ประกาศสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

อาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การ ดำเนินการใดๆ ด้วยวิธีทางการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ

สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) (สบร.) จึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามมาตรการความปลอดภัยที่กำหนด และมีการทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้ โดยมีผู้บริหารเทคโนโลยีสารสนเทศ (CIO) เป็นผู้รับผิดชอบต่อนโยบายในฐานะเป็นผู้กำกับ ติดตามและทบทวนนโยบาย

ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศ ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า ประกาศสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ปี พ.ศ. 2566 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ 2 นิยาม

2.1 "สำนักงาน" หมายถึง สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

2.2 "ผู้บริหารสูงสุด (CEO)" หมายถึง ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้

2.3 "ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)" หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงาน

2.4 "การเข้าถึงการควบคุมการใช้งานสารสนเทศ" หมายถึง การควบคุมการเข้าถึง หรือจำกัดการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่ายระบบปฏิบัติการ โปรแกรมสำเร็จรูปโปรแกรมประยุกต์ โปรแกรมอรรถประโยชน์ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ

2.6 "ข้อมูลสารสนเทศ" หมายถึง ข้อมูลที่ถูกประมวลผลโดยระบบสารสนเทศ และสามารถนำไปใช้งานหรือประมวลผลต่อไปได้

2.7 "ระบบเครือข่าย" หมายถึง ระบบเครือข่ายคอมพิวเตอร์ภายใต้การกำกับดูแลของศูนย์เพื่อใช้ในการติดต่อสื่อสาร หรือ รับ-ส่ง ข้อมูลสารสนเทศระหว่างระบบสารสนเทศต่างๆ ของ สบร.

2.8 "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด (Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ความมั่นคงของระบบสารสนเทศ ถูกบุกรุก คุกคาม และโจมตี

ข้อ 3 วัตถุประสงค์

3.1 เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายของ สบร. มีความมั่นคงปลอดภัยจากสถานการณ์ไม่พึงประสงค์หรือไม่คาดคิดในระบบสารสนเทศ

3.2 เพื่อให้มั่นใจได้ว่าการปฏิบัติงานของ สบร. สามารถดำเนินได้อย่างต่อเนื่อง และเมื่อเกิดผลกระทบจากเหตุการณ์ไม่พึงประสงค์สามารถกู้คืนระบบสารสนเทศได้อย่างรวดเร็วและลดความเสียหายที่อาจจะเกิดขึ้น

3.3 เพื่อเป็นแนวทางปฏิบัติในการใช้งานระบบสารสนเทศอย่างปลอดภัย สำหรับ ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอก

ข้อ 4 ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ กำหนดขึ้นเพื่อสร้างมาตรฐานและแนวทางในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของ สบร. ให้ปลอดภัยจากความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย ของ สบร. โดยเจ้าหน้าที่ ลูกจ้าง และผู้เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานทั้งหมดต้องถือปฏิบัติอย่างเคร่งครัด

ข้อ 5 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีสาระสำคัญประกอบด้วย

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) การมีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

สำนักงานได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัย โดยมีเนื้อหาสาระสำคัญประกอบด้วย

หมวดที่ 1 นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ ประกอบด้วยแนวปฏิบัติดังนี้

1) การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

1.1 มีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงการใช้งานและความมั่นคงปลอดภัย โดยกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตการเข้าถึงระบบสารสนเทศ ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

1.2 กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงไว้อย่างชัดเจน

1.3 ต้องจัดทำข้อปฏิบัติการควบคุมการเข้าถึงสารสนเทศและปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความปลอดภัย

2) การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control)

3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ได้รับอนุญาตแล้ว หรือผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ได้กำหนดแนวทาง ดังนี้

3.1 สร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงข้อกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

3.2 การลงทะเบียนผู้ใช้งาน (User registration) กำหนดไว้เป็นขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

3.3 การบริหารจัดการสิทธิของผู้ใช้งาน (User management) มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

3.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม และใช้งานอย่างปลอดภัย

3.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) สม่ำเสมอ มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

4.1 การใช้งานรหัสผ่าน (Password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

4.2 มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

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

4.4 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.2544

5) การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

5.1 การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

5.2 การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

5.3 การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

5.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and Configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

5.5 การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

5.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

5.7 การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

6) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ได้กำหนดหนดแนวทางปฏิบัติดังนี้

6.1 กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

6.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และกำหนดขั้นตอนทางเทคนิคการยืนยันตัวตนอย่างเหมาะสมเพื่อรองรับการกล่าวอ้างว่าผู้ใช้งานที่ระบุถึง

6.3 การบริหารจัดการรหัสผ่าน (Password management system) จัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

6.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ได้จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

6.5 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

6.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

7) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

7.1 การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

7.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and Teleworking)

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

7.4 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) โดยกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

8) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยผู้ใช้งานจะต้องลงทะเบียนใช้งานกับผู้ดูแลระบบ และนำอุปกรณ์มาขึ้นทะเบียนเพื่อให้สามารถเข้าใช้งานกับเครือข่ายที่ลงทะเบียนได้

9) การควบคุมการใช้อินเทอร์เน็ต (Internet) กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเตอร์เน็ตอย่างปลอดภัย

9.1 กำหนดการใช้เส้นทางเชื่อมต่อระบบอินเทอร์เน็ตที่ปลอดภัย ที่องค์กรจัดไว้ให้เท่านั้น อาทิ Proxy , Firewall, IPS-IDS ห้ามมิให้ผู้ใช้งานเชื่อต่อผ่าน Dial-up Modem

9.2 การรับส่งข้อมูลผ่านอินเทอร์เน็ต ต้องมีการทดสอบไวรัส (Virus Scanning) ก่อนรับส่งข้อมูล

9.3 การดาวน์โหลดข้อมูล หรือโปรแกรมใด ๆ จากอินเทอร์เน็ต ต้องไม่เป็นการละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

9.4 ต้องใช้งานอินเทอร์เน็ทอย่างปลอดภัย และเป็นไปตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

10) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

11) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) โดยเครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานของหน่วยงานควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน และใช้งานอย่างปลอดภัย

12) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผู้ดูแลระบบ จะต้องควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Sever) และควบคุมการเปลี่ยนแปลงต่าง ๆ ที่อาจส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน รวมถึงความมั่นคงปลอดภัยของข้อมูล

13) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดย จัดแบ่งพื้นที่ในการควบคุมตามระดับความสำคัญทางสารสนเทศ ควบคุมการเข้าถึงพื้นที่อย่างปลอดภัย รวมถึงการจัดให้มีการบำรุงรักษาอุปกรณ์สารสนเทศ ให้พร้อมใช้เสมอ

14) การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail) การลงทะเบียนผู้ใช้งาน และการใช้งานจดหมายอิเล็กทรอนิกส์อย่างปลอดภัย

15) การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) อย่างปลอดภัยไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

หมวดที่ 2 นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วยแนวปฏิบัติที่สำคัญดังนี้

1) การสำรองระบบและสำรองข้อมูล

1.1 การจัดลำดับความสำคัญของระบบ เพื่อวางแผนในการจัดทำระบบสำรอง

1.2 กำหนดประเภทของข้อมูลที่ต้องการสำรอง

1.3 การจัดเก็บระบบ และข้อมูลสำรองไว้อย่างปลอดภัย และทดสอบ (Restore) สม่ำเสมอ

2) การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และเตรียมความพร้อมโดยการทดสอบแผนสม่ำเสมอ เพื่อให้มั่นใจได้ว่าเมื่อเกิดเหตุฉุกเฉินสามารถกู้คืน (Recover) กลับมาได้ตามเป้าหมาย

หมวด 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1) จัดให้มีการประเมินความเสี่ยงสม่ำเสมออย่างน้อยปีละ 1 ครั้ง โดยประเมินจัดระดับความสำคัญของความเสี่ยงแต่ละรายการ และวางแผนการจัดการความเสี่ยงอย่างเหมาะสม

2) การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน (Internal auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

หมวด 4 หน้าที่รับผิดชอบด้านสารสนเทศ

ข้อ 6 กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ 9 กุมภาพันธ์ 2566

(นายทวารัฐ สูตะบุตร)

ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้

09ก.พ.66 เวลา 16:13:27 Non-PKI Server Sign

Signature Code : NwAzA-DlAMA-AwAEM-AMQA5

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานบริหารและพัฒนาองค์ความรู้

(องค์การมหาชน)

ประจำปี 2566

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นใน การให้ได้มาซึ่งข้อมูล สารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจใน การดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอ ในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้องความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมมั่นคงปลอดภัยในระบบสารสนนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบาย และแนวปฏิบัติ ด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความ มั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) จึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2566 ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เพื่อให้บุคลากรทุกคนในสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

สารบัญ

1. บทนำ

1.1. หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ในมาตรา 5 *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้อนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

1.2. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ฉบับนี้มีวัตถุประสงค์เพื่อ

1) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

2) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

3) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบเทคโนโลยีสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1.3 องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ สอดคล้องกับมาตรฐานสากล ISO/IEC 27001:2013 โดยแนวทางปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

1.4 บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยผู้บริหารระดับสูง ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

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

1.5. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน(Intranet) และเว็บไซต์ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เพื่อให้บุคลากรของสำนักงาน และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. **สำนักงาน** หมายถึง สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

2. **ส่วนงานกลาง** หมายถึง ส่วนงานภายในของสำนักงานที่คณะกรรมการมีมติให้จัดตั้งขึ้นเพื่อดำเนินภารกิจสนับสนุนและส่งเสริมการดำเนินงานของสำนักงานและหน่วยงานภายใน รวมถึงภารกิจส่งเสริมการเรียนรู้และนวัตกรรมการเรียนรู้ตามพระราชกฤษฎีกาจัดตั้ง สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) (ฉบับที่ 3) ปี พ.ศ. 2561

3. หน่วยงานภายใน หมายถึง หน่วยงานของสำนักงานที่คณะกรรมการบริหารมีมติให้จัดตั้งขึ้นเพื่อดำเนินภารกิจอย่างใดอย่างหนึ่ง ที่อยู่ในวัตถุประสงค์และอำนาจหน้าที่ของสำนักงาน ไม่ว่าจะเรียกชื่อว่า สถาบัน หรือชื่ออื่นใด

4. **ผู้บริหารระดับสูง** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

5. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

6. **ผู้ใช้งาน** หมายความว่า เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้ใช้งานทั่วไป ที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งสำนักงานกำหนดไว้ ดังนี้

6.1. ผู้บริหารสูงสุด หมายความว่า ผู้อำนวยการสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

6.2. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office : CIO) หมายความว่า ผู้บริหารที่ได้รับการแต่งตั้งให้มีหน้าที่ ดำเนินงานการบริหารจัดการและการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

6.3. ผู้ดูแลระบบ/ผู้ดูแลห้องเครื่อง หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

6.4. ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอพพลิเคชั่น

6.5. เจ้าหน้าที่ หมายความว่า เจ้าหน้าที่ของสำนักงาน

6.6. ลูกจ้าง หมายความว่า ลูกจ้างของสำนักงาน

6.7. บุคคลภายนอก หมายความว่า บุคคลที่สำนักงานอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของสำนักงานได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของสำนักงาน เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่

เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับสำนักงาน หรือ ที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิต นักศึกษาฝึกงาน ผู้เข้ามาใช้บริการห้องสมุดหรือพิพิธภัณฑ์

7. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

8. สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

8.1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

8.2. เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

8.3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

9. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

11. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

12. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

13. ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

3. นโยบายการรักษาความมั่นคงปลอดภัย

หมวดที่ 1 นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

1) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของสำนักงาน

2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับสำนักงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1) ฝ่ายสื่อสารองค์กร ฝ่ายดิจิทัลทีเค ฝ่ายดิจิทัลมิวเซียม

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) ผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ 1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติดังนี้

1. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

1.1 ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

1.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

1.2.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

1.2.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล

- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

1.2.1.2 กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

1.2.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

1.2.1.4 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อ ผู้ดูแลระบบ

2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

สำนักงานใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

2.1 จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชีข้อมูลเพื่อการวิเคราะห์ประกอบการตัดสินใจสำหรับผู้บริการ เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลที่เผยแพร่ผ่านทางเว็บไซต์ของสำนักงาน ข้อมูลเพื่อการวิเคราะห์ประกอบการตัดสินใจสำหรับผู้บริการ

2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ ดังนี้

ระดับที่ 1 ข้อมูลที่มีระดับความสำคัญมากที่สุด

ระดับที่ 2 ข้อมูลที่มีระดับความสำคัญปานกลาง

ระดับที่ 3 ข้อมูลที่มีระดับความสำคัญน้อย

2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

“ข้อมูลลับที่สุด” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

“ข้อมูลลับมาก” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

“ข้อมูลลับ” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

“ข้อมูลทั่วไป” หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

2.4 การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร

ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

2.5 การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของสำนักงาน กำหนดไว้เป็นช่วงเวลาเข้าถึงได้ดังนี้

ลำดับ	เวลาที่เข้าถึงได้	ข้อมูล / ช่องทางการเข้าถึงข้อมูล
1	ในวันและเวลาทำการ วันจันทร์ ถึง วันศุกร์ เวลา 09.00 – 17.00 น.	● แชร์ข้อมูลภายในสำนักงาน ● สำนักงานอิเล็กทรอนิกส์ ● ระบบบันทึกเวลาทำงาน
2	นอกวันและเวลาทำการ/วันหยุด/วันหยุดนักขัตฤกษ์	● สำนักงานอิเล็กทรอนิกส์ ● ระบบบันทึกเวลาทำงาน
3	ทุกวัน 24 ชั่วโมง	● สำนักงานอิเล็กทรอนิกส์ ● เว็บไซต์

ส่วนที่ 2 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ

(Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย การใช้งานตามภารกิจและควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติดังนี้

2.1 การควบคุมการเข้าถึงสารสนเทศ

2.1.1 ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2.1.2 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

2.2 จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจดังนี้

2.2.1 Executive คือ กลุ่มผู้บริหาร

2.2.2 Administrator คือ กลุ่มของผู้ดูแลระบบสารสนเทศของสำนักงาน

2.2.3 Officer คือ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

2.2.4 Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

2.2.5 Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศขององค์กร และมั่นใจได้ว่าเฉพาะผู้ที่ได้รับสิทธิการเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้นสามารถเข้าใช้งานระบบสารสนเทศได้ โดยมีแนวปฏิบัติในการบริหารการเข้าถึงระบบสารสนเทศของผู้ใช้งานดังนี้

3.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

3.1.1 สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

3.1.2 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

3.2 การลงทะเบียนผู้ใช้งาน (User Registration)

3.2.1 ผู้ดูแลระบบ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

3.2.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

3.2.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจในส่วนที่ 2

3.2.4 ผู้ดูแลระบบต้องชี้แจง และแจ้งผู้ใช้งาน เป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบ และมาตรการรด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ

3.2.4 ผู้ดูและระบบต้องยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากผู้บังคับบัญชา หรือเมื่อมีการลาออก หรือสิ้นสุดการจ้างเป็นต้น

3.3 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

3.3.1 กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ ความจำเป็นในการใช้งาน และทบทวนสิทธิสม่ำเสมอ

3.3.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

3.3.3 ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากผู้บังคับบัญชา และจัดทำคำร้องเป็นลายลักษณ์อักษรแจ้งต่อผู้ดูแลระบบ โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษ จะต้องระงับการใช้งานทันที

3.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

3.4.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับ เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที ภายใน 3 วัน

3.4.2 การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ 8 หลัก (digits)

3.4.3 กำหนดให้การเข้ารหัสผิดได้ ไม่เกิน 5 ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนด ให้ติดต่อผู้ดูแลระบบ และแจ้งความจำนงค์ขอตั้งรหัสผ่านใหม่

3.4.4 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ 180 วัน

3.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่สิทธิการเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

3.5.1 พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

3.5.2 จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

3.5.3 ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

3.5.4 ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 3 วัน

ส่วนที่ 4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

4.1 การใช้งานรหัสผ่าน (Password Use)

4.1.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน(Password)

4.1.2 การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า 8 ตัวอักษร

- ใช้อักขระพิเศษประกอบ เช่น :;<> เป็นต้น

- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น

- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย

- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น

- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม

- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

4.1.3 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ(Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4.1.4 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.1.5 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทันทีที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

4.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

การป้องกันอุปกรณ์เมื่อไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลได้ดังนี้

4.2.1 มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้ง หรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ, การควบคุมการเข้าออก, การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก, การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

4.2.2 การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตาม แนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดิสก์ (Hard disk) เอ็กเทอนอลฮาร์ดดิสก์ (External Hard disk)	1. ทำลายข้อมูลตามแนวทางของ DOD 5220.22-M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายๆ รอบ 2. ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
2	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
3	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
4	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

4.2.3 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบ การรักษาความลับทางราชการ พ.ศ. 2544 โดยการรับ-ส่งข้อมูลสำคัญ หรือ ข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN

4.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

สำนักงานได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ รวมถึงกำหนดให้ผู้ใช้งานออก จากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติดังนี้

4.3.1 ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

4.3.2 ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าขณะที่ไม่ได้ใช้งาน ภายใน 15 นาที ให้เครื่องล๊อคหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิด หน้าจอได้

4.3.3 ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

4.3.4 กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

4.3.5 ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

4.4 การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศขององค์กร กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งานดังนี้

4.4.1 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

4.4.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

4.4.3 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นบุคคลภายนอก

4.4.4 ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

4.4.5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม

เห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สำนักงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งสำนักงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

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

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

4.4.8 ห้ามใช้สินทรัพย์ของสำนักงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสำนักงาน

4.4.9 ห้ามใช้ระบบสารสนเทศของสำนักงานเพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงาน

4.4.10 ห้ามใช้ระบบสารสนเทศของสำนักงานเพื่อประโยชน์ทางการค้าส่วนบุคคล

4.4.11 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายของสำนักงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบดังนี้

5.1 การใช้งานบริการเครือข่าย

5.1.1 กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

5.1.2 กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

5.1.3 กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย(Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

5.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User authentication for external connections)

5.2.1 เมื่อผู้ใช้งานที่อยู่ภายนอกองค์กร ต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน(Username) ที่สำนักงานกำหนดให้ทุกครั้ง

5.2.2 มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

5.2.3 การเข้าสู่ระบบสารสนเทศของสำนักงานจากอินเทอร์เน็ตต้องได้รับอนุญาตจาก หัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ และต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัยด้วย VPN

5.3 การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

5.3.1 กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

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

5.3.3 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ที่ดูแลระบบเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

5.3.4 ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

5.3.5 จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

5.3.6 แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง

5.4 การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

5.4.1 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.4.2 มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จ าเป็นเท่านั้น

5.4.3 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

5.4.4 ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

5.5 การแบ่งแยกเครือข่าย (Segregation in network)

กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

5.5.1 Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

5.5.2 Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

5.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติดังนี้

5.6.1 จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

5.6.2 ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

5.6.3 การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

5.6.4 ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

5.6.5 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

5.6.6 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

1) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

2) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

3) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

4) ระบบเครือข่ายทั้งหมดของสำนักงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

5) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

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

7) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

8) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.7 การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ สารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ซึ่งมีแนวปฏิบัติ ในการจัดเส้นทางบนเครือข่าย ดังนี้

5.7.1 ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

5.7.2 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

5.7.3 กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

5.7.4 ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง(Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการของสำนักงานโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบดังนี้

6.1 ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

6.1.1 กำหนดให้ระบบไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

6.1.2 กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

6.1.3 จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยผู้ใช้งานจะต้องป้อนรหัสผ่านภายในเวลา 30 นาทีเพื่อเข้าใช้งานระบบ

6.1.4 จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

6.2 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

6.2.1 ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของสำนักงาน

6.2.2 หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องขออนุญาตใช้จาก หัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุญาตไว้

6.3 การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

6.3.1 มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักขระ ตัวเลข และตัวอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ

6.3.2 เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

6.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติดังนี้

6.4.1 การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

6.4.2 โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

6.4.3 จำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เท่านั้น

6.4.4 กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

6.5 การกำหนดระยะเวลายุติการใช้งานระบบสารสนเทศ (Session Time - Out)

6.5.1 กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 30 นาที

6.5.2 ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลา 15 นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

6.6 การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

(Limitation of Connection Time)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูง กำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัยดังนี้

6.6.1 กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ให้ใช้งานได้ภายใน 3 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาราชาการ วันจันทร์ ถึงวันศุกร์ เวลา 8.30 – 16.30 น. เท่านั้น

6.6.2 กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน 3 ชั่วโมงต่อครั้ง

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(Application and Information Access Control)

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการดังนี้

7.1 จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศดังนี้

7.1.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของสำนักงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูล

7.1.2 จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

7.1.3 ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

7.1.4 ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

7.1.5 ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource)ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

7.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ กำหนดให้การควบคุมอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking) โดยกำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไว้ดังนี้

7.2.1 แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็น ถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

7.2.2 ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

1) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์ และระบบ โดยติดตั้งไว้ในในพื้นที่ปลอดภัย

2) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

7.2.3 ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับ ระบบดังกล่าวโดย

1) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงาน ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

2) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจาก หัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ เพื่อเปิดสิทธิให้ปฏิบัติงานจากภายนอกได้

3) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

7.2.4 ควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนด

7.2.5 วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายการสำรองระบบสารสนเทศ

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังนี้

7.3.1 การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งาน อุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต

7.3.2 กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

7.3.3 ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

7.4 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยดังนี้

7.4.1 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่างๆ ภายในหน่วยงาน

7.4.2 การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของ ส่วนตัวต้องได้รับอนุญาตจาก หัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ และผู้ดูแลระบบ

7.4.3 การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากหัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ และผู้ดูแลระบบ โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียดดังนี้

1) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

2) รายละเอียดและลักษณะของระบบงาน

3) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

4) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

5) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

7.4.4 ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

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

7.4.6 ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานโดย ไม่ให้บุคคลอื่นใดสามารถเข้าถึงระบบได้

7.4.7 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

7.4.8 ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อ หัวหน้าส่วนงานที่รับผิดชอบดูแลระบบงานนั้นๆ

7.4.9 ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในหน่วยงาน มีความมั่นคงปลอดภัยกำหนดแนวทางปฏิบัติเพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ดังนี้

8.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจาก ผู้ดูแลระบบที่ได้รับมอบหมาย

8.2 ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งานดังนี้

8.2.1 ลงทะเบียน และกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายเหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

8.2.2 ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

8.2.3 ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

8.2.4 ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

8.2.5 เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

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

8.2.7 เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Addressชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

8.2.8 มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สาย กับเครือข่ายภายในหน่วยงาน

8.2.9 ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อหัวหน้าผู้ดูแลระบบสารสนเทศทันที

ส่วนที่ 9 การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัยดังนี้

9.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าผู้ดูแลระบบสารสนเทศ เป็นลายลักษณ์อักษร

9.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

9.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

9.4 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็น การส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจ

กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

9.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

9.6 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

9.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

9.8 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

9.9 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์(Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

9.10 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ 10 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติดังนี้

10.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่สำนักงานอนุญาตให้ผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของสำนักงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

10.2 โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน ห้ามผู้ใช้งานติดตั้ง แก้ไขโปรแกรมด้วยตนเอง ผู้ดูแลระบบมีหน้าที่จัดหาและลงโปรแกรมในเครื่องของสำนักงานเท่านั้น

10.3 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสำนักงานเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกหน่วยงานเพื่อการใดก็ตาม ต้องขออนุมัติผู้อำนวยการสำนักงาน หรือผู้ที่ได้รับมอบหมายเท่านั้น

10.4 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม

ป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล

10.5 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดย

10.5.1 กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่อง และเก็บรักษารหัสผ่านอย่างปลอดภัย

10.5.2 เมื่อไม่ได้ใช้งานเกิน 30 นาที เครื่องควรตั้งโปรแกรม Screen Saver และต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง และเมื่อเลิกใช้งานควรล็อกเอาท์ (Log Out) ออกจากเครื่อง

10.5.3 ต้องอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์และ โปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

10.5.4 ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ที่สำนักงานติดตั้ง ในเครื่องคอมพิวเตอร์ ส่วนบุคคล

10.5.5 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มิได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบ มาใช้งานและเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับอนุญาตและนำมาขึ้นทะเบียนกับผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ส่วนที่ 11 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

11.1 เครื่องคอมพิวเตอร์แบบพกพาที่สำนักงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของสำนักงาน เพื่อใช้ในการปฏิบัติงาน ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพร้อมใช้งานเสมอ

11.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

11.3 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User Name) และ รหัสผ่าน (Password) เพื่อเปิดเข้าใช้งานเครื่องทุกครั้ง และควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และเก็บรักษาไว้เป็นความลับ

11.4 ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ไม่น้อยกว่า 15 นาที เพื่อล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านอีกครั้งเมื่อกลับมาใช้งาน

11.5 ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งาน

11.6 ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย และทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

11.7 การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ต้องดำเนินการโดยคำนึงถึงความปลอดภัย และไม่ทำให้คอมพิวเตอร์เกิดความเสียหาย

11.8 ความปลอดภัยทางด้านกายภาพ

1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3) หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก

4) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

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

6) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

7) ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แบบพกพาให้อยู่ในสภาพร้อมใช้งาน พักเครื่องเมื่อต้องใช้เป็นระยะเวลานานเกินไป หรือในสภาพที่มีอากาศร้อนจัด

ส่วนที่12 การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

12.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบดังนี้

12.1.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

12.1.2 ผู้ดูแลระบบที่ได้รับมอบหมาย จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของสำนักงาน

12.1.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติจากหัวหน้าผู้ดูแลระบบสารสนเทศ ก่อนดำเนินการ

12.1.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

12.1.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

12.1.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

12.1.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

12.1.8 จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

12.2 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

12.2.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

12.2.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลง ระบบปฏิบัติการ

12.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

12.3.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

12.3.2 ระบุผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

12.3.3 กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

12.3.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ก่อนมีการติดตั้ง

12.3.5 การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

12.4 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

12.4.1 ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจาก หัวหน้าผู้ดูแลระบบสารสนเทศ

12.4.2 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

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

12.4.4 การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากหัวหน้าผู้ดูแลระบบสารสนเทศ ก่อนทุกครั้ง

12.5 มาตรการควบคุมช่องโหว่ทางเทคนิค

12.5.1 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน บริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

2) สถานที่ที่ติดตั้ง

3) เครื่องแม่ข่ายที่ติดตั้ง

4) ผู้ผลิตซอฟต์แวร์

5) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

12.5.2 กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่าง เหมาะสมโดยทันที

12.5.3 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ ดำเนินการ ดังนี้

1) มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบ สารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไข ช่องโหว่ตามความเหมาะสม

2) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบ สารสนเทศของหน่วยงาน

3) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือ ทราบเกี่ยวกับช่องโหว่นั้น

12.5.4 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

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

1) ข้อมูลชื่อบัญชีผู้ใช้งาน

2) ข้อมูลวันเวลาที่เข้าถึงระบบ

3) ข้อมูลวันเวลาที่ออกจากระบบ

4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

5) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

7) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (Configuration) ของระบบ

8) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

10) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง

11) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้

12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

ส่วนที่ 13 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

13.1 ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

13.1.1 กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงาน พื้นที่ควบคุมเฉพาะให้ชัดเจน และควบคุม เพื่อกำหนดสิทธิการเข้าถึงพื้นที่ โดยหัวหน้าผู้ดูแลระบบสารสนเทศ

13.1.2 กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารดังนี้

1) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิการเข้าใช้งานพื้นที่เท่านั้น

2) ควบคุมการเข้าใช้งานในพื้นที่โดยการจดบันทึกหรือแบบพิมพ์นิ้วมือ (Finger Scan)

3) ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวัง การเข้าพื้นที่ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

13.1.3 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

13.1.4 จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอ ต่อความต้องการใช้งาน และมีความพร้อมในการใช้งานดังนี้

1) ติดตั้งระบบไฟฟ้าสำรอง

2) ติดตั้ง ระบบระงับเพลิง

3) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

4) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

5) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

13.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

13.2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

13.2.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

13.2.3 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

13.2.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่างๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

13.2.5 จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

13.2.6 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดล๊อคให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

13.2.7 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

13.3 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

13.3.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

13.3.2 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

13.3.3 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

13.3.4 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำาการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่นพื้นที่ทุกครั้ง

13.3.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก ที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

13.4 การนำทรัพย์สินของสำนักงานออกนอกสำนักงาน (Removal of Property)

13.4.1 ต้องขออนุญาตจากผู้อำนวยการ ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือ นำไปซ่อมบำรุงภายนอก

13.4.2 ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอยู่ในสภาพดี

13.4.3 บันทึกข้อมูลการนำอุปกรณ์ของสำนักงานออกไปใช้งานนอกสำนักงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

13.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment off Premises)

13.5.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินของสำนักงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

13.5.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของสำนักงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

13.5.3 เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

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

13.6.1 ผู้อำนวยการ เป็นผู้อนุมัติในการกำจัด หรือ นำอุปกรณ์สารสนเทศกลับมามาใช้โดยผู้ที่ต้องการกำจัด หรือ นำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

13.6.2 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

ส่วนที่ 14 การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)

14.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของผู้ปฏิบัติงาน ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละครั้ง

14.2 ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิเล็กทรอนิกส์ของสำนักงาน โดยกำหนดสิทธิบัญชีรายชื่อผู้ใช้งาน e-mail รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

14.3 กำหนดให้ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก 180 วัน

14.4 เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

14.5 กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

14.7 ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาภายในระยะเวลา 30 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

14.8 ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ(Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

14.9 ผู้ใช้งานต้องระมัดระวังในการใช้ e-mail เพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน ได้แก่ การละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์รวมทั้งไม่ อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ e-mail ผ่านระบบเครือข่ายของสำนักงาน

14.10 ผู้ใช้งานต้องไม่ใช้ที่อยู่อีเมล (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของอีเมล

14.11 หลังจากการใช้งาน e-mail เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้งเพื่อ ป้องกันบุคคลอื่นเข้าใช้งาน e-mail โดยไม่ได้รับอนุญาต

14.12 ผู้ใช้งานควรตรวจสอบเอกสารแนบจาก e-mail ก่อนทำการเปิด โดยใช้โปรแกรม ป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

14.13 ผู้ใช้งานไม่เปิดหรือส่งต่อ e-mail หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

14.14 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่ง e-mail ที่ไม่เหมาะสม หรือข้อมูลอัน อาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทาง e-mail

14.15 ผู้ใช้งานควรตรวจสอบตู้เก็บ e-mail (Inbox) ของตนเองทุกวัน และควรลบ e-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บน e-mail

ส่วนที่ 15 การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

15.1 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น ได้แก่ เฟสบุ๊ค ไลน์ ยูทูป

15.2 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือ ข้อมูลความลับของสำนักงาน

15.3 ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่ จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน

15.4 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อสำนักงาน ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชา โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

หมวด 2 นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

วัตถุประสงค์

1) เพื่อให้ระบบสารสนเทศของสำนักงานสามารถให้บริการได้อย่างต่อเนื่อง

2) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3) เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดย

ผู้รับผิดชอบ

1) หัวหน้าส่วนงานที่ดูแลระบบสาสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

ส่วนที่ 1 การสำรองข้อมูล (Back Up)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

1.1 จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้ง กำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผน โดยการกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจาก ความสำคัญของข้อมูล , ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูลดังนี้

1.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ ตามความเหมาะสมกับระบบงาน

1.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.2.3 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

1.2.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการวัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล เป็นต้น

1.2.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

1.2.6 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนฉุกเฉินด้านสารสเทศที่กำหนดไว้

1.2.7 วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอลไว้เป็นหลักฐาน

ส่วนที่ 2 การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียม ความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

2.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

2.1.1 กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.1.2 ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นรวมทั้งมาตรการเพื่อ ลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานใน สถานที่ทำงานได้เป็นต้น ทำให้ไม่สามารถเข้ามาใช้งานระบบสารสนเทศได้

2.1.3 กำหนดขั้นตอนปฏิบัติในการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาในการกู้คืนระบบที่สอดคล้องตามเป้าหมายที่หน่วยงานกำหนดไว้

2.1.4 กำหนดขั้นตอนปฏิบัติในกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

2.1.5 กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงาน และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำาเป็นที่จะต้องติดต่อผู้ให้บริการ

2.1.6 สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการ ปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับ ใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

2.3 กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

2.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบ แผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.5 ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่ เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

หมวด 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความ มั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

2) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

3) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

1) หัวหน้าส่วนงานที่ดูแลระบบสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) ผู้ตรวจสอบภายใน

แนวทางปฏิบัติ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

1.1 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

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

2. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

2.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

2.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

2.4.1 กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

2.4.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

2.4.3 กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.4.4 กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

2.4.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด 4 หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยี สารสนเทศระดับสูง (CIO) หัวหน้าส่วนงานที่ดูแลระบบสารสนเทศ ผู้ดูแลระบบ ผู้ที่ได้รับ มอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ 1 ระดับนโยบาย

1.1 ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอัน เนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ

1.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) สำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้ สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.3 หัวหน้าส่วนงานที่ดูแลระบบสารสนเทศ ของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน) ผู้รับผิดชอบ ดังนี้

1.3.1 กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

1.3.2 ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

1.3.3 วางแผน จัดทำทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียม ความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถด าเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

ส่วนที่ 2 ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติการประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

2.1 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

2.1.1 ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.2 ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคง ปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและ ภัยพิบัติ

2.1.3 ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

2.1.4 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

2.1.5 ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.1.6 ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารและพัฒนาองค์ความรู้ (องค์การมหาชน)

2.2 ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด