ประกาศสำนักงานปลัดกระทรวงเกษตรและสหกรณ์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีทางการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ปลัดกระทรวงเกษตรและสหกรณ์โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ พ.ศ. ๒๕๕๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ ตามประกาศนี้มี ๓ ส่วน ดังนี้

๓.๑ แนวทางการจัดทำแนวนโยบายและแนวปฏิบัติ มีแนวทางอย่างน้อย ประกอบด้วย

(๑) การจัดทำเป็นลายลักษณ์อักษร ด้วยการมีส่วนร่วมจากผู้เกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบและผู้ใช้งาน

(๒) จัดให้มีการทบทวนและปรับปรุง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อหน่วยงานโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดมาตรการและกำกับดูแลการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยมีผู้บริหารเทคโนโลยีสารสนเทศ (CIO) เป็นผู้รับผิดชอบต่อนโยบายในฐานะเป็นผู้กำกับ ติดตามการทบทวนนโยบาย

(๓) แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอเพื่อให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและสนับสนุนต่างๆ โดยเคร่งครัด

๓.๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จะต้องมีเนื้อหาสาระสำคัญอย่างน้อย ประกอบด้วย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การมีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓.๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาสาระสำคัญอย่างน้อย ประกอบด้วย

(๑) การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

(๔) การควบคุมการเข้าถึงเครือข่าย (Network access control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

(๗) จัดทำระบบสำรองสำหรับระบบสารสนเทศ (Backup and Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment)

(๙) การกำหนดหน้าที่ความรับผิดชอบผู้ดูแลระบบ (Administrator Responsibility)

รายละเอียดข้อ ๑ – ๙ มีข้อกำหนดอย่างน้อย ดังนี้

ข้อ ๔ การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control) มีข้อกำหนดอย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตการเข้าถึงระบบสารสนเทศ ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

(๓) ต้องมีการกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

(๔) ต้องจัดทำข้อปฏิบัติการควบคุมการเข้าถึงสารสนเทศและปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความปลอดภัย

ข้อ ๕ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๖ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๗ การควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and Configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๘ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๙ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(Application and information access control) ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๐ การจัดทำระบบสำรองข้อมูลระบบสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) การกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) การปฏิบัติและทบทวนแนวทางการสำรองข้อมูล อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

(๑) จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) การทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม

(๓) การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน (Internal auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๒ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๕๖

(นายชวลิต ชูขจร)
ปลัดกระทรวงเกษตรและสหกรณ์

เอกสารหมายเลข ๒

เอกสารแนบท้ายประกาศ
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์
ว่าด้วยคำนิยาม

คำนิยามที่ใช้ประกาศประกอบด้วย

“กระทรวง” หมายถึง กระทรวงเกษตรและสหกรณ์

“สำนักงาน” หมายถึง สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

“หน่วยงาน” หมายถึง สำนักงาน กอง ศูนย์และกลุ่ม รวมถึงหน่วยงานย่อยต่าง ๆ ในสังกัดสำนักงาน หรือหน่วยงานที่ใช้งานสถานที่อยู่ในอาคารสำนักงาน ณ ถนนราชดำเนินนอก

“ศูนย์” หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

“ผู้บริหารสูงสุด (Chief Executive Office : CEO)” หมายถึง ปลัดกระทรวงเกษตรและสหกรณ์

“ผู้บริหารเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO)” หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศของ สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ รองปลัดกระทรวงเกษตรและสหกรณ์ผู้ที่มีหน้าที่และความรับผิดชอบในการบริหารงานเทคโนโลยีสารสนเทศของสำนักงาน การจัดทำแผนแม่บทและแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศของสำนักงาน การจัดทำนโยบายและกำกับดูแลการดำเนินการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กำกับดูแลการดำเนินการตามนโยบายเทคโนโลยีสารสนเทศแห่งชาติและติดตามผลการดำเนินงานตามนโยบาย กำกับดูแลการพัฒนาเทคโนโลยีสารสนเทศให้เป็นไปตามมาตรฐานที่กำหนดและพัฒนาการใช้ให้มีประสิทธิภาพเกิดประโยชน์สูงสุดและคุ้มค่า กำกับดูแลติดตามและประเมินผล และการรายงานผลการปฏิบัติงานสารสนเทศ

“ผู้บังคับบัญชา” หมายถึง ผู้บังคับบัญชาระดับสำนัก/กอง/กลุ่มหรือระดับกรมทั้งบุคคลที่ได้รับมอบหมาย

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้างและพนักงานราชการหรือผู้ที่สำนักงานอนุญาต (Authorized Users) ให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

“มาตรฐาน” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

“ขั้นตอนปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ควรปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของสำนักงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

“เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้สามารถเข้าใช้งานดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงาน ดังนี้

- ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์
- ผู้พัฒนาระบบ (System Developer) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ในการพัฒนาและดูแลรักษาระบบงานสารสนเทศของหน่วยงาน

“หน่วยงานภายนอก” หมายถึง หน่วยงานที่สำนักงานอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูล หรือทรัพย์ชนิดต่างๆ ของสำ นักงาน โดยจะได้รับสิทธิในการใช้ระบบตามประเภทงาน และต้องรับผิดชอบในการรักษาความลับด้วย

“ข้อมูลคอมพิวเตอร์ ” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมู ลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data)” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบคอมพิวเตอร์ (Computer System)” หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางการปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย (Network System)” หมายถึง ระบบที่ใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสำนักงาน ได้แก่ ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet) เป็นต้น

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของ สำนักงาน เข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน
- ระบบอิ นเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสำนักงาน เข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

“ห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room) ” หมายถึง ห้องที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือคอมพิวเตอร์หลัก และอุปกรณ์เครือข่ายหลักที่ใช้งานในสำนักงาน

“จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับ- ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้เครือข่าย ผู้รับสามารถเปิดอ่านข่าวสารหรือพิมพ์ลงกระดาษหรือจะลบทิ้งก็ได้

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“สิทธิ์ของผู้ใช้งาน ” หมายถึง สิทธิ์ทั่วไป สิทธิจำเพาะ สิทธิพิเศษ หรือสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

“รหัสผ่าน (Password)” หมายถึง ตัวอักษร หรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“โปรแกรมไม่ประสงค์ ” หมายถึง โปรแกรมที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ทำให้ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“ระบบเครือข่ายไร้สาย (Wireless) หมายถึง ระบบเครือข่ายสื่อสารข้อมูล โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ ”

“เจ้าของข้อมูล” หมายถึง หน่วยงานที่รับผิดชอบในการนำข้อมูลของสำนักงานเข้าในระบบเทคโนโลยีสารสนเทศ โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ และได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

“สินทรัพย์” หมายถึง ทรัพย์สิน หรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าของหน่วยงาน ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟแวร์ที่มีค่าลิขสิทธิ์ เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจจะรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

เอกสารหมายเลข ๓

เอกสารแนบท้าย

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ พ.ศ. ๒๕๕๖

องค์ประกอบของแนวปฏิบัติ ประกอบด้วย ๗ ส่วน ดังนี้

ส่วนที่ ๑ ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

ส่วนที่ ๒ นโยบายควบคุมการเข้าถึงและการใช้งานระบบระบบสารสนเทศ

(๑) การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

(๔) การควบคุมการเข้าถึงเครือข่าย (network access control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

(๗) การบริหารจัดการการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๘) การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Personal computer and Mobile computing)

(๙) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

(๑๐) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

(๑๑) การควบคุมการใช้งานระบบอินเตอร์เน็ต (Internet)

(๑๒) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

ส่วนที่ ๓ นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment security)

ส่วนที่ ๔ นโยบายการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ(Information Systems Acquisition, Development and Maintenance Policy)

ส่วนที่ ๕ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ (Backup and Recovery)

ส่วนที่ ๖ นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๗ นโยบายการปฏิบัติตามข้อกำหนด

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment)

๒. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ส่วนที่ ๑
ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อให้ได้การจัดประเภทข้อมูล ความสำคัญ และการจัดแบ่งลำดับชั้นความลับของข้อมูล ใช้ในการบริหารจัดการ การควบคุมการเข้าถึงข้อมูลตามสิทธิที่ได้รับได้อย่างถูกต้อง เหมาะสมและปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบ/ผู้ที่เกี่ยวข้อง

แนวปฏิบัติ

สำนักงาน มีการกำหนดประเภทและลำดับความสำคัญของข้อมูล ดังนี้

๑. การจัดแบ่งประเภทของข้อมูล แบ่งออกเป็น ๒ ประเภท คือ

(๑) ข้อมูลสารสนเทศด้านการปฏิบัติงานและการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(๒) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลด้านการเกษตร ข้อมูลเตือนภัยด้านการเกษตร ข้อมูลเพื่อการติดต่อประสานงาน เป็นต้น

๒. การจัดแบ่งลำดับความสำคัญของข้อมูลแต่ประเภท แบ่งออกเป็น ๓ ระดับ คือ

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๓) ข้อมูลที่มีระดับความสำคัญน้อย

๓. การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภท แบ่งออกเป็น ๓ ระดับ คือ

(๑) ลับ หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๒) ลับมาก หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๓) ลับที่สุด หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

ส่วนที่ ๒

นโยบายควบคุมการเข้าถึงและการใช้งานระบบระบบสารสนเทศ (Access control)

วัตถุประสงค์

๑. เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกภัยคุกคามต่าง ๆ

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน และผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับหน่วยงานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบ/ผู้ที่เกี่ยวข้อง

แนวปฏิบัติ

๑. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

สำนักงานได้มีการจัดแบ่งระดับการเข้าถึงข้อมูลและสิทธิ เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

๑.๑ การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูลได้แก่

(๑) ระดับชั้นสำหรับผู้บริหาร
(๒) ระดับชั้นสำหรับผู้ใช้งาน
(๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๑.๒ การแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

(๑) สร้าง/ปรับปรุง/ป้อน (Create)
(๒) อ่าน (Read)
(๓) แก้ไข (Edit)
(๔) ลบ (Delete)
(๕) อนุมัติ (Authorize)

๑.๓ การกำหนดเวลาที่ได้เข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๑.๔ การกำหนดช่องทางการเข้าถึง

ผู้ที่เกี่ยวข้องที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดได้นั้น จะต้องรับสิทธิ์จากศูนย์โดยมีการกำหนดบัญชีผู้เกี่ยวข้องตามระดับการเข้าถึง ให้สามารถเข้าใช้งาน มีการแยกประเภทความรับผิดชอบ และมีการพิสูจน์ตัวตน สิทธิ์ในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

(๑) ระบบเครือข่ายภายใน (Intranet)

(๒) ระบบเครือข่ายอินเตอร์เน็ต (Internet)

(๓) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑.๕ การกำหนดตั้งชื่อบัญชีผู้ใช้งาน (Username) และ รหัสผ่าน (Password) สำหรับการเข้าใช้งาน ดังนี้

(๑) การตั้งชื่อบัญชีผู้ใช้งานและผู้ดูแลระบบต้องแยกกันโดยใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย_และนามสกุล ๒ ตัวแรก หรือใช้เลขที่บัตรประจำตัวประชาชนตามความเหมาะสม

(๒) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดา และต้องมีความแตกต่างกัน

(๓) กำหนดรหัสผ่านให้มีตัวอักษรจำนวนอย่างน้อยหรือมากกว่า ๖ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) การตั้งชื่อบัญชีผู้ใช้งานและรหัสผ่านต้องแยกบัญชีและต้องตั้งรหัสผ่านไม่เหมือนกัน

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน ศูนย์ต้องจัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศและอุปกรณ์ที่เกี่ยวข้องทั้งหมด โดยการกำหนดต้องคำนึงการใช้งานและความปลอดภัย มีแนวปฏิบัติอย่างน้อย **ดังนี้**

๒.๑ จัดให้มีการเผยแพร่ประชาสัมพันธ์ความรู้ความเข้าใจให้กับผู้ใช้งาน เหตุการณ์ด้านความมั่นคงปลอดภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒ จัดให้มีการฝึกอบรมในหลักสูตร ที่มีเนื้อหาเกี่ยวข้องกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) อย่างน้อยปีละ ๑ ครั้ง

๒.๓ กำหนดให้มีการลงทะเบียนผู้ใช้งาน (user registration) โดยมีขั้นตอนปฏิบัติ ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ผู้ใช้งานจะต้องกรอกแบบฟอร์มเพื่อขออนุมัติใช้งานระบบงานตามแบบฟอร์มคำขอใช้บริการด้านสารสนเทศตามที่ศูนย์ได้จัดทำขึ้น และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติใช้งาน

(๓) เมื่อแบบฟอร์มได้รับอนุมัติแล้วส่งให้กับผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบเพื่อดำเนินการตรวจสอบ กำหนดสิทธิ์การใช้งานโดยให้เหมาะสมกับหน้าที่ความรับผิดชอบและจัดเก็บแบบฟอร์ม

(๔) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการอนุมัติเข้าใช้งาน

(๕) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๖) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ เมื่อผู้ใช้งานมีการลาออก โยกย้าย โอน เปลี่ยนตำแหน่ง สิ้นสุดการจ้าง เป็นต้น

๒.๔ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) กำหนดสิทธิการใช้งานระบบเทคโนโลยีสสารสนเทศ โดยให้สิทธิ์เหมาะสมตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งานให้กับผู้ใช้งาน เจ้าหน้าที่ และบุคคลภายนอกที่หน่วยงานอนุญาตให้ใช้งาน

(๒) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๓) ทบทวนสิทธิการใช้งานสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) กำหนดขั้นตอนการปฏิบัติงานสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๓) การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นในการจัดส่ง และกำหนดให้ผู้ใช้งานลงนามรับรหัสผ่านเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน และรับทราบแนวปฏิบัติการใช้งานของหน่วยงาน

(๔) ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และเปลี่ยนตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๕) กรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออกให้หน่วยงานประสานแจ้งศูนย์เพื่อให้ผู้ดูแลระบบทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจากระบบทันที

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบเพื่อพิจารณาความเหมาะสม โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน

(๑) ทบทวนสิทธ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๒) ทบทวนสิทธิผู้ที่มีสิทธิในระดับสูง เช่น สิทธิผู้ดูแลระบบ ด้วยความถี่กว่าสิทธิระดับผู้ใช้งานต้น

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

๓.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) รหัสผ่านสำหรับการเข้าใช้งานระบบของหน่วยงาน ถือว่าเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสให้คนอื่นรับรู้

(๒) ต้องกำหนดรหัสผ่านตามเกณฑ์การกำหนดตั้งชื่อบัญชีผู้ใช้งานของสำนักงาน

(๓) เปลี่ยนรหัสผ่านชั่วคราวทันทีที่เข้าระบบครั้งแรก เพื่อป้องกันบุคคลอื่นลักลอบใช้งาน

(๔) ต้องกำหนดรหัสผ่านตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) ของสำนักงาน

(๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๖) ผู้ใช้งานมีหน้าที่ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ แม้ว่าจะไม่มีการบังคับให้เปลี่ยนจากระบบก็ตาม

(๗) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนมีสิทธิใช้งาน

(๘) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (username) และรหัสผ่าน (password) ของบุคคลใดบุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง

(๙) กรณีผู้ใช้งานของหน่วยงานภายในสำนักงาน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่จะขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งศูนย์เพื่อทำการเปลี่ยนแปลงสิทธิ์ในการเข้าใจงาน

(๑๐) ผู้ใช้งานทุกคนของสำนักงาน มีหน้าที่ระมัดมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้(username) ระบบคอมพิวเตอร์ของตน

๓.๒ การป้องกันอุปกรณ์ที่ขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อป้องกันๆไม่ให้ผู้มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) ออกจากระบบงาน (log out) โดยทันทีเมื่อเสร็จสิ้นงาน

(๒) ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งานเกิน ๑ นาที เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

(๓) การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานหรือถือครองให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ออกจากระบบงาน (log out) โดยทันทีเมื่อเสร็จสิ้นงาน

(๒) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๓) ต้องจัดเก็บ /สำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย เช่น เก็บไว้ในตู้เอกสารที่มีระบบความปลอดภัย

(๔) ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานป ระจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งานเกิน ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

(๕) การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานหรือถือครองให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที

(๖) ให้ขออนุมัติจากผู้บังคับบัญชา ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึก อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงานก่อนทุกครั้ง

(๗) ระมัดระวังและดูแลทรัพย์สินของสำนักงานที่ตนเองใช้งานห รือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ ดังนี้

ผู้ใช้งานต้องทำการเ ข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

๔. การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อป้องการการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต มีแนวปฏิบัติอย่างน้อย ดังนี้

๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ดังนี้

(๑) กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น

(๒) ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (WiFi) ระบบเครือข่ายอินเตอร์เน็ต ระบบสารสนเทศ เป็นต้น โดยการให้สิทธิเฉพาะสำหรับใช้ในการปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้บังคับบัญชา

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) การเข้าสู่เครือข่ายของหน่วยงานผ่านเครือข่ายภายนอก จะต้องมีการพิสูจน์ตัวตนโดยใช้

บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง

(๒) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

(๓) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์ก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

๔.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงนี้

(๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากศูนย์ก่อนจึงจะสามารถดำเนินการได้

(๒) ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์กำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(๓) จะต้องมีการจำกัดสิทธิการเข้าใช้งานอุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและความเหมาะสมในการเข้าถึง

(๔) จัดทำผังระบบเครือข่าย (Network Diagram) ซึ่งมีการระบุรายละเอียดอุปกรณ์บนเครือข่าย อุปกรณ์ที่ติดตั้งในเครือข่าย และข้อมูลอื่นๆที่จำเป็น

๔.๔ การป้องกันพอร์ทที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

(๒) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายกลางที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๓) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(๔) เปิดพอร์ทที่มีความจำเป็นในการใช้งาน และ ยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

(๖) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(๗) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(๘) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

(๙) ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

๔.๕ การแบ่งแยกเครือข่าย (Segregation in networks) ศูนย์ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มงานที่เกี่ยวข้อง ดังนี้

(๑) ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่ายแต่ละกอง/สำนัก หรือที่ตั้งอาคาร ออกจากกันเพื่อป้องกันการละเมิดสิทธิและทรัพยากรเครือข่ายของแต่ละหน่วยงาน

(๒) ผู้ดูแลระบบจะต้องแบ่งแยกเครือข่ายออกเป็นโซนเพื่อความมั่นคงปลอดภัยของระบบจากการบุกรุกทางเครือข่าย ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ศูนย์ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

(๑) การจำกัดสิทธิ การเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(๔) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(๕) ควบคุมไม่ให้มีการเปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(๖) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาตเท่านั้น

๔.๗ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบเครือข่ายจากระยะไกล (remote access) สู่ระบบสารสนเทศ ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายในและต้องดูแลและจัดการอย่างรัดกุม ได้แก่ ช่องทางการเชื่อมต่อเครือข่ายแบบปลอดภัย SSL VPN การควบคุมพอร์ต(Port) เป็นต้น

(๒) การเข้าสู่เครือข่ายของหน่วยงานผ่านเครือข่ายภายนอกต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

(๓) ก่อนการกำหนดสิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการ ศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

(๔) ผู้ใช้งานที่ได้รับสิทธิต้องมีการปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด โดยจะต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว ซึ่งหากระบบมีความเสียหายและสืบทราบมาได้ว่าเกิดจากการผู้ใช้งานจะต้องรับผิดชอบ

๔.๘ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control)

(๑) ผู้ใช้งานมีสิทธิในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตนเอง

(๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(๓) ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(๔) ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานระบบเครือข่ายร่วมกัน เช่น การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่าย

(๕) ระบบเครือข่ายที่มีการเชื่อมต่อไปยังเครือข่ายภายนอกต้องเชื่อมต่อผ่านอุปกรณ์รักษาความปลอดภัย IPS และ Firewall เป็นต้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีแนวปฏิบัติอย่างน้อย ดังนี้

๕.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๑) ผู้ใช้งานจะต้องทำการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๒) ผู้ใช้งานจะต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน

(๓) ผู้ใช้งานจะต้องทำการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเมื่อไม่มีการใช้งานให้ทำการล็อคหน้าจอด้วยรหัสผ่าน

(๔) ผู้ใช้งานต้องทำการลงบันทึกออกทุกครั้งเมื่อไม่ได้ใช้งานเป็นเวลานาน

๕.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

(๑) ผู้ดูแลระบบต้องกำหนดรหัสผ่านให้กับผู้ใช้งานตามหลักเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๒) ผู้ใช้งานจะต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงานที่แยกออกจากกันของแต่ละบุคคลเพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

(๓) ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ตามที่หน่วยงานกำหนดให้

๕.๓ การบริหารจัดการรหัสผ่าน (Password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) การกำหนดรหัสผ่านให้กับผู้ใช้งานตามหลักเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๒) อนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง โดยต้องกำหนดให้เป็นไปตามเงื่อนไขการกำหนดรหัสผ่าน

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

(๑) ห้ามมิให้ลงโปรแกรมออรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาตและยังไม่ผ่านการตรวจสอบ

(๒) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) กำหนดให้มีการถอดถอนโปรแกรมออรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๕) ให้ผู้ดูแลระบบทำบัญชีโปรแกรมที่อนุญาตให้ใช้งานได้

๕.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ ๒ ชม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น หรือช่วงนอกเวลาการทำงาน เป็นต้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง(ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control) โดยต้องมีการควบคุมอย่างน้อยดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

(๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๒) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๑๕ นาที ต้องทำการยุติการใช้งานทันที

(๓) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

- กำหนดสิทธิ์ให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลแต่ละระดับชั้น
- กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

(๔) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิ์และได้รับอนุญาตในการเข้าดำเนินการและจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิ์ที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลต่อกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

๖.๒ ระบบซึ่งไวต่อการรบกวน

(๑) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ศูนย์ต้องแยกระบบ ซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องเซิฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่ บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดติดตั้งห้องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

(๒) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า- ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และ อื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(๓) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิ์การเข้าใช้งานโดยกำหนดค่าที่ Firewall

(๔) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อน ที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(๑) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในสำนักงาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

(๓) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

(๔) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุง สิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

๗. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๗.๑ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๑) กำหนดให้มีรหัสผู้ใช้รหัสผ่าน(Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

(๒) กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการ LOCK ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

(๓) ผู้ดูแลระบบต้อง กำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อย ตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๔) ผู้ดูแลระบบตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๕) ผู้ดูแลระบบต้องทำการ logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๗.๒ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

(๑) ควบคุมการเปลี่ยนแปลงต่อระบบงานของสำนักงาน เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

(๒) ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของสำนักงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) กำหนดให้มีการจัดเก็บ Source Code และ Library สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๕) กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

(๖) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

(๗) ทำการปรับปรุง Library สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับทั้งหมดที่ทำการติดตั้ง

(๘) กำหนดให้ผู้ที่เกี่ยวข้องจัดทำแผนถอยหลังกลับ (Rollback Strategy) ก่อนที่จะดำเนินการติดตั้งระบบงานบนเครื่องให้บริการ

๗.๓ การทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of applications after operating system changes)

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการข องระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่สำนักงาน ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๗.๔ การพัฒนาซอ ฟต์แวร์ และดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศ โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) สำนักงานเป็นผู้มีสิทธ์ในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้การตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) การดำเนินการพัฒนาซอฟแวร์และดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ดำเนินการโดยหน่วยงานภายนอกนั้น ซึ่งหน่วยงานภายนอกจะต้องมีการลงนามในสัญญารักษาความลับรักษาข้อมูลของหน่วยงานก่อนการดำเนินการใด ๆ รวมทั้งจะต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติของหน่วยงานอย่างเคร่งครัดด้วย

๗.๕ ความเป็นเจ้าของและความรับผิดชอบ

(๑) หน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์ Server ต้องกำหนดผู้มีหน้าที่รับผิดชอบเพื่อดูแลเครื่องคอมพิวเตอร์ Server โดยทำการ Update service pack หรือ patch ต่าง ๆ ให้ทันสมัยอยู่เสมอ เพื่อปิดรูรั่วของตัวระบบปฏิบัติการ และตัวโปรแกรม และต้องมีเอกสารในการปรับเปลี่ยนค่าปรับแต่งบนเครื่องคอมพิวเตอร์ Server และต้องมีการระบุรายละเอียดของเครื่องคอมพิวเตอร์ Server ในระบบการจัดการเครือข่าย (Enterprise Management System)

(๒) กำหนด ชื่อ/รหัส ระดับสิทธิ์การใช้ ให้ผู้ใช้งานแต่ละคน

๗.๖ การติดตั้ง

(๑) ห้ามเปิด Services และ Application ใด ๆ ที่ไม่เกี่ยวข้องกับของเครื่องคอมพิวเตอร์server นั้น ๆ โดยเด็ดขาด

(๒) เมื่อมีการปรับแต่งหรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์server นั้น ๆ

๗.๗ การเฝ้าดูและตรวจสอบ

(๑) ต้องดำเนินการเก็บ log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัย ดังต่อไปนี้

- Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา ๙๐ วัน
- ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า ๙๐ วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้ เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

(๒) ผู้ดูแลระบบต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

- การโจมตีในรูปแบบ Post-Scan
- การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น
- เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์ Server ที่เกิดขึ้น

(๓) ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

(๔) ต้องมีการประเมินความเสี่ยงทุก ๖ เดือน หรือตามความเหมาะสม พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

๗.๘ กรณีการจัดซื้อ Server และหรือ Application ใหม่ ที่ให้บริการบนเครื่องแม่ข่ ายของหน่วยงานที่มีศูนย์ ต้องมีข้อกำหนด กำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในการจัดซื้อ และต้องมีการกำหนดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นทิศทางเดียวกับสำนักงาน โดยต้องประสานกับศูนย์ก่อน

๘. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Personal computer and Mobile computing)

๘.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่สำนักงานอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของสำนักงาน ดังนั้นผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้อง ศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์หรือผู้ดูแลระบบของหน่วยงานใน สำนักงานที่มีศูนย์สารสนเทศ เท่านั้น

(๕) กรณีส่งเครื่องคอมพิวเตอร์และการสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่ศูนย์หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศเท่านั้น

(๖) ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของ ศูนย์ หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น

(๗) ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของศูนย์ หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์

(๘) ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของ ศูนย์ หรือผู้ดูแลระบบของหน่วยงานในสำนักงานที่มีศูนย์สารสนเทศเท่านั้น และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสสารเคลื่อนที่ให้มีสภาพเดิม

(๙) เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของสำนักงานจากเจ้าหน้าที่ของศูนย์

(๑๐) การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกสำนักงาน เมื่อนำกลับมาที่สำนักงาน ต้ องทำการเชื่อมต่อระบบเครือข่ายภายในสำนักงานเพื่อทำการอัพเดท (Update) ข้อมูลไวรัสล่าสุด

(๑๑) ห้ามเจ้าหน้าที่ผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครองถูกแก้ไขการตั้งเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ศูนย์ทราบทันที

(๑๒) การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

(๑๓) ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้ เครื่อง คอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกครั้ง

๘.๒ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่ เก็บหรือใช้งานเครื่องคอมพิวเตอร์และการสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองและต้องระวังป้องกันการตกกระทบ

(๓) ไม่ใส่เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

(๔) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และสื่อสารที่ใส่กระเป๋าสำหรับเครื่องเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

(๕) หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

(๖) การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และเช็คไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

(๗) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๘) ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

(๙) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

(๑๐) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และ อุปกรณ์สื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

(๑๑) ไม่วางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และในที่มีการสั่นสะเทือน

๘.๓ การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และรหัสผ่าน

(๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดี ตามเกณฑ์การกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของสำนักงาน

(๓) ผู้ใช้งานต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบ ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๘.๔ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทำการสำ รองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD,DVD หรือ ฮาร์ดดิสค์แบบติดตั้งภายนอก

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๘.๕ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ดาวโหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๙. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๙.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๙.๒ ผู้ดูแลระบบทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๙.๓ ผู้ดูแลระบบต้องกำหนดว่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์ กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๙.๔ ผู้ดูแลระบบเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) หรือชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) หรือชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๙.๕ ผู้ดูแลระบบมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๙.๖ ผู้ดูและระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อผู้บังคับบัญชาให้ทราบทันที

๙.๗ ผู้ใช้งานที่มีความประสงค์จะใช้งานระบบเครือข่ายไร้สาย (Wireless) จะต้องกรอกแบบฟอร์มการขอใช้งานระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติใช้งาน เมื่อได้รับการอนุมัติแล้วให้ส่งต่อผู้บังคับบัญชาของผู้ดูแลระบบเพื่อดำเนินการต่อไป

๑๐. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๐.๑ กำหนดให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน หรือระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ เท่านั้น ในการติดต่อราชการ หรือรับส่งข้อมูลของทางราชการผ่านทางจดหมายอิเล็กทรอนิกส์

๑๐.๒ ศูนย์เป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานและระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งานรวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อการลาออก เป็นต้น

๑๐.๓ การรับ- ส่งข้อมูลของทางราชการที่เป็นความลับ ห้ามรับ- ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์

๑๐.๔ ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันที เมื่อได้รับรหัสผ่าน (Default password) ในการผ่านเข้าสูระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก

๑๐.๕ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องแสดงออกมาในรูปของสัญลักษณ์ เท่านั้น ได้แก่ “X” หรือ ● ในการพิมพ์แต่ละครั้ง

๑๐.๖ ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๐.๗ ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๑๐.๘ ผู้ใช้งานต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน หรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสดวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์ของสำนักงาน

๑๐.๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ทำการออกจากระบบ (Log out) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๐.๑๐ ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานมีการตัดการใช้งานของผู้ใช้งาน (Log out) เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นเวลา๓๐ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๑๐.๑๑ ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยโปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็นExecutable File

๑๐.๑๒ ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักในเครื่องที่อยู่ในระบบเครือข่ายของสำนักงาน

๑๐.๑๓ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๐.๑๔ ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๑๐.๑๕ ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

(๑) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ

(๒) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

๑๐.๑๖ ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๐.๑๗ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสำนักงาน ทำให้เกิดความแตกแยกระหว่างสำนักงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๐.๑๘ ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภ ายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๑๑. การควบคุมการใช้งานระบบอินเตอร์เน็ต (Internet)

๑๑.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy, Firewall และ IPS/IDS

๑๑.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

๑๑.๓ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของสำนักงาน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู้เว็บไซต์ที่ไม่เหมาะสม

๑๑ .๔ ผู้ใช้ งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัด

๑๑.๕ ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของสำนักงาน ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเตอร์เน็ตความลับ

๑๑.๖ ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๑๗ การใช้งานเว็บบอร์ด(Web Board) ของสำนักงานผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน

๑๑.๘ หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๑.๙ ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าวด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ.๒๕๕๐ อย่างเคร่งครัด

๑๒. การใช้งานเครือข่ายสังคมออนไลน์ (social network)

๑๒.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๒.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่งคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๒.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจจะมีผลกระทบต่อหน่วยงาน ผู้ใช้งานต้องเป็นผู้รับผิดชอบ และต้องแจ้งศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสมต่อไป

ส่วนที่ ๓
นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในหน่วยงาน และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศของหน่วยงาน ขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับอนุญาต ความเสียหายที่อาจ ะเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยความตั้งใจหรือจากภัยธรรมชาติ เช่นการโจรกรรม อัคคีภัย หรือสนามแม่เหล็กไฟฟ้า เป็นต้น

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบ/ผู้ที่ได้รับมอบหมาย

แนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ประกอบด้วย

๑. ห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room)

๑.๑ ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๑.๒ ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

๑.๓ ให้ศูนย์กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้ระบบสารสนเทศและการสื่อสาร

๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๕ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ เครื่องกระแสไฟฟ้าสำรอง เครื่องดับเพลิงและเครื่องปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทด สอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจว่าได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจาการล้มเหลวในการทำงานของระบบ

๑.๖ ติดตั้งระบบแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๒. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling security)

๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๒.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

๓. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๓.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๓.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๓.๔ จัดเก็บบันทึกปัญหาแ ละข้อบกพร่องของอุ ปกรณ์ที่พบ เพื่อใช้ในการประเมินแ ละปรับปรุงอุปกรณ์ดังกล่าว

๓.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๓.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริกา รจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property)

๔.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๔.๒ กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๔.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๔.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๔.๕ บันทึกข้อมูลการนำอุปกรณ์ ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๕. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of equipment off-premise)

๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ย งจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในสาธารณะ

๕.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๖. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

๖.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๖.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๖.๓ เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

(๑) คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับและไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

(๒) ทำลายเอกสารลับเหล่านั้นโดยใช้วิธีการดังนี้

ประเภทสื่อข้อมูล	วิธีการทำลาย
Flash Drive	วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
เทป	วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสของกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๗. การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๗.๒ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๗.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเตอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

ส่วนที่ ๔
นโยบายการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information Systems Acquisition Development and Maintenance Policy)

วัตถุประสงค์

เพื่อให้ ระบบสารสนเทศของหน่วยงาน มีความมั่นคงปลอดภัย และมีการควบคุมที่เพียงพอ โดยหน่วยงานและผู้พัฒนาระบบ จะต้องคำนึงถึงความมั่นคงปลอดภัยของระบบงาน และการควบคุมภายในระบบงานต่าง ๆ เช่น แนวทางการจัดจ้างพัฒนาระบบ การตรวจสอบความถูกต้องของข้อมูล เป็นต้น

ผู้รับผิดชอบ

๑. หน่วยงานเจ้าของระบบ
๒. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๓. ผู้ดูแลระบบ/ผู้ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย

๑.๑ หน่วยงานเจ้าของระบบสารสนเทศ ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน

๑.๒ หน่วยงานที่เกี่ยวข้องกับการพัฒนาระบบงาน ต้องปฏิบัติตามนโยบายและ แนวปฏิบัติต่างๆ ของหน่วยงานในการพัฒนาระบบงาน และโปรแกรมประยุกต์

๒. ข้อกำหนดด้านการประมวลผลในระบบสารสนเทศ

๒.๑ การตรวจสอบข้อมูลนำเข้า

(๑) โปรแกรมประยุกต์ของหน่วยงานที่มีการป้อนข้อมูลเข้าสู่ระบบ จะต้องมีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากการป้อนข้อมูล ก่อนที่จะนำข้อมูลนั้นไปประมวลผลต่อ

(๒) ในระบบประมวลผลที่สำคัญของหน่วยงาน ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลที่ป้อนเข้า รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการป้อนข้อมูล

๒.๒ การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

(๑) ระบบประมวลผล ต้องออกแบบให้มีความสามารถ แจ้งถึงความผิดพลาดต่าง ๆ จากการประมวลผล การสอบทานเพื่อตรวจจับกรณีการประมวลผลข้อมูลมีความผิดพลาดหรือเสียหาย

(๒) ระบบประมวลผลที่สำคัญ ต้องมีการตรวจสอบความถูกต้องของการประมวลผลอย่างสม่ำเสมอ

๒.๓ การตรวจสอบความถูกต้องของข้อมูล

สำหรับระบบที่มีความสำคัญและต้องการความครบถ้วนถูกต้องของข้อมูล ต้องมีการพิจารณาใช้เทคนิคที่เหมาะสมมาใช้กับระบบงาน โดยประโยชน์ของการใช้การรับรองข้อมูล ได้แก่

(๑) รักษาความถูกต้องของข้อมูล

(๒) ตรวจสอบการลักลอบแก้ไขข้อมูล

๒.๔ การตรวจสอบข้อมูลผลลัพธ์

(๑) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อมั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบครอบคลุมถึง

- การสอบเทียบความครบถ้วนของข้อมูลผลลัพธ์ที่ได้จากการประมวลผล
- การตรวจสอบถึงความผิดพลาดต่าง ๆ ของรายงาน
- กำหนดให้มีระเบียบปฏิบัติในการทดสอบข้อมูลผลลัพธ์

(๒) ในระบบประมวลที่สำคัญของหน่วยงาน ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลผลลัพธ์ รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการนำข้อ มูลผลลัพธ์ไปใช้

๓. มาตรการในการเข้ารหัสข้อมูล

๓.๑ นโยบายการใช้งานการเข้ารหัสข้อมูล

(๑) กำหนดให้มีระเบียบปฏิบัติในเรื่องการใช้การเข้ารหัส รวมถึงซอฟต์แวร์และมาตรฐานวิธีการเข้ารหัสที่หน่วยงานอนุญาตให้ใช้งานสำหรับข้อมูลในลำดับชั้นต่าง ๆ

(๒) ต้องมีการปรับปรุงรายชื่อซอฟต์แวร์และมาตรฐานในด้านการเข้ารหัสให้ทันสมัยอยู่เสมอ

(๓) ต้องมีการพิจารณาถึงลำดับชั้นของข้อมูลและแนวทางในการจัดการข้อมูลในลำดับชั้นดังกล่าวประกอบการพิจารณาในการใช้งานการเข้ารหัส

(๔) ต้องมีการประเมินความเสี่ยง และพิจารณาผลการประเมินความเสี่ยงก่อน ในการเลือกวิธีในการเข้ารหัสมาใช้งานในระบบงาน

๓.๒ การบริหารจัดการกุญแจเข้ารหัสข้อมูล

ผู้ดูแลระบบแต่ละระบบเป็นผู้จัดการกุญแจรหัสในระบบของตน และต้องกำหนดการป้องกันด้วยวิธีการที่เหมาะสม การจัดการดังกล่าวรวมถึงขั้นตอนการปฏิบัติงานต่าง ๆ มีดังนี้

(๑) การสร้างและการแจกจ่ายกุญแจรหัส

(๒) ความลับของกุญแจส่วนบุคคล

(๓) ความถูกต้องของกุญแจสาธารณะ

(๔) การยกเลิกการใช้กุญแจรหัส

(๕) การกู้คืนกุญแจรหัส

(๖) การสำรองข้อมูลกุญแจรหัส

(๗) การยกเลิกและทำลายกุญแจรหัสที่ไม่ใช้งานแล้ว

(๘) การจัดการที่ไม่ขัดแย้งต่อกฎหมายใด ๆ

(๙) การจำกัดให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในการเข้าใช้อุปกรณ์ที่ใช้ในการสร้าง เก็บหรือสำรองกุญแจรหัส

๔. การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

๔.๑ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการหรือระบบที่ใช้งานจริง

(๑) ก่อนมีการปรับปรุงโปรแกรมเวอร์ชั่นใหม่ในระบบใช้งานจริงจะต้องได้รับเอกสารการอนุมัติการใช้โปรแกรมเวอร์ชั่นใหม่และหลักฐานประกอบอื่น ๆ เช่น รายการผลการทดสอบเพื่อการรับรองความถูกต้องจากผู้ใช้เป็นต้น และต้องปรับเปลี่ยน Source Code ในสมุดทะเบียน (Library) ให้สอดคล้องกัน

(๒) เจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่ได้รับการอนุญาตจากผู้บริหารแล้วเท่านั้น จะเป็นผู้ดำเนินการปรับปรุงซอฟต์แวร์ที่อยู่ในระบบใช้งานจริงเฉพาะส่วนที่ตนเองรับผิดชอบ

(๓) ไม่จัดเก็บ Source Code ของโปรแกรมไว้ในระบบใช้งานจริง

(๔) ต้องจัดเก็บรายการบันทึกเพื่อการตรวจสอบต่าง ๆ ของการแก้ไข Source Code และโปรแกรม

(๕) ต้องมีการสำรองและจัดเก็บโปรแกรมเวอร์ชั่นก่อนการแก้ไขเพื่อนำกลับมาใช้เมื่อมีความจำเป็น

(๖) ก่อนที่จะอนุญาตให้ผู้ให้บริการ /จำหน่วยระบบเข้าถึงระบบที่ใช้งานจริง เพื่อติดตั้ง แก้ปัญหาและ/หรือดูแลรักษาระบบ จะต้องได้รับการอนุมัติจากผู้บริหาร โดยมีพนักงานหรือลูกจ้างของหน่วยงานในการเฝ้าติดตามกิจกรรมต่าง ๆ ของผู้ให้บริการ/จำหน่วย

(๗) มีการลงโปรแกรมแก้ไข (Software Patches) เมื่อผู้ผลิตได้ออกโปรแกรมดังกล่าว เพื่อใช้ในการลดหรือกำจัดข้อบกพร่องด้านความมั่นคงปลอดภัย ที่เกี่ยวข้องกับลักษณะการใช้งานซอฟต์แวร์ในปัจจุบัน

๔.๒ การป้องกันข้อมูลที่ใช้สำหรับการทดสอบระบบ

ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงไปใช้เพื่อการทดสอบระบบงานที่พัฒนาใหม่ ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่าง ๆ ต้องประกอบด้วย

(๑) ได้รับอนุญาตก่อนการนำสำเนาข้อมูลจริงไปใช้ในระบบงานทดสอบในแต่ละครั้ง

(๒) มีการควบคุมในการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ

(๓) มีการดัดแปลงข้อมูลจริงบางส่วนก่อนนำมาใช้ในการทดสอบ

(๔) ทำการลบข้อมูลทดสอบออกจากระบบทันทีที่เมื่อเสร็จสิ้นการทดสอบ

(๕) มีการจัดเก็บบันทึกการทำรายงานในระบบ(Audit Log) เพื่อตรวจสอบกิจกรรมการทดสอบ

๔.๓ การควบคุมการเข้าถึง Source Code ของโปรแกรม

(๑) แต่งตั้งเจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่เก็บ Source Code ของแต่ละระบบในความรับผิดชอบ และต้องมีการจำกัดสิทธิในการเข้าถึง Library ที่เก็บ Source Code ของโปรแกรม

(๒) การอัพเดท Source Code ของโปรแกรมใน Library และการนำ Source Code ของโปรแกรมให้กับผู้พัฒนาระบบ จะต้องดำเนินการโดยเจ้าหน้าที่ผู้ดูแล Library ที่ได้รับมอบหมายในแต่ละระบบ

(๓) ต้องมีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบการเข้าถึง Library ต่าง ๆ

(๔) บันทึกรายละเอียดโปรแกรมเวอร์ชั่นเก่าที่จะทำการจัดเก็บอย่างชัดเจน โดยมีรายละเอียดต่าง ๆ เช่น วัน-เดือน-ปี ที่โปรแกรมเวอร์ชั่นนี้ได้ใช้งานอยู่ในระบบใช้งานจริง ซอฟต์แวร์ต่าง ๆ ที่ทำงานร่วมกันกับโปรแกรมนี้ เป็นต้น

(๕) การปรับปรุงเปลี่ยนแปลงและการทำสำเนา Library จะต้องปฏิบัติตามข้อที่ควรพิจารณาในการควบคุมการเปลี่ยนแปลงของระบบ

๕. การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและการสนับสนุน

๕.๑ ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

(๑) การปรับปรุงแก้ไขระบบงานหรือโปรแกรมต่าง ๆ ต้องปฏิบัติตามระเบียบปฏิบัติของหน่วยงานว่าด้วยเรื่องการปรับปรุงแก้ไขระบบงานหรือโปรแกรม

(๒) การปรับปรุงแก้ไขระบบงานต่าง ๆ ต้องจัดทำเป็นเอกสารและสามารถติดตามสถานะได้ รวมถึงต้องมีเอกสารสนับสนุน เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรม และผลการทดสอบ เป็นต้น

(๓) การปรับปรุงแก้ไขระบบงานควรพิจารณาถึง

- การอนุมัติโดยหน่วยงานเจ้าของระบบงาน
- การระบุถึงเครื่องคอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล ที่จะต้องเปลี่ยนแปลง
- การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน
- การสำรองข้อมูลก่อนการปรับปรุงแก้ไขหรือบำรุงรักษาระบบ
- การจัดทำเอกสารประกอบการเปลี่ยนแปลงให้ทันสมัย
- การควบคุมเวอร์ชั่นของซอฟต์แวร์ที่เปลี่ยนแปลง
- การจัดเก็บบันทึกเพื่อการตรวจสอบการแก้ไข

(๔) การปรับปรุงแก้ไขระบบต้องจัดทำเป็นหนังสือขออนุมัติแก้ไขระบบงานหรือโปรแกรม ซึ่งประกอบด้วยรายละเอียดตามมาตรฐานที่หน่วยงานกำหนด

๕.๒ การตรวจสอบการทำงานของโปรแกรมประยุกต์ภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) ทบทวนมาตรการควบคุม และขั้นตอนปฏิบัติของโปรแกรมประยุกต์ ในด้านความถูกต้องสมบูรณ์ภายหลังการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) ดำเนินการแจ้งการเปลี่ยนแปลงระบบปฏิบัติการให้กับผู้ที่เกี่ยวข้องทราบ ในเวลาที่เหมาะสมเพียงพอสำหรับการเตรียมการทดสอบและการทบทวนก่อนที่จะติดตั้งใช้งานจริง

ทั้งนี้ ให้มีการพิจารณาแต่งตั้งกลุ่มบุคคลเฉพาะเพื่อรับผิดชอบในการตรวจเฝ้าระวังช่องโหว่ และการแก้ไขอุดช่องโหว่ของผู้ให้บริการ/จำหน่ายระบบ

๕.๓ การจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต

ซอฟต์แวร์สำเร็จรูปควรใช้งานโดยปราศจากการแก้ไข ถ้ามีความจำเป็นในการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูปต้องมีการพิจารณาการควบคุมต่าง ๆ ดังนี้

(๑) ความเสี่ยงที่อาจเ กิดขึ้นจากการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ซึ่งอาจมีการละเลยการควบคุมด้านความมั่นคงปลอดภัย

(๒) การได้รับความยินยอมในการแก้ไขจากผู้จำหน่ายซอฟต์แวร์

(๓) ข้อกำหนดความต้องการต่าง ๆ ด้านเทคนิคจากผู้จำหน่ายซอฟต์แวร์

(๔) ผลกระทบและการดูแลรักษาระบบภายหลังการเปลี่ยนแปลง

(๕) การจัดทำสำเนาของซอฟต์แวร์ก่อนการเปลี่ยนแปลง

(๖) การทดสอบการเปลี่ยนแปลง

(๗) การจัดทำเอกสารประกอบการเปลี่ยนแปลง

๕.๔ การป้องกันการรั่วไหลของสารสนเทศ

หน่วยงานต้องมีการควบคุมเพื่อป้องกันการรั่วไหลของสารสนเทศ ซึ่งมีโอกาสที่จะเกิดขึ้นได้จากผลของชุดคำสั่งที่แอบแฝงมากับซอฟต์แวร์สำเร็จรูป ส่งผลกระทบให้ระบบทำงานผิดพลาด หรือแอบเปิดเผยข้อมูลของหน่วยงาน ดังนั้น จึงต้องมีการควบคุมเพื่อป้องกันโปรแกรมหรือชุดคำสั่งที่อาจแอบแฝงมากับซอฟต์แวร์สำเร็จรูปก่อนการจัดซื้อซอฟต์แวร์สำเร็จรูปต้องพิจารณาการควบคุม ดังต่อไปนี้

(๑) จัดซื้อซอฟต์แวร์ที่เป็นเวอร์ชั่นซึ่งจัดจำหน่ายในเชิงพาณิชย์แล้ว (ไม่ใช่เวอร์ชั่นทดลอง) โดยจัดซื้อซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น

(๒) ถ้าเป็นไปได้ให้นำ Source Code มาตรวจสอบก่อนนำมาใช้งานจริง โดยทำการส แกนหาข้อมูลหรือชุดคำสั่งแอบแฝง ตลอดจนการทดสอบก่อนที่จะนำไปติดตั้งในระบบใช้งานจริง

(๓) มีการควบคุมการเข้าถึง Source Code เพื่อป้องกันการแก้ไขโดยไม่ได้รับอนุญาต

(๔) ตรวจและเฝ้าระวังการใช้ทรัพยากรในระบบคอมพิวเตอร์หลังจากที่นำซอฟต์แวร์มาใช้งาน

๕.๕ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

การให้หน่วยงานภายนอกพัฒนาซอฟต์แวร์เพื่อใช้งานภายในหน่วยงานต้องพิจารณาหัวข้อดังต่อไปนี้

(๑) สิทธิบัตรหรือลิขสิทธิ์ความเป็นเจ้าของซอฟต์แวร์

(๒) สิทธิความเป็นเจ้าของใน Source Code ของโปรแกรม

(๓) สัญญาหรือข้อตกลงด้านความมั่นคงปลอดภัยในการพัฒนาโปรแกรม เช่น การไม่เขียนโปรแกรม แอบแฝง เป็นต้น

(๔) ความรับผิดชอบหากเกิดปัญหาในซอฟต์แวร์

(๕) ความน่าเชื่อถือของหน่วยงานภายนอก

(๖) การทดสอบการติดตั้งเพื่อป้องกันชุดคำสั่งหรือโปรแกรมแอบแฝง

(๗) ข้อตกลงการเข้าใช้Source Code ในกรณีบริษัทผู้ผลิตไม่สามารถให้บริการได้(Escrow Arrangement)

(๘) การอบรมให้ความรู้แพนักงานและลูกจ้างของหน่วยงาน

(๙) เอกสารประกอบระบบงาน

๖. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

๖.๑ มาตรการทางเทคนิคในการควบคุมช่องโหว่

หน่วยงานต้องทำการตรวจสอบความเสี่ยงของช่องโหว่ ปรับปรุงโปรแกรมตลอดจนติดตามข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่าง ๆ อย่างสม่ำเสมอเป็นระยะ ๆ โดยมีแนวทางปฏิบัติดังนี้

(๑) กำหนดบทบาทและหน้าที่ความรับผิดชอบ เพื่อมอบหมายให้มีผู้รับผิดชอบในการบริหารจัดการช่องโหว่ ซึ่งรวมถึงการเฝ้าระวังภัยจากช่องโหว่ การประเมินความเสี่ยงที่มีจากช่องโหว่ การอุดช่องโหว่ การติดตามทรัพย์สินสารสนเทศ และการประสานงานตามที่จำเป็นในการบริหารจัดการควบคุมช่องโหว่

(๒) มีแหล่งข้อมูลที่เชื่อถือได้ในการติดตามข่าวสารภัยจากช่องโหว่ และการจัดการด้านเทคนิค เพื่อให้ตระหนักถึงช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์และเทคโนโลยีอื่น ๆ

(๓) จัดการแก้ไขช่องโหว่ตามความรุนแรงของเหตุการณ์

(๔) หากไม่มีชุดคำสั่งอุดช่องโหว่ (Patch) ให้ดำเนินการประเมินความเสี่ยงในการติดตั้งชุดคำสั่งดังกล่าวโดยเปรียบเทียบกับความเสี่ยงจากภัยที่มีจากช่องโหว่

(๕) ทำการทดสอบชุดคำสั่งอุดช่องโหว่ (Patch) และทำการประเมินก่อนที่จะติดตั้งแก้ไขระบบ

(๖) หากไม่มีคำสั่งอุดช่องโหว่ (Patch) ให้พิจารณามาตรการควบคุมอื่น ๆ อย่างเช่น

(๗.๑) ปิดการให้บริการหรือการใช้ระบบในส่วนที่เกี่ยวข้องกับช่องโหว่

(๗.๒) ดัดแปลงหรือเพิ่มมาตรการควบคุม เช่น การกำหนดไฟร์วอลล์ เป็นต้น

(๗.๓) เฝ้าระวังมากขึ้นเพื่อตรวจจับหรือป้องกันการบุกรุกจริง

(๗.๔) แจ้งข่าวสารหรือเพิ่มความตระหนักถึงภัยช่องโหว่

(๘) จัดเก็บ Audit Log ตามระเบียบปฏิบัติ

(๙) ทำการติดตามและประเมินกระบวนการในการบริหารจัดการช่องโหว่อย่างสม่ำเสมอ

(๑๐) ในกรณีระบบที่มีความเสี่ยงสูง ต้องมีการจัดการอย่างเข้มงวด

ส่วนที่ ๕

นโยบายระบบสารสนเทศและระบบสำรองข้อมูลสารสนเทศ (Backup and Recovery)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบ

แนวทางปฏิบัติ

๑. การสำรองข้อมูลและกู้คื นข้อมูลในสถานการณ์ปกติ เมื่อมีระบบงานใหม่หรือข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้

๑.๑ กำหนดให้จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ขนาดข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ระบบปฏิบัติการ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๖) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๗) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๘) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๓ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๑.๔ กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อย ต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

๑.๕ กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหยดโดยเจ้าของข้อมูล หรือระบบ

๑.๖ กำหนดขั้นตอนการจัดทำสองรองข้อมูล และกา รกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

๑.๗ การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของสำนักงานเดือนละ ๒ ครั้ง

๑.๘ ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรองข้อมูลทุกครั้ง

๑.๙ ต้องทำการ ทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๑.๑๐ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

๑.๑๑ การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะ ๆ

๑.๑๒ ต้องตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปีหรือตามความเหมาะสม

๑.๑๓ สื่อบันทึกข้อมูลสำรองต้องมี การเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

๒. ต้องจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไป

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวีการทางอิเล็กทรอนิกส์

๔. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๖
นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

๑. เพื่อป้องกันและรับมือกับเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ

๒. เพื่อให้มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อนำผลที่ได้ไปสู่การบริหารจัดการรวมทั้งดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผล และทันกาล

ผู้รับผิดชอบ

๑. ผู้ดูแลระบบ

๒. ผู้ใช้งาน

แนวปฏิบัติ

การรายงานเหตุการณ์และการจัดการที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๑. ผู้ใช้งานแจ้งไปยังผู้ดูแลระบบ/ผู้เกี่ยวข้อง โดยทันที เมื่อพบเห็นเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศทราบทันที

๒. ผู้ใช้งาน และผู้เกี่ยวข้องจากภายนอกทั้งหมด หากซึ่งพบจุดอ่อนช่องโหว่ในระบบสารสนเทศจะต้องไม่เปิดเผย เผยแพร่ สนทนาหรือกระทำการใดๆ อันเป็นการเผยแพร่ต่อผู้อื่น โดยให้ทำการแจ้งกับผู้ดูแลระบบโดยด่วนที่สุด

๓. ต้องกำหนดคณะทำงานเพื่อหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศ ในการแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย โดยจะต้องได้รับการกำหนดและมอบหมายสิทธิอย่างชัดเจนในการดำเนินการแก้ไขปัญหา

๔. เมื่อผู้ดูแลระบบ/ผู้ที่เกี่ยวข้องได้รับแจ้งเหตุการณ์ คณะทำงานจะต้องดำเนินการวิเคราะห์ความรุนแรงและผลกระทบของเหตุการณ์นั้นๆ และร่วมกันหาวิธีการแก้ไข โดยมีขั้นตอนประกอบด้วย

๔.๑ การตรวจสอบหาสาเหตุของปัญหา

๔.๒ แผนงานในการลดผลกระทบ

๔.๓ ขั้นตอนในการแก้ไข

๔.๔ สื่อสารกับผู้ใช้งานที่เกี่ยวข้อง

๔.๕ ทำเอกสารบันทึกการดำเนินการดังกล่าว

๕. ในกรณีที่มีเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อการรักษาความถูกต้องทางด้านหลักฐาน และดำเนินการทางกฎหมายในกรณีที่จำเป็น ผู้บริหารที่ได้รับมอบหมายเท่านั้นที่จะเป็นตัวแทนของหน่วยงานโดยความร่วมมือกับหน่วยงานด้านกฎหมาย ในการใช้ ระเบียบปฏิบัติที่เกี่ยวกับการก่ออาชญากรรมในการดำเนินคดีต่อผู้ประสงค์ร้า ยต่อหน่วยงาน

ส่วนที่ ๗
นโยบายการปฏิบัติตามข้อกำหนด

วัตถุประสงค์

๑. เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ที่เกี่ยวข้องกับการดำเนินการของหน่วยงาน และเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๒. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ผู้ตรวจสอบภายใน (Internal auditor)

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)

๑.๑ หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อยดังนี้

(๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๑.๒ มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อย ดังนี้

(๑) การทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

(๒) การทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม

(๓) การตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

(๔) มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

- กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- ในกรณีที่จำเป็นเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บ

๒. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐

เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พ.ร.บ. หรือข้อบังคับภายนอกอื่นๆ ที่ได้กำหนดไว้ และจำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยผู้ที่รับผิดชอบเท่านั้น มีข้อแนวปฏิบัติอย่างน้อย ดังนี้

๑. จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง อย่างน้อยเป็นระยะเวลา ๙๐ วัน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๒. จำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log) ดังกล่าวโดยกำหนดสิทธิให้เฉพาะผู้ดูแลระบบที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

๓. มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงข้อมูลเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น