ประกาศสำนักงานเศรษฐกิจการคลัง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล ผู้อำนวยการสำนักงานเศรษฐกิจการคลังโดยความเห็นชอบของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑”

ข้อ ๒ ให้ยกเลิก ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๘

ข้อ ๓ ในประกาศนี้

(๑) สำนักงาน หมายความว่า สำนักงานเศรษฐกิจการคลัง

(๒) ผู้บริหารระดับสูงสุด หมายความว่า ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง

(๓) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้าง ผู้ดูแลระบบ ผู้บริหารของสำนักงาน รวมถึงบุคคลภายนอกที่เป็นหน่วยงานราชการ รัฐวิสาหกิจ ผู้ประกอบการที่เกี่ยวข้องกับสำนักงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน

(๔) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

(๕) สินทรัพย์ (Asset) หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับสำนักงาน

(๖) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายและระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

(๗) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๘) เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๙) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๐) นโยบาย หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลัง

(๑๑) ผู้บริหาร หมายความว่า ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง ที่ปรึกษาด้านเศรษฐกิจการเงิน/การคลัง/ระหว่างประเทศ รองผู้อำนวยการสำนักงานเศรษฐกิจการคลัง หรือผู้ที่ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง มอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลัง

ข้อ ๔ การจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ประกอบด้วยกระบวนการ ดังนี้

(๑) การจัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง

(๒) การประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๔) ทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๗ - ๑๕

ข้อ ๖ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๖.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงานเศรษฐกิจการคลัง

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๖.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้และประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๗ กำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของสำนักงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๘ กำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๙ กำหนดการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๑๐ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสำนักงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ให้มีการทำลายข้อมูลบนสื่อบันทึกข้อมูลของระบบหรืออุปกรณ์คอมพิวเตอร์ที่จะมีการแทงจำหน่ายหรือก่อนที่จะอนุญาตให้ผู้อื่นนำระบบหรืออุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันการเข้าถึงข้อมูลสำคัญบนสื่อบันทึกข้อมูล

(๕) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๑๑ กำหนดการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกสำนักงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานได้

(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) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๒ กำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๓ กำหนดการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) มีการควบคุมการให้บริการหรือการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติจากภายนอกสำนักงาน (Mobile Computing and Teleworking)

(๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๕) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกสำนักงาน

ข้อ ๑๔ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๕ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของสำนักงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้สำนักงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย

ข้อ ๑๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่สำนักงาน หรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของสำนักงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๗ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงาน โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของสำนักงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๑๘ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๘ กุมภาพันธ์ พ.ศ. ๒๕๖๑

(นายสุวิชญ โรจนวานิช)
ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

ดังนั้น การจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลังฉบับนี้ จัดทำขึ้นตามมาตรฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับใช้เป็นมาตรการและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลังและหน่วยงานภายนอกซึ่งเป็นการช่วยลดปัญหา ผลกระทบหรือความเสียหายต่าง ๆ ต่อการดำเนินงาน ทรัพย์สิน และบุคลากรของสำนักงานเศรษฐกิจการคลัง รวมทั้งหน่วยงานภายนอกให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

สำนักงานเศรษฐกิจการคลัง
๒๕๖๑

วัตถุประสงค์

ระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูลของสำนักงานเป็นระบบที่มีความสำคัญต่อการให้บริการประชาชน หน่วยงานทั้งภาครัฐและเอกชน รวมทั้งการใช้งานภายในสำนักงาน จึงได้มีการจัดทำแนวทางปฏิบัติเพื่อให้ระบบสามารถใช้งานได้อย่างเหมาะสม มีประสิทธิภาพและเกิดความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ

เอกสารแนบท้ายประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑ เป็นเอกสารที่จัดทำขึ้นเพื่อใช้เป็นกรอบในการปฏิบัติ โดยได้กำหนดขั้นตอนการดำเนินการตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนเป็นแผนการปรับปรุงเพื่อให้สำนักงานสามารถดำเนินการให้ครอบคลุมด้านความปลอดภัยต่อไป ดังนี้

๑. เพื่อให้เกิดความเชื่อมั่น และมีระบบการรักษาความมั่นคงปลอดภัยการใช้งานในระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของสำนักงานให้ดำเนินงานไปได้อย่างมีประสิทธิภาพ และประสิทธิผล

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของสำนักงาน

๓. เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบเทคโนโลยีสารสนเทศ การสื่อสารข้อมูลของสำนักงาน ยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัย

ส่วนที่ ๑ การประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ต้องทำการประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

๑. หนังสือเวียนภายในสำนักงาน

๒. หนังสือเวียนภายนอกสำนักงาน

๓. เว็บไซต์ของสำนักงาน

ส่วนที่ ๒ ผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่สำนักงานหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของสำนักงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๑. สำนักงานกำหนดวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย โดยมีข้อปฏิบัติการเข้าถึงและการใช้งานสารสนเทศที่เหมาะสม ดังนี้

๑.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศกำหนด เพื่อขอสิทธิในการเข้าระบบเฉพาะส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้อำนวยการสำนัก/กลุ่ม/ศูนย์ เพื่อการจัดเก็บไว้เป็นหลักฐาน

๑.๓ เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามภารกิจและการปฏิบัติงานในหน้าที่เท่านั้น เนื่องจากการใช้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑.๔ เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติเกี่ยวกับข้อมูล สารสนเทศ และ/หรือระบบงานที่รับผิดชอบ เพื่อให้ผู้ใช้งานสามารถนำข้อมูลไปใช้หรือใช้ระบบงานได้อย่างถูกต้อง มีประสิทธิภาพ และเป็นมาตรฐานเดียวกัน

๒. กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ โดยการกำหนดสิทธิต่าง ๆ ให้แก่ผู้ใช้งานในแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ สิทธิในการอ่านอย่างเดียว สิทธิในการสร้างข้อมูล สิทธิในการป้อนข้อมูล สิทธิในการแก้ไข สิทธิในการอนุมัติ รวมถึงการไม่มีสิทธิ โดยผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓. กำหนดสิทธิและมอบอำนาจการใช้งานสารสนเทศแต่ละชนิดเพื่อควบคุมการอนุญาตให้เข้าถึงสารสนเทศที่สำคัญ โดยมีการแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนของงานคอมพิวเตอร์

๓.๑ มีหน่วยงานควบคุมการให้สิทธิการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

๓.๒ แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์

๓.๓ กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

๓.๔ มีบุคลากรสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น ได้แก่ ผู้บริหารระบบเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เป็นต้น

๓.๕ ให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้อำนวยการสำนัก/กลุ่ม/ศูนย์ เป็นลายลักษณ์อักษร

๓.๖ มีการตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

๓.๗ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๘ ต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยมีระบบสารสนเทศที่สำคัญ ดังนี้

(๑) ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application)

(๒) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

(๓) ระบบอินเตอร์เน็ต

๔. กำหนดประเภทของข้อมูลและสารสนเทศที่กำหนดชั้นความลับ (Confidential Data and Information) ซึ่งเป็นข้อมูลและสารสนเทศที่มีความสำคัญและเป็นความลับ หากถูกเปิดเผยออกไปแล้วจะเกิดความเสียหายหรือเกิดผลเสียอื่น ๆ ต่อหน่วยงาน ต้องกำหนดประเภทของข้อมูล จัดแบ่งลำดับความสำคัญของข้อมูล จัดแบ่งลำดับชั้นความลับของข้อมูล จัดแบ่งระดับชั้นการเข้าถึง กำหนดเวลาเข้าถึงได้ และกำหนดช่องทางการเข้าถึงสำหรับสารสนเทศอย่างเคร่งครัด ดังต่อไปนี้

๔.๑ กำหนดประเภทของข้อมูล ดังนี้

(๑) ข้อมูลและสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(๒) ข้อมูลและสารสนเทศที่ให้บริการ ได้แก่ ข้อมูลด้านเศรษฐกิจ การเงิน การคลัง เป็นต้น

๔.๒ จัดแบ่งลำดับความสำคัญของข้อมูล ดังนี้

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๓) ข้อมูลที่มีระดับความสำคัญน้อย

๔.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้

๔.๓.๑ กำหนดบุคคลผู้ทำหน้าที่เป็นผู้บริหารจัดการสารสนเทศภายในหน่วยงาน เป็นผู้ทำหน้าที่จัดหมวดหมู่ทรัพย์สินสารสนเทศ ได้แก่ ข้อมูลดิจิตอล (Digital Data) หรือสารสนเทศดิจิทัล (Digital Information) โดยระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และต้องมีการจัดลำดับชั้นความลับเป็นอย่างหนึ่งอย่างใดต่อไปนี้

(๑) “ชั้นลับที่สุด”

(๒) “ชั้นลับมาก”

(๓) “ชั้นลับ”

(๔) “ชั้นไม่ลับ หรือ ชั้นเปิดเผย”

กำหนดให้บุคลากรประจำหน่วยงาน เป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานในการจัดเก็บข้อมูลและสารสนเทศที่อยู่ในชั้นไม่ลับ หรือชั้นเปิดเผยนี้ เข้าสู่ระบบบริหารจัดการองค์ความรู้ (Knowledge Management System) หรือระบบจัดเก็บเอกสาร (Document Image System) ตามความเหมาะสม โดยให้ผู้อำนวยการสำนัก/กลุ่ม/ศูนย์ พิจารณาอนุมัติในแบบฟอร์มการจัดเก็บทรัพย์สินสารสนเทศก่อนทุกครั้ง

๔.๓.๒ เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

๔.๓.๓ ให้บุคลากรประจำหน่วยงานเป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันสารสนเทศของสำนักงาน ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยสำนักงานจัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศ กำหนดให้มีชั้นความลับที่สุด ชั้นลับมาก ชั้นลับ และชั้นไม่ลับ หรือชั้นเปิดเผย การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูลของสำนักงาน ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม มีการกำหนดชั้นความลับโดยมีข้อพิจารณาดังนี้

(๑) ชั้นลับที่สุด กำหนดให้มีระดับความปลอดภัยที่ ๔ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงานมากที่สุด ต้องได้รับการรักษาความลับของเนื้อหาโดยการเข้ารหัสอย่างยาก (Strong Encryption) และจำกัดการเข้าถึง (Access Control) เป็นอย่างดี ได้แก่ Private Key ของสำนักงาน หรือข้อมูลที่จากการประชุมที่มีมติที่ประชุมกำหนดให้เป็นชั้นความลับนี้ ตัวอย่างข้อมูลชั้นลับที่สุด ได้แก่ นโยบายหรือแผนการที่สำคัญยิ่งของสำนักงาน ซึ่งถ้าเปิดเผยก่อนเวลาอันสมควร อาจก่อให้เกิดผลเสียหายอย่างร้ายแรงแก่สำนักงาน แผนยุทธศาสตร์ที่เกี่ยวกับข้อมูลสำคัญในการปฏิบัติภารกิจของสำนักงานร่วมกับหน่วยงานอื่น เอกสารของสำนักงานที่เกี่ยวข้องกับความมั่นคงปลอดภัย เป็นต้น

(๒) ชั้นลับมาก กำหนดให้มีระดับความปลอดภัยที่ ๓ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงานมาก ต้องได้รับการรักษาความลับของเนื้อหาโดยการเข้ารหัส (Encryption) หรือจำกัดการเข้าถึง (Access Control) ตัวอย่างข้อมูลชั้นลับมาก ได้แก่ รายงานเสนอการแต่งตั้ง ถอดถอนหรือโยกย้ายพนักงานในตำแหน่งที่สำคัญมาก การเจรจาข้อตกลงที่สำคัญกับหน่วยงานอื่น เทคนิคที่ต้องอาศัยความชำนาญพิเศษ เป็นต้น

(๓) ชั้นลับ กำหนดให้มีระดับความปลอดภัยที่ ๒ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงาน โดยจำกัดการเข้าถึง (Access Control) ตัวอย่างข้อมูลชั้นลับ ได้แก่ การดำเนินการที่เกี่ยวกับการเปลี่ยนแปลงตำแหน่งที่สำคัญในสำนักงาน ระเบียบวาระการประชุมลับ ประกาศหรือคำสั่งที่สำคัญที่อยู่ระหว่างการดำเนินการ เป็นต้น

(๔) ชั้นไม่ลับ หรือ ชั้นเปิดเผย กำหนดให้มีระดับความปลอดภัยที่ ๑ สำหรับข้อมูลและสารสนเทศที่ไม่มีความลับ สามารถเผยแพร่ได้ ตัวอย่างข้อมูลชั้นไม่ลับ หรือชั้นเปิดเผย ประกอบด้วย ข้อมูลและสารสนเทศที่เป็นความรู้ของหน่วยงานในลักษณะงานวิจัย นโยบาย ข้อกฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา พระราชกำหนด ข้อมูลและสารสนเทศที่เป็นประกาศ คำสั่งแต่งตั้ง ข่าวประชาสัมพันธ์

๔.๓.๔ ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลายและกำหนดเป็นระเบียบปฏิบัติให้ข้าราชการและลูกจ้างของสำนักงาน ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

๔.๔ จัดแบ่งระดับชั้นการเข้าถึง

(๑) ผู้บริหารระบบ (Administrator) ต้องได้รับสิทธิในการเข้าใช้งานจากศูนย์เทคโนโลยีสารสนเทศ โดยมีการกำหนด User และ Password ในการเข้าใช้งาน โดยผ่านทาง Secure Shell ซึ่งแยกประเภทตามความรับผิดชอบ ได้แก่ Network, Admin, System Admin และ Database Admin เป็นต้น

(๒) ผู้ใช้งาน ต้องได้รับสิทธิในการเข้าใช้งานจากศูนย์เทคโนโลยีสารสนเทศ โดยต้องใช้งานผ่านระบบ Single Sign-On ของสำนักงาน และต้องใช้ User และ Password เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

๔.๕ กำหนดเวลาเข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๔.๖ กำหนดช่องทางการเข้าถึงสำหรับสารสนเทศอย่างเคร่งครัด

ผู้ได้รับสิทธิทำการ Log In ด้วย User และ Password ผ่านระบบ Single Sign-On เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

๕. กำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๕.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๕.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีข้อปฏิบัติดังนี้

๑. <u>การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน</u>

สร้างความรู้ความเข้าใจ วิธีการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์อย่างมั่นคงปลอดภัยให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบ รวมถึงการป้องกันการกระทำผิดจากการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกันตามความเหมาะสม มีข้อปฏิบัติดังนี้

๑.๑ ประกาศหรือเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑.๒ มีการฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศอย่างไม่ถูกต้องหรือไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

๑.๓ จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของสำนักงาน อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการพัฒนาระบบสารสนเทศขึ้นมาใช้งาน หรือมีการปรับปรุง/ปรับเปลี่ยนการใช้งานของระบบสารสนเทศ

๑.๔ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของสำนักงาน

๑.๕ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม อาจใช้วิธีการเสริมเนื้อหา แนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของสำนักงาน

๑.๖ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้

๑.๗ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๑.๘ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๒. <u>การลงทะเบียนผู้ใช้งาน</u> (User Registration)

ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบ และมีหน้าที่ลงทะเบียนผู้ใช้งาน รวมถึงการตัดออกจากทะเบียนผู้ใช้งานทั่วไปและผู้ใช้งานระบบ กำหนดให้มีข้อปฏิบัติดังนี้

๒.๑ การลงทะเบียนผู้ใช้งานทั่วไป สำหรับระบบสารสนเทศที่จำเป็นพื้นฐานซึ่งเป็นการเข้าใช้งานบนระบบอินทราเน็ต (Intranet) ได้แก่ ระบบการลงเวลาการปฏิบัติงาน ระบบการลาอิเล็กทรอนิกส์ ระบบจองรถยนต์ ระบบการจองห้องประชุม ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ ระบบ e-Learning เป็นต้น รวมถึงการเข้าใช้งานบนระบบอินเทอร์เน็ต (Internet) ได้แก่ ระบบเว็บไซต์สำนักงาน ระบบไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) เป็นต้น ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะทำหน้าที่ประสานกับส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม เพื่อดำเนินการลงทะเบียนผู้ใช้งานทั่วไป

๒.๒ การลงทะเบียนผู้ใช้งานระบบสารสนเทศด้านการอำนวยการ ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบบริหารจัดการวัสดุและครุภัณฑ์ ระบบการขอจัดซื้อจัดจ้าง ระบบบริหารจัดการงบประมาณ เป็นต้น ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะทำหน้าที่ประสานกับส่วนบริหารทั่วไป ส่วนบริหารงานพัสดุ และส่วนบริหารงานคลัง สำนักงานเลขานุการกรม เพื่อดำเนินการลงทะเบียนผู้ใช้งานระบบ

๒.๓ การลงทะเบียนผู้ใช้งานระบบสารสนเทศสนับสนุนภารกิจ ได้แก่ ระบบสารสนเทศสถาบันการเงิน (FIs Management System : FI) ระบบสารสนเทศสถาบันการเงินเฉพาะกิจ (SFIs Management System : SFI) ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะทำหน้าที่ประสานกับหน่วยงานภายในสำนักงาน (สำนัก/กลุ่ม/ศูนย์) ที่เป็นเจ้าของระบบงาน เพื่อดำเนินการลงทะเบียนผู้ใช้งานระบบตามสิทธิการเข้าใช้ระบบอย่างถูกต้อง เพียงพอ และเหมาะสมตามความจำเป็นในการใช้งาน ทั้งนี้ ภายหลังจากที่ได้รับแจ้งรายชื่อ ตำแหน่งและวัตถุประสงค์ในการใช้ระบบงาน โดยสำนัก/กลุ่ม/ศูนย์ ต้องจัดทำเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบเป็นลายลักษณ์อักษรส่งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศลงนามอนุมัติ และเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

๒.๔ หากบุคลากรมีการโอน/ย้าย/ลาออก/สิ้นสุดการจ้าง หรือเมื่อเปลี่ยนตำแหน่งงานภายในหน่วยงาน หรือกรณีไปช่วยราชการที่อื่น ศูนย์เทคโนโลยีสารสนเทศจะทำหน้าที่ประสานกับส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม จะทำการระงับการใช้งานของรหัสผ่านทันทีเมื่อบุคลากรพ้นจากภารกิจ รวมถึงทำการยกเลิกและตัดสิทธิการเข้าใช้งานระบบสารสนเทศทุกระบบพร้อมลบชื่อออกจากทะเบียนผู้ใช้งานทั่วไปและผู้ใช้งานระบบภายใน ๓๐ วัน ทั้งนี้ ภายหลังจากที่ได้รับแจ้งรายชื่อ ตำแหน่งและวันที่มีผลบังคับใช้ โดยมีหลักฐานเป็นลายลักษณ์อักษรจากส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม หรือหน่วยงานที่เกี่ยวข้องแล้ว

๒.๕ ศูนย์เทคโนโลยีสารสนเทศจะกำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในเบื้องต้น โดยใช้ข้อมูลจากส่วนกลางที่จัดเก็บใน Active Directory (AD) และส่งมอบให้แก่ผู้ใช้งานซึ่งระบบงานอนุญาตให้ผู้ใช้งานเปลี่ยนรหัสผ่านได้ด้วยตนเอง และหากมีปัญหา ได้แก่ ผู้ใช้งานลืมรหัสผ่าน เป็นต้น ศูนย์เทคโนโลยีสารสนเทศดำเนินการกำหนดรหัสผ่านใหม่ให้

๓. <u>การบริหารจัดการสิทธิของผู้ใช้งาน</u> (User Management)

เป็นการกำหนดรายละเอียดที่เกี่ยวกับการกำหนดระดับสิทธิ การควบคุมและจำกัดสิทธิการใช้งานให้แก่ผู้ใช้งานในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งานเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงการมอบหมายสิทธิ สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง โดยมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบ และมีหน้าที่บริหารจัดการสิทธิของผู้ใช้งาน โดยจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศ กำหนดให้มีข้อปฏิบัติดังนี้

๓.๑ กำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบตัวตนจริง และควบคุมการเข้าถึงข้อมูลในแต่ละชั้นความลับ โดยจำแนกผู้ใช้งานออกเป็นกลุ่มต่าง ๆ ตามระดับการใช้งานที่เหมาะสม โดยคำนึงถึงชั้นความลับของข้อมูลเพื่อกำหนดกลุ่มผู้ใช้งานและระดับการใช้ข้อมูลในการปฏิบัติงาน ได้แก่ กลุ่มผู้ใช้ที่มีสิทธิเข้าถึงระบบฐานข้อมูลและแฟ้มข้อมูล (Database and File System) กลุ่มผู้ใช้ที่มีสิทธิเข้าถึงเฉพาะข้อมูลสารสนเทศ รวมถึงผู้ใช้ระดับใดควรมีสิทธิแก้ไขข้อมูล ระดับใดควรสร้าง/ลบข้อมูลได้ และระดับใดสามารถเรียกดูข้อมูลได้เพียงอย่างเดียว เป็นต้น

๓.๒ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดนอกเหนือจากผู้ใช้ปกติ ได้แก่ ผู้ตรวจสอบภายใน เป็นต้น ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา และต้องได้รับความเห็นชอบ และอนุมัติจาก ผอ. สำนัก/กลุ่ม/ศูนย์ นั้น ๆ ก่อน

(๑) ควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน เป็นต้น

๓.๓ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๓.๔ ระบบงานสารสนเทศต้องออกแบบให้มีระบบการตรวจสอบ โดยต้องมีการเก็บบันทึก (Record) เป็นหลักฐานที่สามารถทำการตรวจสอบ (Audit Trial) ภายหลังได้ว่า ณ เวลาที่เข้าถึงระบบของผู้ใช้ (Events Logging) ว่าผู้ใช้เป็นใคร ทำอะไร จากที่ไหน และทำสำเร็จหรือไม่ โดยที่แฟ้มข้อมูลของระบบการตรวจสอบจะต้องได้รับการปกป้องและตรวจสอบได้เสมอ

๓.๕ ระบบฐานข้อมูลที่สำคัญ ได้แก่ ระบบการเงิน เป็นต้น ต้องสามารถบันทึกรายละเอียดเกี่ยวกับการเข้าถึงฐานข้อมูลในแต่ละครั้ง และต้องมีรายละเอียดที่เพียงพอเพื่อประโยชน์ในการอ้างอิงได้ภายหลัง ได้แก่ วัน เวลาที่เข้าถึง ชื่อเจ้าหน้าที่ที่เข้าถึง และวัตถุประสงค์ของการเข้าถึง เป็นต้น

๔. <u>การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน</u> (User Password Management)

ศูนย์เทคโนโลยีสารสนเทศเป็นผู้บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุมและมีความมั่นคงปลอดภัย เนื่องจากรหัสผ่านเป็นวิธีพื้นฐานในการตรวจสอบตัวตนของผู้ใช้ระบบ ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่า ผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบของสำนักงานอย่างแท้จริง กำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านดังนี้

๔.๑ ผู้ใช้ระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนแก่บุคคลอื่น

๔.๒ ผู้ใช้รายใหม่จะได้รับรหัสผ่านเริ่มแรก (รหัสผ่านชั่วคราว) ในการใช้ผ่านเข้าสู่ระบบในครั้งแรก และระบบต้องบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก ผู้ใช้สามารถสร้างรหัสผ่านที่มีคุณภาพและยากต่อการคาดเดา โดยใช้แนวทางการสร้างรหัสผ่านที่มีคุณภาพ (ส่วนที่ ๕ ข้อ ๑ ข้อย่อย ๑.๑๓)

๔.๓ ไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้

๔.๔ รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้ที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้ที่มีสิทธิใช้งานระบบได้ ได้แก่ มีรายชื่อในระบบ Active Directory (AD) เป็นต้น

๔.๕ แสดงรหัสผ่านในรูปของสัญลักษณ์ หรือตัวอักษร “x” หรือ “o” หรือ “•” ในขณะพิมพ์รหัสผ่านแต่ละตัวอักษร โดยต้องไม่ปรากฏหรือแสดงรหัสผ่านที่แท้จริงออกมา

๔.๖ การตั้งรหัสผ่านต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับสำนักงาน หรือเป็นข้อมูลส่วนตัวของผู้ใช้งาน ซึ่งง่ายแก่การคาดเดา ได้แก่ เลขที่บัตรประชาชน เลขที่บัตรประกันสังคม รหัสบัตรต่าง ๆ ที่อยู่ หมายเลขโทรศัพท์ ชื่อบุคคลในครอบครัว เป็นต้น รวมถึงต้องไม่ใช้ศัพท์ที่มาจากพจนานุกรม ชื่อภาพยนตร์ ชื่อสถานที่หรือชื่อสิ่งลึกลับ เพราะศัพท์ต่าง ๆ เหล่านี้ ง่ายต่อการคาดเดาของผู้โจมตีระบบ (Hackers)

๔.๗ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Saved Password) สำหรับเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองอยู่ รวมถึงไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๔.๘ กำหนดวิธีการส่งมอบรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย ได้แก่ การใส่ซองปิดผนึก การส่งทางไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) และบังคับให้ใส่วัน เดือน ปีเกิด ในการเปิดอ่านไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

กรณีระบบที่ต้องการความมั่นคงปลอดภัยมากเป็นพิเศษ กำหนดให้การจัดส่งและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยยิ่งขึ้น โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งานพร้อมแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งาน และรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๔.๙ การตั้งรหัสผ่าน ควรมีส่วนประกอบของอักษร อักขระพิเศษ และ/หรือ ตัวเลขที่ประสมกันตามลักษณะดังต่อไปนี้

- ความยาวอย่างน้อย ๘ ตัวอักษรหรือตามที่ผู้บริหารจัดการระบบกำหนด
- อักษรตัวพิมพ์ใหญ่ ได้แก่ A, B, C,.... เป็นต้น
- อักษรตัวพิมพ์เล็ก ได้แก่ a, b, c,..... เป็นต้น
- ตัวเลข ได้แก่ ๐, ๑, ๒,.... เป็นต้น
- สัญลักษณ์พิเศษ ได้แก่ !, @, #, $,..... เป็นต้น

๔.๑๐ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๔.๑๑ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๔.๑๒ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔.๑๓ รหัสผ่านเข้าระบบบริหารจัดการด้านเครือข่ายและระบบงานที่สำคัญ ได้แก่ การเข้า Root , Enable , NT Admin , Application Admin Account เป็นต้น จะต้องมีการเปลี่ยนรหัสผ่านเป็นประจำอย่างน้อยทุก ๓ เดือน

๔.๑๔ รหัสผ่านของผู้ใช้งาน ได้แก่ e-Mail , Website , Desktop Computer, Notebook , ระบบเทคโนโลยีสารสนเทศ เป็นต้น ต้องเปลี่ยนเป็นประจำอย่างน้อยทุก ๖ เดือน ทั้งนี้แนะนำให้เปลี่ยนเป็นประจำทุก ๓ เดือน จะสร้างความปลอดภัยได้ดียิ่งขึ้น

๔.๑๕ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน ถ้ารหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๔.๑๖ ผู้ใช้งานไม่ควรเปลี่ยนรหัสผ่านของผู้อื่น ยกเว้นผู้มีหน้าที่ในการบริหารจัดการรายชื่อผู้ใช้งานและรหัสผ่านเท่านั้น

๕. <u>การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน</u> (Review Of User Access Rights)

๕.๑ เจ้าของข้อมูล จะต้องมีการทบทวนสิทธิการเข้าใช้งานและสิทธิการเข้าถึงข้อมูลของผู้ใช้งานและปรับปรุงบัญชีผู้ใช้งานให้มีความเหมาะสมอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด ทุก ๆ ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับเปลี่ยนเคลื่อนย้ายบุคลากร ได้แก่ การโอน/ย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ ลาออก สิ้นสุด/ยกเลิกการจ้าง เป็นต้น เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๕.๒ การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษ ต้องทบทวนบ่อยกว่าปกติ โดยทำทุก ๆ ๓ เดือน

๕.๓ การจัดสรรสิทธิพิเศษ ต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดเพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

๕.๔ การเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษ ต้องถูกบันทึกเพื่อการทบทวน

๕.๕ กรณีมีปัญหาการใช้หรือนำระบบงานไปปฏิบัติโดยไม่ได้รับอนุญาต ศูนย์เทคโนโลยีสารสนเทศจะดำเนินการติดตาม ตรวจสอบ และทบทวนการใช้งาน หากมีผลที่คาดว่าจะกระทบถึงระบบงานในอนาคต ศูนย์เทคโนโลยีสารสนเทศอาจพิจารณายกเลิกการใช้งานนั้น

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีข้อปฏิบัติดังนี้

๑. การใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)

กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๑.๑ ผู้ใช้งานต้องเก็บรักษารหัสผ่านไว้ในที่ปลอดภัย ถือเป็นความลับ

๑.๒ หลีกเลี่ยงการบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกลงในกระดาษ หรือในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

๑.๓ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ หรือโปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

๑.๔ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านระบบเครือข่ายคอมพิวเตอร์

๑.๕ ไม่ใช้รหัสผ่านเดียวกันในกรณีปฏิบัติงานและใช้ส่วนตัว

๑.๖ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องจดจำรหัสผ่านหลายตัว ควรใช้รหัสผ่านเดียวกันที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๑.๗ ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

๑.๘ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑.๙ เมื่อเจ้าหน้าที่ของสำนัก/กลุ่ม/ศูนย์ ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้สำนัก/กลุ่ม/ศูนย์ แจ้งศูนย์เทคโนโลยีสารสนเทศทันที เพื่อดำเนินการเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ที่ลาออก จากระบบทันทีที่ได้รับแจ้ง

๑.๑๐ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิพิเศษ ต้องได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการเวียนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๑.๑๑ กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๑.๑๒ เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๑.๑๓ แนวทางการสร้างรหัสผ่านที่มีคุณภาพ

(๑) กำหนดรหัสผ่านที่ง่ายต่อการจดจำเฉพาะตน แต่ต้องไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่าย ได้แก่ ชื่อ-นามสกุล หมายเลขโทรศัพท์ และวันเกิด เป็นต้น หรือ ชื่อ-นามสกุลของบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน

(๒) รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการประสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๓) รหัสผ่านต้องไม่มีคำซ้ำหรือตัวอักษรซ้ำ ต้องไม่เป็นตัวเลขทั้งหมด หรือตัวอักษรทั้งหมด

(๔) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน ได้แก่ ชื่อสกุล วัน เดือน ปีเกิด หรือที่อยู่ เป็นต้น

(๕) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๑.๑๔ กรณีมีการแอบอ้างรหัสผ่านหรือนำรหัสผ่านไปใช้โดยไม่ได้รับอนุญาตให้ผู้ใช้งานรีบดำเนินการแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที เพื่อระงับการใช้รหัสผ่านดังกล่าว หรือมีปัญหาการใช้งาน กรณีลืมชื่อผู้ใช้หรือรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ

๑.๑๕ ผู้ใช้ต้องพึงระลึกเสมอว่า ความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศของสำนักงานที่ตนเองรับผิดชอบอยู่นั้น มีความสำคัญต่อตนและสำนักงานเป็นอย่างยิ่ง ต้องไม่ให้ผู้อื่นบุกรุก แอบอ้าง หรือนำไปใช้ในทางที่ผิด เพราะอาจก่อให้เกิดผลเสียหายเป็นวงกว้างต่องานของตนเองและของสำนักงาน

๒. <u>การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์</u>

กำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสำนักงานในขณะที่ไม่มีผู้ดูแล

๒.๑ ผู้ใช้ต้องทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่หน้าจอ

๒.๒ ผู้ใช้ต้องทำการ Log Out ออกจากระบบทันที เมื่อเลิกใช้ระบบสารสนเทศ หรือผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน ระบบเครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

๒.๓ ผู้ดูแลระบบ ต้องกำหนดให้มีการป้องกันบุคคลอื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศ โดยต้องบังคับให้ใส่รหัสผ่านที่ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๓. <u>การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์</u> (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน มีข้อปฏิบัติดังนี้

๓.๑ มีการกำหนดมาตรการป้องกันสินทรัพย์ของสำนักงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ ดังนี้

๓.๑.๑ <u>การจัดการบริเวณล้อมรอบ</u> (Physical Security Management)

(๑) กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

(๒) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center) ให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๓) มีระบบป้องกันการบุกรุกที่ติดตั้งครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

(๔) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้ได้ตามปกติ

(๕) บุคลากรของสำนักงานต้องล็อค และปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแล เพื่อป้องกันทรัพย์สินของสำนักงาน

๓.๑.๒ <u>การควบคุมการเข้า-ออก</u> (Physical Entry Controls)

(๑) ให้มีการบันทึกวันและเวลาเข้า - ออก พื้นที่สำคัญของผู้มาเยือน (Visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ

(๔) บุคคลภายนอกต้องแจ้งเหตุผลที่เพียงพอในการเข้าถึงบริเวณที่มีความสำคัญ

(๕) สร้างความตระหนักให้ผู้มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์ หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๖) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๗) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๘) มีการพิสูจน์ตัวตน โดยการใช้บัตรรูด และ/หรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า – ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๙) จัดเก็บบันทึกการเข้า – ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบภายหลังเมื่อมีความจำเป็น

(๑๐) เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการปฏิบัติงาน

(๑๑) ผู้ที่มาเยือนต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

(๑๒) ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๓) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๓.๑.๓ <u>การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก</u> (Public Access, Delivery and Loading Areas)

(๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

(๓) จัดพื้นที่หรือบริเวณที่ส่งมอบไว้เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในสำนักงาน

(๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะเคลื่อนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๕) ลงทะเบียน ตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของสำนักงาน

๓.๑.๔ <u>การจัดวางและการป้องกันอุปกรณ์</u> (Equipment Setting and Protection)

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง Data Center ให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในห้อง Data Center

(๔) ดำเนินการตรวจสอบ สอดส่องและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว โดยมีการตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๑.๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีการสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของสำนักงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ได้แก่ ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศ และควบคุมความชื้น เป็นต้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากความล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๓.๑.๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

(๑) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่าง ๆ กัดสาย

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๔) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๓.๑.๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมสอดส่องดูแลการปฏิบัติงานของผู้รับเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน

(๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๑.๘ การนำทรัพย์สินออกนอกสำนักงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกสำนักงาน

(๒) บันทึกข้อมูลการนำอุปกรณ์ออกนอกสำนักงานเพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๓) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม

๓.๑.๙ <u>การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน</u> (Security of Equipment Off - Premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของสำนักงานออกไปใช้งานข้างนอก

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของสำนักงานไว้ในที่สาธารณะ

(๓) ให้เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๓.๑.๑๐ <u>การทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง</u> (Secure Disposal or Reuse of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะทำลายอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๓.๒ การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

๓.๓ มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๓.๔ มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีเมื่อพิมพ์งานเสร็จ

๓.๕ ในการทำลายข้อมูล และสื่อบันทึกข้อมูลประเภทต่าง ๆ เพื่อป้องกันข้อมูลรั่วไหล และการนำกลับมาใช้ใหม่ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๔. ผู้ใช้งานข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อกำหนดในการรับ-ส่งข้อมูลที่เป็นความลับหรือข้อมูลที่มีความอ่อนไหวสูงให้ดำเนินการผ่านระบบเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ระหว่างสำนักงานกับหน่วยงานภายนอก โดยมีข้อปฏิบัติดังนี้

๔.๑ ใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ในการเพิ่มการรักษาความมั่นคงและความปลอดภัยของข้อมูลให้เป็นไปตามมาตรฐานสากล โดยใช้อุปกรณ์จัดเก็บที่มีความปลอดภัยสูง ได้แก่ Smart Card, Token, Hardware Security Module : HSM เป็นต้น ร่วมกับใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกและรับรองโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: CA) ที่ได้รับมาตรฐานสากล (Trusted Third-Party Certification Authority) ในการเข้ารหัสข้อมูลที่รับ-ส่งระหว่างกันเพื่อพิสูจน์และยืนยันตัวบุคคลของผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์

๔.๒ ผู้ใช้งานข้อมูลที่เป็นความลับต้องปฏิบัติตามระเบียบและเงื่อนไขการขอใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอย่างเคร่งครัด โดยต้องกรอกแบบฟอร์มคำขอใบรับรองอิเล็กทรอนิกส์พร้อมยื่นหลักฐานยืนยันตัวตน ประกอบด้วย สำเนาบัตรประจำตัวประชาชนของผู้ขอใบรับรอง พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

๔.๓ กรณีมอบหมายให้บุคคลอื่นทำหน้าที่แทนในการรับและส่งข้อมูลจะต้องมีหนังสือมอบอำนาจพร้อมติดอากรแสตมป์ ๓๐ บาท ตามจำนวนผู้รับมอบอำนาจพร้อมสำเนาบัตรประจำตัวประชาชนของผู้รับมอบอำนาจเพิ่มเติม

๔.๔ ผู้ขอใบรับรองต้องลงนามในแบบตอบรับใบรับรองอิเล็กทรอนิกส์เพื่อเปิดใช้งาน (Activate) หลังจากที่ส่งคำขอและได้แบบตอบรับ

๔.๕ ผู้ขอใบรับรองมีหน้าที่ดูแลและเก็บรักษารหัสลับ (Private Key) ที่บันทึกอยู่ในอุปกรณ์ตามข้อ ๔.๑ โดยห้ามมิให้บุคคลอื่นซึ่งไม่มีอำนาจหรือหน้าที่ที่เกี่ยวข้องใช้รหัสลับดังกล่าว และหากกรณี Private Key สูญหายหรือถูกล่วงรู้ไปถึงบุคคลอื่นซึ่งไม่มีอำนาจหรือหน้าที่ที่เกี่ยวข้อง ผู้ขอใบรับรองมีหน้าที่ที่จะต้องแจ้งต่อหน่วยงานรับลงทะเบียนของผู้ให้บริการออกใบรับรองโดยทันที

๔.๖ ผู้ขอใบรับรองต้องไม่นำใบรับรองอิเล็กทรอนิกส์ไปใช้ในทางที่ขัดต่อกฎหมายและความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รวมทั้งต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติ (CP&CPS) ของผู้ให้บริการออกใบรับรอง

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๑. การใช้งานบริการเครือข่ายของสำนักงาน กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น ได้แก่ ๑) ระบบอินเทอร์เน็ต (Internet) ๒) ระบบไปรษณีย์อิเล็กทรอนิกส์ (e-mail) และ ๓) เครือข่ายสังคมออนไลน์ (Social Network : LINE, Facebook, Twitter) เป็นต้น โดยมีข้อปฏิบัติในการควบคุมการเข้าถึงเครือข่าย ดังนี้

๑.๑ ระบบอินเทอร์เน็ต (Internet)

(๑) กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สำนักงานจัดสรรไว้เท่านั้น ได้แก่ Proxy , firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น โดยการใช้ Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น

(๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

(๓) ผู้ใช้งานต้องไม่ใช้เครือข่ายระบบอินเทอร์เน็ตของสำนักงาน เพื่อแสวงหาประโยชน์ในเชิงธุรกิจส่วนตัว หรือทำการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม ละเมิดสิทธิของผู้อื่น เป็นข้อมูลที่อาจก่อความเสียหายและส่งผลกระทบต่อหน่วยงานได้

(๔) การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือเว็บไซต์ที่ขัดต่อศีลธรรม หรือเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน

(๕) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน โดยผ่านความเห็นชอบจากผู้อำนวยการสำนัก/กลุ่ม/ศูนย์

(๖) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

(๗) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

(๘) การใช้งานเว็บบอร์ด (Web Board) ของสำนักงาน ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

(๙) หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบโดยปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ที่ไม่ได้รับอนุญาต

(๑๐) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

(๑๑) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

๑.๒ <u>ระบบไปรษณีย์อิเล็กทรอนิกส์</u> (e-mail)

(๑) ผู้ใช้งานที่ต้องการใช้ระบบ e-mail ของสำนักงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศเพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Username and Password)

(๒) เปลี่ยนรหัสผ่านโดยทันที หลังจากการเข้าสู่ระบบเป็นครั้งแรก

(๓) เก็บรักษาชื่อผู้ใช้และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง และปฏิบัติตามวิธี<u>การใช้งานรหัสผ่าน</u> (Password Use) และ<u>การเปลี่ยนรหัสผ่าน</u> (Change Password) ที่ได้กำหนดไว้อย่างเคร่งครัด

(๔) ใช้ e-mail ของสำนักงานเพื่อติดต่องานของราชการเท่านั้น

(๕) ไม่ใช้ e-mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ e-mail และให้ถือว่าเจ้าของ e-mail เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน e-mail ของตน

(๖) ไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๗) ผู้ใช้งานพึงระมัดระวังการใช้ e-mail เพื่อไม่ให้เกิดความเสียหายต่อสำนักงานหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ e-mail ผ่านระบบเครือข่ายของสำนักงาน

(๘) ไม่ระบุความสำคัญของข้อมูลลงบนหัวข้อไปรษณีย์อิเล็กทรอนิกส์ กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ

(๙) ตรวจสอบไฟล์เอกสารแนบที่มาจาก e-mail โดยใช้โปรแกรมป้องกันไวรัสทุกครั้งก่อนเปิดไฟล์ที่เป็น Executable File (ไฟล์นามสกุล .exe, .com)

(๑๐) หลังจากการใช้งาน e-mail เสร็จสิ้น ต้องทำการ Logout ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานไปรษณีย์อิเล็กทรอนิกส์

(๑๑) ไม่เปิดหรือส่งต่อ e-mail หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๒) ตรวจสอบ e-mail ของตนเองทุกวัน จัดเก็บแฟ้มข้อมูลและ e-mail ของตนให้เหลือจำนวนน้อยที่สุด และลบ e-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ในระบบ

๑.๓ <u>เครือข่ายสังคมออนไลน์</u> (Social Network : LINE, Facebook, Twitter)

(๑) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่สำนักงานได้กำหนดไว้เท่านั้น

(๒) ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับสำนักงานจากการใช้งานเครือข่ายสังคมออนไลน์

(๓) หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับสำนักงาน ผู้ใช้งานต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๒. <u>การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกสำนักงาน</u> (User Authentication for External Connections) ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของสำนักงาน มีแนวทางปฏิบัติ ดังนี้

๒.๑ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๒.๒ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๒.๓ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน

๒.๔ การเข้าสู่ระบบสารสนเทศของสำนักงานจากระบบอินเทอร์เน็ตนั้น ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๒.๕ การใช้งานระบบอินเทอร์เน็ตเพื่อเข้ามายังระบบสารสนเทศของสำนักงาน ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN เป็นต้น

๒.๖ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ หรือเครือข่ายระบบอินเทอร์เน็ต หรือเครือข่ายไร้สาย

๒.๗ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๒.๘ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๓. <u>การระบุอุปกรณ์บนเครือข่าย</u> (Equipment Identification In Networks)

มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง มีข้อปฏิบัติดังนี้

๓.๑ กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๓.๒ มีการควบคุมการใช้งานอย่างเหมาะสม

(๑) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๒) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับอนุมัติจากสำนักงานและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๓) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

(๔) การบริหารจัดการ การบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก โดยบันทึกการเข้า/ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

(๕) มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (เก็บ Log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๓.๓ จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(๑) กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

(๒) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๔. <u>การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ</u> (Remote Diagnostic And Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย มีข้อปฏิบัติดังนี้

๔.๑ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของสำนักงาน ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔.๒ IP Address ของระบบงานเครือข่ายภายในสำนักงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศได้โดยง่าย

๔.๓ หากผู้บริหารระบบ (Administrator) จำเป็นต้องใช้งานผ่านพอร์ต ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๔.๔ แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

๔.๕ กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

๔.๖ ปิดการใช้งานเพื่อป้องกันพอร์ตที่ไม่มีการใช้งาน

๔.๗ ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๕. <u>การแบ่งแยกเครือข่าย</u> (Segregation In Networks)

มีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่ออำนวยความสะดวกในการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ ดังนี้

๕.๑ เครือข่ายภายนอก

๕.๒ เครือข่ายสาธารณะ

๕.๓ เครือข่ายภายในสำนักงาน

๕.๔ เครือข่ายไร้สาย

๖. <u>การควบคุมการเชื่อมต่อทางเครือข่าย</u> (Network Connection Control)

๖.๑ ระบบเครือข่ายทั้งหมดของสำนักงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

๖.๒ ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy, Firewall, และ IPS/IDS เป็นต้น

๖.๓ การควบคุมการเข้าถึงระบบเครือข่ายภายในของสำนักงาน

(๑) การเข้าสู่ระบบเครือข่ายภายในของสำนักงาน โดยผ่านทางระบบอินเทอร์เน็ตจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ก่อนที่จะสามารถใช้งานได้ทุกกรณี

(๒) การเข้าสู่ระบบเครือข่ายภายในสำนักงาน ผ่านทางระบบอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๖.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

(๑) ผู้ใช้ต้องการเข้าถึงระบบเครือข่ายไร้สายของสำนักงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตามความจำเป็นในการใช้งาน

(๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๗. <u>การควบคุมการจัดเส้นทางบนเครือข่าย</u> (Network Routing Control)

๗.๑ กำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้บริหารจัดการสิทธิให้แก่ผู้ใช้งานในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๗.๒ ผู้ใช้งานมีสิทธิในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิที่ได้รับอนุญาตตามภารกิจหน้าที่ของตนเองเท่านั้น

๗.๓ กำหนดหมายเลขเครือข่าย (IP Address) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อแสดงตัวตนและควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือ

การประยุกต์ใช้งานตามภารกิจ โดยผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบเครือข่ายทุกครั้ง และห้ามมิให้เปิดเผยหมายเลขเครือข่าย (IP Address) แก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้องกับการใช้หมายเลขเครือข่ายดังกล่าว

๗.๔ กำหนดบุคคลที่รับผิดชอบในการกำหนด หรือแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งผู้ดูแลระบบเครือข่ายให้รับทราบทุกครั้ง

๗.๕ บริหารจัดการระบบเครือข่ายโดยการแปลงหมายเลขเครือข่ายเพื่อแบ่งแยกเครือข่ายย่อย เพื่อจำกัดสิทธิในการใช้งานระบบเครือข่ายร่วมกันภายในหน่วยงาน (สำนัก/กลุ่ม/ศูนย์) ที่มีภารกิจหน้าที่เดียวกัน ได้แก่ การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่าย เป็นต้น

๗.๖ ระบบเครือข่ายที่มีความจำเป็นต้องเชื่อมต่อไปยังเครือข่ายภายนอกสำนักงาน จะต้องทำการเชื่อมต่อกับอุปกรณ์รักษาความปลอดภัย (Firewall) และติดตั้งระบบป้องกันการรุกราน (Intrusion Prevention System : IPS)

๗.๗ ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายมาติดตั้งโดยมิได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๗.๘ กำหนดมาตรการบังคับใช้เส้นทางเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อจำกัดการใช้เส้นทางบนเครือข่ายโดยทำการเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ เพื่อควบคุมการเข้าใช้งานระบบเครือข่ายจากภายนอก มีข้อปฏิบัติดังนี้

(๑) การเข้าสู่ระบบเครือข่ายจากระยะไกล (Remote Access) ให้ใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องมีการควบคุมอย่างเข้มงวด และต้องได้รับการอนุมัติใช้ระบบเครือข่ายจากระยะไกลจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือบุคคลที่ได้รับมอบหมายจากสำนักงานก่อนทุกครั้ง

(๒) การให้สิทธิในการเข้าสู่ระบบเครือข่ายจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานพร้อมระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือบุคคลที่ได้รับมอบหมายจากสำนักงานก่อนทุกครั้ง และการอนุญาตให้ผู้ใช้เข้าสู่ระบบเครือข่ายจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

(๓) ควบคุมพอร์ต (Port) ที่ใช้เชื่อมต่อเข้าสู่ระบบเครือข่ายอย่างรัดกุม ไม่เปิด Port ทิ้งไว้โดยไม่จำเป็น และให้ตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗.๙ ใช้ข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อควบคุมและติดตามผู้ใช้งานระบบ ดังนี้

(๑) กำหนดให้ผู้ดูแลระบบเครือข่ายมีหน้าที่ความรับผิดชอบในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ลงบนสื่อเก็บข้อมูลที่รักษาความครบถ้วน ถูกต้อง แท้จริง โดยข้อมูลสามารถระบุถึงตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยกำหนดชั้นความลับในการเข้าถึงเพื่อป้องกันและจำกัดสิทธิการเข้าถึงเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ห้ามแก้ไขหรือเปลี่ยนแปลงข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย

(๒) บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของสำนักงาน จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้ กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงานโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย กำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ มีข้อปฏิบัติดังนี้

