ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตาม วิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยใน การทำธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕”

ข้อ ๒ ในกรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย ของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดในแนบท้ายประกาศฉบับนี้

ข้อ ๓ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ประกาศ ณ วันที่๑๓ พฤศจิกายน พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุดิษฐ์นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบ สารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ นั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศ ต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามบัญชีแนบ ท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้มาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น ๑๑ ข้อ ได้แก่

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
๓. การบริหารจัดการทรัพย์สินสารสนเทศ
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความ ต่อเนื่อง
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศ นโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน (Information security policy document)

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการ มอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ (Management commitment to information security)

๒.๒ สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงาน ร่วมกันได้ระหว่างระบบเดิมและระบบใหม่ (Authorization process for information processing facilities)

๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-Disclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูล สารสนเทศ (Confidentiality agreements)

๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน (Addressing security when dealing with customers)

๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของ หน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมี ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง (Addressing security in third-party agreements)

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูล ที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง (Inventory of assets)

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๔.๑ กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน หรือหน่วยงาน หรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้ (Roles and responsibilities)

๔.๒ ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้ (Management of responsibilities)

๔.๓ กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน (Disciplinary process)

๔.๔ กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน (Termination responsibilities)

๔.๕ พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน (Return of assets)

๔.๖ ให้ยกเลิกสิทธิของพนักงาน หน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการ เข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น (Removal of access rights)

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศ (Physical security perimeter)

๕.๒ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติเช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น (Protecting against external and environmental threats)

๕.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อ ป้องกันการเข้าถึงโดยมิได้รับอนุญาต (Equipment siting and protection)

๕.๔ มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

๕.๕ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้ งานอยู่เสมอ (Equipment maintenance)

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๖.๑ มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้ (Documented operating procedures)

๖.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่างจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับ การให้บริการ (Service delivery)

๖.๓ มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการ แก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ (Monitoring and review of third party services)

๖.๔ จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชั่นใหม่และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ (System acceptance)

๖.๕ มีขั้นตอนควบคุม การตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มี การสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์ (Controls against malicious code)

๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรอง ข้อมูลที่หน่วยงานประกาศใช้ (Information back-up)

๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์รวมทั้งข้อมูลสารสนเทศ ที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว (Network controls)

๖.๘ มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการ ในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยัง ผู้ให้บริการภายนอก (Security of network services)

๖.๙ จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ (Information exchange policies and procedures)

๖.๑๐ จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือ หน่วยงานภายนอก (Exchange agreements)

๖.๑๑ จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ (Business information systems)

๖.๑๒มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต (Electronic commerce)

๖.๑๓ มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่หรือถูกส่งซ้ำโดยมิได้รับอนุญาตำ (Online transactions)

๖.๑๔ สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลง โดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ (Publicly available information)

๖.๑๕ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เก่ยวกับความมั่นคงปลอดภัยต่างๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการ ติดตามการควบคุมการเข้าถึง (Audit logging)

๖.๑๖ มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตาม สังเกตดังกล่าวอย่างสม่ำเสมอ (Monitoring system use)

๖.๑๗ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต (Protection of log information)

๖.๑๘ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator) (Administrator and operator logs)

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์

๗.๑ จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าว สอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคง ปลอดภัยระบบสารสนเทศ (Access control policy)

๗.๒ จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน (User registration)

๗.๓ การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม (Privilege management)

๗.๔ ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน (Unattended user equipment)

๗.๕ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน (Policy on use of network services)

๗.๖ ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้ (User identification and authentication)

๗.๗ ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติหากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้ (Session time-out)

๗.๘ จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้ (Information access restriction)

๗.๙ กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือ สมาร์ทโฟน (Smartphone) เป็นต้น (Mobile computing policy)

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบ คอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๘.๑ ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่หรือการปรับปรุงระบบสารสนเทศเดิม ให้มี การระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย (Security requirements analysis and specification)

๘.๒ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์ (Outsourced software development)

ข้อ ๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการ ที่เหมาะสมโดยเร็วที่สุด (Security incident management)

ข้อ ๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ภายในระยะเวลาที่กำหนดไว้ (Business continuity management)

ข้อ ๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Compliance)

๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตาม กฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็น ปัจจุบันอยู่เสมอ (Identification of applicable legislation)

๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)

๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผล การใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์ การใช้งานและคงความมีประสิทธิผลอยู่เสมอ

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ไว้อย่างชัดเจน (Allocation of information security responsibilities)

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน (Contact with special interest groups)

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน (Independent review of information security)

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศ

๓.๑ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน (Ownership of assets)

๓.๒ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสารและมี การประกาศใช้ในหน่วยงาน (Acceptable use of assets)

๓.๓ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน (Classification Guideline)

๓.๔ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และการจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงาน ประกาศใช้ (Information labelling and handling)

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความ มั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง (Information security awareness, education and training)

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถาน

ที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ (Securing offices, rooms and facilities)

๕.๒ ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต (Removal of property)

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๖.๑ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ (Change management)

๖.๒ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม (Capacity management)

๖.๓ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

๖.๔ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าว อย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม (Fault logging)

๖.๕ ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลา ที่เชื่อถือได้ (Clock synchronization)

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์

๗.๑ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด (Password use)

๗.๒ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น (Policy on use of network services)

๗.๓ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล (User authentication for external connections)

๗.๔ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์ (Remote diagnostic and configuration)

๗.๕ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน (Segregation in networks)

๗.๖ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น (Network routing control)

๗.๗ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์ (Secure log-on procedure)

๗.๘ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย (Password

management system)

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบ คอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๘.๑ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม (Input validation)

๘. ๒ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม (Output validation)

๘.๓ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน (Key Management)

๘.๔ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมี แนวทางควบคุมและป้องกันข้อมูลรั่วไหล (Protection of system test data)

๘.๕ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม (Access control to program source code)

๘.๖ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผล กระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน (Technical review of applications after operating system changes)

ข้อ ๙. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

๙.๑ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน (Including information security in the business continuity management process)

๙.๒ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่อง ในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความ มั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล (Business continuity planning framework)

๙.๓ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ (Testing, maintaining and re-assessing business continuity plans)

ข้อ ๑๐. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๐.๑ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน (Data protection and privacy of personal information)

๑๐.๒ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน (Regulation of cryptographic controls)

๑๐.๓ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับ

มาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Technical compliance checking)

๑๐.๔ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ (Information systems audit controls)

๑๐.๕ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) (Protection of information systems audit tools)

๓. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและ ระดับกลาง และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๑.๑ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information security coordination)

๑.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือ หน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ ต่าง ๆ ไว้อย่างชัดเจน

๑ .๓ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของ หน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต (Identification of risks related to external parties)

ข้อ ๒. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๒.๑ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึง ระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน (Screening)

๒.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา (Terms and conditions of employment)

ข้อ ๓. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๓.๑ ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ (Physical entry controls)

๓.๒ มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคง ปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน (Working in secure areas)

๓.๓ มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูล สารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต (Public access, delivery and loading areas)

๓.๔ มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น (Cabling security)

๓.๕ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงาน ของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ (Security of equipment off-premises)

๓.๖ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลาย ข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและ ติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก (Secure disposal or re-use of equipment)

ข้อ ๔. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๔.๑ มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท (Segregation of duties)

๔.๒ มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยง ในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต่ (Separation of development, test and operational facilities)

๔.๓ มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคง ปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจท่เกี่ยวข้องและการประเมินความเสี่ยงี อย่างต่อเนื่อง

๔.๔ หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บแอพพลิเคชั่นที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบาย การรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้ (Controls against mobile code)

๔.๕ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้(Removable media) (Management of removable media)

๔.๖ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้(Removable media) อย่างมั่นคงปลอดภัย (Disposal of media)

๔.๗ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึงโดยมิได้รับอนุญาต (Security of system documentation)

๔.๘ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศ ได้รับความเสียหาย (Physical media in transit)

๔.๙ ให้มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์(Electronic

messaging) เช่น จดหมายอิเล็กทรอนิกส์(E - mail) EDI หรือ Instant messaging)

ข้อ ๕. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์

๕.๑ จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ (User password management)

๕.๒ กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ (Review of user access rights)

๕.๓ มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บในอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ท่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้และนโยบาย Clear screen สำหรับระบบสารสนเทศ (Clear desk and clear screen policy)

๕.๔ ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ(Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่ กำหนดไว้เท่านั้น ทั้งนี้จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต (Automatic equipment identification)

๕.๕ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้ (Use of system utilities)

๕.๖ จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความ มั่นคงปลอดภัย (Limitation of connection time)

๕.๗ สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยก ออกมาต่างหาก โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น (Sensitive system isolation)

๕.๘ กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

ข้อ ๖. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบ คอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ

๖.๑ ให้มีการตรวจสอบ (Validate) การทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด (Control of internal processing)

๖. ๒ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม (Message integrity)

๖.๓ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ (Policy on the use of cryptographic controls)

๖.๔ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Control of operational software)

๖.๕ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่

เป็นทางการ (Change control procedures)

๖.๗ ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด (Restrictions on changes to software packages)

๖.๘ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ (Information leakage)

ข้อ ๗. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๗.๑ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ (Reporting security weaknesses)

๗.๒ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดอย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล (Responsibilities and procedures)

๗.๓ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทางอาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ (Collection of evidence)

ข้อ ๘. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความ ต่อเนื่อง ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผล กระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ (Business continuity and risk assessment)

ข้อ ๙. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการ ใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๙.๑ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการ ใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ (Intellectual property rights)

๙.๒ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้อง กับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ (Protection of organizational records)