ประกาศสำนักงานปลัดกระทรวงการคลัง
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการคลัง
พ.ศ. ๒๕๕๙

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินการต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล สำนักงานปลัดกระทรวงการคลังจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการคลัง โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. ๒๕๕๙”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓. สำนักงานปลัดกระทรวงการคลังได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง เป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ ประกอบด้วยเนื้อหาอย่างน้อยครอบคลุมตามประกาศนี้มี ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดในข้อ ๔

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดในข้อ ๕ - ๑๕

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มีดังนี้

๔.๑ การจัดทำนโยบายต้องมีผู้บริหาร เจ้าหน้าที่ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

๔.๒ นโยบายต้องจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงานปลัดกระทรวงการคลัง

๔.๓ มีการกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวไว้ชัดเจน

๔.๔ มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๕ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๔.๖ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๔.๗ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

๔.๘ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๔.๙ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔.๑๐ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑๑ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๔.๑๒ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๕. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) ประกอบด้วย

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

๕.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๕.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ซึ่งได้รับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ประกอบด้วย

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ประกอบด้วย

๗.๑ การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘. การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ประกอบด้วย

๘.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และ

การส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ประกอบด้วย

๙.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๙.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (application and information access control) ประกอบด้วย

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

๑๑.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

๑๑.๒ หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๑๑.๓ สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๑๑.๔ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

ข้อ ๑๒. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ประกอบด้วย

๑๒.๑ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๒.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑๒.๖ มีศูนย์คอมพิวเตอร์สำรองซึ่งตั้งอยู่ในสถานที่ที่ปลอดภัยพร้อมระบบคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน

ข้อ ๑๓. การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ประกอบด้วย

๑๓.๑ ต้องมีการจัดทำแผนด้านระบบสารสนเทศ

๑๓.๒ ต้องมีการจัดทำแผนด้านระบบคอมพิวเตอร์และระบบเครือข่าย

๑๓.๓ ต้องมีการจัดทำแผนด้านบุคลากรผู้รับผิดชอบ สถานที่ในการปฏิบัติงาน เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน

ข้อ ๑๔. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

๑๔.๑ ต้องมีการจัดทำแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

๑๔.๒ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๔.๓ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดย ผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๕. สำนักงานปลัดกระทรวงการคลัง กำหนดความรับผิดชอบให้เป็นไปตามเอกสารแนบท้ายประกาศ ส่วนที่ ๖

๑๕.๑ ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

๑๕.๒ ระดับปฏิบัติ

๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ
ผู้รับผิดชอบ ได้แก่
๑.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๑.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน ผู้รับผิดชอบ ได้แก่
๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๒.๓) ผู้ใช้งาน

๓) การควบคุมการเข้าถึงเครือข่าย ผู้รับผิดชอบ ได้แก่
๓.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๓.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๓.๓) ผู้ใช้งาน

๔) การควบคุมการเข้าถึงระบบปฏิบัติการ ผู้รับผิดชอบ ได้แก่
๔.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๕) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
ผู้รับผิดชอบ ได้แก่
๕.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๕.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๖) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
ผู้รับผิดชอบ ได้แก่
๖.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๖.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๖.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๗) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
ผู้รับผิดชอบ ได้แก่
๗.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๘) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

๘.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๘.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๙) การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ผู้รับผิดชอบ ได้แก่

๙.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๙.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐)การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑๐.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๐.๒) ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๑๐.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๑)นโยบายการสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑๑.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๑.๓) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๑๖. องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. ๒๕๕๙” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของหน่วยงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๑๕ มิถุนายน พ.ศ. ๒๕๕๙

(นายสมชัย สัจจพงษ์)
ปลัดกระทรวงการคลัง

เอกสารแนบ ๒

เอกสารแนบท้ายประกาศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานปลัดกระทรวงการคลัง พ.ศ. ๒๕๕๙

สารบัญ

คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัติฯ นี้ ประกอบด้วย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศของสำนักงานปลัดกระทรวงการคลัง ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (username) และรหัสผ่าน (password)

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงการคลัง การป้องกันข้อมูลที่เป็นความลับ ความถูกต้องครบถ้วนของข้อมูล และความพร้อมใช้งานของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์อิเล็กทรอนิกส์สื่อสารพกพา

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)” หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

“ชื่อโดเมนย่อย (Sub Domain Name)” หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

“ชื่อผู้ใช้งาน (Username)” หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

“ดับเบิ้ลยู พี เอ WPA (Wi-Fi Protected Access)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

“ดับเบิ้ลยู อี พี WEP (Wired Equivalent Privacy)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“โทเค็น คีย์ (Token Key)” หมายความว่า อุปกรณ์ที่ใช้เก็บข้อมูล Digital Certificate รูปแบบหนึ่ง ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานเพื่อแสดงว่าเป็นบุคคลนั้นจริง ให้เข้าถึงฐานข้อมูลสารสนเทศของหน่วยงานได้ อุปกรณ์สามารถใช้งานได้ผ่านพอร์ต USB ของเครื่องคอมพิวเตอร์ ซึ่งมีลักษณะภายนอกคล้าย กับ Thump drive แต่ไม่ใช่ Thumb drive โดยผู้ใช้งานจะต้องมีอุปกรณ์ Token Key และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตน

“บัญชีผู้ใช้บริการ (Account)” หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

“บิตทอร์เรนต์ (BitTorrent)” หมายความว่า เป็นการสื่อสารที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์ด้วยกันโดยตรง ผ่านเครือข่ายอินเทอร์เน็ต

“โปรแกรมประสงค์ร้าย (Malware)” หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาให้มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

“ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของสำนักงานปลัดกระทรวงการคลังและสำนักงานรัฐมนตรี รวมถึงผู้รับบริการ ผู้ใช้งานอื่นๆ ทั่วไป ที่สำนักงานปลัดกระทรวงการคลังอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงการคลังได้

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานปลัดกระทรวงการคลัง

“ผู้บริหารระดับสูงสุด” หมายความว่า ปลัดกระทรวงการคลัง

“ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ” หมายความว่า ปลัดกระทรวงการคลังหรือผู้ที่ปลัดกระทรวงการคลังมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

“ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ผอ.ศทส.)” หมายความว่า ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง หรือผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

“แผนผังระบบเครือข่าย (Network Diagram)” หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

“ไฟร์วอลล์ (Firewall)” หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

“แม็ค แอดเดรส MAC Address (Media Access Control Address)” หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

“ระบบแลน LAN (Local Area Network)” และ **“ระบบอินทราเน็ต (Intranet)”** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

“รหัสผ่าน (Password)” หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“เลขที่อยู่ไอพี (IP Address)” หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

“ลงบันทึกเข้า (Login)” หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อ ผู้ใช้ (username) และรหัสผ่าน (password) ให้ถูกต้อง

“ลงบันทึกออก (Logout)” หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

“วี พี เอ็น VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“เว็บเซอร์ฟเวอร์ (Web Server)” หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

“ศูนย์ฯ” หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และระบบเครือข่ายขององค์กร

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“สารสนเทศ (Information)” หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงานปลัดกระทรวงการคลัง

“สินทรัพย์” หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ซอฟต์แวร์โปรแกรมประยุกต์ที่หน่วยงานพัฒนาขึ้น รวมทั้งสิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

“สื่อบันทึกพกพา” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

“หน่วยงาน” หมายความว่า สำนักงานปลัดกระทรวงการคลัง ทั้งนี้ให้หมายรวมถึงสำนักงานรัฐมนตรี

“หน่วยงานภายนอก” หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“อัพเดท (Update)” หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

“อีมูล (Emule)” หมายความว่า เป็นโปรแกรมสำหรับใช้กับ ระบบ P2P (ระบบแชร์ไฟล์ คล้าย Bit) แต่จะมีระบบ Search Engine มี Server ให้เลือกเข้า Download มากมาย และแต่ละ Server มีการแชร์ไฟล์ด้วยกันเอง ทำให้หาไฟล์ได้โดยไม่จำเป็นต้องมีใน Server นั้นอย่างเดียว

“อุปกรณ์กระจายสัญญาณข้อมูล (Switch)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

“อุปกรณ์จัดเส้นทาง (Router)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“เอสเอสไอดี SSID (Service Set Identifier) ” หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

ส่วนที่ ๑
นโยบายและแนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้ผู้รับผิดชอบ และผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานได้รับรู้เข้าใจ นโยบายในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของสำนักงานปลัดกระทรวงการคลัง และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

๒.๒.๑ ผู้ดูแลระบบเครือข่าย (System Network)

๒.๒.๒ ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

๒.๒.๓ ผู้ดูแลระบบ (System Administrator)

๒.๒.๔ ผู้พัฒนาระบบ (System Developer)

๒.๒.๕ ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๒.๒.๖ เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

๒.๓ เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๒.๔ ผู้ใช้งาน

๓. แนวนโยบายและแนวปฏิบัติ

สำนักงานปลัดกระทรวงการคลังมีแนวนโยบายและแนวปฏิบัติด้านต่าง ๆ ดังต่อไปนี้

๓.๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๓.๑.๑ แนวนโยบาย

(๑) ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๒) มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓) มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

(๔) มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

(๕) การเข้าถึงระบบด้วยการ Remote User ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบ จากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เท่านั้น

(๖) ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆ ในทางที่ผิดตามประกาศของสำนักงานปลัดกระทรวงการคลัง

(๗) การควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานได้จัดแบ่งประเภทของข้อมูลออกเป็นสองประเภท คือ

(๗.๑) ข้อมูลสารสนเทศด้านการบริหารราชการ ได้แก่ ข้อมูลการบริหารทรัพยากรบุคคล ข้อมูลเศรษฐกิจการคลัง ข้อมูลนโยบายและแผน ข้อมูลตรวจสอบ

(๗.๒) ข้อมูลสารสนเทศด้านการสนับสนุน ได้แก่ ข้อมูลงานสารบรรณ ข้อมูลข่าวสารประชาสัมพันธ์ กฎหมาย ระเบียบ ประกาศ สถิติ

(๘) ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบสารสนเทศนั้น ๆ ด้วย

(๙) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๑๐)กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑๐.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

(๑๐.๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๑๐.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑.๒ แนวทางปฏิบัติ

หน่วยงานได้กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ การจัดแบ่งระดับการเข้าถึงข้อมูลและสิทธิ เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

(๑) การจัดแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- อ่านอย่างเดียว (Read Only)
- สร้างข้อมูล (Create)
- แก้ไข (Edit)
- ลบ (Delete)

- อนุมัติ (Authorize)

(๒) การจัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ ระดับความสำคัญมากที่สุด ระดับความสำคัญปานกลาง ระดับความสำคัญน้อย

(๓) การจัดแบ่งลำดับชั้นความลับของข้อมูล ได้แก่

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ได้แก่

- ระดับชั้นสำหรับผู้บริหารระดับสูง หมายถึง รัฐมนตรีว่าการกระทรวงการคลัง รัฐมนตรีช่วยว่าการกระทรวงการคลัง ที่ปรึกษารัฐมนตรีฯ ปลัดกระทรวงการคลัง รองปลัดกระทรวงการคลัง ผู้ตรวจราชการ ที่ปรึกษาด้านต่าง ๆ อธิบดี รองอธิบดี
- ระดับชั้นสำหรับผู้บริหารทั่วไป หมายถึง ผู้อำนวยการสำนักฯ ผู้อำนวยการกลุ่ม
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป หมายถึง บุคลากรในสังกัดสำนักงานปลัดกระทรวงการคลัง และสำนักงานรัฐมนตรี
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย หมายถึง ผู้ที่มีหน้าที่รับผิดชอบดูแลในระบบงานนั้นๆ

(๕) การกำหนดเวลาที่สามารถเข้าถึงได้ ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

(๖) การกำหนดช่องทางการเข้าถึง ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากหน่วยงาน โดยมีการกำหนดบัญชีผู้ใช้งานตามระดับการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายอินเตอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๗) กำหนดเงื่อนไขในการระงับหรือยกเลิกสิทธิของผู้ใช้งานในการใช้งานระบบสารสนเทศในแต่ละประเภทของข้อมูล

(๘) ผู้ดูแลระบบต้องมีการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๓.๑.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๓.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๒.๑ แนวนโยบาย

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตจากหน่วยงานเจ้าของระบบ และได้ผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) ของสำนักงานปลัดกระทรวงการคลัง เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต จะต้องประกอบด้วย

(๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (user access) ประกอบด้วย

(๑.๑) มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)

(๑.๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ประกอบด้วย

(๒.๑) ต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานระบบตามความเหมาะสมในแต่ละระบบงานที่ได้รับอยู่ในความรับผิดชอบของสำนักงานปลัดกระทรวงการคลัง

(๒.๒) ต้องจัดทำบัญชีผู้ใช้งานระบบ อย่างน้อยต้องประกอบด้วย

- รายชื่อผู้ขออนุญาตเข้าใช้งานระบบ
- รายชื่อผู้ได้รับการอนุมัติเข้าใช้งานระบบ
- กำหนดสิทธิการเข้าใช้งานข้อมูล
- ผู้อนุมัติ หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานระบบ

(๒.๓) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๒.๔) ต้องกำหนดหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๒.๕) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือความต้องการของสำนักงานปลัดกระทรวงการคลัง

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ประกอบด้วย

(๓.๑) มีการแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ซึ่งหมายรวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงข้อมูลสารสนเทศ

(๓.๒) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๓.๓) ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่าย ระบบงาน และระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ประกอบด้วย

(๔.๑) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัยอย่างรัดกุม

(๔.๒) มีการกำหนดให้เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น และไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

(๔.๓) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๔.๔) ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

(๔.๕) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๔.๖) มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

(๔.๗) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

(๕) การทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน (review of user access rights) ประกอบด้วย

(๕.๑) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอ โดยผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น

(๕.๒) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในหน่วยงาน

(๕.๓) การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(๕.๔) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

๓.๒.๒ แนวทางปฏิบัติ

(๑) การลงทะเบียนผู้ใช้งาน (user registration) มีดังนี้

(๑.๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ

(๑.๒) อบรมหรือจัดทำคู่มือการใช้งานระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบสารสนเทศทราบ

(๑.๓) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบงานสารสนเทศลงในแบบฟอร์ม และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(๑.๔) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย พิจารณาคำขอลงทะเบียนอนุมัติ กำหนดระดับการเข้าใช้งานสารสนเทศเท่าที่จำเป็นในแต่ละระบบงาน และทำการบันทึกจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(๑.๕) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล และไม่ซ้ำซ้อนกัน

(๑.๖) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๑.๗) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(๑.๘) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือความต้องการของสำนักงานปลัดกระทรวงการคลังให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(๑.๙) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๑.๑๐) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งานแต่ละรายในระบบเมื่อได้รับรายงาน บัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่ง หรือย้ายหน่วยงาน

(๒) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

(๒.๑) ผู้ดูแลระบบแสดงกระบวนการในการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒.๒) ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งานระบบเท่านั้น

(๒.๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบ หรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้

(๒.๔) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(๒.๕) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจหน้าที่ หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(๒.๖) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

(๓) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) มีดังนี้

(๓.๑) จัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

(๓.๒) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยมีการผสมผสาน ตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๓.๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

(๓.๔) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๓.๕) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓.๖) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๓.๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๓.๘) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๓.๙) ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

(๓.๑๐) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๓.๑๑) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(๓.๑๒) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

(๓.๑๓) ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(๔) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) มีดังนี้

(๔.๑) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

(๔.๒) ปรับปรุงบัญชีผู้ใช้งาน และบันทึกการเปลี่ยนแปลงสิทธิบัญชีผู้ใช้งาน

(๔.๓) การทบทวนสิทธิการเข้าใช้งาน ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๔.๔) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๒.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) ผู้ใช้งาน

๓.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๓.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานทุกคนในสำนักงานปลัดกระทรวงการคลังและผู้ดูแลระบบครอบคลุมเรื่องต่าง ๆ ดังนี้

(๑) ต้องกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อกำหนดแนวทางในการป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงระบบและอุปกรณ์ต่าง ๆ ของหน่วยงานในขณะที่ไม่มีผู้ดูแลควรมีดังนี้

(๒.๑) มีมาตรการป้องกันดูแลอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๒) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(๒.๓) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้งเสมอ

(๒.๔) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๕) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่มีการดูแลชั่วคราว

(๒.๖) ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบ หรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศ

(๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and Clear screen Policy) ควรมีดังนี้

(๓.๑) มีมาตรการการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศจากผู้ไม่มีส่วนเกี่ยวข้อง

(๓.๒) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้มีความเหมาะสม ไม่ให้ได้รับความเสี่ยง

(๓.๓) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๓.๔) บุคลากรของสำนักงานปลัดกระทรวงการคลังทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(๓.๕) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๖) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๗) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของ ศทส. อย่างสม่ำเสมอ

(๓.๘) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๙) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของสำนักงานปลัดกระทรวงการคลังจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของ ศทส. และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารด้าน IT หรือผู้ที่ได้รับมอบอำนาจก่อนเข้าพื้นที่ เท่านั้น

(๓.๑๐) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น ชื่อผู้ใช้งานและรหัสผ่าน

(๓.๑๑) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๔) ข้อมูลสารสนเทศใดที่เป็นความลับ ผู้ดูแลระบบอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

(๕) กำหนดให้ต้องบันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๓.๓.๒ แนวทางปฏิบัติ

(๑) วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password use) มีข้อปฏิบัติ ดังนี้

(๑.๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๑.๒) กำหนดรหัสผ่านต้องมีความยาวมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยต้องผสมผสาน ตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๑.๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

(๑.๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๑.๕) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๑.๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๑.๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๑.๘) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑.๙) ต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอทุก ๓ ถึง ๖ เดือน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑.๑๐) หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน หรือรหัสผ่านเดิมสำหรับระบบงานอื่นๆ ที่ตนใช้งาน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ มีข้อปฏิบัติ ดังนี้

(๒.๑) ผู้ดูแลระบบ หรือผู้รับผิดชอบกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ระบบคอมพิวเตอร์และระบบสารสนเทศที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒.๒) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(๒.๓) เจ้าพนักงานเครื่องคอมพิวเตอร์ หรือผู้รับผิดชอบจะต้องมีมาตรการป้องกันระบบคอมพิวเตอร์และอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๔) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(๒.๕) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๖) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

(๓) การควบคุมทรัพย์สินและการใช้งานระบบ (Clear desk and Clear screen Policy) มีข้อปฏิบัติ ดังนี้

(๓.๑) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๓.๒) บุคลากรของสำนักงานปลัดกระทรวงการคลังทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(๓.๓) บุคลากรจะต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๔) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๕) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

(๓.๖) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๗) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของสำนักงานปลัดกระทรวงการคลังจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมายอำนาจ ก่อนเข้าพื้นที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

(๓.๘) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๙) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๓.๑๐) ผู้ดูแลระบบ หรือผู้รับผิดชอบจัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งระบุผู้รับผิดชอบเมื่อต้องให้บริการระบบเครือข่ายคอมพิวเตอร์

(๓.๑๑) ผู้ใช้งานระบบและเครื่องคอมพิวเตอร์ ต้องลงทะเบียนการใช้งานทุกครั้งเพื่อเป็นการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง

(๓.๑๒) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดมาตรการการป้องกัน ดังนี้

- ให้ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ต้องลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ต้องจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- Log off เครื่องคอมพิวเตอร์ หรือ ล็อคหน้าจอทุกครั้งเมื่อไม่ได้ใช้งาน
- หัวหน้างานธุรการ หรือผู้รับผิดชอบจัดทำทะเบียนการใช้เครื่องโทรสาร เครื่องถ่ายเอกสาร
- ผู้ใช้งานต้องขออนุญาตและลงชื่อการใช้งานเครื่องโทรสาร และเครื่องถ่ายเอกสาร
- ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๓.๑๓) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยผู้ใช้งานต้องทำการเข้ารหัสข้อมูล)Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

๓.๓.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๓) ผู้ดูแลระบบ (System Administrator)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) ผู้ใช้งาน

๓.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๔.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายกระทรวงการคลังโดยไม่ได้รับอนุญาต ประกอบด้วย

(๑) การกำหนดขอบเขตและสิทธิของผู้ใช้งานสามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานกำหนดเท่านั้น

(๒) การกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) มีการทบทวนสิทธิการเข้าถึงบริการระบบเครือข่าย อย่างน้อยปีละ ๑ ครั้ง และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานผู้รับผิดชอบ เท่านั้น

(๔) มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้

(๕) มีวิธีการระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) เพื่อใช้ในการตรวจสอบการเข้าถึงอุปกรณ์บนระบบเครือข่ายของหน่วยงาน

(๖) มีการกำหนดหลักเกณฑ์ในการควบคุมและการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๗) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๘) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน

(๙) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ของหน่วยงานที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างกันให้มีความสอดคล้องกับหน่วยงาน

(๑๐) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย

(๑๑) มีการกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน

๓.๔.๒ แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบเครือข่ายจัดทำบันทึกการกำหนดขอบเขตและสิทธิของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

(๒) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๔) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ ดังนี้

(๔.๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

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

(๔.๓) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

(๕) การระบุอุปกรณ์บนเครือข่าย (equipments identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๕.๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนจึงจะสามารถดำเนินการได้

(๕.๒) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(๕.๓) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

(๖) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๖.๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล๊อกอินเข้ามาใช้งาน

(๖.๒) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๖.๓) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(๖.๔) เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๖.๕) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

(๖.๖) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(๖.๗) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(๖.๘) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

(๖.๙) ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

(๗) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๘) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๙) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

(๑๐) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

(๑๐.๑) การจำกัดสิทธิ การเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(๑๐.๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๑๐.๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(๑๐.๔) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(๑๐.๕) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(๑๐.๖) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(๑๑) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

(๑๑.๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

(๑๑.๒) กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

(๑๑.๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

(๑๒) ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน ที่ต้องผ่านการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน และต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบ เป็นลายลักษณ์อักษร เท่านั้น และผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานอย่างเคร่งครัด โดยดำเนินการดังนี้

(๑๒.๑) ผู้ดูแลระบบเครือข่ายต้องไม่เปิด port และ modem ทิ้งเอาไว้โดยไม่จำเป็น

(๑๒.๒) ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็น เท่านั้น

(๑๒.๓) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

(๑๒.๔) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (remote access) ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

๓.๔.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(๓) ผู้ใช้งาน

๓.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๕.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ควรดำเนินการดังนี้

(๑) การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุม โดยการยืนยันตัวตนตามระบบรักษาความมั่นคงปลอดภัยของหน่วยงาน

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งาน สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) มีการแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) มีการจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้

(๖) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

๓.๕.๒ แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(๒.๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒.๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๒.๓) จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๒.๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้ ดังนี้

(๓.๑) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๓.๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นของหน่วยงานทางด้านธุรกิจหรือด้านเทคนิค

(๓.๓) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (interactive) หรือต้องทำงานในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

(๕.๑) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

(๕.๒) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(๕.๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๕.๔) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕.๕) กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๐ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๘) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(๙) กำหนดระยะเวลาในการจำกัดการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๒ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

๓.๕.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๓.๖.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ ดำเนินการดังนี้

(๑) กำหนดมาตรการการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(๒) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะได้รับการแยกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ได้แก่ ระบบคลังข้อมูลเศรษฐกิจการคลัง

(๔) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๖.๒ แนวปฏิบัติ

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องดำเนินการดังนี้

(๑.๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

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

(๑.๓) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

- กำหนดสิทธิให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น
- กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

(๑.๔) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(๒) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(๒.๑) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องเครื่องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

(๒.๒) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และอื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(๒.๓) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

(๒.๔) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๓) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

(๓.๑) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(๓.๒) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในสำนักงานก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

(๓.๓) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

(๓.๔) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

๓.๖.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)
(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๓.๗.๑ แนวนโยบาย

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่เข้ามาใช้งานในระบบเครือข่ายไร้สาย เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

๓.๗.๒ แนวปฏิบัติ

(๑) การใช้งานเครือข่ายไร้สาย (Wireless Policy)
(๑.๑) ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network
(๑.๒) การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด
(๑.๓) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้
(๑.๔) ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (access point), wireless routers, wireless USB client, หรือ wireless card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้รับผิดชอบของหน่วยงาน
(๑.๕) การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายของหน่วยงาน
(๒) การใช้งานระบบไฟร์วอลล์ (Fire wall) และระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)
(๒.๑) มีการระบุขอบเขต (Trust Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, โซนการเชื่อมต่อภายนอก เครือข่ายภายในองค์กร และโซน remote access และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน
(๒.๒) มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ
(๒.๓) มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ
(๒.๔) มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล
(๓) การใช้งานเครือข่าย (Internet Security Policy)
(๓.๑) มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๒) มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๓) มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๔) มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

(๓.๕) จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

(๔) การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่าย

(๔.๑) ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่นนอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

(๔.๒) ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

(๕) ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

(๕.๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๕.๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๕.๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๕.๔) ควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๓.๗.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๘ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsource Access Control)

๓.๘.๑ แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก ควรประกอบด้วย

(๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

(๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(๓) สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

๓.๘.๒ แนวปฏิบัติ

(๑) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

(๒) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้อง ทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๓) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

(๓.๑) เหตุผลในการขอใช้

(๓.๒) ระยะเวลาในการใช้

(๓.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๓.๔) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๓.๕) กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล

(๔) หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(๕) หน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(๖) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๗) องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๘) ต้องกำหนดให้หน่วยงานภายนอก หรือผู้ให้บริการจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของหน่วยงานภายนอก หรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

๓.๘.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(๒.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

ส่วนที่ ๒
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๑. ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑.๑ ศูนย์กลางข้อมูลและระบบเครือข่าย (Data Center and Network Center) ผู้ดูแลระบบเครือข่าย ผู้ดูแลข้อมูลสารสนเทศ มีหน้าที่ปฏิบัติดังนี้

๑.๑.๑ ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งาน ได้แก่ ข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสารภายใน ระบบเครือข่ายสื่อสารภายนอก ห้องควบคุมการปฏิบัติงาน พื้นที่จัดเก็บอุปกรณ์ต่าง ๆ พื้นที่จัดเก็บเอกสาร สื่อบันทึก เป็นต้น ให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

๑.๑.๒ ให้ศูนย์เป็นผู้กำหนดสิทธิและลำดับชั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศระบบเครือข่ายสื่อสาร

๑.๑.๓ ให้ศูนย์กำหนดมาตรการควบคุมการเข้าออกพื้นที่ของศูนย์ทั้งหมด และกำหนดพื้นที่ที่มีความเสี่ยงห้ามมิให้บุคคลภายนอกหรือผู้มีส่วนเกี่ยวข้องเข้าถึงได้

๑.๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาเชื่อมต่อกับระบบเครือข่ายภายในหน่วยงาน จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๑.๕ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำ และเครื่องดับเพลิง ระบบปรับอากาศ และควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ

๑.๒ การติดตั้งระบบสายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security) ผู้ดูแลระบบเครือข่ายมีหน้าที่ปฏิบัติดังนี้

๑.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๑.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๑.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๑.๒.๔ ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๑.๒.๕ วางแผนการใช้งานสายไฟเบอร์ออฟติก (Fiber Obtics) แทนสายสัญญาณสื่อสารแบบเดิมกับข้อมูลที่มีความสำคัญ

๑.๓ การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ผู้ดูแลทรัพย์สิน บริษัทผู้รับจ้างบริการ มีหน้าที่ปฏิบัติดังนี้

๑.๓.๑ ผู้ดูแลทรัพย์สินกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่หน่วยงานกำหนด

๑.๓.๒ บริษัทผู้รับจ้างปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่กำหนด

๑.๓.๓ บริษัทผู้รับจ้างจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๑.๓.๔ บริษัทผู้รับจ้างจัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๑.๓.๕ ผู้ดูแลทรัพย์สิน ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๑.๓.๖ ผู้ดูแลทรัพย์สิน จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกเป็นลายลักษณ์อักษร

๑.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property) ผู้ดูแลทรัพย์สินหรือผู้ได้รับมอบหมายจากผู้บริหาร มีหน้าที่ปฏิบัติดังนี้

๑.๔.๑ ผู้บริหารมอบอำนาจ หรือกำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน

๑.๔.๒ กำหนดมาตรการความปลอดภัยและผู้รับผิดชอบเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน

๑.๔.๓ ควบคุมดูแลให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน และต้องได้รับอนุญาตจากผู้มีอำนาจ เท่านั้น

๑.๔.๔ กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน

๑.๔.๕ บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน พร้อมทั้งมีการบันทึกผู้รับผิดชอบในการดูแลรักษาทรัพย์สินหรืออุปกรณ์นอกพื้นที่

๑.๔.๖ เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบจำนวนทรัพย์สินกับเอกสาร การชำรุดเสียหายของทรัพย์สินด้วยทุกครั้ง

๑.๔.๗ บุคลากรที่มีส่วนเกี่ยวข้องทุกคนต้องไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะโดยไม่มีผู้รับผิดชอบ

๑.๔.๘ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑.๕ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment) ผู้ดูแลทรัพย์สินมีหน้าที่ปฏิบัติดังนี้

๑.๕.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑.๕.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๑.๕.๓ เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

(๑) คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

(๒) ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการ ดังนี้

- ประเภท Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
- ประเภทกระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ประเภทแผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
- ประเภทเทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ประเภทฮาร์ดดิสก์	ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๑.๖ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ ผู้ดูแลระบบ ผู้ดูแลข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้อง มีหน้าที่ปฏิบัติดังนี้

๑.๖.๑ จัดแบ่งหมวดหมู่ประเภทของเอกสารและจัดหาสถานที่จัดเก็บเอกสารที่เหมาะสม

๑.๖.๒ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัยตามที่กำหนด

๑.๖.๓ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๑.๖.๔ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๒. ด้านการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ผู้ดูแลเครือข่ายและผู้ดูแลระบบ มีหน้าที่ปฏิบัติดังนี้

๒.๑.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๒.๑.๒ จัดเก็บบันทึกการติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ

๒.๑.๓ ไม่ควรติดตั้งซอร์สโค้ด และคอมไพเลอร์ (complier) ของระบบงานในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

๒.๑.๔ จัดเก็บซอร์สโค้ดและไลบรารี่ของซอฟต์แวร์ระบบ ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และกำหนดลำดับชั้นของสิทธิการเข้าถึงข้อมูล

๒.๑.๕ ให้มีการระบุความต้องการทางสารสนเทศ สำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๒.๑.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศให้ถูกต้องตรงตามความต้องการของระบบ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ไว้ให้บริการ

๒.๑.๗ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๒.๑.๘ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๒.๒ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก ผู้ดูแลระบบ และผู้ดูแลข้อมูล มีหน้าที่ปฏิบัติดังนี้

๒.๒.๑ กำกับ ควบคุม ดูแล โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างจากภายนอก

๒.๒.๒ ระบุชื่อผู้รับผิดชอบ หน้าที่ความรับผิดชอบ โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างให้บริการจากภายนอก

๒.๒.๓ ให้กำหนดเรื่องลิขสิทธิ์ของซอฟต์แวร์ ซอร์สโค้ด และซอฟต์แวร์ที่ใช้ในการพัฒนาและติดตั้งต้องเป็นของหน่วยงานทั้งหมด

๒.๒.๔ ศูนย์จัดหาสถานที่ที่ใช้ในการพัฒนาซอฟต์แวร์ในกรณีที่บริษัทผู้รับจ้างต้องเข้ามาดำเนินการพัฒนา และทดสอบซอฟต์แวร์ระบบในหน่วยงาน

๒.๒.๕ กำหนดสิทธิการเข้าถึงอุปกรณ์และสารสนเทศเพื่อใช้ในการพัฒนาซอฟต์แวร์ให้กับบริษัทผู้รับจ้างได้เท่าที่จำเป็น

๒.๒.๖ จัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ของเจ้าหน้าที่หน่วยงานภายนอก (Outsource) และบันทึกการเข้าใช้งานระบบเครือข่ายของหน่วยงาน

๒.๒.๗ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๒.๒.๘ ผู้ดูแลระบบจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับจัดการช่องโหว่ของซอฟต์แวร์ระบบ ต้องมีรายละเอียดอย่างน้อย

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- หน่วยงานที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ชื่อผู้รับผิดชอบซอฟต์แวร์หรือระบบงาน

๒.๒.๙ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๓ มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลดังนี้

๒.๓.๑ ชื่อบัญชีผู้ใช้งาน

๒.๓.๒ วันเวลาที่เข้าออก-ระบบ

๒.๓.๓ เหตุการณ์สำคัญที่เกิดขึ้น

๒.๓.๔ การเปลี่ยนคอนฟิกกูเรชันของระบบ

๒.๓.๕ แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

๒.๓.๖ ไอพีแอดเดรสที่เข้าถึง

๒.๓.๗ โพรโตคอลเครือข่ายที่ใช้

๒.๔ ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

๒.๕ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๓. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์

๓.๑ การใช้งานทั่วไป

๓.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลและรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของหน่วยงาน

๓.๑.๒ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

๓.๑.๓ การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแล

๓.๑.๔ ผู้ใช้งานจะต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงาน หรือเป็นข้อมูลส่วนบุคคล

๓.๑.๕ ผู้ใช้งานจะต้องรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง โดยผู้ใช้งานแต่ละคนจะต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองโดยเฉพาะ ห้ามมิให้ใช้ร่วมกับผู้อื่น ห้ามมิให้ทำการเผยแพร่ แจกจ่าย หรือ ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

๓.๑.๖ ห้ามไม่ให้ผู้ใช้งานใช้โปรแกรมบางประเภท เช่น บิตทอร์เรนต์ (BitTorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาต

๓.๑.๗ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์

๓.๑.๘ คอมพิวเตอร์ของผู้ใช้งานจะติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Anti-Mailware) ตามที่หน่วยงานได้กำหนด

๓.๑.๙ ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในศูนย์ฯให้ตรงกันโดยให้อิงกับเวลามาตรฐานกลางของโลก เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

๓.๒ การสำรองข้อมูลและการกู้คืน

๓.๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๓.๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓.๒.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๔. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล หรือใช้การพิสูจน์ตัวตนด้วย Token Key

๔.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๔.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๕. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๕.๑ การใช้งานสำหรับผู้ใช้งาน

๕.๑.๑ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่ผิดกฎระเบียบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๕.๑.๒ E-mail จะถูกเก็บเป็นความลับ ห้ามผู้ใดพยายามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิใน E-mail ดังกล่าว

๕.๑.๓ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายลูกโซ่ ข่มขู่ ลามกอนาจาร หรือไม่สุภาพ

๕.๑.๔ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายกระจาย โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๕.๑.๕ การรับส่งเอกสารทางราชการจะต้องใช้อีเมล์ของหน่วยงาน ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังออกให้เท่านั้น

๕.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (system administrator)

๕.๒.๑ กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๕.๒.๒ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง

๕.๒.๓ มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๕.๒.๔ มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๖. การใช้งานระบบอินเทอร์เน็ต (internet)

๖.๑ การควบคุมการใช้งาน (Access Control Policy)

๖.๑.๑ ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

๖.๑.๒ มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

๖.๑.๓ มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

๖.๑.๔ มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

๖.๑.๕ การเข้าถึงระบบด้วย Remote User ต้องได้รับการอนุญาตจากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๖.๑.๖ ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสมหากผู้ใช้งานกระทำการใดๆ ในทางที่ผิด

๖.๑.๗ ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบด้วย

๖.๒ การใช้และการเปลี่ยนรหัสผ่าน สำหรับใช้ในการเข้าถึงฐานข้อมูลของเจ้าหน้าที่ ต้องปฏิบัติดังนี้

๖.๒.๑ การกำหนดให้รหัสผ่านควรมีมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยต้องผสมผสานกันระหว่างตัวอักษรตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๖.๒.๒ ไม่ควรกำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

๖.๒.๓ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๖.๒.๔ ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

๖.๒.๕ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

๖.๒.๖ ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๖.๒.๗ เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น

๖.๒.๘ ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

๖.๓ การใช้งานเครือข่ายไร้สาย (Wireless Policy) ปฏิบัติดังนี้

๖.๓.๑ ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

๖.๓.๒ การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

๖.๓.๓ เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

๖.๓.๔ ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็น access point, wireless routers, wireless USB client, หรือ wireless card ภายในสำนักงานปลัดกระทรวงการคลัง ยกเว้นจะได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ

๖.๓.๕ การเข้าถึงระบบเครือข่ายไร้สาย (wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบและมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายขององค์กร

๖.๔ การใช้งานระบบไฟร์วอล และระบบ IDS/IPS ปฏิบัติดังนี้

๖.๔.๑ มีการระบุขอบเขต (Truth Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, remote access โซนการเชื่อมต่อภายนอกในองค์กร และโซนภายในเครือข่าย และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

๖.๔.๒ มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

๖.๔.๓ มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

๖.๔.๔ มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

๖.๕ การใช้งานเครือข่าย (Internet Security Policy) ปฏิบัติดังนี้

๖.๕.๑ มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

๖.๕.๒ มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

๖.๕.๓ มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

๖.๕.๔ มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

๖.๕.๕ จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

๖.๖ ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่น นอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

๖.๗ ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันทีถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

๖.๘ การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๖.๙ ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

๖.๑๐ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๖.๑๑ ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

ส่วนที่ ๓
นโยบายและแนวปฏิบัติระบบสำรองของสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
๒.๓ ผู้ดูแลระบบสารสนเทศ

๓. แนวนโยบาย

๓.๑ ต้องจัดทำแผนและระบบสำรองสำหรับระบบสารสนเทศ เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน
๓.๒ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
๓.๓ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
๓.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
๓.๕ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง
๓.๖ มีศูนย์คอมพิวเตอร์สำรองซึ่งตั้งอยู่ในสภาพที่ปลอดภัยพร้อมระบบคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน
๓.๗ ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๔. แนวทางปฏิบัติ

๔.๑ พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูล และกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความสำคัญของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานมากไปหาน้อย

๔.๓ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๔.๔ ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔.๕ มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๔.๖ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ

๔.๗ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔.๘ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔.๙ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยด่วน

๔.๑๐ กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

๔.๑๑ กำหนดให้ผู้ดูแลระบบ (System Administrator) ต้องสำรองข้อมูลที่สำคัญ ได้แก่ ข้อมูลและค่า Configure ของ Database Server, Web Server, Mail Server และ Firewall Server เป็นประจำอย่างน้อย ๓ เดือนครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ส่วนที่ ๔
นโยบายและแนวปฏิบัติการประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวนโยบาย

๓.๑ ต้องมีการจัดแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

๓.๒ ต้องมีผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๓ ต้องมีการรายงานผลการบริหารความเสี่ยงด้านระบบสารสนเทศให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๔. แนวทางปฏิบัติ

๔.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ควรประกอบด้วย

๔.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๔.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๔.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๔.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๔.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๔.๒ มีการกำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๔.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๔.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๔.๔ กำหนดให้กลุ่มตรวจสอบภายในของสำนักงานปลัดกระทรวงการคลังมีหน้าที่ในการตรวจสอบและประเมินความเสี่ยง และจัดทำรายงานพร้อมข้อเสนอแนะ อย่างน้อยปีละ ๑ ครั้ง

๔.๕ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๖ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง และป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๗ ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๔.๘ ควรกำหนดให้แยกเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕
นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๑. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงการคลังมีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและน่าเชื่อถือ จึงกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง เพื่อให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงการคลังทุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ และตั้งใจปฏิบัติอย่างเคร่งครัด ตามแนวทางดังนี้

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๓.๒ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคล ให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี รวมทั้งการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓.๓ จัดทำแนวปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคลของสำนักงานปลัดกระทรวงการคลัง เพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคลให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้

๓.๔ แจ้งหรือจัดให้มีประกาศแนวนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงการคลัง ให้แก่บุคลากรและบุคคลที่เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๓.๕ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๓.๖ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๓.๗ ระดมการมีส่วนร่วมด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๖
การกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัย ของสำนักงานปลัดกระทรวงการคลัง

เพื่อสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินและอุปกรณ์ของสำนักงานปลัดกระทรวงการคลัง ซึ่งมีความสำคัญและคุณค่า ผู้บริหารจะให้การสนับสนุนในการกำหนดมาตรการป้องกัน ได้แก่ นโยบายความมั่นคงปลอดภัย ขั้นตอนปฏิบัติ และเอกสารสนับสนุนอื่นๆรวมทั้งกระบวนการในการทบทวนมาตรการดังกล่าว เพื่อให้สามารถปรับปรุงหรือแก้ไขข้อบกพร่องหรือปัญหาทางด้านความมั่งคงปลอดภัยได้อย่างมีประสิทธิภาพ

หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

๑. ผู้บริหารระดับสูงสุด (CEO)

๑.๑ กำกับให้มีการกำหนด จัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัยอยู่เสมอ

๑.๒ กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ผู้ใดฝ่าฝืน หรือละเลยการปฏิบัติตามแนวทางนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ มอบหมาย อำนาจ หน้าที่ให้ผู้ดูแล ควบคุมและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๒. ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

๒.๑ กำกับให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน (Procedures) กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)

๒.๒ กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๒.๓ กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๒.๔ จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

๓. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (IT Director)

๓.๑ กำหนดให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน (Procedures) กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)

๓.๒ กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๓.๓ กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๓.๔ จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

๔. ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

๔.๑ กำหนดมาตรการควบคุม กำหนดสิทธิการใช้งานระบบงานต่าง ๆ ของหน่วยงาน

๔.๒ ควบคุม การบริหารจัดการใช้งานระบบงานหรือแอพพลิเคชั่นของหน่วยงาน

๕. ผู้ดูแลระบบคอมพิวเตอร์ (System Administrator)

๕.๑ ดูแลบัญชีผู้ใช้ กำหนดสิทธิ และทบทวนสิทธิการใช้งานของผู้ใช้ระบบ

๕.๒ บริหารจัดการเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายให้มีความมั่งคงปลอดภัย และสามารถใช้งานได้ตลอดเวลา

๕.๓ ตรวจสอบข้อมูลล็อกของเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายรวมทั้งจัดทำรายงานสรุปเสนอผู้บังคับบัญชา

๕.๔ ทำการสำรองข้อมูลและตรวจสอบข้อมูลที่สำรองไว้

๖. ผู้พัฒนาระบบ (System Developer)

๖.๑ ร่วมกับเจ้าของระบบหรือแอพพลิเคชั่นเพื่อกำหนด User requirement และ Security requirement สำหรับระบบหรือแอพพลิเคชั่น

๖.๒ พัฒนาระบบโดยคำนึงถึงความถูกต้องของข้อมูลนำเข้า ข้อมูลที่อยู่ในระหว่างการประมวลผล และข้อมูลนำออก

๖.๓ ทำการทดสอบระบบหรือแอพพลิเคชั่นก่อนเริ่มต้นการใช้งานจริง

๖.๔ จัดทำคู่มือการใช้งาน คู่มือสำหรับระบบ และหรือคู่มือสำหรับการดำเนินงาน

๖.๕ จัดอบรมการใช้งานระบบหรือแอพพลิเคชั่นให้กับผู้ใช้งานที่เกี่ยวข้อง

๗. ผู้ดูแลระบบเครือข่าย (System Network)

๗.๑ บันทึกเหตุการณ์ ตรวจสอบการเข้าถึงระบบเครือข่ายของหน่วยงาน

๗.๒ ควบคุมดูแลระบบเครือข่ายสื่อสารให้สามารถใช้งานได้ตลอดเวลา

๗.๓ ควบคุมการดำเนินการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นแนวทางตามที่ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดไว้

๘. ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๘.๑ ร่วมกับเจ้าของระบบหรือแอพพลิเคชั่นเพื่อกำหนด Security requirements สำหรับระบบหรือแอพพลิเคชั่น

๘.๒ กำหนดมาตรการควบคุม กำหนดสิทธิการใช้ระบบเครือข่ายสื่อสารของหน่วยงาน

๘.๓ ตรวจสอบป้องกันการบุกรุกจู่โจมจากผู้ไม่ประสงค์ดี

๙. เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

๙.๑ ช่วยเหลือและประสานงานกับเจ้าหน้าที่ผู้ใช้งานของสำนักงานปลัดกระทรวงการคลัง (End User) ในการแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์

๙.๒ ทำหน้าที่รับมือกับเหตุการณ์ความมั่งคงปลอดภัยตามที่ได้รับรายงานโดยปฏิบัติตามขั้นตอนปฏิบัติอย่างเคร่งครัด

๙.๓ บันทึกข้อมูลปัญหาการใช้งานเครื่องคอมพิวเตอร์และข้อมูลเหตุการณ์ความมั่งคงปลอดภัยและจัดทำรายงานสรุปปัญหาและเสนอผู้บังคับบัญชา

๑๐.ผู้ใช้งาน (End User)

๑๐.๑ ปฏิบัติตามนโยบายฉบับนี้โดยเคร่งครัด

ส่วนที่ ๑
นโยบายและแนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้ผู้รับผิดชอบ และผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานได้รับรู้เข้าใจ นโยบายในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของสำนักงานปลัดกระทรวงการคลัง และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

๒.๒.๑ ผู้ดูแลระบบเครือข่าย (System Network)

๒.๒.๒ ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

๒.๒.๓ ผู้ดูแลระบบ (System Administrator)

๒.๒.๔ ผู้พัฒนาระบบ (System Developer)

๒.๒.๕ ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๒.๒.๖ เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

๒.๓ เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๒.๔ ผู้ใช้งาน

๓. แนวนโยบายและแนวปฏิบัติ

สำนักงานปลัดกระทรวงการคลังมีแนวนโยบายและแนวปฏิบัติด้านต่าง ๆ ดังต่อไปนี้

๓.๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๓.๑.๑ แนวนโยบาย

(๑) ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๒) มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓) มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

(๔) มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

(๕) การเข้าถึงระบบด้วยการ Remote User ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบ จากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เท่านั้น

(๖) ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆ ในทางที่ผิดตามประกาศของสำนักงานปลัดกระทรวงการคลัง

(๗) การควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานได้จัดแบ่งประเภทของข้อมูลออกเป็นสองประเภท คือ

(๗.๑) ข้อมูลสารสนเทศด้านการบริหารราชการ ได้แก่ ข้อมูลการบริหารทรัพยากรบุคคล ข้อมูลเศรษฐกิจการคลัง ข้อมูลนโยบายและแผน ข้อมูลตรวจสอบ

(๗.๒) ข้อมูลสารสนเทศด้านการสนับสนุน ได้แก่ ข้อมูลงานสารบรรณ ข้อมูลข่าวสารประชาสัมพันธ์ กฎหมาย ระเบียบ ประกาศ สถิติ

(๘) ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบสารสนเทศนั้น ๆ ด้วย

(๙) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๑๐)กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑๐.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

(๑๐.๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๑๐.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑.๒ แนวทางปฏิบัติ

หน่วยงานได้กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ การจัดแบ่งระดับการเข้าถึงข้อมูลและสิทธิ เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

(๑) การจัดแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- อ่านอย่างเดียว (Read Only)
- สร้างข้อมูล (Create)
- แก้ไข (Edit)
- ลบ (Delete)

- อนุมัติ (Authorize)

(๒) การจัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ ระดับความสำคัญมากที่สุด ระดับความสำคัญปานกลาง ระดับความสำคัญน้อย

(๓) การจัดแบ่งลำดับชั้นความลับของข้อมูล ได้แก่

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ได้แก่

- ระดับชั้นสำหรับผู้บริหารระดับสูง หมายถึง รัฐมนตรีว่าการกระทรวงการคลัง รัฐมนตรีช่วยว่าการกระทรวงการคลัง ที่ปรึกษารัฐมนตรีฯ ปลัดกระทรวงการคลัง รองปลัดกระทรวงการคลัง ผู้ตรวจราชการ ที่ปรึกษาด้านต่าง ๆ อธิบดี รองอธิบดี
- ระดับชั้นสำหรับผู้บริหารทั่วไป หมายถึง ผู้อำนวยการสำนักฯ ผู้อำนวยการกลุ่ม
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป หมายถึง บุคลากรในสังกัดสำนักงานปลัดกระทรวงการคลัง และสำนักงานรัฐมนตรี
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย หมายถึง ผู้ที่มีหน้าที่รับผิดชอบดูแลในระบบงานนั้นๆ

(๕) การกำหนดเวลาที่สามารถเข้าถึงได้ ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

(๖) การกำหนดช่องทางการเข้าถึง ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากหน่วยงาน โดยมีการกำหนดบัญชีผู้ใช้งานตามระดับการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายอินเตอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๗) กำหนดเงื่อนไขในการระงับหรือยกเลิกสิทธิของผู้ใช้งานในการใช้งานระบบสารสนเทศในแต่ละประเภทของข้อมูล

(๘) ผู้ดูแลระบบต้องมีการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๓.๑.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๓.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๒.๑ แนวนโยบาย

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตจากหน่วยงานเจ้าของระบบ และได้ผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) ของสำนักงานปลัดกระทรวงการคลัง เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต จะต้องประกอบด้วย

(๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (user access) ประกอบด้วย

(๑.๑) มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)

(๑.๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ประกอบด้วย

(๒.๑) ต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานระบบตามความเหมาะสมในแต่ละระบบงานที่ได้รับอยู่ในความรับผิดชอบของสำนักงานปลัดกระทรวงการคลัง

(๒.๒) ต้องจัดทำบัญชีผู้ใช้งานระบบ อย่างน้อยต้องประกอบด้วย

- รายชื่อผู้ขออนุญาตเข้าใช้งานระบบ
- รายชื่อผู้ได้รับการอนุมัติเข้าใช้งานระบบ
- กำหนดสิทธิการเข้าใช้งานข้อมูล
- ผู้อนุมัติ หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานระบบ

(๒.๓) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๒.๔) ต้องกำหนดหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๒.๕) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือความต้องการของสำนักงานปลัดกระทรวงการคลัง

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ประกอบด้วย

(๓.๑) มีการแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ซึ่งหมายรวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงข้อมูลสารสนเทศ

(๓.๒) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๓.๓) ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่าย ระบบงาน และระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ประกอบด้วย

(๔.๑) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัยอย่างรัดกุม

(๔.๒) มีการกำหนดให้เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น และไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

(๔.๓) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๔.๔) ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

(๔.๕) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๔.๖) มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

(๔.๗) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

(๕) การทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน (review of user access rights) ประกอบด้วย

(๕.๑) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอ โดยผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น

(๕.๒) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในหน่วยงาน

(๕.๓) การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(๕.๔) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

๓.๒.๒ แนวทางปฏิบัติ

(๑) การลงทะเบียนผู้ใช้งาน (user registration) มีดังนี้

(๑.๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ

(๑.๒) อบรมหรือจัดทำคู่มือการใช้งานระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบสารสนเทศทราบ

(๑.๓) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบงานสารสนเทศลงในแบบฟอร์ม และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(๑.๔) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย พิจารณาคำขอลงทะเบียนอนุมัติ กำหนดระดับการเข้าใช้งานสารสนเทศเท่าที่จำเป็นในแต่ละระบบงาน และทำการบันทึกจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(๑.๕) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล และไม่ซ้ำซ้อนกัน

(๑.๖) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๑.๗) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(๑.๘) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือความต้องการของสำนักงานปลัดกระทรวงการคลังให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(๑.๙) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๑.๑๐) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งานแต่ละรายในระบบเมื่อได้รับรายงาน บัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่ง หรือย้ายหน่วยงาน

(๒) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

(๒.๑) ผู้ดูแลระบบแสดงกระบวนการในการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒.๒) ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งานระบบเท่านั้น

(๒.๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบ หรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้

(๒.๔) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(๒.๕) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจหน้าที่ หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(๒.๖) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

(๓) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) มีดังนี้

(๓.๑) จัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

(๓.๒) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยมีการผสมผสาน ตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๓.๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

(๓.๔) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๓.๕) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓.๖) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๓.๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๓.๘) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๓.๙) ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

(๓.๑๐) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๓.๑๑) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(๓.๑๒) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

(๓.๑๓) ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(๔) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) มีดังนี้

(๔.๑) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

(๔.๒) ปรับปรุงบัญชีผู้ใช้งาน และบันทึกการเปลี่ยนแปลงสิทธิบัญชีผู้ใช้งาน

(๔.๓) การทบทวนสิทธิการเข้าใช้งาน ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๔.๔) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๒.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) ผู้ใช้งาน

๓.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๓.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานทุกคนในสำนักงานปลัดกระทรวงการคลังและผู้ดูแลระบบครอบคลุมเรื่องต่าง ๆ ดังนี้

(๑) ต้องกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อกำหนดแนวทางในการป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงระบบและอุปกรณ์ต่าง ๆ ของหน่วยงานในขณะที่ไม่มีผู้ดูแลควรมีดังนี้

(๒.๑) มีมาตรการป้องกันดูแลอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๒) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(๒.๓) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้งเสมอ

(๒.๔) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๕) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่มีการดูแลชั่วคราว

(๒.๖) ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบ หรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศ

(๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and Clear screen Policy) ควรมีดังนี้

(๓.๑) มีมาตรการการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศจากผู้ไม่มีส่วนเกี่ยวข้อง

(๓.๒) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้มีความเหมาะสม ไม่ให้ได้รับความเสี่ยง

(๓.๓) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๓.๔) บุคลากรของสำนักงานปลัดกระทรวงการคลังทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(๓.๕) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๖) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๗) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของ ศทส. อย่างสม่ำเสมอ

(๓.๘) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๙) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของสำนักงานปลัดกระทรวงการคลังจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของ ศทส. และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารด้าน IT หรือผู้ที่ได้รับมอบอำนาจก่อนเข้าพื้นที่ เท่านั้น

(๓.๑๐) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น ชื่อผู้ใช้งานและรหัสผ่าน

(๓.๑๑) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๔) ข้อมูลสารสนเทศใดที่เป็นความลับ ผู้ดูแลระบบอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

(๕) กำหนดให้ต้องบันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๓.๓.๒ แนวทางปฏิบัติ

(๑) วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password use) มีข้อปฏิบัติ ดังนี้

(๑.๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๑.๒) กำหนดรหัสผ่านต้องมีความยาวมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยต้องผสมผสาน ตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๑.๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

(๑.๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๑.๕) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๑.๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๑.๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๑.๘) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑.๙) ต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอทุก ๓ ถึง ๖ เดือน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑.๑๐) หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน หรือรหัสผ่านเดิมสำหรับระบบงานอื่นๆ ที่ตนใช้งาน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ มีข้อปฏิบัติ ดังนี้

(๒.๑) ผู้ดูแลระบบ หรือผู้รับผิดชอบกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ระบบคอมพิวเตอร์และระบบสารสนเทศที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒.๒) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(๒.๓) เจ้าพนักงานเครื่องคอมพิวเตอร์ หรือผู้รับผิดชอบจะต้องมีมาตรการป้องกันระบบคอมพิวเตอร์และอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๔) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(๒.๕) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๖) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

(๓) การควบคุมทรัพย์สินและการใช้งานระบบ (Clear desk and Clear screen Policy) มีข้อปฏิบัติ ดังนี้

(๓.๑) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(๓.๒) บุคลากรของสำนักงานปลัดกระทรวงการคลังทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(๓.๓) บุคลากรจะต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๔) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๕) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

(๓.๖) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๗) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของสำนักงานปลัดกระทรวงการคลังจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมายอำนาจ ก่อนเข้าพื้นที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

(๓.๘) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๙) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๓.๑๐) ผู้ดูแลระบบ หรือผู้รับผิดชอบจัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งระบุผู้รับผิดชอบเมื่อต้องให้บริการระบบเครือข่ายคอมพิวเตอร์

(๓.๑๑) ผู้ใช้งานระบบและเครื่องคอมพิวเตอร์ ต้องลงทะเบียนการใช้งานทุกครั้งเพื่อเป็นการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง

(๓.๑๒) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดมาตรการการป้องกัน ดังนี้

- ให้ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ต้องลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ต้องจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- Log off เครื่องคอมพิวเตอร์ หรือ ล็อคหน้าจอทุกครั้งเมื่อไม่ได้ใช้งาน
- หัวหน้างานธุรการ หรือผู้รับผิดชอบจัดทำทะเบียนการใช้เครื่องโทรสาร เครื่องถ่ายเอกสาร
- ผู้ใช้งานต้องขออนุญาตและลงชื่อการใช้งานเครื่องโทรสาร และเครื่องถ่ายเอกสาร
- ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๓.๑๓) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยผู้ใช้งานต้องทำการเข้ารหัสข้อมูล)Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

๓.๓.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๓) ผู้ดูแลระบบ (System Administrator)

(๒.๔) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(๓) ผู้ใช้งาน

๓.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๓.๔.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายกระทรวงการคลังโดยไม่ได้รับอนุญาต ประกอบด้วย

(๑) การกำหนดขอบเขตและสิทธิของผู้ใช้งานสามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานกำหนดเท่านั้น

(๒) การกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) มีการทบทวนสิทธิการเข้าถึงบริการระบบเครือข่าย อย่างน้อยปีละ ๑ ครั้ง และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานผู้รับผิดชอบ เท่านั้น

(๔) มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้

(๕) มีวิธีการระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) เพื่อใช้ในการตรวจสอบการเข้าถึงอุปกรณ์บนระบบเครือข่ายของหน่วยงาน

(๖) มีการกำหนดหลักเกณฑ์ในการควบคุมและการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๗) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๘) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน

(๙) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ของหน่วยงานที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างกันให้มีความสอดคล้องกับหน่วยงาน

(๑๐) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย

(๑๑) มีการกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน

๓.๔.๒ แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบเครือข่ายจัดทำบันทึกการกำหนดขอบเขตและสิทธิของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

(๒) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๔) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ ดังนี้

(๔.๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

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

(๔.๓) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

(๕) การระบุอุปกรณ์บนเครือข่าย (equipments identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๕.๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนจึงจะสามารถดำเนินการได้

(๕.๒) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(๕.๓) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

(๖) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๖.๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล๊อกอินเข้ามาใช้งาน

(๖.๒) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๖.๓) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(๖.๔) เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๖.๕) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

(๖.๖) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(๖.๗) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(๖.๘) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

(๖.๙) ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

(๗) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๘) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๙) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

(๑๐) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

(๑๐.๑) การจำกัดสิทธิ การเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(๑๐.๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๑๐.๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(๑๐.๔) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(๑๐.๕) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(๑๐.๖) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(๑๑) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

(๑๑.๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

(๑๑.๒) กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

(๑๑.๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

(๑๒) ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน ที่ต้องผ่านการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน และต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบ เป็นลายลักษณ์อักษร เท่านั้น และผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานอย่างเคร่งครัด โดยดำเนินการดังนี้

(๑๒.๑) ผู้ดูแลระบบเครือข่ายต้องไม่เปิด port และ modem ทิ้งเอาไว้โดยไม่จำเป็น

(๑๒.๒) ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็น เท่านั้น

(๑๒.๓) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

(๑๒.๔) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (remote access) ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

๓.๔.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(๓) ผู้ใช้งาน

๓.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๕.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ควรดำเนินการดังนี้

(๑) การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุม โดยการยืนยันตัวตนตามระบบรักษาความมั่นคงปลอดภัยของหน่วยงาน

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งาน สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) มีการแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) มีการจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้

(๖) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

๓.๕.๒ แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(๒.๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒.๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๒.๓) จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๒.๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้ ดังนี้

(๓.๑) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๓.๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นของหน่วยงานทางด้านธุรกิจหรือด้านเทคนิค

(๓.๓) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (interactive) หรือต้องทำงานในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

(๕.๑) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

(๕.๒) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(๕.๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๕.๔) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕.๕) กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๐ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๘) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(๙) กำหนดระยะเวลาในการจำกัดการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๒ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

๓.๕.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้พัฒนาระบบ (System Developer)

(๒.๔) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๓.๖.๑ แนวนโยบาย

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ ดำเนินการดังนี้

(๑) กำหนดมาตรการการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(๒) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะได้รับการแยกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ได้แก่ ระบบคลังข้อมูลเศรษฐกิจการคลัง

(๔) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๖.๒ แนวปฏิบัติ

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องดำเนินการดังนี้

(๑.๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

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

(๑.๓) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

- กำหนดสิทธิให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น
- กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

(๑.๔) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(๒) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(๒.๑) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องเครื่องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

(๒.๒) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และอื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(๒.๓) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

(๒.๔) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๓) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

(๓.๑) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(๓.๒) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในสำนักงานก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

(๓.๓) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

(๓.๔) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

๓.๖.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๓.๗.๑ แนวนโยบาย

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่เข้ามาใช้งานในระบบเครือข่ายไร้สาย เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

๓.๗.๒ แนวปฏิบัติ

(๑) การใช้งานเครือข่ายไร้สาย (Wireless Policy)

(๑.๑) ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

(๑.๒) การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

(๑.๓) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

(๑.๔) ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (access point), wireless routers, wireless USB client, หรือ wireless card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้รับผิดชอบของหน่วยงาน

(๑.๕) การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายของหน่วยงาน

(๒) การใช้งานระบบไฟร์วอลล์ (Fire wall) และระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

(๒.๑) มีการระบุขอบเขต (Trust Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, โซนการเชื่อมต่อภายนอก เครือข่ายภายในองค์กร และโซน remote access และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

(๒.๒) มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

(๒.๓) มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

(๒.๔) มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

(๓) การใช้งานเครือข่าย (Internet Security Policy)

(๓.๑) มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๒) มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(๓.๓) มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๔) มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

(๓.๕) จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

(๔) การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่าย

(๔.๑) ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่นนอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

(๔.๒) ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

(๕) ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

(๕.๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๕.๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๕.๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๕.๔) ควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๓.๗.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบ (System Administrator)

(๒.๓) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๓.๘ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsource Access Control)

๓.๘.๑ แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก ควรประกอบด้วย

(๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย

(๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(๓) สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

๓.๘.๒ แนวปฏิบัติ

(๑) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

(๒) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้อง ทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๓) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

(๓.๑) เหตุผลในการขอใช้

(๓.๒) ระยะเวลาในการใช้

(๓.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๓.๔) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๓.๕) กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล

(๔) หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(๕) หน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(๖) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๗) องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๘) ต้องกำหนดให้หน่วยงานภายนอก หรือผู้ให้บริการจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของหน่วยงานภายนอก หรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

๓.๘.๓ ผู้รับผิดชอบ

(๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

(๒.๑) ผู้ดูแลระบบเครือข่าย (System Network)

(๒.๒) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(๒.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

ส่วนที่ ๒
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๑. ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑.๑ ศูนย์กลางข้อมูลและระบบเครือข่าย (Data Center and Network Center) ผู้ดูแลระบบเครือข่าย ผู้ดูแลข้อมูลสารสนเทศ มีหน้าที่ปฏิบัติดังนี้

๑.๑.๑ ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งาน ได้แก่ ข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสารภายใน ระบบเครือข่ายสื่อสารภายนอก ห้องควบคุมการปฏิบัติงาน พื้นที่จัดเก็บอุปกรณ์ต่าง ๆ พื้นที่จัดเก็บเอกสาร สื่อบันทึก เป็นต้น ให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

๑.๑.๒ ให้ศูนย์เป็นผู้กำหนดสิทธิและลำดับชั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสาร

๑.๑.๓ ให้ศูนย์กำหนดมาตรการควบคุมการเข้าออกพื้นที่ของศูนย์ทั้งหมด และกำหนดพื้นที่ที่มีความเสี่ยงห้ามมิให้บุคคลภายนอกหรือผู้มีส่วนเกี่ยวข้องเข้าถึงได้

๑.๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาเชื่อมต่อกับระบบเครือข่ายภายในหน่วยงาน จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๑.๕ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำ และเครื่องดับเพลิง ระบบปรับอากาศ และควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ

๑.๒ การติดตั้งระบบสายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security) ผู้ดูแลระบบเครือข่ายมีหน้าที่ปฏิบัติดังนี้

๑.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๑.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๑.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๑.๒.๔ ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๑.๒.๕ วางแผนการใช้งานสายไฟเบอร์ออฟติก (Fiber Obtics) แทนสายสัญญาณสื่อสารแบบเดิมกับข้อมูลที่มีความสำคัญ

๑.๓ การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ผู้ดูแลทรัพย์สิน บริษัทผู้รับจ้างบริการ มีหน้าที่ปฏิบัติดังนี้

๑.๓.๑ ผู้ดูแลทรัพย์สินกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่หน่วยงานกำหนด

๑.๓.๒ บริษัทผู้รับจ้างปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่กำหนด

๑.๓.๓ บริษัทผู้รับจ้างจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๑.๓.๔ บริษัทผู้รับจ้างจัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๑.๓.๕ ผู้ดูแลทรัพย์สิน ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๑.๓.๖ ผู้ดูแลทรัพย์สิน จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกเป็นลายลักษณ์อักษร

๑.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property) ผู้ดูแลทรัพย์สินหรือผู้ได้รับมอบหมายจากผู้บริหาร มีหน้าที่ปฏิบัติดังนี้

๑.๔.๑ ผู้บริหารมอบอำนาจ หรือกำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน

๑.๔.๒ กำหนดมาตรการความปลอดภัยและผู้รับผิดชอบเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน

๑.๔.๓ ควบคุมดูแลให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน และต้องได้รับอนุญาตจากผู้มีอำนาจ เท่านั้น

๑.๔.๔ กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน

๑.๔.๕ บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน พร้อมทั้งมีการบันทึกผู้รับผิดชอบในการดูแลรักษาทรัพย์สินหรืออุปกรณ์นอกพื้นที่

๑.๔.๖ เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบจำนวนทรัพย์สินกับเอกสาร การชำรุดเสียหายของทรัพย์สินด้วยทุกครั้ง

๑.๔.๗ บุคลากรที่มีส่วนเกี่ยวข้องทุกคนต้องไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะโดยไม่มีผู้รับผิดชอบ

๑.๔.๘ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑.๕ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment) ผู้ดูแลทรัพย์สินมีหน้าที่ปฏิบัติดังนี้

๑.๕.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑.๕.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๑.๕.๓ เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

(๑) คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

(๒) ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการ ดังนี้

- ประเภท Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
- ประเภทกระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ประเภทแผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
- ประเภทเทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ประเภทฮาร์ดดิสก์	ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๑.๖ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ ผู้ดูแลระบบ ผู้ดูแลข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้อง มีหน้าที่ปฏิบัติดังนี้

๑.๖.๑ จัดแบ่งหมวดหมู่ประเภทของเอกสารและจัดหาสถานที่จัดเก็บเอกสารที่เหมาะสม

๑.๖.๒ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัยตามที่กำหนด

๑.๖.๓ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๑.๖.๔ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๒. ด้านการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ผู้ดูแลเครือข่ายและผู้ดูแลระบบ มีหน้าที่ปฏิบัติดังนี้

๒.๑.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๒.๑.๒ จัดเก็บบันทึกการติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ

๒.๑.๓ ไม่ควรติดตั้งซอร์สโค้ด และคอมไพเลอร์ (complier) ของระบบงานในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

๒.๑.๔ จัดเก็บซอร์สโค้ดและไลบรารี่ของซอฟต์แวร์ระบบ ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และกำหนดลำดับชั้นของสิทธิการเข้าถึงข้อมูล

๒.๑.๕ ให้มีการระบุความต้องการทางสารสนเทศ สำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๒.๑.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศให้ถูกต้องตรงตามความต้องการของระบบ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ไว้ให้บริการ

๒.๑.๗ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๒.๑.๘ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๒.๒ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก ผู้ดูแลระบบ และผู้ดูแลข้อมูล มีหน้าที่ปฏิบัติดังนี้

๒.๒.๑ กำกับ ควบคุม ดูแล โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างจากภายนอก

๒.๒.๒ ระบุชื่อผู้รับผิดชอบ หน้าที่ความรับผิดชอบ โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างให้บริการจากภายนอก

๒.๒.๓ ให้กำหนดเรื่องลิขสิทธิ์ของซอฟต์แวร์ ซอร์สโค้ด และซอฟต์แวร์ที่ใช้ในการพัฒนาและติดตั้งต้องเป็นของหน่วยงานทั้งหมด

๒.๒.๔ ศูนย์จัดหาสถานที่ที่ใช้ในการพัฒนาซอฟต์แวร์ในกรณีที่บริษัทผู้รับจ้างต้องเข้ามาดำเนินการพัฒนา และทดสอบซอฟต์แวร์ระบบในหน่วยงาน

๒.๒.๕ กำหนดสิทธิการเข้าถึงอุปกรณ์และสารสนเทศเพื่อใช้ในการพัฒนาซอฟต์แวร์ให้กับบริษัทผู้รับจ้างได้เท่าที่จำเป็น

๒.๒.๖ จัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ของเจ้าหน้าที่หน่วยงานภายนอก (Outsource) และบันทึกการเข้าใช้งานระบบเครือข่ายของหน่วยงาน

๒.๒.๗ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๒.๒.๘ ผู้ดูแลระบบจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับจัดการช่องโหว่ของซอฟต์แวร์ระบบ ต้องมีรายละเอียดอย่างน้อย

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- หน่วยงานที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ชื่อผู้รับผิดชอบซอฟต์แวร์หรือระบบงาน

๒.๒.๙ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒.๓ มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลดังนี้

๒.๓.๑ ชื่อบัญชีผู้ใช้งาน

๒.๓.๒ วันเวลาที่เข้าออก-ระบบ

๒.๓.๓ เหตุการณ์สำคัญที่เกิดขึ้น

๒.๓.๔ การเปลี่ยนคอนฟิกกูเรชันของระบบ

๒.๓.๕ แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

๒.๓.๖ ไอพีแอดเดรสที่เข้าถึง

๒.๓.๗ โพรโตคอลเครือข่ายที่ใช้

๒.๔ ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

๒.๕ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๓. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์

๓.๑ การใช้งานทั่วไป

๓.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลและรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของหน่วยงาน

๓.๑.๒ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

๓.๑.๓ การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแล

๓.๑.๔ ผู้ใช้งานจะต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงาน หรือเป็นข้อมูลส่วนบุคคล

๓.๑.๕ ผู้ใช้งานจะต้องรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง โดยผู้ใช้งานแต่ละคนจะต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองโดยเฉพาะ ห้ามมิให้ใช้ร่วมกับผู้อื่น ห้ามมิให้ทำการเผยแพร่ แจกจ่าย หรือ ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

๓.๑.๖ ห้ามไม่ให้ผู้ใช้งานใช้โปรแกรมบางประเภท เช่น บิตทอร์เรนต์ (BitTorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาต

๓.๑.๗ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์

๓.๑.๘ คอมพิวเตอร์ของผู้ใช้งานจะติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Anti-Mailware) ตามที่หน่วยงานได้กำหนด

๓.๑.๙ ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในศูนย์ฯให้ตรงกันโดยให้อิงกับเวลามาตรฐานกลางของโลก เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

๓.๒ การสำรองข้อมูลและการกู้คืน

๓.๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๓.๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓.๒.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๔. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล หรือใช้การพิสูจน์ตัวตนด้วย Token Key

๔.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๔.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๕. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๕.๑ การใช้งานสำหรับผู้ใช้งาน

๕.๑.๑ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่ผิดกฎระเบียบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๕.๑.๒ E-mail จะถูกเก็บเป็นความลับ ห้ามผู้ใดพยายามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิใน E-mail ดังกล่าว

๕.๑.๓ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายลูกโซ่ ข่มขู่ ลามกอนาจาร หรือไม่สุภาพ

๕.๑.๔ ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายกระจาย โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๕.๑.๕ การรับส่งเอกสารทางราชการจะต้องใช้อีเมล์ของหน่วยงาน ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังออกให้เท่านั้น

๕.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (system administrator)

๕.๒.๑ กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๕.๒.๒ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง

๕.๒.๓ มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๕.๒.๔ มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๖. การใช้งานระบบอินเทอร์เน็ต (internet)

๖.๑ การควบคุมการใช้งาน (Access Control Policy)

๖.๑.๑ ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

๖.๑.๒ มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

๖.๑.๓ มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

๖.๑.๔ มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

๖.๑.๕ การเข้าถึงระบบด้วย Remote User ต้องได้รับการอนุญาตจากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๖.๑.๖ ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสมหากผู้ใช้งานกระทำการใดๆ ในทางที่ผิด

๖.๑.๗ ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบด้วย

๖.๒ การใช้และการเปลี่ยนรหัสผ่าน สำหรับใช้ในการเข้าถึงฐานข้อมูลของเจ้าหน้าที่ ต้องปฏิบัติดังนี้

๖.๒.๑ การกำหนดให้รหัสผ่านควรมีมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยต้องผสมผสานกันระหว่างตัวอักษรตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๖.๒.๒ ไม่ควรกำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

๖.๒.๓ ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๖.๒.๔ ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

๖.๒.๕ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

๖.๒.๖ ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๖.๒.๗ เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น

๖.๒.๘ ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

๖.๓ การใช้งานเครือข่ายไร้สาย (Wireless Policy) ปฏิบัติดังนี้

๖.๓.๑ ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

๖.๓.๒ การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

๖.๓.๓ เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

๖.๓.๔ ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็น access point, wireless routers, wireless USB client, หรือ wireless card ภายในสำนักงานปลัดกระทรวงการคลัง ยกเว้นจะได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ

๖.๓.๕ การเข้าถึงระบบเครือข่ายไร้สาย (wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบและมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายขององค์กร

๖.๔ การใช้งานระบบไฟร์วอล และระบบ IDS/IPS ปฏิบัติดังนี้

๖.๔.๑ มีการระบุขอบเขต (Truth Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, remote access โซนการเชื่อมต่อภายนอกในองค์กร และโซนภายในเครือข่าย และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

๖.๔.๒ มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

๖.๔.๓ มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

๖.๔.๔ มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

๖.๕ การใช้งานเครือข่าย (Internet Security Policy) ปฏิบัติดังนี้

๖.๕.๑ มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

๖.๕.๒ มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

๖.๕.๓ มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

๖.๕.๔ มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

๖.๕.๕ จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

๖.๖ ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่น นอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

๖.๗ ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันทีถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

๖.๘ การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๖.๙ ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

๖.๑๐ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๑ เดือน หรือตามที่หน่วยงานกำหนด

๖.๑๑ ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

ส่วนที่ ๓
นโยบายและแนวปฏิบัติระบบสำรองของสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
๒.๓ ผู้ดูแลระบบสารสนเทศ

๓. แนวนโยบาย

๓.๑ ต้องจัดทำแผนและระบบสำรองสำหรับระบบสารสนเทศ เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน
๓.๒ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
๓.๓ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
๓.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
๓.๕ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง
๓.๖ มีศูนย์คอมพิวเตอร์สำรองซึ่งตั้งอยู่ในสภาพที่ปลอดภัยพร้อมระบบคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน
๓.๗ ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๔. แนวทางปฏิบัติ

๔.๑ พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูล และกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความสำคัญของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานมากไปหาน้อย

๔.๓ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๔.๔ ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔.๕ มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๔.๖ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ

๔.๗ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔.๘ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔.๙ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยด่วน

๔.๑๐ กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

๔.๑๑ กำหนดให้ผู้ดูแลระบบ (System Administrator) ต้องสำรองข้อมูลที่สำคัญ ได้แก่ ข้อมูลและค่า Configure ของ Database Server, Web Server, Mail Server และ Firewall Server เป็นประจำอย่างน้อย ๓ เดือนครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ส่วนที่ ๔
นโยบายและแนวปฏิบัติการประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวนโยบาย

๓.๑ ต้องมีการจัดแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

๓.๒ ต้องมีผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๓ ต้องมีการรายงานผลการบริหารความเสี่ยงด้านระบบสารสนเทศให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๔. แนวทางปฏิบัติ

๔.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ควรประกอบด้วย

๔.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๔.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๔.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๔.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๔.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๔.๒ มีการกำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๔.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๔.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๔.๔ กำหนดให้กลุ่มตรวจสอบภายในของสำนักงานปลัดกระทรวงการคลังมีหน้าที่ในการตรวจสอบและประเมินความเสี่ยง และจัดทำรายงานพร้อมข้อเสนอแนะ อย่างน้อยปีละ ๑ ครั้ง

๔.๕ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๖ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง และป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๗ ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๔.๘ ควรกำหนดให้แยกเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕
นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๑. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงการคลังมีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและน่าเชื่อถือ จึงกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง เพื่อให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงการคลังทุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ และตั้งใจปฏิบัติอย่างเคร่งครัด ตามแนวทางดังนี้

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวปฏิบัติ

๓.๑ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๓.๒ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี รวมทั้งการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓.๓ จัดทำแนวปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง เพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้

๓.๔ แจ้งหรือจัดให้มีประกาศแนวนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงการคลัง ให้แก่บุคลากรและบุคคลที่เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๓.๕ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๓.๖ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๓.๗ ระดมการมีส่วนร่วมด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๖
การกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัย ของสำนักงานปลัดกระทรวงการคลัง

เพื่อสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินและอุปกรณ์ของสำนักงานปลัดกระทรวงการคลัง ซึ่งมีความสำคัญและคุณค่า ผู้บริหารจะให้การสนับสนุนในการกำหนดมาตรการป้องกัน ได้แก่ นโยบายความมั่นคงปลอดภัย ขั้นตอนปฏิบัติ และเอกสารสนับสนุนอื่นๆรวมทั้งกระบวนการในการทบทวนมาตรการดังกล่าว เพื่อให้สามารถปรับปรุงหรือแก้ไขข้อบกพร่องหรือปัญหาทางด้านความมั่งคงปลอดภัยได้อย่างมีประสิทธิภาพ

หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

๑. ผู้บริหารระดับสูงสุด (CEO)

๑.๑ กำกับให้มีการกำหนด จัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัยอยู่เสมอ

๑.๒ กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ผู้ใดฝ่าฝืน หรือละเลยการปฏิบัติตามแนวทางนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ มอบหมาย อำนาจ หน้าที่ให้ผู้ดูแล ควบคุมและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๒. ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

๒.๑ กำกับให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน (Procedures) กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)

๒.๒ กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๒.๓ กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๒.๔ จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

๓. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (IT Director)

๓.๑ กำหนดให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน (Procedures) กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)

๓.๒ กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๓.๓ กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงการคลัง

๓.๔ จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

๔. ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

๔.๑ กำหนดมาตรการควบคุม กำหนดสิทธิการใช้งานระบบงานต่าง ๆ ของหน่วยงาน

๔.๒ ควบคุม การบริหารจัดการใช้งานระบบงานหรือแอพพลิเคชั่นของหน่วยงาน

๕. ผู้ดูแลระบบคอมพิวเตอร์ (System Administrator)

๕.๑ ดูแลบัญชีผู้ใช้ กำหนดสิทธิ และทบทวนสิทธิการใช้งานของผู้ใช้ระบบ

๕.๒ บริหารจัดการเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายให้มีความมั่งคงปลอดภัย และสามารถใช้งานได้ตลอดเวลา

๕.๓ ตรวจสอบข้อมูลล็อกของเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายรวมทั้งจัดทำรายงานสรุปเสนอผู้บังคับบัญชา

๕.๔ ทำการสำรองข้อมูลและตรวจสอบข้อมูลที่สำรองไว้

๖. ผู้พัฒนาระบบ (System Developer)

๖.๑ ร่วมกับเจ้าของระบบหรือแอพพลิเคชั่นเพื่อกำหนด User requirement และ Security requirement สำหรับระบบหรือแอพพลิเคชั่น

๖.๒ พัฒนาระบบโดยคำนึงถึงความถูกต้องของข้อมูลนำเข้า ข้อมูลที่อยู่ในระหว่างการประมวลผล และข้อมูลนำออก

๖.๓ ทำการทดสอบระบบหรือแอพพลิเคชั่นก่อนเริ่มต้นการใช้งานจริง

๖.๔ จัดทำคู่มือการใช้งาน คู่มือสำหรับระบบ และหรือคู่มือสำหรับการดำเนินงาน

๖.๕ จัดอบรมการใช้งานระบบหรือแอพพลิเคชั่นให้กับผู้ใช้งานที่เกี่ยวข้อง

๗. ผู้ดูแลระบบเครือข่าย (System Network)

๗.๑ บันทึกเหตุการณ์ ตรวจสอบการเข้าถึงระบบเครือข่ายของหน่วยงาน

๗.๒ ควบคุมดูแลระบบเครือข่ายสื่อสารให้สามารถใช้งานได้ตลอดเวลา

๗.๓ ควบคุมการดำเนินการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นแนวทางตามที่ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดไว้

๘. ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

๘.๑ ร่วมกับเจ้าของระบบหรือแอพพลิเคชั่นเพื่อกำหนด Security requirements สำหรับระบบหรือแอพพลิเคชั่น

๘.๒ กำหนดมาตรการควบคุม กำหนดสิทธิการใช้ระบบเครือข่ายสื่อสารของหน่วยงาน

๘.๓ ตรวจสอบป้องกันการบุกรุกจู่โจมจากผู้ไม่ประสงค์ดี

๙. เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

๙.๑ ช่วยเหลือและประสานงานกับเจ้าหน้าที่ผู้ใช้งานของสำนักงานปลัดกระทรวงการคลัง (End User) ในการแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์

๙.๒ ทำหน้าที่รับมือกับเหตุการณ์ความมั่งคงปลอดภัยตามที่ได้รับรายงานโดยปฏิบัติตามขั้นตอนปฏิบัติอย่างเคร่งครัด

๙.๓ บันทึกข้อมูลปัญหาการใช้งานเครื่องคอมพิวเตอร์และข้อมูลเหตุการณ์ความมั่งคงปลอดภัยและจัดทำรายงานสรุปปัญหาและเสนอผู้บังคับบัญชา

๑๐.ผู้ใช้งาน (End User)

๑๐.๑ ปฏิบัติตามนโยบายฉบับนี้โดยเคร่งครัด