเทศต้องกำกับหรือจัดให้มีการตรวจสอบซอร์สโค้ด (Source Code Review) ด้วยวิธีการที่เหมาะสม และดำเนินการแก้ไขในกรณีที่พบว่าซอร์สโค้ดดังกล่าวอาจมีความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๑๒ ก่อนนำระบบสารสนเทศขึ้นให้บริการ ทดสอบด้านความมั่นคงปลอดภัยก่อนนำขึ้นให้บริการ ต้องทำการตรวจสอบช่องโหว่ทางเทคนิค ปิดช่องโหว่ตรวจพบ อัปเดตระบบให้เป็นเวอร์ชันล่าสุด ต้องปรับแต่งค่าด้านความมั่นคงปลอดภัยให้เหมาะสม (Hardening) และสอดคล้องกับค่าพื้นฐานที่ สนข. กำหนด (Configuration Baseline) รวมทั้งประสานงานกับ ศทท. ให้ทราบถึงแผนและแนวทางในการติดตั้งและเปิดใช้งานระบบ เพื่อให้ผู้ที่ได้รับมอบหมายดำเนินการตรวจสอบการปรับแต่งค่าต่าง ๆ ของระบบให้มีความมั่นคงปลอดภัยก่อนการเปิดให้บริการ

๑.๑๓ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (Development Environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบโดยคำนึงถึงเรื่อง ดังนี้

(๑) การรักษาความลับของข้อมูลที่น่ามาประมวลผล จัดเก็บ ส่งผ่านระบบการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(๒) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(๓) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(๔) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอก สนข. ที่มีความมั่นคงปลอดภัย

๑.๑๔ ควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ โดยอย่างน้อย ดังนี้

(๑) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๒) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้น เนื่องจากการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

(๓) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(๔) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(๕) จัดเก็บโปรแกรมเวอร์ชัน (Program Version) ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (Fall-Back) ของระบบงานในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(๖) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(๗) บันทึกและจัดเก็บหลักฐานทั้งหมด (Audit Trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

ข้อ ๒ การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลโดยผู้ให้บริการภายนอก ผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๒.๑ ต้องปฏิบัติตามขั้นตอนปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เกิดจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๒.๒ จัดทำผังแสดงการเชื่อมโยงเครือข่าย ระบบ และการไหลของข้อมูล (Network and System's Data Flow Diagram) ที่แสดงถึงรายละเอียด Data Flow และการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างชัดเจน โดยได้รับอนุมัติจากผู้มีอำนาจจัดเก็บไว้เป็นความลับ และควบคุมการเข้าถึงอย่างเข้มงวด

๒.๓ ติดตามและทดสอบสภาพความพร้อมใช้งาน (Availability) ของการเชื่อมต่อหลัก และการเชื่อมต่อสำรองกับผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๒.๔ กำหนดมาตรการด้านความมั่นคงปลอดภัย (Security Controls) เพื่อตรวจจับและป้องกันการบุกรุกผ่านการเชื่อมต่อระบบเครือข่ายของผู้ให้บริการภายนอกอย่างรัดกุมเพียงพอและมีการสอบทานมาตรการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๒.๕ การเปลี่ยนแปลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกต้องผ่านขั้นตอนปฏิบัติการบริหารจัดการการเปลี่ยนแปลงที่ สนข. กำหนด

๒.๖ กำหนดให้มีหน่วยงานภายในหรือผู้รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอก ที่ให้บริการ เพื่อร่วมกันพัฒนาปรับปรุงการรักษาความมั่นคงปลอดภัยของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างต่อเนื่อง

ข้อ ๓ การประเมินและวิเคราะห์ศักยภาพของผู้ให้บริการภายนอกในขั้นตอนของการคัดเลือก (Due Diligence) และการบริหารจัดการสัญญา ผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๓.๑ กำหนดให้มีการประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ก่อนทำสัญญาว่าจ้างผู้ให้บริการภายนอก (Due Diligence) รวมถึงมีการจัดเก็บและปรับปรุงรายชื่อผู้ให้บริการภายนอกให้เป็นปัจจุบันอยู่เสมอ

๓.๒ จัดทำสัญญากับผู้ให้บริการภายนอก โดยมีการระบุข้อกำหนดในการรักษาความมั่นคงปลอดภัย (Security Requirement) หลักการวิศวกรรมด้านความมั่นคงปลอดภัย ข้อกำหนดด้านการให้บริการคลาวด์ หรือมาตรฐานทางเทคนิคอื่น ๆ ที่เกี่ยวข้อง รวมถึงข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) ซึ่งผู้ให้บริการภายนอกต้องปฏิบัติไว้ในสัญญาอย่างชัดเจน ทั้งนี้ ข้อกำหนดดังกล่าว ต้องสอดคล้องตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยที่ สนข. กำหนด