๑. <u>การควบคุมการเข้าถึงระบบปฏิบัติการ</u>

กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๑.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๑.๒ ผู้ใช้ต้องกำหนดรหัสผ่านที่มีคุณภาพดี (Good Password)

๑.๓ ผู้ใช้ต้องทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่ที่หน้าจอ

๑.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบสารสนเทศทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. <u>การระบุและยืนยันตัวตนของผู้ใช้งาน</u> (User Identification and Authentication)

กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง มีข้อปฏิบัติดังนี้

๒.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๒.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) โดยระบบมีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๒.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Smart Card ร่วมได้

๓. <u>การบริหารจัดการรหัสผ่าน</u> (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ มีข้อปฏิบัติดังนี้

๓.๑ มีระบบบริหารจัดการรหัสผ่านซึ่งจะติดตั้งบนระบบเครือข่ายสารสนเทศของสำนักงาน โดยระบบจะยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๓.๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ และให้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ที่ได้กำหนดไว้

๓.๓ มีระบบแจ้งระดับความความปลอดภัยของรหัสผ่าน

๔. <u>การใช้งานโปรแกรมอรรถประโยชน์</u> (User of System Utilities)

เพื่อป้องกันการละเมิดลิขสิทธิ์หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว เนื่องจากการใช้งานซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกหรือโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้และมีความเสี่ยงในการใช้งานโปรแกรมไม่ประสงค์ดี จึงต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ มีข้อปฏิบัติดังนี้

๔.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๔.๒ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

๔.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก หากไม่ได้ใช้งานเป็นประจำ

๔.๔ มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๔.๕ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๔.๖ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกสำนักงานที่ไม่มีลิขสิทธิ์ รวมทั้งการใช้ไฟล์อื่น ๆ ที่ไม่อนุญาตให้ใช้งาน

๔.๗ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๔.๘ ให้ติดตั้งซอฟต์แวร์ เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศ

๔.๙ กำหนดหน้าที่ความรับผิดชอบ ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ

๔.๑๐ มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๔.๑๑ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดี ว่าต้องดำเนินการอย่างไร

๕. <u>การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน</u> (Session Time-out)

๕.๑ ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่าย มีการยกเลิก และหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๕.๓ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง โดยเฉพาะระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๔ ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๕.๕ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง มีข้อปฏิบัติดังนี้

๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น และกำหนดให้ระบบยกเลิกการเชื่อมต่อหากผู้ใช้งานไม่มีการใช้งานเกิน ๓๐ นาที

๖.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ หรือระบบงานที่มีความสำคัญสูง หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖.๓ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application And Information Access Control)

๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยกำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ดังนี้

๑.๑ ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ

(๑) กำหนดประเภทของข้อมูลและสารสนเทศตามแนวทางปฏิบัติ ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

(๒) ขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับต้องประกอบด้วยวิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำป้ายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

(๓) ให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๔) มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

(๕) มีความตระหนัก และมาตรการป้องกันข้อมูลสำคัญที่มีการสั่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น

(๖) จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๑.๒ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security Of System Documentation)

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ (อินเทอร์เน็ต) เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๑.๓ กำหนดขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures)

(๑) จัดทำแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่างสำนักงานกับหน่วยงานภายนอก โดยห้ามใช้เพื่อก่อความรำคาญแก่ผู้อื่น หรือทำให้ผู้อื่นสูญเสียชื่อเสียง หรือการปลอมเป็นบุคคลอื่น

(๒) มีวิธีการทางเทคนิคป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลงแก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

(๓) จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่สำนักงานต้องปฏิบัติตาม

๑.๔ ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreement) จัดทำแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างสำนักงานกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูล ที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล (การรับ/ส่งข้อมูล)

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญเสียหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ โดยการใช้กุญแจที่ใช้ในการเข้ารหัส (Token Key) หรือการใช้เทคนิคพิเศษในการเข้ารหัสหรือการแปลงรหัส

๑.๕ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)

พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกันระหว่างสำนักงาน หรือหน่วยงานที่ประสงค์จะเชื่อมโยง มีดังต่อไปนี้

(๑) กำหนดมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรืออนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้ใช้งานข้อมูลสำคัญหรือลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๑.๖ <u>การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ</u> (Audit Logging)

บันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลชื่อเทอร์มินัล

(๖) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๘) ข้อมูลการเปลี่ยนคอนฟิกูเรชัน (Configurations) ของระบบ

(๙) ข้อมูลแสดงการใช้สิทธิของผู้ดูแลระบบ

(๑๐) ข้อมูลแสดงการใช้งานแอปพลิเคชัน

(๑๑) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ ได้แก่ เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๒) ข้อมูล IP Address ที่เข้าถึง

(๑๓) ข้อมูลโปรโตคอลเครือข่ายที่ใช้

(๑๔) ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบ

(๑๕) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(๑๖) ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ ๆ

(๑๗) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑.๗ <u>การพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก</u>

(๑) ควรจัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างหรือผู้ให้บริการภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๑.๘ <u>มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)</u> กรณีมีการว่าจ้างเหมาผู้ให้บริการภายนอกเข้ามาดำเนินการพัฒนา บำรุงรักษาระบบสารสนเทศและระบบเครือข่ายของสำนักงาน กำหนดมาตรการควบคุมดังนี้

๑.๘.๑ การคัดเลือกผู้ให้บริการภายนอก

(๑) กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอก และคัดเลือกผู้ให้บริการภายนอกที่มีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และเป็นที่น่าเชื่อถือ

(๒) สัญญาต้องระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

๑.๘.๒ การควบคุมผู้ให้บริการภายนอก

(๑) ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของสำนักงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒) กรณีที่ใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ โดยให้เจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการภายนอกอย่างใกล้ชิดในกรณีที่ผู้ให้บริการภายนอกมาปฏิบัติหน้าที่ที่สำนักงาน (Onsite Service) และให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการภายนอกอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ทันทีที่การให้บริการเสร็จสิ้น

(๓) การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวจะตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานและจะเปิดให้ใช้ได้เมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

(๔) ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงาน โดยทันที ภายในระยะเวลาที่กำหนดไว้

(๕) ดำเนินการเพิกถอน ลบ หรือเปลี่ยนรหัสผ่านของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

(๖) ดำเนินการลบหรือเปลี่ยนชื่อของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงาน ออกจากเอกสารต่าง ๆ ของสำนักงานที่มีชื่อของบุคคลดังกล่าวอยู่ในนั้น

(๗) ดำเนินการให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(๘) กำหนดให้ผู้ให้บริการภายนอกรายงานการปฏิบัติงาน ปัญหาต่าง ๆ ที่เกิดขึ้นหรือมีโอกาสที่จะเกิดขึ้นได้พร้อมแนวทางแก้ไข

(๙) มีขั้นตอนในการตรวจรับงานของผู้ให้บริการภายนอก

๒. <u>การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน</u>

ระบบซึ่งไวต่อการรบกวน ระบบที่มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน ได้แก่ ระบบสารสนเทศสถาบันการเงินและสถาบันการเงินเฉพาะกิจซึ่งมีการแลกเปลี่ยนและรับส่งข้อมูลด้านการเงินกับธนาคารแห่งประเทศไทย สถาบันการเงินและสถาบันการเงินเฉพาะกิจตามช่วงระยะเวลาที่กำหนดในบันทึกข้อตกลงความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง เป็นต้น ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ และหากจำเป็นต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ รวมถึงการปฏิบัติงานจากภายนอกสำนักงาน (Mobile Computing and Teleworking) มีข้อปฏิบัติดังนี้

๒.๑ จัดให้มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ห้องปฏิบัติการคอมพิวเตอร์ ดังนี้

(๑) กำหนดระเบียบหรือแนวทางปฏิบัติในการเข้า-ออกพื้นที่ห้องปฏิบัติการคอมพิวเตอร์

(๒) ควบคุมการเข้า-ออก ด้วยระบบ Hand Scan และระบบ Finger Print พร้อมระบบ CCTV

(๓) ติดตั้งระบบสำรองกระแสไฟฟ้า (UPS)

(๔) จัดหาเครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๕) ติดตั้งระบบระบายอากาศ

(๖) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

(๗) ติดตั้งระบบดับเพลิง ระบบตรวจสอบควันไฟและน้ำรั่วซึม

๒.๒ มีการสำรองข้อมูลและกู้คืนระบบคอมพิวเตอร์ (Backup And Recovery) ระบุไว้ในแผนสำรองข้อมูลและระบบสารสนเทศ

๒.๓ มีแผนฉุกเฉิน กรณีระบบคอมพิวเตอร์ขัดข้อง ระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

๒.๔ มีแผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติ ระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

๒.๕ ในระบบที่มีผลกระทบและความสำคัญสูงต่อสำนักงาน หากต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ ซึ่งมิใช่ทรัพย์สินของสำนักงานต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๓. <u>การควบคุมอุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่</u> (Mobile Computing and Teleworking)

กำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ รวมถึงการดูแลรักษาความปลอดภัยในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ดังนี้

๓.๑ <u>การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล</u> (Use of Personal Computer)

๓.๑.๑ <u>แนวทางปฏิบัติในการใช้งานทั่วไป</u>

(๑) เครื่องคอมพิวเตอร์ที่สำนักงาน อนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของสำนักงาน ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสำนักงานต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสำนักงานเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองใช้งานเมื่อใช้งานเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของสำนักงาน ยกเว้นจะได้รับการตรวจสอบจากศูนย์เทคโนโลยีสารสนเทศก่อนการใช้งาน

๓.๑.๒ แนวทางปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ได้กำหนดไว้

๓.๑.๓ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ ได้แก่ Hard Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับไปรษณีย์อิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนด

๓.๑.๔ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓.๒ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook computer) และอุปกรณ์สื่อสารเคลื่อนที่

๓.๒.๑ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ที่สำนักงานอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของสำนักงาน ดังนั้น ผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การตกจากโต๊ะทำงาน หรือหลุดมือ

(๖) หลีกเลี่ยงการใช้นิ้ว หรือของแข็ง หรือปลายปากกา นำไปสัมผัสหน้าจอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงานซึ่งอาจทำให้แตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินของสำนักงานมาใช้กับระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศก่อนการใช้งาน

๓.๒.๒ <u>ความปลอดภัยทางด้านกายภาพ</u>

(๑) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหายโดยจะต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน และไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้ต้องไม่เก็บ หรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น หรือฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๓.๒.๓ <u>แนวทางปฏิบัติในการใช้งานรหัสผ่าน</u>

ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่าน

๓.๒.๔ <u>การสำรองข้อมูลและการกู้คืน</u>

(๑) ผู้ใช้ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงาน โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้จะต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่มีความเสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๔. <u>การปฏิบัติงานจากภายนอกสำนักงาน</u> (Teleworking)

ศูนย์เทคโนโลยีสารสนเทศ กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในสำนักงาน เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก มีข้อปฏิบัติดังนี้

๔.๑ ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกสำนักงาน

๔.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสำนักงาน การควบคุมบุคคลที่เข้าสู่ระบบของสำนักงานจากระยะไกล ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๔.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๔.๔ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอและต้องได้รับการอนุมัติจากสำนักงาน

๔.๕ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องเหมาะสมแล้วเท่านั้น

๔.๖ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

ส่วนที่ ๙ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

๑. <u>การคัดเลือกและจัดทำระบบสำรองสำหรับระบบสารสนเทศ</u>

ระบบสารสนเทศที่สำคัญที่ได้พิจารณาคัดเลือกจัดทำระบบสำรอง ได้แก่ ๑) ระบบงาน e-Office ประกอบด้วย ระบบงานสารบรรณอิเล็กทรอนิกส์ ระบบการลงเวลาการปฏิบัติงาน ระบบการลา และระบบ e-Learning ๒) ระบบงาน Back Office ประกอบด้วย ระบบจองรถ ระบบจองห้องประชุม และระบบการเบิกจ่ายพัสดุ ๓) ระบบการจัดเก็บเอกสาร ๔) ระบบเว็บไซต์ของสำนักงาน และ ๕) ระบบห้องสมุดอิเล็กทรอนิกส์ (e-Library) โดยนำข้อมูลไปเก็บสำรองไว้ที่ศูนย์สำรองข้อมูล (DR Site) ตามวิธีการและข้อปฏิบัติของกระทรวงการคลัง

สำหรับระบบสารสนเทศอื่นที่ไม่ได้จัดเก็บสำรองไว้ที่ศูนย์สำรองข้อมูล (DR Site) ของกระทรวงการคลัง หากมีความจำเป็นต้องทำการสำรองข้อมูลเก็บไว้ มีข้อปฏิบัติดังนี้

๑.๑ กำหนดรายละเอียดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ ประกอบด้วยข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการและซอฟแวร์อื่น ๆ ที่เกี่ยวข้อง เป็นต้น

๑.๒ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง

๑.๓ กำหนดวิธีการสำรองแบบ Full Backup หรือ Incremental Backup ที่เหมาะสมกับระบบงาน โดยคำนึงถึงความสำคัญของระบบงานและข้อมูลสารสนเทศของระบบงานนั้น

๑.๔ เตรียมอุปกรณ์ที่จำเป็นต่อการสำรองข้อมูล และการกู้คืนข้อมูล

๑.๕ ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไว้นั้นมีความครบถ้วน

๑.๖ ต้องนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๒. <u>การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน</u>

๒.๑ ระบุวัตถุประสงค์หลักของแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒.๒ จัดทำบัญชีรายชื่อของระบบงานที่มีความสำคัญ รวมทั้งปรับปรุงบัญชีรายชื่อดังกล่าวให้มีความทันสมัยอยู่เสมอ

๒.๓ กำหนดปัจจัยเสี่ยงและภัยพิบัติที่อาจส่งผลกระทบกับระบบงานที่สำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบในกรณีต่าง ๆ ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒.๔ ประเมินสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๕ จัดทำแผนกู้คืนเพื่อรับมือกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๒.๕.๑ กำหนดหน้าที่ความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๒.๕.๒ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน โดยมีแนวทางและข้อปฏิบัติตามแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency plan)

๒.๕.๓ การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก หรือผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เมื่อเกิดเหตุจำเป็นต้องติดต่อ

๒.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๗ ให้ทำการปรับปรุงแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง

๒.๘ ให้จัดประชุมและแจ้งให้ผู้เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งเมื่อมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

๓. <u>การกำหนดหน้าที่และความรับผิดชอบของบุคลากร</u>

กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ระบุไว้ในแผนบริหารความเสี่ยงเพื่อความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ แผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan) แผนสำรองข้อมูลและระบบสารสนเทศ

๔. <u>การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน</u>

ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง โดยดำเนินการดังนี้

๔.๑ ทำการตรวจสอบว่าระบบสำรองที่เกิดขึ้นนั้นได้กระทำสำเร็จครบถ้วน หรือไม่

๔.๒ ให้ทำการตรวจสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีแก้ไขอย่างเป็นลายลักษณ์อักษร

๕. <u>ระยะความถี่ของการปฏิบัติ</u>

๕.๑ ระยะความถี่การสำรองข้อมูลของระบบงาน ขึ้นอยู่กับความสำคัญของระบบ และสภาพการเปลี่ยนแปลงของระบบงานนั้น ๆ โดยระบบงานที่มีการเปลี่ยนแปลงบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๕.๒ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ และความพร้อมในการใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๕.๓ ให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศเพื่อป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ มีข้อปฏิบัติดังนี้

๑. <u>มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ</u> มีเนื้อหาอย่างน้อยดังนี้

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

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของสำนักงาน (Internal Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

๒. <u>แนวทางในการตรวจสอบและประเมินความเสี่ยง</u> ต้องดำเนินการอย่างน้อยดังนี้

๒.๑ ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ ตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ มีขั้นตอนอย่างน้อยดังนี้

(๑) จัดลำดับความสำคัญของความเสี่ยง

(๒) ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

(๓) ข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

(๔) สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๒.๔ การตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยให้ครอบคลุมหัวข้ออย่างน้อยต่อไปนี้

(๑) การตรวจสอบและประเมินด้านการบริหารสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(๒) การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

(๓) การตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการ

(๔) การตรวจสอบและประเมินการควบคุมการเข้าถึง

(๕) การตรวจสอบและประเมินการพัฒนาระบบ จัดซื้อจัดหาระบบ และการดูแลรักษาระบบ

(๖) การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์

๒.๕ มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อยดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log ที่แสดงการเข้าถึงนั้นซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) กรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต
