



ประกาศสำนักงานปลัดสำนักนายกรัฐมนตรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดสำนักนายกรัฐมนตรี พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคีรัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ

สำนักงานปลัดสำนักนายกรัฐมนตรีจึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี เป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามมาตรการความปลอดภัยที่กำหนด และมีการทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในหน่วยงาน โดยให้อยู่ในอำนาจหน้าที่ความรับผิดชอบของปลัดสำนักนายกรัฐมนตรี และมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำสำนักงานปลัดสำนักนายกรัฐมนตรี (Department Chief Information Office :DCIO) เป็นผู้รับผิดชอบต่อนโยบายในฐานะเป็นผู้กำกับ ติดตามและทบทวนนโยบาย

ปลัดสำนักนายกรัฐมนตรี สำนักงานปลัดสำนักนายกรัฐมนตรี โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดสำนักนายกรัฐมนตรี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี พ.ศ. ๒๕๖๕” ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๒ นิยาม

- | | | |
|-----|--|---|
| ๒.๑ | “องค์กร” | หมายถึง สำนักงานปลัดสำนักนายกรัฐมนตรี |
| ๒.๒ | “CEO” | หมายถึง ปลัดสำนักนายกรัฐมนตรี |
| ๒.๓ | “DCIO” | หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำสำนักงานปลัดสำนักนายกรัฐมนตรี |
| ๒.๔ | “สินทรัพย์” | หมายถึง สิ่งใดก็ตามที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับสำนักงานปลัดสำนักนายกรัฐมนตรี |
| ๒.๕ | “การเข้าถึงการควบคุมการใช้งานสารสนเทศ” | หมายถึง การควบคุมการเข้าถึง หรือจำกัดการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่ายระบบปฏิบัติการ โปรแกรมสำเร็จรูป โปรแกรมประยุกต์ |

โปรแกรมอรรถประโยชน์ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๖ “ข้อมูลสารสนเทศ” หมายถึง ข้อมูลที่ถูกประมวลผลโดยระบบสารสนเทศ และสามารถนำไปใช้งานหรือประมวลผลต่อไปได้

๒.๗ “ระบบเครือข่าย” หมายถึง ระบบเครือข่ายคอมพิวเตอร์ภายใต้การกำกับดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใช้ในการติดต่อสื่อสาร หรือ รับ-ส่ง ข้อมูลสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของสำนักงานปลัดสำนักนายกรัฐมนตรี

๒.๘ “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด (Incident)” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ความมั่นคงของระบบสารสนเทศ ถูกบุกรุกคุกคาม และโจมตี

ข้อ ๓ วัตถุประสงค์

๓.๑ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายของสำนักงานปลัดสำนักนายกรัฐมนตรี มีความมั่นคงปลอดภัยจากสถานการณ์ไม่พึงประสงค์หรือไม่คาดคิดในระบบสารสนเทศ

๓.๒ เพื่อให้มั่นใจได้ว่าการปฏิบัติงานของสำนักงานปลัดสำนักนายกรัฐมนตรี สามารถดำเนินได้อย่างต่อเนื่อง และเมื่อเกิดผลกระทบจากเหตุการณ์ไม่พึงประสงค์สามารถกู้คืนระบบสารสนเทศได้อย่างรวดเร็ว และลดความเสียหายที่อาจจะเกิดขึ้น

๓.๓ เพื่อเป็นแนวทางปฏิบัติในการใช้งานระบบสารสนเทศอย่างปลอดภัย สำหรับผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอก

ข้อ ๔ ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ กำหนดขึ้นเพื่อสร้างมาตรฐานและแนวทางในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรีให้ปลอดภัยจากความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่ายของสำนักงานปลัดสำนักนายกรัฐมนตรี โดยข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างโครงการ และผู้เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานทั้งหมด ต้องถือปฏิบัติอย่างเคร่งครัด

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีสาระสำคัญประกอบด้วย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การมีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

องค์กรได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัย โดยมีเนื้อหาสาระสำคัญประกอบด้วย

หมวดที่ ๑ นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ ประกอบด้วยแนวปฏิบัติดังนี้

๑. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

๑.๑ มีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงการใช้งานและความมั่นคงปลอดภัย โดยกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตการเข้าถึงระบบสารสนเทศ ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจของสำนักงานปลัดสำนักนายกรัฐมนตรี

๑.๒ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงไว้อย่างชัดเจน

๑.๓ ต้องจัดทำข้อปฏิบัติการควบคุมการเข้าถึงสารสนเทศและปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความปลอดภัย

๒. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างตระหนักรู้เรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ได้กำหนดแนวทาง ดังนี้

๓.๑ สร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงข้อกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๒ การลงทะเบียนผู้ใช้งาน (User Registration) กำหนดไว้เป็นขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๓.๓ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะสิทธิ์พิเศษและสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม และใช้งานอย่างปลอดภัย

๓.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) สมำเสมอ มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

๔.๑. การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๔.๒. มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๔.๓. กำหนดให้การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งาน ออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔.๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

๕.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอก หน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่าย ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุม การเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการ ควบคุมการเข้าถึง

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุม การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ได้กำหนดหนดแนวทางปฏิบัติดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการ จะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้มีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และกำหนดขั้นตอนทางเทคนิค การยืนยันตัวตนอย่างเหมาะสมเพื่อรองรับการกล่าวอ้างว่าผู้ใช้งานที่ระบุถึง

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System) จัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ได้จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๖.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time - Out)

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๗.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเอง โดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) โดยกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกสำนักงานปลัดสำนักนายกรัฐมนตรี

๘. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยผู้ใช้งานจะต้องลงทะเบียนใช้งานกับผู้ดูแลระบบ และนำอุปกรณ์มาขึ้นทะเบียนเพื่อให้สามารถเข้าใช้งานกับเครือข่ายที่ลงทะเบียนได้

๙. การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย ดังนี้

๙.๑ กำหนดการใช้เส้นทางเชื่อมต่อระบบอินเทอร์เน็ตที่ปลอดภัยที่องค์กรจัดไว้ให้เท่านั้น ได้แก่ Proxy , Firewall, IPS-IDS ห้ามมิให้ผู้ใช้งานเชื่อมต่อผ่าน Dial-up Modem

๙.๒ การรับส่งข้อมูลผ่านอินเทอร์เน็ต ต้องมีการทดสอบไวรัส (Virus Scanning) ก่อนรับส่งข้อมูล

๙.๓ การดาวน์โหลดข้อมูล หรือโปรแกรมใด ๆ จากอินเทอร์เน็ต ต้องไม่เป็นการละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๙.๔ ต้องใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นไปตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๑. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) โดยเครื่องคอมพิวเตอร์แบบพกพาที่สำนักงานปลัดสำนักนายกรัฐมนตรีอนุญาตให้ใช้งาน เป็นสินทรัพย์ของสำนักงานปลัดสำนักนายกรัฐมนตรี เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน และใช้งานอย่างปลอดภัย

๑๒. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผู้ดูแลระบบ จะต้องควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) และควบคุมการเปลี่ยนแปลงต่าง ๆ ที่อาจส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน รวมถึงความมั่นคงปลอดภัยของข้อมูล

๑๓. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยจัดแบ่งพื้นที่ในการควบคุมตามระดับความสำคัญทางสารสนเทศ ควบคุมการเข้าถึงพื้นที่อย่างปลอดภัย รวมถึงการจัดให้มีการบำรุงรักษาอุปกรณ์สารสนเทศให้พร้อมใช้เสมอ

๑๔. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic mail : E-mail) การลงทะเบียนผู้ใช้งาน และการใช้งานจดหมายอิเล็กทรอนิกส์อย่างปลอดภัย

๑๕. การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) อย่างปลอดภัยไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

หมวดที่ ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วยแนวปฏิบัติที่สำคัญ ดังนี้

๑. การสำรองระบบและสำรองข้อมูล

๑.๑ การจัดลำดับความสำคัญของระบบ เพื่อวางแผนในการจัดทำระบบสำรอง

๑.๒ กำหนดประเภทของข้อมูลที่ต้องการสำรอง

๑.๓ การจัดเก็บระบบ และข้อมูลสำรองไว้อย่างปลอดภัย และทดสอบ (Restore) สมำเสมอ

๒. การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และเตรียมความพร้อมโดยการทดสอบแผนสมำเสมอ เพื่อให้มั่นใจได้ว่า เมื่อเกิดเหตุฉุกเฉินสามารถกู้คืน (Recover) กลับมาได้ตามเป้าหมาย

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. จัดให้มีการประเมินความเสี่ยงสมำเสมออย่างน้อยปีละ ๑ ครั้ง โดยประเมินจัดระดับความสำคัญของความเสี่ยงแต่ละรายการ และวางแผนการจัดการความเสี่ยงอย่างเหมาะสม

๒. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในสำนักงานปลัดสำนักนายกรัฐมนตรี (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี

หมวดที่ ๔ หน้าที่รับผิดชอบด้านสารสนเทศ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๒๗ กันยายน พ.ศ. ๒๕๖๕



(นายธีรภัทร ประยูรสิทธิ)

ปลัดสำนักนายกรัฐมนตรี

นโยบายและแนวปฏิบัติในการรักษา
ความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดสำนักนายกรัฐมนตรี
พ.ศ. ๒๕๖๕

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหาร และการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศที่มีรูปแบบหลากหลาย ส่งผลทวิความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจนและการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

สำนักงานปลัดสำนักนายกรัฐมนตรี จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี พ.ศ. ๒๕๖๕ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในสำนักงานปลัดสำนักนายกรัฐมนตรี และบุคลากรทุกคนในสำนักงานปลัดสำนักนายกรัฐมนตรี มีความรู้เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

สำนักงานปลัดสำนักนายกรัฐมนตรี

สารบัญ

บทที่ ๑ บทนำ

๑.๑. หลักการ	๑
๑.๒. วัตถุประสงค์	๑
๑.๓. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๒
๑.๔. บทบังคับใช้	๒
๑.๕. การเผยแพร่และทบทวน	๒

บทที่ ๒ คำนิยาม

๓

บทที่ ๓ นโยบายการรักษาความมั่นคงปลอดภัย

๖

หมวด ๑ นโยบายการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access control)	๖
ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business requirement for access control)	๘
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๙
ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)	๑๐
ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)	๑๓
ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๑๘
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	๑๙
ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)	๒๓
ส่วนที่ ๙ การควบคุมการใช้อินเทอร์เน็ต (Internet)	๒๔
ส่วนที่ ๑๐ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)	๒๕
ส่วนที่ ๑๑ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)	๒๖
ส่วนที่ ๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)	๒๗
ส่วนที่ ๑๓ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)	๓๑
ส่วนที่ ๑๔ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : E-mail)	๓๓
ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	๓๕
หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล	
ส่วนที่ ๑ การสำรองข้อมูล (Back Up)	๓๖
ส่วนที่ ๒ การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน	๓๗
หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	
ส่วนที่ ๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๙
ส่วนที่ ๒ มีแนวทางในการตรวจสอบและประเมินความเสี่ยง	๓๙

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

ส่วนที่ ๑ ระดับนโยบาย

๔๐

ส่วนที่ ๒ ระดับปฏิบัติงาน

๔๐

บทที่ ๑ บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่าอย่างยิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๑.๒ วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรีฉบับนี้ มีวัตถุประสงค์เพื่อ

๑) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๒) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยี และการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรีมีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจเกิดขึ้นในระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี

๑.๓ องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยแนวทางปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี

๑.๔ บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี บุคลากรที่เกี่ยวข้อง มีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) ประจำสำนักงานปลัดสำนักนายกรัฐมนตรี

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดสำนักนายกรัฐมนตรี ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) สำนักงานปลัดสำนักนายกรัฐมนตรี เผยแพร่ให้บุคลากรสำนักงานปลัดสำนักนายกรัฐมนตรี และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

บทที่ ๒ คำนิยาม

๑. คำเรียกแทนหน่วยงานในเอกสารฉบับนี้ เช่น กรม สำนักงาน องค์การ หมายความว่า สำนักงานปลัดสำนักนายกรัฐมนตรี

๒. ผู้บริหารระดับสูงสุด หมายความว่า ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO)

๓. การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดสำนักนายกรัฐมนตรี

๔. ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

๔.๑ ผู้บริหารระดับสูงสุด หมายความว่า ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO)

๔.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Office : DCIO) ประจำสำนักงานปลัดสำนักนายกรัฐมนตรี หมายความว่า รองปลัดสำนักนายกรัฐมนตรีที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๓ ผู้ดูแลระบบ/ผู้ดูแลศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ รวมทั้งผู้ดูแลระบบของหน่วยงานในสำนักงานปลัดสำนักนายกรัฐมนตรี ที่มีศูนย์สารสนเทศของตนเอง

๔.๔ ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

๔.๕ เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร

๔.๖ บุคคลภายนอก หมายความว่า บุคคลที่สำนักงานปลัดสำนักนายกรัฐมนตรีอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรีได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของกรมฯ เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับสำนักงานปลัดสำนักนายกรัฐมนตรี หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิตนักศึกษาฝึกงาน

๕. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี

๖. สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๖.๑. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒. ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๖.๓. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจ กำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อีกได้

๘. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) ห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๙. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคง ปลอดภัย

๑๐. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัย ถูกคุกคาม

๑๑. การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับ ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดสำนักนายกรัฐมนตรี

๑๒. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ใน ระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๓. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงาน ของสำนักงานปลัดสำนักนายกรัฐมนตรีที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล สารสนเทศ และอื่น ๆ

๑๔. เจ้าของข้อมูล หมายถึง เจ้าหน้าที่ของหน่วยงานในสำนักงานปลัดสำนักนายกรัฐมนตรี ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบดูแลปรับปรุงข้อมูลของระบบงานนั้น ๆ ซึ่งเป็นผู้ได้รับ ผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๕. จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐาน ที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP

๑๖. รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

บทที่ ๓ นโยบายการรักษาความมั่นคงปลอดภัย

หมวดที่ ๑ นโยบายการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

- ๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี
- ๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับสำนักงานปลัดสำนักนายกรัฐมนตรี ได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ๑) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่มีศูนย์สารสนเทศของตนเอง
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๓) ผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติ ดังนี้

๑.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

๑.๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

๑.๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑.๑.๒.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

- ๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
 - อ่านอย่างเดียว
 - สร้างข้อมูล
 - ป้อนข้อมูล
 - แก้ไข
 - อนุมัติ
 - ไม่มีสิทธิ์

๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล สำนักงานปลัดสำนักนายกรัฐมนตรีใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๒.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลภายนอกสามารถเปิดเผยได้
- ข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล

๑.๒.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ ดังนี้

- ระดับที่ ๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ระดับที่ ๒ ข้อมูลที่มีระดับความสำคัญปานกลาง
- ระดับที่ ๓ ข้อมูลที่มีระดับความสำคัญน้อย

๑.๒.๓ จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

“ข้อมูลลับที่สุด” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน

จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

“ข้อมูลลับมาก” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน

จะก่อให้เกิดความเสียหายอย่างร้ายแรง

“ข้อมูลลับ” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด

ความเสียหาย

“ข้อมูลทั่วไป” หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๒.๔ การจัดแบ่งระดับชั้นการเข้าถึง

- ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหาร
- ระดับที่ ๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับที่ ๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๑.๒.๕ การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของสำนักงาน กำหนดไว้เป็นช่วงเวลาเข้าถึงได้ ดังนี้

ลำดับ	เวลาที่เข้าถึงได้	ข้อมูล / ช่องทางการเข้าถึงข้อมูล
๑	ในวันจันทร์ ถึง วันศุกร์ เวลา ๐๗.๐๐ – ๑๘.๐๐ น.	การเชื่อมโยงฐานข้อมูลทะเบียน ราษฎร กรมการปกครอง (Linkage Center)
๒	ทุกวัน เวลา ๐๕.๐๐ – ๒๓.๕๙ น.	การลงเวลาปฏิบัติราชการขององค์กร
๓	ทุกวัน ๒๔ ชั่วโมง	เว็บไซต์และระบบสารสนเทศทุก ระบบขององค์กร

ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย การใช้งานตามภารกิจ ควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติ ดังนี้

๒.๑ การควบคุมการเข้าถึงสารสนเทศ

๒.๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๒.๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๒.๑.๓ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยต้องมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการจัดเก็บไว้เป็นหลักฐาน

๒.๑.๔ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑.๕ เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและหรือเจ้าของระบบงาน

๒.๒ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ์และภารกิจ ดังนี้

๒.๒.๑ Executive คือ กลุ่มผู้บริหาร ปลัดสำนักนายกรัฐมนตรี รองปลัดสำนักนายกรัฐมนตรี ผู้ช่วยปลัดสำนักนายกรัฐมนตรี ผู้ตรวจราชการสำนักนายกรัฐมนตรี และผู้อำนวยการสำนัก

๒.๒.๒ Administrator คือ กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒.๓ Officer คือ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของสำนักงานปลัดสำนักนายกรัฐมนตรี

๒.๒.๔ Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับสำนักงานปลัดสำนักนายกรัฐมนตรี

๒.๒.๕ Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศขององค์กร และมั่นใจได้ว่าเฉพาะผู้ที่ได้รับสิทธิ์การเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้นสามารถเข้าใช้งานระบบสารสนเทศได้ โดยมีแนวปฏิบัติในการบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ดังนี้

๓.๑ สร้างความรู้ ความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

๓.๑.๑ สำนักงานปลัดสำนักนายกรัฐมนตรีจัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่มีระดับระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๓.๑.๒ กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิ์เพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิ์การเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๓.๒ กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (User Registration) ดังนี้

๓.๒.๑ การระบุข้อมูลผู้ใช้งานแยกเป็นรายบุคคล

๓.๒.๒ การกำหนดชื่อผู้ใช้ กำหนดจากชื่อภาษาอังกฤษไม่เกิน ๖ อักขระ และตามด้วยอักขระ ๒ ตัวแรกของนามสกุล หากซ้ำ ให้เปลี่ยนในอักขระสุดท้ายเป็นตัวอักษรถัดไปของนามสกุล

๓.๒.๓ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานต้นสังกัด

๓.๒.๔ มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

๓.๓ การบริหารจัดการสิทธิ์ผู้ใช้งาน (User Management)

๓.๓.๑ ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศโปรแกรมประยุกต์ (Application) ภายในสำนักงาน จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย (Wireless LAN) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๓.๒ ผู้ดูแลระบบต้องปรับปรุงสิทธิ์การเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิ์ให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

๓.๓.๓ ในกรณีที่ต้องให้สิทธิ์พิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานต้นสังกัด และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้

๑) ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓) กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ให้มีการเปลี่ยนรหัสผ่านทุก ๓ เดือน

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๔.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนด ชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนชื่อของชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่น ๆ ให้มีความแตกต่างกัน

๓.๔.๒ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องใส่ซองปิดผนึกและประทับตรา “ลับ” ส่งไปยังผู้ใช้งาน พร้อมแจ้งช่องทางการเข้าถึง “แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” เพื่อสร้างความรู้ความเข้าใจ และให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

๓.๔.๓ การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสที่มีความยากในการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข สัญลักษณ์พิเศษ ๘ หลัก (Digits)

๓.๔.๔ การทบทวนเปลี่ยนรหัสผ่านของผู้ใช้งาน ให้มีการเปลี่ยนรหัสผ่านทุก ๓ เดือน

๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่สิทธิการเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

๓.๕.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

๓.๕.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

๓.๕.๓ ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

๓.๕.๔ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงาน ภายใน ๑๕ วันทำการ นับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๔.๑ การใช้งานรหัสผ่าน (Password Use)

๔.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

๔.๑.๒ การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้มีความยาวไม่น้อยกว่าหรือเท่ากับ ๘ ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

- ใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น

- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น

- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย

- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล หรือวันเกิด เป็นต้น

- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคล

ในครอบครัว

๔.๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๔.๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๔.๑.๕ ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔.๑.๖ ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในโปรเจกต์อิเล็กทรอนิกส์ โดยไม่มีการเข้ารหัส หรือแบบฟอร์มอิเล็กทรอนิกส์ต่าง ๆ

๔.๑.๗ ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔.๑.๘ ในกรณีที่ลืมหรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่านทันที หรือแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

๔.๑.๙ กรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทำการยกเลิกสิทธิ์ของผู้ที่ลาออก ออกจากระบบทันที

๔.๑.๑๐ กรณีผู้ใช้งานของหน่วยงานภายในสำนักงาน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

๔.๑.๑๑ ผู้ใช้งานทุกคนของสำนักงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลได้ ดังนี้

๔.๒.๑ มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้เกิดการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

๔.๒.๒ การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
๑	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดดิสก์ (Hard Disk) เอ็กเทอนอล ฮาร์ดดิสก์ (External Hard Disk)	๑. ทำลายข้อมูลตามแนวทางของ DOD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลาย ๆ รอบ

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
		๒. ทบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
๒	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เฆา ทำให้สิ้นสภาพการใช้งาน
๓	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
๔	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

๔.๒.๓ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยการรับ-ส่งข้อมูลสำคัญ หรือ ข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN

๔.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

องค์กรได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึง โดยผู้ซึ่งไม่มีสิทธิ์ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติ ดังนี้

๔.๓.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๔.๓.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอขณะที่ไม่ได้ใช้งาน เช่น ภายใน ๑๕ นาที ให้เครื่องล็อกหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๔.๓.๓ ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๔.๓.๔ กรณีข้อมูลสำคัญที่บันทึกไว้ในกระดาษ สื่อบันทึกข้อมูลแฟลชไดรฟ์ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๔.๓.๕ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่ได้มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๔.๔ การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศขององค์กร กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๔.๔.๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะเป็นการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔.๔.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สิทธิ์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเป็นเกิดจากรหัสผ่านล็อกก็ติ หรือเกิดจากความผิดพลาดใด ๆ ก็ติ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๔.๔.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นบุคคลภายนอก

๔.๔.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๔.๔.๕ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ต้องกรต้องตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรอาจแต่งตั้งให้ผู้ที่ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๔.๔.๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องได้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๔.๔.๗ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น

๔.๔.๘ ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

๔.๔.๙ ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร

๔.๔.๑๐ ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อประโยชน์ทางการค้า

๔.๔.๑๑ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตามห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๕.๑ การใช้งานบริการเครือข่าย

๕.๑.๑ กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบบเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๕.๑.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๑.๓ กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN)

ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๕.๑.๔ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) และ DMZ Zone เป็นต้น เพื่อเป็นการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections)

๕.๒.๑ เมื่อผู้ใช้งานที่อยู่ภายนอกองค์กร เมื่อต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๕.๒.๒ มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

๕.๒.๓ การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความปลอดภัยด้วย VPN

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network)

๕.๓.๑ ต้องลงทะเบียน Mac Address ประจำเครื่อง เพื่อระบุอุปกรณ์บนเครือข่าย และต้องใช้หมายเลข IP Address ที่กำหนดให้โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๕.๓.๒ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายขององค์กร โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

๕.๓.๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับอนุญาตเท่านั้น

๕.๓.๔ ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

๕.๓.๕ จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวข้องกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๕.๓.๖ แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๕.๔.๑ การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๕.๔.๒ มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

๕.๔.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

๕.๔.๔ ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Network)

กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

๕.๕.๑ Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๕.๕.๒ Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติ ดังนี้

๕.๖.๑ จำกัดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๕.๖.๒ ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

๕.๖.๓ การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

๕.๖.๔ ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๕.๖.๕ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๕.๖.๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

๑) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๖) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๗) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๘) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๙) มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๑๐) การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๑๑) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๕.๖.๗ อุปกรณ์เครือข่ายหากมีการเชื่อมต่อด้วย SNMP ต้องกำหนดค่า Community String ไม่เป็นค่าพื้นฐาน

๕.๖.๘ เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายทุกเครื่องจะต้องมีการกำหนดผู้รับผิดชอบประจำแต่ละเครื่อง หากเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายที่ใช้เป็นส่วนกลางต้องกำหนดเจ้าหน้าที่ ฝ่ายบริหารงานทั่วไปหรือเจ้าหน้าที่ในหน่วยงานที่ได้รับมอบหมายเป็นเจ้าของเครื่อง พร้อมทั้งจัดทำบัญชีการใช้งานสำหรับเครื่องดังกล่าวไว้เป็นหลักฐาน โดยต้องเก็บข้อมูลชื่อผู้ใช้งาน วันที่ใช้งาน เวลาเริ่มและสิ้นสุดการใช้งาน

๕.๖.๙ กรณีได้รับเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายมาใหม่ หรือจากหน่วยงานอื่น และต้องการเข้าใช้งานระบบเครือข่ายสำนักงาน เจ้าของเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายนั้น ๆ จะต้องปฏิบัติดังนี้

๑) หน่วยงานทำหนังสือขอเข้าใช้ระบบเครือข่ายต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒) ผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้บริหารจัดการการใช้งานระบบเครือข่าย

๓) เมื่อต้องการเปลี่ยนแปลงเจ้าของเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่าย ต้องทำการยกเลิกความเป็นเจ้าของเครื่องทุกครั้ง การยกเลิกความเป็นเจ้าของ ทำได้ ๒ กรณี ดังนี้

กรณีที่ ๑ ยกเลิกโดยเจ้าของเครื่องเอง โดยเจ้าของต้องเข้าไปทำการยกเลิกความเป็นเจ้าของในระบบ และทำการ Shutdown หากยังไม่ทำการ Shutdown จะถือความเป็นเจ้าของยังคงอยู่จนสิ้นสุดวันนั้น พร้อมทั้งแจ้งผู้ได้รับมอบหมายการควบคุมดูแลบัญชีการใช้งานของหน่วยงานนั้นทราบ

กรณีที่ ๒ ยกเลิกโดยผู้ดูแลระบบ ให้หน่วยงาน แจกศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางหนังสือโดยมีรายละเอียด ดังนี้

- หมายเลขครุภัณฑ์
- ชื่อเจ้าของเครื่องเดิม
- หน่วยงานเจ้าของเครื่องเดิม
- ชื่อเจ้าของเครื่องใหม่
- หน่วยงานเจ้าของเครื่องใหม่

โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะดำเนินการยกเลิก/เปลี่ยนแปลง ให้ภายใน ๑ วันทำการ หลังจากที่ได้รับหนังสือแจ้งการเปลี่ยนแปลงจากหน่วยงานและถือว่าวันที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทำการยกเลิกเป็นวันสิ้นสุดการใช้งานของเจ้าของเดิมและศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะทำหนังสือยืนยันวันที่สิ้นสุดการใช้งานไปยังหน่วยงาน

๔) ผู้ได้รับมอบหมายควบคุมดูแลบัญชีการใช้งานของหน่วยงานในสำนักงาน ต้องจัดทำบัญชีเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายของหน่วยงานของตน พร้อมทั้งต้องปรับปรุงสถานการณ์ใช้งานของแต่ละเครื่องได้แก่ ชื่อเจ้าของเครื่อง วันที่เริ่มต้นเจ้าของเครื่องรับผิดชอบ วันที่สิ้นสุดเจ้าของเครื่องรับผิดชอบ

๕) เครื่องที่ลงทะเบียนแล้วจะย้ายไปใช้ต่างของหน่วยงานไม่ได้ เว้นแต่จะดำเนินการยกเลิกความเป็นเจ้าของ

๖) ในการเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายที่มีการลงทะเบียนแล้ว ไปใช้ในห้องประชุม ให้แจ้งความจำนงค์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เจ้าหน้าที่ดูแลระบบดำเนินการ

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ซึ่งมีแนวปฏิบัติ ในการจัดเส้นทางบนเครือข่าย ดังนี้

๕.๗.๑ ควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๕.๗.๒ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๕.๗.๓ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยเครือข่ายภายในและภายนอก

๕.๗.๔ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการขององค์กรโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๖.๑ ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๖.๑.๑ กำหนดให้ระบบไม่ให้เกิดรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๖.๑.๒ กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีภัยคุกคามหรือการโจมตีที่รุนแรง

๖.๑.๓ จำกัดระยะเวลาสำหรับการใช้ในการป้อนรหัสผ่าน

๖.๑.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๖.๒.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๖.๒.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องขออนุญาตใช้จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุญาตไว้

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีในการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๖.๓.๑ มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักษร ตัวเลข และตัวอักษรพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ

๖.๓.๒ เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ การใช้โปรแกรมมอรรดประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมมอรรดประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติดังนี้

๖.๔.๑ การใช้โปรแกรมมอรรดประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมมอรรดประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๖.๔.๒ โปรแกรมมอรรดประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๖.๔.๓ จัดเก็บโปรแกรมมอรรดประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๖.๔.๔ จำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมมัลแวร์ประโยชน์เท่านั้น

๖.๔.๕ กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมมัลแวร์ประโยชน์ที่ไม่จำเป็นออกจากระบบ รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมมัลแวร์ประโยชน์ได้

๖.๕ การกำหนดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time - Out)

๖.๕.๑ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ตามความต้องการเจ้าของระบบ

๖.๕.๒ ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลาการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลา ๑๕ นาที หรือตามความต้องการเจ้าของระบบ เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูง กำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัย ดังนี้

๖.๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานตามความต้องการเจ้าของระบบ ต่อการเชื่อมต่อ ๑ ครั้ง หรือกำหนดให้ใช้งานได้เฉพาะช่วงเวลาเท่านั้น

๖.๖.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ โดยผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๓ ชั่วโมง หรือตามความต้องการเจ้าของระบบ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการดังนี้

๗.๑ จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศ และฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศ ดังนี้

๗.๑.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูล

๗.๑.๒ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

๗.๑.๓ ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

๗.๑.๔ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการจ้างโดยทันที

๗.๑.๕ ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

๗.๑.๖ มีการกำหนดข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายในข้อมูลลับ

๗.๑.๗ มีขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ควรประกอบด้วย วิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ ระยะเวลาที่สามารถเข้าถึง และช่องทางการเข้าถึง

๗.๑.๘ มีการจำกัดการเข้าถึงข้อมูลตามระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๗.๑.๙ มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่น่าออกจากระบบงานมีความถูกต้อง และสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

๗.๑.๑๐ มีการจัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๗.๑.๑๑ การเข้าถึงต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๗.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking) โดยกำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไว้ดังนี้

๗.๒.๑ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

๗.๒.๒ ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

๑) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์และระบบ โดยติดตั้งไว้ในพื้นที่ปลอดภัย

๒) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

๗.๒.๓ ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับ ระบบดังกล่าวโดย

๑) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงาน ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

๒) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากภายนอกได้

๓) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

๗.๒.๔ ควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนด

๗.๒.๕ วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายการสำรองระบบสารสนเทศ

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ต้องปฏิบัติตามนี้

๗.๓.๑ การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของ หน่วยงานโดยไม่ได้รับอนุญาต

๗.๓.๒ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

๗.๓.๓ ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

๗.๓.๔ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่สำนักงานอนุญาตให้ผู้ใช้งานเป็นสินทรัพย์ของสำนักงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

๗.๓.๕ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗.๓.๖ ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๗.๓.๗ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น

๗.๓.๘ กรณีส่งเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

๗.๓.๙ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น

๗.๓.๑๐ ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศ

๗.๓.๑๑ ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้มีสภาพเดิม

๗.๓.๑๒ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของสำนักงาน จากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๓.๑๓ การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกสำนักงาน เมื่อนำกลับมาที่สำนักงาน ต้องทำการเชื่อมต่อระบบเครือข่ายภายในสำนักงาน เพื่อทำการอัปเดต (Update) ข้อมูลไวรัสล่าสุด

๗.๓.๑๔ ห้ามผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๗.๓.๑๕ การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๗.๓.๑๖ ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกครั้ง

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

๗.๔.๑ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน

๗.๔.๒ การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๔.๓ การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียด ดังนี้

- ๑) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน
- ๒) รายละเอียดและลักษณะของระบบงาน
- ๓) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

๔) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

๕) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

๗.๔.๔ ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๗.๔.๕ การเข้าสู่ระบบระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๗.๔.๖ ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานโดยไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

๗.๔.๗ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๗.๔.๘ ผู้ดูแลระบบจะทำการยกเลิกสิทธิ์การเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงานแก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาของอนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๔.๙ ผู้ดูแลระบบต้องทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในหน่วยงาน มีความมั่นคงปลอดภัยกำหนดแนวทางปฏิบัติเพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ ดังนี้

๘.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๒ ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งาน ดังนี้

๘.๒.๑ ลงทะเบียน และกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายเหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน หรือลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สายก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๘.๒.๒ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๘.๒.๓ ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier) เพื่อความปลอดภัย

๘.๒.๔ เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

๘.๒.๕ กำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจาย (Access Point) เพื่อให้ยากต่อการดักจับ เพื่อความปลอดภัย

๘.๒.๖ ใช้วิธีการควบคุม ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หรือ MAC Address (Media Access Control Address) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หรือ อุปกรณ์ที่มี MAC Address ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

๘.๒.๗ ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๘.๒.๘ กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๘.๒.๙ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทันที

ส่วนที่ ๙ การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย ดังนี้

๙.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร

๙.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๙.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๙.๔ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๙.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๙.๖ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๙.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิด ความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๙.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับ ความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๙.๙ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๙.๑๐ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

๙.๑๑ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บน อินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

ส่วนที่ ๑๐ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติ ดังนี้

๑๐.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตให้ผู้ใช้งานระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๐.๒ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบน เครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๐.๓ ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศ

๑๐.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการ โดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญา กับหน่วยงานเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกหน่วยงานเพื่อการใดก็ตาม ต้องขออนุมัติผู้บริหารระดับสูงที่กำกับหน่วยงานเจ้าของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเป็นลายลักษณ์อักษรเท่านั้น

๑๐.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกัน ไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล

๑๐.๖ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ดังนี้

๑๐.๕.๑ กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่อง และเก็บรักษาห้สผ่านอย่างปลอดภัย

๑๐.๕.๒ เมื่อไม่ได้ใช้งานเกิน ๑๕ นาที เครื่องควรตั้งโปรแกรม Screen Saver และต้องใช้ รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง และเมื่อเลิกใช้งานควรล็อกเอาท์ (Log Out) ออกจากเครื่อง

๑๐.๕.๓ ต้องอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์และ โปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๑๐.๕.๔ เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของสำนักงาน จากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๐.๕.๕ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มีได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบมาใช้งานและเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับพิจารณาอนุมัติจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนการใช้งาน

๑๐.๕.๖ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

๑๐.๕.๗ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น

๑๐.๕.๘ การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในหน่วยงานในสำนักงาน จะต้องแจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศดำเนินการให้เท่านั้น

๑๐.๕.๙ กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบโดยผู้รับจ้าง เมื่อตรวจสอบเสร็จแล้วต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

๑๐.๕.๑๐ ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงานทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบของหน่วยงานภายในสำนักงานที่มีศูนย์สารสนเทศ

๑๐.๕.๑๑ ผู้ใช้งานไม่ควรสร้าง Short-Cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของสำนักงาน

๑๐.๕.๑๒ ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบทันที

๑๐.๕.๑๓ ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

ส่วนที่ ๑๑ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

๑๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน

๑๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๑.๓ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) เพื่อเปิดใช้งานเครื่องทุกครั้ง และควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และเก็บรักษาไว้เป็นความลับ

๑๑.๔ ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ไม่น้อยกว่า ๑๕ นาที เพื่อล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านอีกครั้งเมื่อกลับมาใช้งาน

๑๑.๕ ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งาน

๑๑.๖ ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสู่ระบบที่เก็บข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๗ การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับเกิดความเสียหายได้

๑๑.๘ หลีกเลี่ยงการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๑.๙ ความปลอดภัยทางด้านกายภาพ

๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๓) หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก

๔) ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๕) หลีกเลี่ยงการใช้วัสดุ หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนไม่วางของทับบนหน้าจอและแป้นพิมพ์ หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๖) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๗) ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แบบพกพาให้อยู่ในสภาพพร้อมใช้งาน ปิดเครื่องเมื่อต้องใช้เป็นระยะเวลานานเกินไป หรือในสภาพที่มีอากาศร้อนจัด

ส่วนที่ ๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑๒.๑ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑๒.๑.๑ กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๑๒.๑.๒ กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิได้ หากเกินกว่าที่กำหนดระบบ
ต้องทำการ Lock ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

๑๒.๑.๓ ผู้ดูแลระบบควรตั้งระบบการล็อกหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งาน
ผู้ใช้อาจใส่รหัสผ่าน

๑๒.๑.๔ ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่
หน้าจอเป็นเวลานาน

๑๒.๒ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ
โดยผู้ดูแลระบบ ดังนี้

๑๒.๒.๑ ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกัน
ความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

๑๒.๒.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่
ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

๑๒.๒.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติ
จากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนดำเนินการ

๑๒.๒.๔ ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Compiler) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์
แม่ข่ายที่ให้บริการ

๑๒.๒.๕ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบ
สารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

๑๒.๒.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศ
ตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย
ที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

๑๒.๒.๗ วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน
ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑๒.๒.๘ จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้
ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

๑๒.๒.๙ ทำการปรับปรุง Library สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัย
และสอดคล้องกับทั้งหมดที่ทำการติดตั้ง

๑๒.๒.๑๐ กำหนดให้ผู้ที่เกี่ยวข้องจัดทำแผนถอยหลังกลับ (Rollback strategy) ก่อนที่จะ
ดำเนินการติดตั้งระบบงานบนเครื่องให้บริการ

๑๒.๓ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากการเปลี่ยนแปลง
ระบบปฏิบัติการ

๑๒.๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลง
ระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการ
เปลี่ยนแปลงระบบปฏิบัติการ

๑๒.๓.๒ วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลัง
จากที่เปลี่ยนแปลงระบบปฏิบัติการ

๑๒.๔ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๑๒.๔.๑ กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๑๒.๔.๒ ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก ควรระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด

๑๒.๔.๓ กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๑๒.๔.๔ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ก่อนมีการติดตั้ง

๑๒.๔.๕ การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกร่องระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๑๒.๕ มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

๑๒.๕.๑ ผู้ให้บริการที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของหน่วยงาน จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๒.๕.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

๑๒.๕.๓ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๑๒.๕.๔ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนทุกครั้ง

๑๒.๖ มาตรการควบคุมช่องโหว่ทางเทคนิค

๑๒.๖.๑ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ๑) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- ๒) สถานที่ที่ติดตั้ง
- ๓) เครื่องแม่ข่ายที่ติดตั้ง
- ๔) ผู้ผลิตซอฟต์แวร์
- ๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๑๒.๖.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๑๒.๖.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

- ๑) มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไข ช่องโหว่ตามความเหมาะสม
- ๒) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- ๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๑๒.๖.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑๒.๖.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

- ๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
- ๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
- ๓) ข้อมูลวันเวลาที่ออกจากระบบ
- ๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- ๕) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ
- ๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- ๗) ข้อมูลการเปลี่ยนคอนฟิกูเรชัน (Configuration) ของระบบ
- ๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)
- ๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- ๑๐) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง
- ๑๑) ข้อมูลโปรโตคอล (Protocol) เครือข่ายที่ใช้
- ๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
- ๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๒.๖.๖ Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา ๙๐ วัน

๑๒.๖.๗ ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า ๙๐ วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้ เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

๑๒.๖.๘ ผู้ดูแลระบบ ต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

- ๑) การโจมตีในรูปแบบ Port-Scan
- ๒) การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิ์ในการใช้งานระบบนั้น
- ๓) เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์ Server ที่เกิดขึ้น

๑๒.๖.๙ ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

๑๒.๖.๑๐ ต้องมีการประเมินความเสี่ยงทุก ๖ เดือน พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

๑๒.๖.๑๑ กรณีการจัดซื้อ Server และหรือ Application ใหม่ ที่ให้บริการบนเครื่องแม่ข่ายของหน่วยงานที่มีศูนย์สารสนเทศ ต้องมีข้อกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในการจัดซื้อ และต้องมีการกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นทิศทางเดียวกับสำนักงาน โดยต้องประสานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน

ส่วนที่ ๑๓ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑๓.๑ ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

๑๓.๑.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงานพื้นที่ควบคุมเฉพาะให้ชัดเจนและควบคุม เพื่อกำหนดสิทธิ์การเข้าถึงพื้นที่ โดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๓.๑.๒ กำหนดมาตรการการควบคุมการเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ดังนี้

- ๑) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิ์การเข้าใช้งานพื้นที่เท่านั้น
- ๒) มีการพิสูจน์ตัวตน โดยการอ่านบัตรหรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า - ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)
- ๓) ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวัง การเข้าพื้นที่ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์
- ๔) ให้มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)
- ๕) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
- ๖) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว
- ๗) สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ
- ๘) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่
- ๙) จัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
- ๑๐) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน
- ๑๑) ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๒) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๓.๑.๓ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑๓.๑.๔ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

- ๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง
- ๒) ติดตั้งระบบประจักษ์เพลิง
- ๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น
- ๔) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายใน

ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) ทำงานผิดปกติหรือหยุดการทำงาน

๕) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๑๓.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

๑๓.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

๑๓.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๑๓.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๑๓.๒.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๑๓.๒.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๑๓.๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๑๓.๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๑๓.๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑๓.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑๓.๓.๑ กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ ๓ ครั้ง

๑๓.๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๑๓.๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๑๓.๓.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

๑๓.๓.๕ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๓.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๑๓.๔.๑ ต้องขออนุญาตจากผู้บริหารระดับสูงที่กำกับหน่วยงานเจ้าของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือนำไปซ่อมบำรุงภายนอก

๑๓.๔.๒ ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าว กลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอยู่ในสภาพดี

๑๓.๔.๓ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๑๓.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off Premises)

๑๓.๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๑๓.๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

๑๓.๕.๓ เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๓.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๑๓.๖.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๑๓.๖.๒ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

๑๓.๖.๓ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ ๑๔ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : E-mail)

๑๔.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานปลัดสำนักนายกรัฐมนตรีให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๑๔.๒ ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน หรือระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐเท่านั้น ในการติดต่อราชการ หรือรับ – ส่งข้อมูลของทางราชการผ่านทางจดหมายอิเล็กทรอนิกส์

๑๔.๓ ผู้ดูแลระบบรับเรื่องการใช้งานจดหมายอิเล็กทรอนิกส์ขององค์กร โดยกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานจดหมายอิเล็กทรอนิกส์ รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

๑๔.๔ กำหนดให้ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก ๑๘๐ วัน

๑๔.๕ ผู้ดูแลระบบไม่สามารถเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น 'x' หรือ 'o' ในการพิมพ์แต่ละตัวอักษร

๑๔.๖ กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๕ ครั้ง

๑๔.๗ ผู้ใช้งานควรหลีกเลี่ยงการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๔.๘ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงาน ได้แก่ การละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ รวมทั้งไม่อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของหน่วยงาน

๑๔.๙ ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์

๑๔.๑๐ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๑๔.๑๑ ผู้ใช้งานควรตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๑๔.๑๒ ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๔.๑๓ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ - ส่ง จดหมายอิเล็กทรอนิกส์ ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียงหรือข้อมูลทำให้เกิดความแตกแยกผ่านทางจดหมายอิเล็กทรอนิกส์

๑๔.๑๔ ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บนจดหมายอิเล็กทรอนิกส์

๑๔.๑๕ ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

- ๑) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ
- ๒) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
- ๓) ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- ๔) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

๑๔.๑๖ ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox)

ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๕.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๕.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความระมัดระวังในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือ ข้อมูลความลับของหน่วยงาน

๑๕.๓ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

๑๕.๔ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

วัตถุประสงค์

- ๑) เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
- ๒) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
- ๓) เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

- ๑) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่มีศูนย์สารสนเทศของตนเอง
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

ส่วนที่ ๑ การสำรองข้อมูล (Back Up)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้

๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผน โดยกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล และการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูลหรือระบบ โดยมีรายละเอียดการสำรองข้อมูล ดังนี้

๑.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ ดังนี้

- ๑) ข้อมูลคอนฟิกูเรชัน (Configuration) สำหรับระบบ
- ๒) ฐานข้อมูล (Database) ในระบบสารสนเทศ
- ๓) ซอฟต์แวร์ (Software) ต่าง ๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์

ระบบงาน หรือซอฟต์แวร์อื่น ๆ ที่สำคัญ

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็นการสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑.๒.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

๑.๒.๔ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการวัน/เวลา ขนาดข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๑.๒.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

๑.๒.๖ ในกรณีที่จัดเก็บข้อมูลสำรองนั้นในสื่อเก็บข้อมูล ต้องขี้งบสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของ ชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

๑.๒.๗ จัดเก็บข้อมูลที่สามารถสำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้ที่นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนฉุกเฉินด้านสารสนเทศที่กำหนดไว้

๑.๒.๘ วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

๑.๒.๙ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๑.๒.๑๐ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

๑.๒.๑๑ การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของสำนักงาน เดือนละ ๒ ครั้ง

๑.๒.๑๒ ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรองข้อมูลทุกครั้ง

๑.๒.๑๓ ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๑.๒.๑๔ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

๑.๒.๑๕ ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี

๑.๒.๑๖ สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

ส่วนที่ ๒ การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑.๑ กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นรวมทั้งมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทำให้ไม่สามารถเข้ามาใช้งานระบบสารสนเทศได้

๒.๑.๓ กำหนดขั้นตอนปฏิบัติในการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาในการกู้คืนระบบที่สอดคล้องตามเป้าหมายที่หน่วยงานกำหนดไว้

๒.๑.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑.๕ กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงาน และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ

๒.๑.๖ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๕ ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

- ๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
- ๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
- ๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ผู้รับผิดชอบ

- ๑) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่มีศูนย์สารสนเทศของตนเอง
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๓) ผู้ตรวจสอบภายใน

แนวทางปฏิบัติ

ส่วนที่ ๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๒ มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

๒.๔.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบแบบอ่านได้

อย่างเดียว

๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันอย่างเหมาะสม

๒.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

๒.๔.๕ ในกรณีที่มือเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Office : DCIO) ประจำสำนักงานปลัดสำนักนายกรัฐมนตรี ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ ๑ ระดับนโยบาย

๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของสำนักงานปลัดสำนักนายกรัฐมนตรี เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Office : DCIO) ประจำสำนักงานปลัดสำนักนายกรัฐมนตรี เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดสำนักนายกรัฐมนตรี ผู้รับผิดชอบ ดังนี้

๑.๓.๑ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๑.๓.๒ ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๑.๓.๓ วางแผน จัดทำทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๒ ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติการประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

๒.๑.๑ ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคง ปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๓ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบ ระยะเวลาที่กำหนด

๒.๑.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๖ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดสำนักนายกรัฐมนตรี

๒.๒ ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด