ประกาศสภาวิศวกร
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสภาวิศวกร พ.ศ. ๒๕๖๓

ตามมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีระบบสารสนเทศ ที่มีความมั่นคงปลอดภัยและเชื่อถือได้

สภาวิศวกรจึงสมควรให้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบสารสนเทศของสภาวิศวกร มีความมั่นคงปลอดภัยเป็นไปอย่างถูกต้องตามกฎหมาย สามารถให้บริการได้อย่างต่อเนื่อง สร้างความมั่นใจให้กับผู้ใช้งาน และมิให้มีการกระทำด้วยประการใด ๆ ทำให้ระบบสารสนเทศไม่สามารถทำงานได้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศ เพื่อเผยแพร่ข้อมูลอันเป็นเท็จ ซึ่งอาจก่อให้เกิดความเสียหายแก่สภาวิศวกร และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และเพื่อให้สอดคล้องตามพระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ คณะกรรมการสภาวิศวกรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภาวิศวกร ตามประกาศดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสภาวิศวกร เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสภาวิศวกร พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

(๑) “ระบบสารสนเทศ” หมายความว่า ระบบงานของสภาวิศวกร ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สภาวิศวกรสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการ ติดต่อสื่อสาร ซึ่งมีองค์ประกอบได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล สารสนเทศ และอื่นๆ

(๒) “ผู้ใช้งาน” หมายความว่า กรรมการสภาวิศวกร กรรมการจรรยาบรรณ ผู้ตรวจสภาวิศวกร อนุกรรมการ คณะทำงาน ผู้ชำนาญการพิเศษ ที่ปรึกษา เจ้าหน้าที่สภาวิศวกร หรือลูกจ้างของสภาวิศวกร รวมทั้งผู้รับบริการและผู้ใช้งานทั่วไปที่ได้รับอนุญาตให้สามารถเข้าใช้งานบริการหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสภาวิศวกร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทที่สภาวิศวกรกำหนดไว้

(๓) “ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่สภาวิศวกรที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ

(๔) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสภาวิศวกร

(๕) “การเข้าถึงและการใช้งานระบบสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๖) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติ ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๗) “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๘) “ข้อมูล” หมายความว่า ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์

ข้อ ๔ วัตถุประสงค์ของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสภาวิศวกร มีดังนี้

(๑) สร้างความมั่นใจว่าการใช้งานและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภาวิศวกร เป็นไปอย่างถูกต้องตามกฎหมาย และข้อบังคับที่เกี่ยวข้อง

(๒) มีแนวปฏิบัติที่รัดกุมเพื่อปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบต่าง ๆ ได้แก่ การสูญหาย การถูกทำลาย การแก้ไข โดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้ หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบสารสนเทศ มีความถูกต้อง เชื่อถือได้ และสามารถให้บริการได้อย่างต่อเนื่อง

(๓) ให้ผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้องทราบและเข้าใจถึงแนวปฏิบัติ ข้อควรระวังและความรับผิดชอบในการใช้งานนั้นๆ เพื่อส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ และการใช้งานตรงตามวัตถุประสงค์ของสภาวิศวกร รวมทั้งไม่ขัดต่อระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

ข้อ ๕ ขอบเขตการดำเนินการ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภาวิศวกรมีขอบเขตครอบคลุม มีดังนี้

(๑) การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม สภาวิศวกรจำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็นและความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความมั่นคงปลอดภัยของสภาวิศวกร

(๒) การบริหารจัดการระบบสารสนเทศและระบบสำรองของระบบสารสนเทศ เพื่อบริหารจัดการระบบสารสนเทศและจัดทำระบบสำรองของระบบสารสนเทศ เพื่อให้ข้อมูลสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย ให้สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความพร้อมใช้งาน (Availability Risk)

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้เกิดการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อสามารถจัดการกับความเสี่ยงที่ตรวจพบได้อย่างเหมาะสม และสอดคล้องกับมาตรฐานและข้อบังคับต่างๆ ที่เกี่ยวข้องกับสภาวิศวกร

(๔) โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศและการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อจัดโครงสร้างของหน่วยงานภายในที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม และกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการกำกับดูแลกิจกรรมต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ และเพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้อง ได้รับความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

(๕) การบริหารจัดการทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของสภาวิศวกร เป็นไปอย่างมีระเบียบและถูกต้องทั้งในด้านจริยธรรมจรรยาบรรณ และด้านกฎหมาย รวมทั้งให้ผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้อง ใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพ

(๖) การป้องกันภัยคุกคามเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของสภาวิศวกร และอาจสร้างความเสียหายและส่งผลกระทบต่อการใช้งานและการให้บริการของระบบสารสนเทศและต่อภาพลักษณ์ของสภาวิศวกร

ข้อ ๖ องค์ประกอบนโยบาย มีดังนี้

(๑) นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(ก) ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพสิ่งแวดล้อม

๑) ต้องมีการการจัดแบ่งพื้นที่ออกเป็นออกเป็นอย่างน้อย ๒ พื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๒) การป้องกันห้องเซิร์ฟเวอร์ (Server) และระบบเครือข่าย ต้องมีการควบคุมทั้งในด้านกายภาพ และด้านการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

(ข) ด้านการควบคุมการเข้า-ออกพื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๑) ต้องมีการควบคุมการเข้าไปในพื้นที่ควบคุม

๒) ต้องมีการควบคุมการเข้าไปในพื้นที่จำกัดการเข้าถึง

(ค) ด้านการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)

๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยสารสนเทศ

๒) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ให้กำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๓) กำหนดให้มีการแบ่งประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

(ง) ด้านการกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

๑) ควบคุมการเข้าถึงสารสนเทศ ให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ

๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และความต้องการทางธุรกิจที่เปลี่ยนไป

(จ) ด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑) สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อให้มีความรู้ความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๒) ลงทะเบียนผู้ใช้งาน (User Registration) เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ

๓) ยกเลิกสิทธิการใช้งานระบบสารสนเทศ และตัดออกจากทะเบียนผู้ใช้งาน เมื่อผู้ใช้งานสิ้นสุดภาระหน้าที่ และมีการยกเลิกเพิกถอนการอนุญาต

๔) บริหารจัดการสิทธิของผู้ใช้งาน (User Management) เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศ แต่ละชนิดตามความเหมาะสม

๕) บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) เพื่อความรัดกุมของการใช้งานรหัสผ่านของผู้ใช้งาน

๖) ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) โดยจัดทำเป็นกระบวนการ ตามรอบระยะเวลาที่กำหนดไว้

(ฉ) ด้านการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑) ให้การใช้งานรหัสผ่าน (Password Use) เป็นไปตามข้อกำหนดที่ดี เพื่อให้การกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน ที่มีคุณภาพ

๒) ให้ป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ขององค์กรในขณะที่ไม่มีผู้ดูแล

๓) ควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และเพื่อกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔) เข้ารหัสข้อมูลที่เป็นความลับ เพื่อรักษาความลับของข้อมูล โดยผู้ใช้งานสามารถใช้มาตรการการเข้ารหัสข้อมูล สำหรับข้อมูลที่ถูกจัดลำดับชั้นความลับ ตามข้อกำหนดเกี่ยวกับลำดับชั้นความลับของข้อมูลที่กำหนดไว้ตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ หรือตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

(ช) ด้านการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๑) การใช้บริการระบบเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๓) การระบุอุปกรณ์บนระบบเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนระบบเครือข่ายได้ และให้ใช้การระบุอุปกรณ์บนระบบเครือข่ายเป็นการยืนยัน

๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่าย

๕) การแบ่งแยกระบบเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ

๖) การควบคุมการเชื่อมต่อทางระบบเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึง หรือใช้งานระบบเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อ ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๗) การควบคุมการจัดเส้นทางบนระบบเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนระบบเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๘) การใช้งานอินเตอร์เน็ต ต้องเชื่อมต่อเครื่องคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น ต้องติดตั้งโปรแกรมตรวจจับไวรัสบนเครื่องที่จะใช้เชื่อมต่อ และต้องตรวจสอบไวรัสทุกครั้งเมื่อมีการรับ-ส่งข้อมูลผ่านทางอินเตอร์เน็ต ไม่ใช้อินเตอร์เน็ตขององค์กรในการทำธุรกรรมหรือการกระทำใด ๆ ที่ไม่เหมาะสม หรือละเมิดกฎหมาย หรือทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กรหรือทำลายความสัมพันธ์ของพนักงานหน่วยงานอื่น ๆ หรือเพื่อหาแสวงหาผลประโยชน์ส่วนตัว

๙) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Network) เป็นความรับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศที่ต้องพิจารณาอนุญาตทั้งในด้านการติดตั้งระบบเครือข่ายไร้สาย การลงทะเบียนอุปกรณ์และผู้ใช้งาน การกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ การกำหนดรหัสผ่านในการเข้าใช้งาน การทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ การตั้งค่าอุปกรณ์ให้มีความมั่นคงปลอดภัย การติดตั้งไฟร์วอลล์ เพื่อป้องกันการเข้าถึงเครือข่ายภายในจากการเชื่อมต่อผ่านเครือข่ายไร้สาย

(๒) ด้านการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต

๑) กำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานที่มีความมั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการ ต้องควบคุมโดยวิธีการยืนยันตัวตน ที่มีความมั่นคงปลอดภัย

๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งาน มีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งส่งผลให้การกำหนดรหัสผ่านที่มีคุณภาพ

๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ หรือที่มีอยู่แล้ว

๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Timeout)

๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(ฌ) ด้านการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน ของระบบสารสนเทศ (Application and Information Access Control)

๑) การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องมีการกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับหน้าที่ความรับผิดชอบของพนักงาน มีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ มีการตรวจสอบตัวตนของผู้เข้าใช้ด้วยบัญชีชื่อผู้ใช้ และรหัสผ่าน ระมัดระวังการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ไม่ให้เกิดความเสียหายต่อองค์กร หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม ไม่แสวงหาประโยชน์ และใช้เพื่อการทำงานขององค์กรเท่านั้น รวมถึงต้องมีการตรวจสอบไวรัสของเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดใช้งาน

๒) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรทางด้านสารสนเทศการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๓) การจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (Outsource) ต้องมีการลงนามในการรักษาความลับ ห้ามเปิดเผยข้อมูลขององค์กรก่อนปฏิบัติหน้าที่

๔) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๕) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๖) การปฏิบัติงานจากภายนอกองค์กร (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงาน จากภายนอกองค์กร

(๒) นโยบายการจัดทำระบบสำรองของระบบสารสนเทศ การจัดให้มีระบบสารสนเทศและระบบสำรองของระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ให้ปฏิบัติดังนี้

(ก) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองของระบบสารสนเทศ ที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(ข) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(ค) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองของระบบสารสนเทศ และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(ง) ต้องมีการทดสอบและซักซ้อมสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองของระบบสารสนเทศและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(จ) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๓) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

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

(ข) ในการตรวจสอบและประเมินความเสี่ยง ต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

(๔) นโยบายโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศและการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(ก) การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ให้ฝ่ายเทคโนโลยีสารสนเทศสภาวิศวกร เป็นผู้รับผิดชอบดำเนินการ ให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง

(ข) ฝ่ายเทคโนโลยีสารสนเทศ สภาวิศวกร ต้องจัดให้มีกิจกรรมการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้ใช้งานและบุคคลที่เกี่ยวข้อง ได้รับความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง อย่างน้อยปีละ ๑ ครั้ง

(๕) นโยบายการบริหารจัดการทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

(ก) ด้านการบริหารจัดการทรัพย์สิน

๑) ต้องมีการควบคุมการเข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ขององค์กร การนำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) การนำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมต่อเข้าระบบเครือข่าย

๒) ต้องมีการป้องกันการใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ การคัดลอกหรือทำสำเนาแฟ้มข้อมูล ที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

๓) ต้องมีการกำหนดหน้าที่รับผิดชอบต่อทรัพย์สินที่องค์กรมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งาน การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยพนักงานที่องค์กรมอบหมาย

๔) ต้องมีการกำหนดให้ชดใช้ค่าเสียหาย หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน ไม่ว่าทรัพย์สินนั้น ชำรุดหรือสูญหาย ตามระเบียบขององค์กร

๕) ต้องมีการกำหนดห้ามไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือคอมพิวเตอร์ประเภทพกพา ไม่ว่าในกรณีใด ๆ

๖) ต้องมีการควบคุมการนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่องค์กรจัดเตรียมไว้ให้ใช้งานไปใช้ในกิจกรรมที่องค์กรไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์กร และต้องมีการกำหนดความรับผิดชอบกับผู้ที่ก่อความเสียหายโดยให้ถือเป็นความผิดส่วนบุคคล

(ข) ด้านการบริหารจัดการข้อมูลองค์กร

๑) ต้องมีการสร้างความตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นเป็นขององค์กร หรือบุคคลภายนอก โดยห้ามให้มีการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายข้อมูลที่ถือเป็นทรัพย์สินขององค์กร โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๒) ต้องกำหนดความรับผิดชอบในการดูแลรักษาข้อมูลขององค์กร และความรับผิดชอบต่อความเสียหายของข้อมูล หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด หรือถูกเผยแพร่โดยไม่ได้รับอนุญาต และต้องมีการป้องกันดูแลรักษาไว้ ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๓) การป้องกันข้อมูลส่วนบุคคลเป็นสิทธิของผู้ใช้งาน ซึ่งองค์กรให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น

(ค) ด้านการบริหารจัดการระบบสารสนเทศ

๑) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายกลไกการรักษาความปลอดภัยระบบสารสนเทศ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบ

๒) ต้องควบคุมไม่ให้มีการทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๓) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๔) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๕) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่เป็นการทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

๖) ต้องควบคุมไม่ให้มีการนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๗) ต้องควบคุมไม่ให้เปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๘) ต้องควบคุมไม่ให้เปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง ในระหว่างเวลาปฏิบัติงาน

๙) ต้องควบคุมไม่ให้ใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดขององค์กรที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมหรือเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร หรือความมั่นคงของประเทศ

๑๐) ต้องควบคุมไม่ให้ใช้ทรัพยากรทุกประเภทที่เป็นขององค์กร เพื่อประโยชน์ทางการค้า

๑๑) ต้องควบคุมไม่ให้กระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพเสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๑๒) ต้องควบคุมไม่ให้กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศขององค์กร ต้องหยุดชะงัก

๑๓) ต้องควบคุมไม่ให้ใช้ระบบสารสนเทศขององค์กร เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๔) ต้องควบคุมไม่ให้กระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งาน หรือรับรู้รหัสส่วนบุคคล ของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๕) ต้องควบคุมไม่ให้ติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อให้เข้าถึงระบบสารสนเทศขององค์กร โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ

(ง) ด้านการปฏิบัติตามข้อบังคับ

๑) บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบขององค์กรที่กำหนด หรือออกกฎระเบียบโดยอาศัยนโยบายดังกล่าวข้างต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๒) ซอฟต์แวร์ (Software) ที่องค์กร อนุญาตให้ใช้งาน หรือที่องค์กรมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และผู้ใช้งานต้องไม่ติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่

ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์องค์กร ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๓) ซอฟต์แวร์ (Software) ที่องค์กรได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการปฏิบัติงาน ผู้ใช้งาน ต้องไม่ติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือ ทำสำเนาเพื่อนำไปใช้งานที่อื่น

๔) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ ๒) พ.ศ. ๒๕๖๐ โดยจัดเก็บไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง เป็นระยะเวลาอย่างน้อย ๙๐ วัน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องมีการกำหนดชั้นความลับในการเข้าถึง

๕) ต้องตั้งเวลานาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๖) ต้องควบคุมไม่ให้ผู้ดูแลระบบ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือบุคคลที่องค์กรมอบหมายเท่านั้น

๗) ต้องควบคุมไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลในสื่อเก็บข้อมูลดังกล่าว และจำกัดสิทธิการเข้าถึงข้อมูลเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๖) นโยบายการป้องกันภัยคุกคามเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

(ก) ด้านการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่องค์กรได้จัดหาหรือได้ประกาศให้ใช้ เว้นแต่เครื่องคอมพิวเตอร์นั้น เป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

๒) ข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๓) ต้องควบคุมให้มีการปรับปรุงข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๔) ต้องสร้างความตระหนักและพึงระวังเกี่ยวกับไวรัสและโปรแกรมไม่ประสงค์ดี และต้องแจ้งเหตุแก่ผู้ดูแลระบบหากพบสิ่งผิดปกติ

๕) ต้องควบคุมไม่ให้เชื่อมต่อเครื่องคอมพิวเตอร์ที่ติดไวรัสเข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๖) ต้องกำหนดให้ผู้ใช้งานไม่ลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินขององค์กร หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๗) ต้องควบคุมไม่ให้เผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สินขององค์กร

(ข) ด้านการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) ต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุกเอาไว้ในตำแหน่งที่มีความเสี่ยงต่อการถูกโจมตี หรือบุกรุกได้

๒) ต้องมีการปรับแต่ง (Tuning) การทำงานของระบบตรวจจับและป้องกันการบุกรุก โดยให้ป้องกันได้มากที่สุด และเกิดการตรวจจับที่ผิดพลาด (False Positive) น้อยที่สุด

๓) ต้องมีการตั้งระบบตรวจจับและป้องกันการบุกรุก ให้สามารถ Update Signature ได้โดยอัตโนมัติ หรือผู้ดูแลระบบเครือข่ายต้อง Update Signature ทุกสัปดาห์

๔) ต้องตรวจสอบการทำงานของระบบตรวจจับและป้องกันการบุกรุกและตรวจสอบ Log พร้อมทดสอบการทำงานทุกเดือน

๕) การเปลี่ยนแปลงใดๆ ที่เกี่ยวกับระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการบันทึก และรายงานต่อผู้บริหารที่รับผิดชอบ

๖) อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ และให้ติดตั้งในห้องที่มีการรักษาความปลอดภัย

(ค) ด้านการจัดการเหตุการณ์ (Incident) ด้านความมั่นคงปลอดภัยสารสนเทศ

๑) ต้องกำหนดมีการแจ้งไปยังผู้ดูแลระบบ/ผู้เกี่ยวข้อง โดยทันที เมื่อพบเห็นเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

๒) หากพบจุดอ่อนช่องโหว่ในระบบสารสนเทศ จะต้องไม่เปิดเผย เผยแพร่ สนทนา หรือกระทำการใดๆ อันเป็นการเผยแพร่ต่อผู้อื่น ต้องให้แจ้งต่อผู้ดูแลระบบ โดยด่วนที่สุด

๓) ต้องกำหนดให้มีคณะทำงานเพื่อทำหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศในการแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๔) เมื่อได้รับแจ้งเหตุการณ์ คณะทำงานจะต้องดำเนินการวิเคราะห์ความรุนแรงและผลกระทบของเหตุการณ์นั้น ๆ และร่วมกันหาวิธีการแก้ไข

๕) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศ โดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อการรักษาความถูกต้องทางด้านหลักฐาน และดำเนินการทางกฎหมาย ในกรณีที่จำเป็น

ข้อ ๗ รายละเอียดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสภาวิศวกร ให้จัดทำเป็นคู่มือ เมื่อได้รับความเห็นชอบจากคณะกรรมการสภาวิศวกรแล้ว ให้ใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ข้อ ๘ ให้คณะอนุกรรมการเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการกำกับดูแลให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้คณะกรรมการสภาวิศวกรเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

จึงประกาศให้ทราบโดยทั่วกัน และขอให้ผู้ใช้งานถือเป็นแนวทางในการปฏิบัติต่อไป

ประกาศ ณ วันที่ ๓๑ กรกฎาคม พ.ศ. ๒๕๖๓

(นายสุชัชวีร์ สุวรรณสวัสดิ์)
นายกสภาวิศวกร

รายละเอียดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศสภาวิศวกร

ตามข้อ ๗ ของประกาศสภาวิศวกร

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศสภาวิศวกร

พ.ศ. ๒๕๖๓

Ver.02/2564

ส่วนที่ ๑ แนวปฏิบัติการเข้าถึงการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้ที่เกี่ยวข้องได้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบแนวปฏิบัติ

๑. ฝ่ายเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ใช้งาน

คำนิยามเพิ่มเติม

“สินทรัพย์” หมายความว่า สินทรัพย์ที่เป็นข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสภาวิศวกร ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ซอฟต์แวร์โปรแกรมประยุกต์ที่หน่วยงานพัฒนาเองหรือจ้างพัฒนาขึ้น รวมทั้งสิ่งใดก็ตามที่มีคุณค่าสำหรับสภาวิศวกรในลักษณะเดียวกันดังกล่าว

แนวปฏิบัติ

๑. ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and Environment Security)

เพื่อรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

(๑.๑) การรักษาความมั่นคงปลอดภัยบริเวณห้องเซิร์ฟเวอร์ (Server Room) ให้ปฏิบัติดังนี้

(๑.๑.๑) พื้นที่ใช้งานระบบสารสนเทศและการสื่อสารแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บ อุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย และพื้นที่สำหรับผู้มาติดต่อ

(๑.๑.๒) จัดทำแผนผังพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๑.๑.๓) กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๑.๑.๔) การควบคุมการเปิด-ปิด ห้องเซิร์ฟเวอร์

(๑.๑.๕) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่าย ภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมี เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้อำนาจอนุมัติลงนาม

(๑.๑.๖) ให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการ ใช้งานโดยให้มีระบบไฟฟ้าสำรอง ระบบดับเพลิง ระบบปรับอากาศ กล้องวงจรปิด(CCTV)

(๑.๑.๗) ติดตั้งระบบแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือ หยุดการทำงาน

(๑.๑.๘) เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก และสำนักงานหรือห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๑.๑.๙) เจ้าหน้าที่ผู้ได้รับมอบหมายต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ที่ตนได้รับมอบหมายตามห้วงเวลาที่กำหนด เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก อุปกรณ์ต่างๆ สื่อบันทึกข้อมูลที่สำคัญถูกจัดเก็บ หรือได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

(๑.๒) การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ล ดำเนินการ ดังต่อไปนี้

(๑.๒.๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๑.๒.๒) ให้มีการร้อยท่อสายสัญญาณ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๑.๒.๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้ากระแสสลับแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวน ของสัญญาณซึ่งกันและกัน

(๑.๒.๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการเชื่อมต่อสายสัญญาณผิดเส้น

(๑.๒.๕) จัดทำผังสายสัญญาณสื่อสาร ให้ครบถ้วนและถูกต้อง โดยให้ถือเป็นเอกสารลับขององค์กร

(๑.๒.๖) ห้อง และตู้อุปกรณ์ที่มีสายสัญญาณสื่อสารต่างๆ ให้มีการป้องกันการเข้าถึงจากบุคคลภายนอก

(๑.๓) การบำรุงรักษาอุปกรณ์ให้ปฏิบัติ ดังนี้

(๑.๓.๑) ให้มีการบำรุงรักษาอุปกรณ์ตามห้วงระยะเวลาที่กำหนด

(๑.๓.๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๑.๓.๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๑.๓.๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุง อุปกรณ์ ดังกล่าว

(๑.๓.๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๑.๓.๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๑.๔) การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน ให้ปฏิบัติ ดังนี้

(๑.๔.๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งานนอกหน่วยงาน

(๑.๔.๒) กำหนดผู้มีอำนาจอนุมัติในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๑.๔.๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงานเมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๑.๔.๔) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐาน ป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๑.๕) การป้องกันอุปกรณ์ที่ใช้งานนอกหน่วยงาน ให้ปฏิบัติ ดังนี้

(๑.๕.๑) ให้มีการป้องกันอุปกรณ์ มิให้โดนกระแทก แตกหักในระหว่างการขนส่งหรือเคลื่อนย้าย

(๑.๕.๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๑.๕.๓) ในการนำอุปกรณ์ไปใช้งานภายนอกหน่วยงานให้ผู้ยืมรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นทรัพย์สินของตนเอง

(๑.๖) การจำหน่ายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ ให้ปฏิบัติ ดังนี้

(๑.๖.๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะจำหน่ายอุปกรณ์ หรือส่งมอบอุปกรณ์ให้ผู้อื่นในลักษณะการซ่อมหรือยืม

(๑.๖.๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับ จัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ หรือทำลาย เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

(๑.๗) การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ เช่น ผังเครือข่าย การตั้งค่าระบบอุปกรณ์ IP address Maps address ทั้งในรูปแบบอิเล็กทรอนิกส์ และกระดาษ ให้ปฏิบัติ ดังนี้

(๑.๗.๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๑.๗.๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๑.๗.๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่าย

๒. ด้านการควบคุมการเข้า-ออกพื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

เพื่อควบคุมการเข้าถึงทางกายภาพให้เข้าได้เฉพาะผู้ได้รับอนุญาตเท่านั้น เพื่อป้องกันสินทรัพย์ในห้องห้องเซิร์ฟเวอร์จากการสูญหาย เสียหาย รวมถึงการเข้าถึงระบบโดยไม่ได้รับอนุญาต ให้ปฏิบัติ ดังนี้

(๒.๑) การขออนุญาตเข้าปฏิบัติงานห้องเซิร์ฟเวอร์ (Server)

(๒.๑.๑) เจ้าหน้าที่สภาวิศวกรต้องได้รับความเห็นชอบ และลงบันทึกการเข้าออก

(๒.๑.๒) หน่วยงานภายนอกต้องได้รับอนุมัติเป็นลายลักษณ์อักษร และลงบันทึกการเข้าออก

(๒.๒) การใช้ห้องเซิร์ฟเวอร์ (Server) ให้ปฏิบัติ ดังนี้

(๒.๒.๑) ให้ลงบันทึกการเข้าออกผู้เข้าปฏิบัติงานห้องเซิร์ฟเวอร์ ก่อนเข้าห้องเซิร์ฟเวอร์

(๒.๒.๒) ห้ามเข้าห้องเซิร์ฟเวอร์ ก่อนได้รับอนุญาตจากผู้ดูแล หรือผู้ที่สำนักงานมอบหมาย

(๒.๒.๓) ห้ามเปิดประตูห้องเซิร์ฟเวอร์ ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตาม เข้าภายในโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจหรือผู้ที่สำนักงานมอบหมาย และได้ลงทะเบียนชื่อ ตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องเซิร์ฟเวอร์ เรียบร้อยแล้ว

(๒.๒.๔) แต่งกายให้สุภาพ ห้ามสูบบุหรี่ หรือกระทำการอื่นใดที่อาจก่อให้เกิดฝุ่นละออง หรืออัคคีภัย ห้ามนำอาหารหรือเครื่องดื่มเข้ามาในห้องเซิร์ฟเวอร์

(๒.๒.๕) ต้องได้รับอนุญาตจากผู้ดูแลหรือผู้ที่สำนักงานมอบหมาย เมื่อต้องการนำกล่องเครื่องมือหรือหีบห่อ หรือกระเป๋า เข้าและออกห้องเซิร์ฟเวอร์

(๒.๒.๖) การนำอุปกรณ์เข้าติดตั้งหรือการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ ต้องได้รับอนุมัติก่อนจึงจะสามารถนำอุปกรณ์เข้าห้องเซิร์ฟเวอร์ และให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์เพื่อใช้เป็นหลักฐานในกรณีนำอุปกรณ์เข้า หรือออก

(๒.๒.๗) ผู้ดูแล หรือผู้ที่สำนักงานมอบหมายตรวจสอบก่อน ในกรณีที่ไม่มีให้ กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ก่อนและต้องได้รับอนุมัติ จึงจะสามารถนำอุปกรณ์ออก จากห้องเซิร์ฟเวอร์ (Server)

(๒.๒.๘) เมื่อปฏิบัติงานเสร็จแล้วให้กรอกแบบรายงานการเข้าปฏิบัติงานห้องเซิร์ฟเวอร์ (Server) แล้วให้ผู้ดูแลหรือผู้ที่สำนักงานมอบหมายตรวจสอบก่อน

(๒.๓) ข้อกำหนดในการดูแลห้องเซิร์ฟเวอร์ ให้ผู้ดูแลระบบปฏิบัติดังนี้

(๒.๓.๑) บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิด (CCTV) ไว้อย่างน้อย ๑ เดือน เพื่อใช้ในการ ตรวจสอบในภายหลัง

(๒.๓.๒) ตรวจสอบประตูเข้า–ออกห้องศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ให้ปิดล็อคอยู่เสมอ

(๒.๓.๓) ให้มีการดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องเซิร์ฟเวอร์อย่างสม่ำเสมอ

๓. ด้านการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)

(๓.๑) ให้มีการจัดทำบัญชีสินทรัพย์

(๓.๑.๑) จำแนกตามประเภททรัพยากรของระบบ

(๓.๑.๒) จำแนกตามประเภทผู้ใช้งาน การทำงาน และสิทธิผู้ใช้งาน

(๓.๒) ให้มีการกำหนดเกณฑ์ในเรื่อง

(๓.๒.๑) การเข้าถึงการใช้งานสารสนเทศ

(๓.๒.๒) การอนุญาต การกำหนดสิทธิ การมอบอำนาจ และการระงับสิทธิ

(๓.๓) สิทธิในการใช้ข้อมูลต้องครอบคลุมการสร้างข้อมูล การป้อนข้อมูล การแก้ไขข้อมูล การอ่านข้อมูล รวมถึงการปลอดจากสิทธิด้วย เหล่านี้เป็นอย่างน้อย

(๓.๔) การขอสิทธิใช้งานระบบสารสนเทศของหน่วยงานมีแนวทางปฏิบัติดังนี้

(๓.๔.๑) ให้มีการตรวจสอบสิทธิก่อนขออนุมัติ

(๓.๔.๒) ผู้ประสงค์จะขอสิทธิการใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษร และผ่านการพิจารณาอนุญาตจากผู้มีอำนาจการอนุมัติ

(๓.๔.๓) เจ้าหน้าที่เทคนิคฯ แจ้งรหัสการใช้งานไปยังผู้ขอสิทธิ โดยวิธีการที่มั่นคงปลอดภัย

(๓.๕) การจัดเก็บข้อมูลมีขั้นตอนปฏิบัติดังนี้

(๓.๕.๑) กำหนดหน่วยงาน บุคคล หรือกลุ่มบุคคล ผู้รับผิดชอบในระบบข้อมูล

(๓.๕.๒) การจัดประเภทของข้อมูล ประกอบด้วย

๑) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารสภาวิศวกร (Back Office)

๒) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการยื่นคำขอ คำร้อง การจดทะเบียน การขึ้นทะเบียน การร้องเรียน และอื่น ๆ ภายใต้พระราชบัญญัติวิศวกร พ.ศ. ๒๕๔๒

(๓.๕.๓) การจัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทข้างต้น ดังนี้

๑) ข้อมูลที่มีระดับความสาคัญมากที่สุด

๒) ข้อมูลที่มีระดับความสาคัญปานกลาง

๓) ข้อมูลที่มีระดับความสาคัญน้อย

(๓.๕.๔) จัดแบ่งลำดับชั้นความลับของข้อมูล แบ่งออกเป็น

๑) ข้อมูลลับมาก หมายถึง ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๒) ข้อมูลลับ หมายถึง ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๓) ข้อมูลปกปิด หมายถึงข้อมูลซึ่งไม่เปิดเผยต่อสาธารณะโดยไม่ได้รับอนุญาต

(๓.๕.๕) ข้อมูลทางเทคนิคของระบบสารสนเทศ ให้ถือว่าเป็นข้อมูลลับมาก

(๓.๕.๖) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทข้างต้น ดังนี้

๑) สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ

๒) สามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานแล้วเท่านั้น

๓) สามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

๔) สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

(๓.๕.๗) การกำหนดเวลาการเข้าถึง ดังนี้

๑) การเข้าถึงสารสนเทศในเวลาทำการ (๐๘.๐๐ –๑๗.๐๐ น.)

๒) การเข้าถึงสารสนเทศนอกเวลาทำการ (นอกช่วงเวลา ๐๘.๐๐ –๑๗.๐๐ น.)

๓) การเข้าถึงในช่วงเวลาวันหยุดทำการ (วันหยุดทำการ และวันหยุดนักขัตฤกษ์)

๔) การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

(๓.๕.๘) การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้

๑) ระบบอินทราเน็ต (Intranet)

๒) ระบบอินเทอร์เน็ต (Internet)

๓) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๔. ด้านการกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๔.๑) หัวหน้าสำนักงานเป็นผู้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้อง และปรับปรุงแนวทางการควบคุมการเข้าถึง

(๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบ สารสนเทศ ตามที่ได้รับอนุมัติ

(๔.๓) ผู้ดูแลระบบมีหน้าที่ในการบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และเฝ้าระวังการละเมิด ความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๕. ด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๕.๑) ฝ่ายเทคโนโลยีสารสนเทศ และงานบุคคล ผสานงานจัดฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งานเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย สารสนเทศ (Information Security Awareness Training) เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบ ที่เกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมาตรการเชิงป้องกัน ตามห้วงระยะเวลาที่กำหนด

(๕.๒) การลงทะเบียนและการจัดการผู้ใช้งาน (User Registration and Management)

(๕.๒.๑) ผู้ใช้งานกรอกข้อมูลคำขอใช้งานในแบบฟอร์มการขอใช้ระบบสารสนเทศ และขอความเห็นชอบจาก ผู้มีอำนาจอนุมัติ

(๕.๒.๒) ผู้ที่เกี่ยวข้องทำการตรวจสอบคัดกรองและกำหนดสิทธิ

(๕.๒.๓) ผู้ดูแลระบบทำการกำหนดสิทธิลงในระบบ และแจ้งกลับต่อผู้ใช้งาน โดยผ่านช่องทางที่ความมั่นคง

(๕.๓) สิทธิพิเศษเพื่อปฏิบัติงานเฉพาะกิจ ต้องได้รับอนุมัติจากผู้มีอำนาจอนุมัติโดยกำหนดระยะเวลาและรายละเอียดของสิทธิ รวมทั้งต้องกำหนดให้มีรหัสการใช้งานต่างจากปกติ

(๕.๔) กำหนดการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๕.๔.๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๕.๔.๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวที่ยากต่อการเดา และต้องมีความแตกต่างกัน ระบบที่มีความสำคัญต้องเปลี่ยนรหัสผ่านอย่างน้อย ทุก ๖ เดือน

(๕.๔.๓) ผู้ดูแลระบบต้องส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการจัดส่งรหัสผ่านและผู้ใช้งาน ควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๕.๔.๔) ผู้ดูแลระบบต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้อง ก่อนที่จะอนุญาต ให้เปลี่ยนรหัสใหม่

(๕.๖) ต้องมีกระบวนการ ในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง การทบทวนสิทธิผู้ดูแลระบบ อย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง หรือการเปลี่ยนแปลงอื่นใดในลักษณะเดียวกันนี้ และให้มี พร้อมทั้ง บันทึกการเปลี่ยนแปลงของการทบทวน

๖. ความรับผิดชอบของผู้ใช้งาน

(๖.๑) การใช้งานรหัสผ่านให้ผู้ใช้งานปฏิบัติ ดังต่อไปนี้

(๖.๑.๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๖.๑.๓) ให้กำหนดรหัสผ่าน ในลักษณะที่เหมาะสม ยากต่อการคาดเดา และเป็นไปตามเทคโนโลยีที่มีการเปลี่ยนแปลง เช่น ไม่ใช้ชื่อ นามสกุล วันเกิด ตัวเลขล้วน ไม่ใช้รหัสผ่านตัวเดียวกันสำหรับหลายทะเบียนการใช้งานหรือหลายระบบงาน หรือไม่ใช้รหัสผ่านตัวเดิมหมุนเวียน

(๖.๑.๔) ห้ามใช้บัญชีการใช้งานส่วนบุคคลของผู้อื่น และไม่มีการใช้บัญชีใช้งานร่วมกัน

(๖.๑.๕) กรณีที่มีความจำเป็นต้องบอกรหัสผ่าน แก่ผู้อื่นตามความจำเป็นของสภาพงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๖.๑.๖) ให้เปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน

(๖.๑.๗) หากทราบหรือสงสัยว่ารหัสผ่านถูกเปิดเผยหรือเป็นที่ล่วงรู้ ให้เปลี่ยนรหัสผ่านทันที พร้อมทั้งแจ้งผู้บังคับบัญชาและผู้ดูแลระบบเป็นลายลักษณ์อักษร

(๖.๑.๘) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานของตนเว้นแต่พิสูจน์ได้ว่า การกระทำดังกล่าวตนไม่ได้รู้เห็นหรือยินยอมด้วย

(๖.๑.๙) หากได้รับการร้องขอให้เปลี่ยนรหัสผ่านผู้ใช้งานต้องตรวจสอบ ความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวเพื่อให้มั่นใจว่าไม่ได้เป็นการหลอกลวง

(๖.๒) แนวทางการดูแลโต๊ะทำงาน (Clear Desk and Clear Screen Policy) ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๖.๒.๑) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย โดยห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

๓) ปิดเครื่องคอมพิวเตอร์ (Log Off) ทุกครั้งหลังเลิกงานหรือไม่ใช้งาน

๔) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๕ นาที โดยต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๕) ออกจากระบบ (Log Out) จากระบบสารสนเทศหรือระบบคอมพิวเตอร์ทันที เมื่อใช้งานเสร็จหรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๖) การส่งเครื่อง ไปตรวจซ่อมจะต้องดำเนินการโดย ผู้ดูแลระบบ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ที่ได้ทำสัญญากับหน่วยงานเท่านั้น และให้มีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๗) ให้ระวังการเก็บข้อมูลสำคัญของหน่วยงานบนคอมพิวเตอร์ทั้งของหน่วยงานและของส่วนตัว

๘) ไม่นำอาหารหรือเครื่องดื่มมาวางหรือดื่มกินใกล้บริเวณเครื่องคอมพิวเตอร์

๙) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๑๐) ให้ใช้ความระมัดระวังในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ โดยใส่กล่อง หรือห่อหุ้มด้วยวัสดุป้องกันการกระแทก เพื่อป้องกันอันตรายจากการ กระทบกระเทือน

๑๑) การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดพักเครื่องเป็นระยะ

๑๒) หลีกเลี่ยงการใช้ปลายปากกา หรือวัสดุอื่นใดกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือแตกเสียหายได้

๑๓) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๔) ตรวจสอบ สายไฟ สายเมาส์ สายแป้นพิมพ์ หรือสายสัญญาณของอุปกรณ์คอมพิวเตอร์ อื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์และ คอมพิวเตอร์ได้รับความเสียหาย

๑๕) ทำความสะอาดอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้ เครื่องคอมพิวเตอร์เกิดการขัดข้อง/เสียหาย

๑๖) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์และสื่อบันทึกต่าง ๆ มิให้ถูกขโมยหรือสูญหายหรือการใช้งานโดยไม่ได้รับอนุญาต โดยล็อคเครื่องขณะไม่ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มี ความเสี่ยงต่อการสูญหาย และหากจำเป็นให้เก็บไว้ในตู้ที่สามารถล็อคได้หรือวิธีอื่นตามเหมาะสม

๑๗) ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

๑๘) ห้ามเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

๑๙) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกแบบภายนอกชนิด CD, DVD, External Hard Disk หรืออื่นๆ ที่เหมาะสม และทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

(๖.๒.๒) ผู้ใช้งานต้องให้ความร่วมมือในการป้องกันและแก้ไขไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี (malware)

๑) เครื่องคอมพิวเตอร์ที่ใช้งานต้องมีโปรแกรมป้องกันไวรัสติดตั้งอยู่และต้องเปิดใช้งานตลอดเวลาที่ใช้งาน

๒) ต้องปรับปรุงฐานข้อมูลป้องกันไวรัส (Update Virus Signature) ให้เป็นปัจจุบันอยู่เสมอ

๓) ห้ามทำการใดเพื่อขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๔) ควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่ปลอดภัยเท่านั้น และทำการตรวจหาไวรัสทุกครั้ง

๕) ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวังโดยเปิดเฉพาะเว็บไซต์ที่เกี่ยวข้องกับการทำงานเท่านั้น และต้องไม่เปิดเว็บไซต์ หรือพฤติการณ์อื่นใดที่มีความเสี่ยงต่อการติดไวรัส

๖) ห้ามติดตั้งโปรแกรม Java, ActiveX หรือโปรแกรมประเภท Active Code อื่นใดจากแหล่งที่ไม่น่าเชื่อถือ

๗) ไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักหรือชื่อเรื่องที่ไม่เคยติดต่อกันมาก่อน หรือสงสัยว่าไม่ปลอดภัย

๘) ไม่เปิด Share Drive หากมีความจำเป็นให้เปิดเพียง" Share Folder โดยต้องอนุญาต ใช้รหัสผ่าน และอนุญาตให้อ่านอย่างเดียว

๙) ห้ามสร้าง เก็บ หรือเผยแพร่ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์ บอมบ์ หรือซอฟต์แวร์ไม่ประสงค์ดีอื่นใด

๑๐) ให้ความสำคัญกับการแจ้งเตือนจากโปรแกรมป้องกันไวรัส หากมีข้อสงสัยหรือพบว่า เครื่องคอมพิวเตอร์ทำงานผิดปกติหรือโปรแกรมป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติ ต้องแจ้งผู้ดูแลระบบและดำเนินการยับยั้งหรือจำกัดความเสียหายในชั้นต้นตามคำแนะนำตามสมควร

(๖.๓) การจัดการเอกสารลับบนกระดาษหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

(๖.๓.๑) มีการจัดหมวดหมู่เอกสารลับไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างเพียงพอ

(๖.๓.๒) จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

(๖.๓.๓) ระมัดระวังการกระจาย ส่ง หรือแจกจ่ายเอกสารลับให้จำกัดไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

(๖.๓.๔) ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์ทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์

(๖.๓.๕) ควรใช้วิธีการทางเทคนิคในการเข้ารหัสลับข้อมูลสำหรับเพื่อเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์และสื่ออิเล็กทรอนิกส์

(๖.๑๔) เมื่อพ้นจากการปฏิบัติหน้าที่ หรือละเมิดกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์หรือกฎหมายอื่นใดที่เกี่ยวข้อง ผู้ใช้งานต้องคืนสินทรัพย์ทั้งหมดที่เกี่ยวข้องกับระบบงานคอมพิวเตอร์ โดยหมายรวมทั้งด้านกายภาพและด้านระบบงาน เช่น กุญแจ บัตรประจำตัว พนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และ

อุปกรณ์ต่อพ่วง คู่มือ และเอกสาร รหัสการใช้งาน ข้อมูลสำคัญ เป็นต้น โดยผู้ดูแลระบบต้องกำกับดูแลให้เป็นไปตามนั้น

(๖.๑๕) การใช้งานระบบเครือข่ายอินเทอร์เน็ต ผ่านเครือข่ายของหน่วยงาน ต้องปฏิบัติดังนี้

(๖.๑๕.๑) ต้องทำการลงทะเบียนผู้ใช้งาน

(๖.๑๕.๒) ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง การใช้งานนั้นต้องไม่เป็นสาเหตุให้หน่วยงาน และบุคคลผู้ที่เกี่ยวข้องกับหน่วยงาน เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

(๖.๑๕.๓) การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง และใช้เครื่องลูกข่ายที่ได้รับอนุมัติ ที่ได้จัดเตรียมไว้ หรือ ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะการนี้เท่านั้น ทั้งนี้ หน่วยงานขอสงวนสิทธิ ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน

(๖.๑๕.๔) ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบ Pop-up หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

(๖.๑๕.๕) ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือ ผิดกฎหมาย

(๖.๑๕.๖) ห้ามการแสดงความคิดเห็นส่วนตัวโดยใช้ทะเบียนผู้ใช้งานอินเตอร์เน็ตที่ออกให้โดยหน่วยงานผ่านทางเว็บบอร์ด บล็อก หรือสื่อสังคม ออนไลน์อื่นใด ทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบ ของผู้ใช้งานนั้น

(๖.๑๕.๗) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์จากเว็บไซต์ หรือแหล่งข้อมูลที่ไม่น่าเชื่อถือหรือไม่ปลอดภัยต่อระบบ สารสนเทศ เว้นแต่ในกรณีที่มีความจำเป็นให้แจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษรเพื่อพิจารณาความปลอดภัยและความเหมาะสม

(๖.๑๕.๘) กรณีที่มีความจำเป็นต้องดาวน์โหลดข้อมูลหรือไฟล์ขนาดใหญ่เกิน 10 MB ผ่านอินเทอร์เน็ต ควรกระทำนอกเวลาทำการ เพื่อป้องกันผลกระทบต่อปริมาณข้อมูลในเครือข่าย ในกรณีที่ไฟล์มีขนาดใหญ่มากให้ประสานงานกับผู้ดูแลระบบเพื่อลดผลกระทบต่อเครือข่าย

(๖.๑๕.๙) ตรวจสอบไวรัสในข้อมูลหรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตทุกครั้ง ก่อนติดตั้งหรือใช้งาน

(๖.๑๕.๑๐) ผู้ใช้งานมีหน้าที่ระมัดระวังการใช้งาน และต้องรับผิดชอบต่องานหรือผลที่เกิดจากการเรียกใช้ บริการบนอินเทอร์เน็ต โดยไม่กระทำการอันขัดต่อกฎหมายว่าด้วยการกระทำผิดทางคอมพิวเตอร์และไม่ก่อให้เกิดความเสียหายต่อหน่วยงาน

(๖.๑๕.๑๑) ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิในการเรียกใช้บริการบนอินเทอร์เน็ตได้ทันที เมื่อพบว่า ผู้ใช้มีการกระทำเข้าข่ายอันไม่สมควร

๗. ด้านการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

(๗.๑) กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๗.๒) การใช้งานระบบเครือข่ายไร้สาย (Wireless)

(๗.๒.๑) การเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานต้องทำผ่านทะเบียนผู้ใช้งานที่จัดให้โดยหน่วยงาน

(๗.๒.๒) ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังต่อไปนี้

๑) ในกรณีที่ระบบผู้ใช้งานแยกส่วนจากระบบงานของหน่วยงาน ผู้ใช้งานเครือข่ายไร้สายต้องลงทะเบียนการใช้งาน โดยดำเนินการตามขั้นตอนในลักษณะเดียวกับการขอใช้งานระบบงาน

๒) ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๓) ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๔) ต้องเปลี่ยนค่าชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและต้องใช้ชื่อผู้ใช้และรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๕) ใช้การเข้ารหัสข้อมูลในการใช้สัญญาณ Wireless ให้เป็นไปตามมาตรฐานที่เป็นปัจจุบัน

๖) การเข้าใช้งานระบบเครือข่ายไร้สาย ให้มีการลงทะเบียนหรือเก็บข้อมูลผู้ใช้งาน

๗) ให้มีการกำหนดช่องทางการเชื่อมต่อระหว่างเครือข่ายไร้สายกับเครือข่ายมีสายของหน่วยงานให้จำกัดและชัดเจน และให้มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายมีสายของหน่วยงาน

๘) ให้ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบ เครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้บังคับบัญชา

(๗.๓) การใช้ระบบงานสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน

(๗.๓.๑) การเข้าสู่ระบบสารสนเทศของหน่วยงานผ่านอินเทอร์เน็ตหรือเครือข่ายภายนอกหน่วยงานต้องขออนุญาตจากผู้มีอำนาจอนุมัติ

(๗.๓.๒) การใช้งานระบบสารสนเทศขององค์กรผ่านอินเทอร์เน็ตหรือเครือข่ายภายนอกหน่วยงาน ต้องมีการเข้ารหัสลับที่เป็นมาตรฐานสากล ด้วย VPN

(๗.๔) การระบุอุปกรณ์บนเครือข่าย (Networks Equipment Identification)

(๗.๔.๑) ระบะและจัดทำบัญชี ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล, IP Address และ Mac Address

(๗.๔.๒) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ที่ได้รับมอบหมาย หรือผู้ที่ได้รับอนุญาตเท่านั้น

(๗.๔.๓) ต้องปรับแต่งไฟร์วอลล์กำหนดหมายเลขอุปกรณ์ ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

(๗.๕) การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๗.๕.๑) การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และ ทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๗.๕.๒) มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบ

(๗.๖) ข้อกำหนดการแบ่งแยกเครือข่าย (Segregation in Networks) ให้แยกเป็น

(๗.๖.๑) Management Zone เป็นระบบเครือข่ายที่ใช้ในการควบคุมการบริหารจัดการระบบคอมพิวเตอร์ และเครือข่าย Server DNS Database

(๗.๖.๒) Intranet Zone เป็นระบบเครือข่ายภายในหน่วยงาน สำหรับการใช้งานข้อมูลสารสนเทศ ที่มีความสำคัญและเข้าถึงได้เฉพาะบุคลากรของหน่วยงานที่ได้รับอนุญาตเท่านั้น

(๗.๖.๓) DMZ Zone เป็นระบบคอมพิวเตอร์และเครือข่ายที่ให้บริการข้อมูลข่าวสารทั้งภายในหน่วยงาน (Intranet Zone) และภายนอกหน่วยงาน (Extranet Zone)

(๗.๖.๔) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(๗.๖.๕) ทำการทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อย ปีละ ๑ ครั้ง

(๗.๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

(๗.๗.๑) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือ ไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๗.๗.๒) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๗.๗.๓) กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายใน และเครือข่ายภายนอก

(๗.๗.๔) ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น และต้องทบทวนการใช้เส้นทางเหล่านี้อย่างน้อยปีละ ๒ ครั้ง

(๗.๘) ข้อกำหนดการป้องการบุกรุก (Firewall Policy)

(๗.๘.๑) นโยบายการเปิดพอร์ตหรือเส้นทาง เป็นความรับผิดชอบของหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

(๗.๘.๒) การบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด เป็นหน้าที่ของผู้ดูแลระบบที่ได้มอบหมาย

(๗.๘.๓) ต้องเปิดการเชื่อมต่อในลักษณะที่เหมาะสมเฉพาะเส้นทางที่ได้รับอนุมัติเป็นลายลักษณ์อักษรเท่านั้น หากไม่ได้รับอนุมัติให้ถือว่าเป็นเส้นทางที่ต้องบล็อก (หรือปฏิเสธ)

(๗.๘.๔) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

(๗.๘.๕) ต้องตรวจสอบและทบทวนการกำหนดค่าต่างๆ ทุก ๓ เดือน และมีการสำรองข้อมูลการกำหนดค่าอย่างน้อยเดือนละครั้ง

(๗.๘.๖) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ ต้องส่งไปจัดเก็บ ที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

(๗.๘.๗) การเชื่อมต่อแบบ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก CIO และต้องมีเจ้าหน้าที่เทคนิคกำกับดูแล การอนุญาต การกำกับ และการจำกัดการใช้งาน

(๗.๙) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log)

(๗.๙.๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(๗.๙.๒) ข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของระบบที่ต้องจัดเก็บ ดังต่อไปนี้เป็นอย่างน้อย

๑) Firewall/Proxy/Gateway ข้อมูล IP Address ของเครื่องทั้งภายในและภายนอกที่มีการเชื่อมต่อกับเครือข่ายของหน่วยงาน

๒) Authentication ต้องจัดเก็บข้อมูลจราจรฯ การพิสูจน์ตัวตนของผู้ใช้งาน

๓) Web Server ต้องจัดเก็บข้อมูลจราจรฯ การเข้าถึงเว็บเซิร์ฟเวอร์

๔) Web Application ต้องจัดเก็บข้อมูลจราจรฯ การพิสูจน์ตัวตนของผู้ใช้งาน

(๗.๙.๓) ห้ามแก้ไขเปลี่ยนแปลงบันทึกข้อมูลจราจร และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. ด้านการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๘.๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องมีการยืนยัน ตัวตนที่มีความมั่นคงปลอดภัยจากการโจมตีผ่านระบบเข้าใช้งาน

(๘.๒) การระบุและยืนยันตัวตนของผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)และหากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับ ความจำเป็นในด้านเทคนิคหรือความสอดคล้องกับการปฏิบัติงาน รวมถึงต้องมีหลักฐานและรายชื่อการใช้งานร่วมกันเป็นลายลักษณ์อักษร

(๘.๓) ข้อปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

(๘.๓.๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๘.๓.๒) ให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๘.๓.๓) หน่วยงานไม่สนับสนุนการติดตั้งและ/หรือใช้งานโปรแกรมละเมิดลิขสิทธิ์หากเกิดข้อพิพาท ผู้ที่ติดตั้งและ/หรือใช้งานโปรแกรมดังกล่าวต้องเป็นผู้รับผิดชอบ

(๘.๓.๔) กำหนดให้ระบบงานที่มีความสำคัญสูง ใช้งานในสถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการเชื่อมต่อให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น และมีการจำกัดระยะเวลาการเชื่อมต่อที่สั้นขึ้น

๙. ด้านการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชัน ของระบบสารสนเทศ (Application and Information Access Control)

(๙.๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) โดยผู้ดูแลระบบดังต่อไปนี้

(๙.๑.๑) ต้องลงทะเบียนผู้ใช้งานตามข้อกำหนดการลงทะเบียน

(๙.๑.๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด ต้องยกเลิกการเชื่อมต่อระบบ

(๙.๑.๓) ต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๙.๑.๔) ต้องมีกระบวนการ หรือแนวทางการควบคุมการใช้งานและการใช้ข้อมูลโดยผู้ให้บริการภายนอก (Outsource)

(๙.๒) การบริหารจัดการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(๙.๒.๑) ต้องมีการระบุระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๙.๒.๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆและควบคุมสภาพแวดล้อมทางกายภาพและการใช้งาน

(๙.๒.๓) ต้องมีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูง กับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า

(๙.๒.๕) มีการสำรองและทดสอบการกู้คืนระบบ ตามนโยบาย และแนวทางการสำรองระบบสารสนเทศ

(๙.๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing) ที่หน่วยงานจัดให้แก่บุคลากร เพื่อป้องกันการถูกเข้าถึงโดยไม่ได้รับอนุญาตการสูญหาย เสียหาย ถูกขโมย ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๙.๓.๑) อุปกรณ์คอมพิวเตอร์เคลื่อนที่หมายรวมถึงอุปกรณ์พกพาหรือยกย้ายได้โดยสะดวก เช่น สมาร์ทโฟน โน้ตบุ้ค แท็บเล็ต หรืออุปกรณ์อื่นใดในลักษณะเดียวกัน

(๙.๓.๔) ให้จัดเตรียมวิธีการทางเทคนิคในการเข้ารหัสลับข้อมูลสำหรับข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๙.๓.๕) เมื่อพบซอฟต์แวร์ไม่ประสงค์ดีในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ปฏิบัติตามข้อปฏิบัติในการป้องกันซอฟต์แวร์ไม่ประสงค์ดีและที่เกี่ยวข้อง

(๙.๓.๘) ไม่ให้เชื่อมต่ออุปกรณ์คอมพิวเตอร์เคลื่อนที่ที่ไม่ได้รับอนุญาต เข้ากับเครือข่ายของหน่วยงาน

(๙.๓.๙) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก และเก็บรักษาสื่อข้อมูลสำรองไว้ในสถานที่ที่เหมาะสมและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๙.๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) เพื่อป้องกันการใช้งานระบบสารสนเทศ โดยไม่ได้รับอนุญาตจากการปฏิบัติงานจากภายนอกหน่วยงานให้ปฏิบัติ ดังนี้

(๙.๔.๑) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับ อนุญาตจากผู้มีอำนาจอนุมัติหรือหน่วยงานเป็นลายลักษณ์อักษร และต้องยกเลิกสิทธิเมื่อครบเวลาตามที่ขอไว้หรือเมื่อหมดความจำเป็น

(๙.๔.๒) ให้มีการเข้ารหัสลับ (Encryption) สำหรับการเชื่อมโยงและสื่อสารที่เป็นมาตรฐานสากล

(๙.๔.๓) ให้ผู้ได้รับอนุญาตเท่านั้นเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดยห้ามมิให้สมาชิก ในครอบครัวหรือบุคคลอื่น ที่ไม่ได้รับอนุญาต และขอสงวนสิทธิในการระงับหรือยกเลิกสิทธิหากพบว่าไม่ปฏิบัติ ตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

ส่วนที่ ๒ แนวปฏิบัติระบบสำรองสารสนเทศ

(Information Backup)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศและเครือข่ายของหน่วยงานสามารถใช้งานได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ฝ่ายเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ใช้งาน

แนวปฏิบัติ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ให้ปฏิบัติ ดังนี้

๑.๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน

๑.๒ ทบทวนตามข้อ ๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๑.๓ ชนิดข้อมูลที่ต้องสำรองอย่างน้อยต้องประกอบด้วย

(๑) ค่า Configuration สำหรับระบบ และอุปกรณ์ computer และเครือข่ายทุกชนิด

(๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

(๓) ฐานข้อมูล และข้อมูลสำคัญของระบบสารสนเทศของหน่วยงาน

(๔) ซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นใดที่เห็นควรทำการสำรอง

๑.๔ กำหนดขั้นตอนและความถี่ในการสำรองและกู้คืนข้อมูลอย่าง ประกอบด้วย

(๑) ระบบงาน ต้องสำรอง อย่างน้อย 3 เดือนต่อครั้ง๑.๔.๒ ผู้ใช้งาน ต้องสำรองข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ส่วนบุคคลทุกวันหลังเลิกงาน

(๒) จัดทำขั้นตอนการกู้คืน การทดสอบการสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑.๕ กำหนดรูปแบบการสำรองข้อมูล การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๑.๖ สำหรับระบบงานต้องบันทึกข้อมูล ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล

๑.๗ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ และดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๑.๘ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๒ ต้องประเมินสถานการณ์ความเสี่ยงสำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยี

๒.๓ กำหนดช่องทางในการติดต่อผู้ให้บริการภายนอกที่จะต้องติดต่อเมื่อเกิดเหตุจำเป็นฉุกเฉิน

๒.๔ สร้างความตระหนัก ให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน หรือความรู้อื่นใดในการเตรียมความพร้อมกรณีฉุกเฉิน

๒.๕ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(IT Risk Management)

วัตถุประสงค์

เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ฝ่ายเทคโนโลยีสารสนเทศ
๒. ผู้ตรวจสอบทั้งภายใน ภายนอก
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ข้อกำหนดในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบ เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. ข้อกำหนดในการดำเนินการตรวจสอบและประเมินความเสี่ยง ให้ปฏิบัติ ดังนี้

๒.๑ ให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๒.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งให้มีการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๒.๓ ควรให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลประวัติแสดงการเข้าถึงนั้น (Logs) ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๒.๔ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ แยกการติดตั้งเครื่องมือ ที่ใช้ในการ ตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการ เข้าถึงโดยไม่ได้รับอนุญาต

๓. จัดทำแผนลดความเสี่ยง

๔. รายงานผลการตรวจสอบและประเมินความเสี่ยง และแผนลดความเสี่ยง ให้กับผู้บริหาร อนุเทคโนโลยีสารสนเทศ ตามรอบที่ผู้ตรวจประเมิน และทั้งระบบอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔ แนวปฏิบัติการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผู้รับผิดชอบ

๑. ฝ่ายเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมายจากคณะกรรมการดูแลกำกับฝ่าย
๓. หัวหน้าหน่วยงานต่าง ๆ

แนวปฏิบัติ

๑. การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ให้ฝ่ายเทคโนโลยีสารสนเทศสภาวิศวกร เป็นผู้รับผิดชอบดำเนินการ ให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติ อย่างน้อย ปีละ ๑ ครั้ง

๒. การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานให้ปฏิบัติดังนี้

๒.๑ จัดฝึกอบรม ฝึกอบรมเชิงปฏิบัติ และสัมมนา อย่างน้อยปีละ ๑ ครั้ง หรือตามสภาพความจำเป็น ตลอดจนจัดทำคู่มือและมีการเผยแพร่ภายในหน่วยงาน

๒.๒ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวัง ในรูปแบบ ที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๒.๓ กำกับ ติดตาม ประเมินผล และสำรวจความเห็นของผู้ใช้งาน

ส่วนที่ ๕ แนวปฏิบัติการบริหารจัดการทรัพยากรระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้บัญชีทรัพย์สิน มีการบริหารจัดการข้อมูล บริหารจัดการระบบสารสนเทศของสภาวิศวกร และการกำหนดแนวทางการป้องกันความเสี่ยงต่อทรัพย์สินเหล่านั้นอย่างเหมาะสม

ผู้รับผิดชอบ

๑. ฝ่ายเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. ด้านการบริหารจัดการทรัพย์สิน

๑.๑ ต้องมีการสำรวจและจัดทำทะเบียนทรัพย์สินทางสารสนเทศ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล และทบทวนปรับปรุงให้ตรงตามความเป็นจริงเสมอ

๑.๒ ต้องควบคุมการเข้าไปในห้องคอมพิวเตอร์แม่ข่าย การนำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย การนำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมต่อเข้าระบบเครือข่ายของสภาฯ

๑.๓ ผู้ใช้งานต้องมีการป้องกันการใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ การคัดลอกหรือทำสำเนาแฟ้มข้อมูล ที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

๑.๔ ผู้ใช้งานต้องมีการกำหนดหน้าที่รับผิดชอบต่อทรัพย์สินที่องค์กรมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งาน การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยพนักงานที่องค์กรมอบหมาย และมีแนวทางให้ผู้ใช้งานชดใช้ค่าเสียหายตามระเบียบของสภาฯ

๑.๕ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือคอมพิวเตอร์ประเภทพกพา ไม่ว่าในกรณีใด ๆ

๑.๖ ผู้ใช้งานต้องมีการควบคุมการนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่องค์กรจัดเตรียมไว้ให้ใช้งานไปใช้ในกิจกรรมที่องค์กรไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์กร และต้องมีการกำหนดความรับผิดชอบกับผู้ที่ก่อความเสียหายโดยให้ถือเป็นความผิดส่วนบุคคล

๒ ด้านการบริหารจัดการข้อมูลองค์กร

๒.๑ ต้องสร้างความตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นเป็นขององค์กรหรือบุคคลภายนอก โดยห้ามให้มีการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายข้อมูลที่ถือเป็นทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๒.๒ ผู้ใช้งานต้องรับผิดชอบในการดูแลรักษาข้อมูลขององค์กร และรับผิดชอบต่อความเสียหายของข้อมูล หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด หรือถูกเผยแพร่โดยไม่ได้รับอนุญาต และต้องดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๒.๓ สภาวิศวกรให้ความสำคัญกับการป้องกันข้อมูลส่วนบุคคล และไม่อนุญาตให้ผู้ใช้งานทำการละเมิดข้อมูลส่วนบุคคล

๓. ด้านการบริหารจัดการระบบสารสนเทศ

๓.๑ การพัฒนาโปรแกรม การจัดหาโปรแกรม หรือฮาร์ดแวร์ใด ๆ ทางฝ่ายเทคโนโลยีสารสนเทศจะต้องตรวจสอบและกำกับ

๑) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายกลไกการรักษาความปลอดภัยระบบสารสนเทศ รวมทั้งการกระทำในลักษณะเป็นการดักจับรหัสผ่านหรือ การวางช่องทางเพื่อลักลอบเข้าสู่ระบบ

๒) ต้องควบคุมไม่ให้มีการทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

๓) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๔) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๕) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

๖) ต้องควบคุมไม่ให้มีการนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๗) ต้องควบคุมไม่ให้เปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๘) ต้องควบคุมไม่ให้เปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิงในระหว่างเวลาปฏิบัติงาน

๙) ต้องควบคุมไม่ให้ใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดขององค์กรที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม หรือเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร หรือความมั่นคงของประเทศ

๑๐) ต้องควบคุมไม่ให้ใช้ทรัพยากรทุกประเภทที่เป็นขององค์กร เพื่อประโยชน์ทางการค้า

๑๑) ต้องควบคุมไม่ให้กระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดก็ตาม

๑๒) ต้องควบคุมไม่ให้กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศขององค์กรต้องหยุดชะงัก

๑๓) ต้องควบคุมไม่ให้ใช้ระบบสารสนเทศขององค์กร เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๔) ต้องควบคุมไม่ให้ติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อให้เข้าถึงระบบสารสนเทศขององค์กร โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ

๔. ด้านการปฏิบัติตาม ประกาศ ระเบียบข้อบังคับ และกฎหมาย

๔.๑ การดำเนินการด้านสารสนเทศ ขององค์กร ให้เป็นไปตามประกาศ ระเบียบข้อบังคับ และกฎหมาย ถ้าการดำเนินการนั้นเป็นการกระทำโดยพลการของผู้ใช้งาน ถือเป็นความผิดส่วนบุคคล

๔.๒ ผู้ใช้งานสามารถขอใช้งานตามหน้าที่ความจำเป็น ซอฟต์แวร์ (Software) ที่องค์กร อนุญาตให้ใช้งาน หรือที่องค์กรมีลิขสิทธิ์และผู้ใช้งานต้องไม่ติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์องค์กร ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๔.๓ ซอฟต์แวร์ (Software) ที่องค์กรได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการปฏิบัติงาน ผู้ใช้งาน ต้องไม่ติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือ ทำสำเนาเพื่อนำไปใช้งานที่อื่น

๔.๔ ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ โดยจัดเก็บไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง เป็นระยะเวลาอย่างน้อย ๙๐ วัน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องมีการกำหนดชั้นความลับในการเข้าถึง

๔.๕ ต้องตั้งเวลานาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๔.๖ ต้องควบคุมไม่ให้ผู้ดูแลระบบ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือบุคคลที่องค์กรมอบหมายเท่านั้น

๔.๗ ต้องควบคุมไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลในสื่อเก็บข้อมูลดังกล่าว และจำกัดสิทธิการเข้าถึงข้อมูลเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๖ แนวปฏิบัติการป้องกันภัยคุกคามระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้หน่วยงานมีการป้องกันไวรัส และโปรแกรมไม่ประสงค์ดี มีการป้องกันและ ตรวจจับการบุกรุก รวมถึงมีการจัดการเหตุการณ์ไม่พึงประสงค์ที่เกิดขึ้น

ผู้รับผิดชอบแนวปฏิบัติ

๑. ฝ่ายเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. ผู้ใช้งาน

คำนิยามเพิ่มเติม

“**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด**” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสภาวิศวกรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

แนวปฏิบัติ

๑. ด้านการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑.๑ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่องค์กร ได้จัดหาหรือได้ประกาศให้ใช้

๑.๒ ข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๑.๓ ต้องควบคุมให้มีการปรับปรุงข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๑.๔ ต้องสร้างความตระหนักและพึงระวังเกี่ยวกับไวรัสและโปรแกรมไม่ประสงค์ดีและต้องแจ้งเหตุแก่ผู้ดูแลระบบหากพบสิ่งผิดปกติ

๑.๕ ต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ติดไวรัสเข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๒. ด้านการป้องกันระบบเครือข่ายคอมพิวเตอร์และตรวจจับการบุกรุก

๒.๑ ต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุกเอาไว้ในตำแหน่งที่มีความเสี่ยงต่อการถูกโจมตีหรือบุกรุกได้

๒.๒ ต้องมีการปรับแต่ง (Tuning) การทำงานของระบบตรวจจับและป้องกันการบุกรุก โดยให้ป้องกันได้มากที่สุด และเกิดการตรวจจับที่ผิดพลาด (False Positive) น้อยที่สุด

๒.๓ ต้องมีการตั้งระบบตรวจจับและป้องกันการบุกรุก ให้สามารถ Update Signature ได้โดยอัตโนมัติ และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องตรวจสอบ Signature ทุกสัปดาห์

๒.๔ ต้องตรวจสอบการทำงานของระบบตรวจจับและป้องกันการบุกรุกและตรวจสอบ Log พร้อมทดสอบการทำงานทุก ๓ เดือน

๒.๕ การเปลี่ยนแปลงใดๆ ที่เกี่ยวกับระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการบันทึกและรายงานต่อผู้บริหารที่รับผิดชอบ

๒.๖ อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ

๓. ด้านการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident)

๓.๑ ต้องมีระบบการตรวจจับและแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย

๓.๒ มีการจัดทำแผนบริหารความเสี่ยงเพื่อการรับมือเหตุการณ์อันไม่พึงประสงค์

๓.๓ หากพบจุดอ่อนช่องโหว่ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบสารสนเทศ จะต้องไม่เปิดเผย เผยแพร่สนทนาหรือกระทำการใด ๆ อันเป็นการเผยแพร่ต่อผู้อื่น ต้องให้แจ้งต่อผู้ดูแลระบบโดยด่วนที่สุด

๓.๔ ต้องกำหนดให้มีคณะทำงานเพื่อทำหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศในการแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๓.๕ เมื่อได้รับแจ้งเหตุการณ์ คณะทำงานจะต้องดำเนินการวิเคราะห์ความรุนแรงและผลกระทบของเหตุการณ์นั้น ๆ และร่วมกันหาวิธีการแก้ไข

๓.๖ ต้องมีการฝึกอบรมและให้ความรู้แก่คณะทำงานตามความเหมาะสม อย่างน้อยปีละ ๑ ครั้ง

๓.๗ ในกรณีที่มีเหตุการณ์อันไม่พึงประสงค์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศต้องมีการดำเนินการเพื่อการรักษาความถูกต้องทางด้านหลักฐาน และดำเนินการทางกฎหมาย ในกรณีที่จำเป็น