๓.๓ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงความรับผิดชอบในการรักษาความมั่นคง ปลอดภัยข้อมูล/ข้อมูลส่วนบุคคล ของ สนข. ที่ผู้ให้บริการภายนอกเป็นผู้ดูแล รับส่ง จัดเก็บ และประมวลผล

๓.๔ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงความรับผิดชอบในการรับมือ ต่อเหตุการณ์ ผิดปกติด้านการรักษาความมั่นคงปลอดภัยไว้อย่างชัดเจน

๓.๕ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องระบุถึงแนวทางการรักษาความมั่นคงปลอดภัย สำหรับการส่งคืนข้อมูลสำคัญหรือการทำลายข้อมูลสำคัญในกรณีที่มีการยกเลิกสัญญา

๓.๖ สัญญาที่จัดทำกับผู้ให้บริการภายนอกต้องมีการระบุสิทธิเรียกร้องค่าเสียหายในกรณี ที่ผู้ให้บริการภายนอกไม่สามารถปฏิบัติตามที่ สนข. กำหนดไว้

๓.๗ สัญญาที่จัดทำกับผู้ให้บริการภายนอกมีการระบุบทบาท หน้าที่ และความรับผิดชอบ ในการรายงานช่องโหว่และเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยแก่ สนข.

๓.๘ มีแนวทางรองรับกรณียกเลิกหรือยุติการใช้บริการ (Termination/Exit Strategy) จากผู้ให้บริการภายนอกเพื่อลดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของ สนข.

ข้อ ๔ การติดตามความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการ ภายนอก ผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๔.๑ ประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก ที่สำคัญอย่างสม่ำเสมอ

๔.๒ มีการสอบทานแผนรับมือจากเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Resilience Plan) ของผู้ให้บริการภายนอกที่สำคัญอย่างสม่ำเสมอ

๔.๓ กำหนดให้มีการติดตามดูแลการเข้าถึงทางกายภาพ (Physical) และทาง Logical จากผู้ให้บริการภายนอก

๔.๔ จัดให้มีการตรวจสอบการบริหารจัดการผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า สนข. มีกระบวนการติดตาม รายงาน และแก้ไขปัญหาอย่างมีประสิทธิภาพ

๔.๕ กำหนดขอบเขตและความถี่ในการติดตามการปฏิบัติงานตามระดับความเสี่ยงของ ผู้ให้บริการภายนอก

๔.๖ ระบุการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เมื่อมีความจำเป็นต้อง รวบรวมและจัดเก็บข้อมูลที่ได้มาจากผู้ให้บริการภายนอก

๔.๗ ตรวจสอบ หรือสอบทานรายงานตรวจสอบจากผู้ตรวจสอบหรือผู้เชี่ยวชาญภายนอก ที่มีมาตรฐานเป็นที่ยอมรับ เช่น SSAE ๑๘ Type ๒ หรือ SOC ๒ เพื่อประเมินความเพียงพอของการควบคุม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกที่สำคัญ เช่น ที่ให้บริการประมวลผล จัดเก็บ และรับส่งข้อมูล เป็นต้น

๔.๘ ติดตามการเข้าถึงข้อมูลสำคัญ (Sensitive Data)/ข้อมูลส่วนบุคคล (Data Privacy) จากผู้ให้บริการภายนอก ทั้งข้อมูลที่อยู่ในระบบของ สนข. และระบบที่ใช้บริการจากผู้ให้บริการภายนอก ให้เป็นไปตามหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) พร้อมทั้งกำกับดูแลการปฏิบัติตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล หากผู้ให้บริการภายนอกมีการประมวลผลข้อมูลส่วนบุคคลในระบบสารสนเทศนั้น

ข้อ ๕ โปรแกรมคอมพิวเตอร์มาตรฐานสำหรับการใช้งานของ สนข. ผู้ที่ได้รับมอบหมายต้องดำเนินการดังนี้

ให้มีการจัดทำรายการโปรแกรมคอมพิวเตอร์มาตรฐานที่อนุญาตให้ใช้งาน และประกาศไว้บนอินทราเน็ต ซึ่งผู้ใช้งาน ผู้ดูแลระบบ และเจ้าของระบบ ต้องตรวจสอบรายการดังกล่าว อย่างสม่ำเสมอ เพื่อป้องกันมิให้มีการติดตั้งโปรแกรมคอมพิวเตอร์ที่นอกเหนือจากที่ สนข. กำหนด ในกรณีที่พบการติดตั้งโปรแกรมคอมพิวเตอร์ที่ไม่ได้อยู่ในรายการจะถือเป็นความผิดส่วนบุคคล และถือว่าได้ละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข.

ผู้จัดทำร่าง

นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรัชก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายนฤฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๓. นายพิสิษฐ์ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร