การไฟฟ้านครหลวง
Metropolitan Electricity Authority

ประกาศการไฟฟ้านครหลวง
ที่ ๘๓/๒๕๖๕
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๖๕

ตามมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐ มีระบบสารสนเทศที่มีความมั่นคงปลอดภัยและเชื่อถือได้

จึงสมควรให้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการไฟฟ้านครหลวง เพื่อให้ระบบสารสนเทศของการไฟฟ้านครหลวง มีความมั่นคงปลอดภัย เป็นไปอย่างถูกต้องตามกฎหมาย สามารถให้บริการได้อย่างต่อเนื่อง สร้างความมั่นใจให้กับผู้ใช้งาน และมิให้มีการกระทำด้วยประการใด ๆ ทำให้ระบบสารสนเทศไม่สามารถทำงานได้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือ ใช้ระบบสารสนเทศ เพื่อเผยแพร่ข้อมูลอันเป็นเท็จ ซึ่งอาจก่อให้เกิดความเสียหายแก่การไฟฟ้านครหลวง และเป็นความผิดตามพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และเพื่อให้สอดคล้องตามพระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัย-ของระบบสารสนเทศ ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ดังนั้น จึงให้ยกเลิกประกาศการไฟฟ้า-นครหลวง ที่ ๒๕/๒๕๕๙ ลงวันที่ ๒๗ เมษายน พ.ศ. ๒๕๕๙ เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๕๘ และกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการไฟฟ้านครหลวง ตามประกาศดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศการไฟฟ้านครหลวง เรื่อง นโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๖๕”

ข้อ ๒ วัตถุประสงค์

(๑) สร้างความมั่นใจว่าการใช้งานและการรักษาความมั่นคงปลอดภัยระบบสารสนเทศภายในการไฟฟ้านครหลวง เป็นไปอย่างถูกต้องตามกฎหมาย และข้อบังคับที่เกี่ยวข้อง

(๒) มีแนวปฏิบัติที่รัดกุม เพื่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(๓) ให้ผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้องทราบและเข้าใจถึงแนวปฏิบัติ ข้อควรระวัง และความรับผิดชอบในการใช้งานนั้น ๆ เพื่อส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ และการใช้งานตรงตามวัตถุประสงค์ของการไฟฟ้านครหลวง รวมทั้งไม่ขัดต่อระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

(๔) ปกป้องระบบสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบต่าง ๆ ได้แก่ การสูญหาย การถูกทำลาย การแก้ไข โดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้ หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบสารสนเทศ มีความถูกต้อง เชื่อถือได้ และสามารถให้บริการได้อย่างต่อเนื่อง

ข้อ ๓ ขอบเขตการดำเนินการ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๖๕ มีขอบเขตครอบคลุม ดังต่อไปนี้

(๑) การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม การไฟฟ้านครหลวง จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็นและความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความมั่นคงปลอดภัยของการไฟฟ้านครหลวง

(๒) การบริหารจัดการระบบสารสนเทศและระบบสำรองของระบบสารสนเทศ

เพื่อบริหารจัดการระบบสารสนเทศและจัดทำระบบสำรองของระบบสารสนเทศ เพื่อให้ข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย ให้สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความพร้อมใช้งาน (Availability Risk)

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

เพื่อให้เกิดการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อสามารถจัดการกับความเสี่ยงที่ตรวจพบได้อย่างเหมาะสม และสอดคล้องกับมาตรฐานและข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับการไฟฟ้านครหลวง

(๔) โครงสร้างความมั่นคงปลอดภัยและการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อจัดโครงสร้างของหน่วยงานภายในที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม และกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการกำกับดูแลกิจกรรมต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ และเพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้อง ได้รับความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

(๕) การบริหารจัดการทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

เพื่อให้การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของการไฟฟ้านครหลวง เป็นไปอย่างมีระเบียบและถูกต้องทั้งในด้านจริยธรรมจรรยาบรรณ และด้านกฎหมาย รวมทั้งให้ผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้อง ใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพ

(๖) การป้องกันภัยคุกคามเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของการไฟฟ้านครหลวง และอาจสร้างความเสียหายและส่งผลกระทบต่อการใช้งานและการให้บริการของระบบสารสนเทศและต่อภาพลักษณ์ของการไฟฟ้านครหลวง

ข้อ ๔ องค์ประกอบนโยบาย

(๑) นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๑.๑) ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(๑.๑.๑) ต้องมีการจัดแบ่งพื้นที่ออกเป็นอย่างน้อย ๒ พื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

(๑.๑.๒) การป้องกันห้องควบคุมระบบและระบบเครือข่าย ต้องมีการควบคุมทั้งในด้านกายภาพ และด้านการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

(๑.๒) ด้านการควบคุมการเข้า ออกห้องควบคุมระบบและระบบเครือข่าย

(๑.๒.๑) ต้องมีการควบคุมการเข้าไปในพื้นที่ควบคุม

(๑.๒.๒) ต้องมีการควบคุมการเข้าไปในพื้นที่จำกัดการเข้าถึง

(๑.๓) ด้านการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

(๑.๓.๑) กำหนดให้มีการควบคุมการเข้าถึงระบบสารสนเทศ

(๑) การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยสารสนเทศ

(๒) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ให้กำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน

(๑.๓.๒) กำหนดให้มีการแบ่งประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

(๑.๓.๓) การกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๑) การควบคุมการเข้าถึงสารสนเทศ ให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ

(๒) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และความต้องการทางธุรกิจที่เปลี่ยนไป

(๑.๓.๔) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๑) สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อให้มีความรู้ความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ

(๓) การยกเลิกสิทธิการใช้งานระบบสารสนเทศ และตัดออกจากทะเบียนผู้ใช้งาน เมื่อผู้ใช้งานสิ้นสุดภาระหน้าที่ และมีการยกเลิกเพิกถอนการอนุญาต

(๔) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศ แต่ละชนิดตามความเหมาะสม

(๕) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) เพื่อความรัดกุมของการใช้งานรหัสผ่านของผู้ใช้งาน

(๖) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) โดยจัดทำเป็นกระบวนการตามรอบระยะเวลาที่กำหนดไว้

(๑.๓.๕) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

(๑) ให้การใช้งานรหัสผ่าน (Password Use) เป็นไปตามข้อกำหนดที่ดี เพื่อให้การกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) ให้ป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์เพื่อไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ขององค์กรในขณะที่ไม่มีผู้ดูแล

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

(๔) เข้ารหัสข้อมูลที่เป็นความลับ เพื่อรักษาความลับของข้อมูล โดยผู้ใช้งานสามารถใช้มาตรการการเข้ารหัสข้อมูล สำหรับข้อมูลที่ถูกจัดลำดับชั้นความลับ ตามข้อกำหนดเกี่ยวกับลำดับชั้นความลับของข้อมูล ที่กำหนดไว้ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และที่แก้ไขเพิ่มเติม หรือตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

(๑.๓.๖) การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

(๑) การใช้งานบริการระบบเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กร สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศขององค์กรได้

(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) การใช้งานอินเทอร์เน็ต ต้องเชื่อมต่อเครื่องคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น ต้องติดตั้งโปรแกรมตรวจจับไวรัสบนเครื่องที่จะใช้เชื่อมต่อ และต้องตรวจสอบไวรัสทุกครั้งเมื่อมีการรับ ส่งข้อมูลผ่านทางอินเทอร์เน็ต ไม่ใช้อินเทอร์เน็ตขององค์กรในการทำธุรกรรมหรือการกระทำใด ๆ ที่ไม่เหมาะสม หรือละเมิดกฎหมาย หรือทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร หรือทำลายความสัมพันธ์ของพนักงานหน่วยงานอื่น ๆ หรือเพื่อหาแสวงหาผลประโยชน์ส่วนตัว

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

(๑๐) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Network) เป็นความรับผิดชอบของฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูลที่ต้องพิจารณาอนุญาตทั้งในด้านการติดตั้งระบบเครือข่ายไร้สาย การลงทะเบียนอุปกรณ์และผู้ใช้งาน การกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ การกำหนดรหัสผ่าน

ในการเข้าใช้งาน การทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ การตั้งค่าอุปกรณ์ให้มีความมั่นคงปลอดภัย การติดตั้งไฟร์วอลล์เพื่อป้องกันการเข้าถึงเครือข่ายภายในจากการเชื่อมต่อผ่านเครือข่ายไร้สาย

(๑.๓.๗) การควบคุมการเข้าถึงระบบปฏิบัติการ (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

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

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรทางด้านสารสนเทศ การเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ

ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) การจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (Outsource) ต้องมีการลงนามในการรักษาความลับ ห้ามเปิดเผยข้อมูลขององค์กรก่อนปฏิบัติหน้าที่

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

(๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๕) การปฏิบัติงานจากภายนอกองค์กร (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกองค์กร

(๒) นโยบายการบริหารจัดการระบบสารสนเทศและระบบสำรองของระบบสารสนเทศ

การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ให้ปฏิบัติดังนี้

(๒.๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองของระบบสารสนเทศที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒.๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๒.๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองของระบบสารสนเทศ และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๒.๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองของระบบสารสนเทศ และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๒.๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๓) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

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

(๓.๒) ในการตรวจสอบและประเมินความเสี่ยง ต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์กร (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

(๔) นโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ และการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๔.๑) การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ให้ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง

(๔.๒) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล ต้องจัดให้มีกิจกรรมการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้ใช้งานและบุคคลที่เกี่ยวข้อง ได้รับความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง อย่างน้อยปีละ ๑ ครั้ง

(๕) นโยบายการบริหารจัดการทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

(๕.๑) 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 และต้องมีการกำหนดความรับผิดชอบกับผู้ที่ก่อความเสียหาย โดยให้ถือเป็นความผิดส่วนบุคคล

(๕.๒) ด้านการบริหารจัดการข้อมูลองค์กร

(๑) ต้องมีการสร้างความตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นเป็นขององค์กร หรือบุคคลภายนอก โดยห้ามให้มีการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายข้อมูลที่ถือเป็นทรัพย์สินขององค์กร โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

(๒) ต้องกำหนดความรับผิดชอบในการดูแลรักษาข้อมูลขององค์กร และความรับผิดชอบต่อความเสียหายของข้อมูล หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด หรือถูกเผยแพร่โดยไม่ได้รับอนุญาต และต้องมีการป้องกันดูแลรักษาไว้ ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

(๓) การป้องกันข้อมูลส่วนบุคคลเป็นสิทธิของผู้ใช้งาน ซึ่งองค์กรให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น

(๕.๓) ด้านการบริหารจัดการระบบสารสนเทศ

(๑) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่เป็นการทำลายกลไกการรักษาความปลอดภัยระบบสารสนเทศ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบ

(๒) ต้องควบคุมไม่ให้มีการทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๓) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๔) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๕) ต้องควบคุมไม่ให้มีการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่เป็นการทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๖) ต้องควบคุมไม่ให้มีการนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

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

(๘) ต้องควบคุมไม่ให้เปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างเวลาปฏิบัติงาน

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

(๑๐) ต้องควบคุมไม่ให้ใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า

(๑๑) ต้องควบคุมไม่ให้กระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

(๑๒) ต้องควบคุมไม่ให้กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศขององค์กร ต้องหยุดชะงัก

(๑๓) ต้องควบคุมไม่ให้ใช้ระบบสารสนเทศขององค์กร เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

(๑๔) ต้องควบคุมไม่ให้กระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

(๑๕) ต้องควบคุมไม่ให้ติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อให้เข้าถึงระบบสารสนเทศขององค์กร โดยไม่ได้รับอนุญาตจากฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

(๕.๔) ด้านการปฏิบัติตามข้อบังคับ

(๑) บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบขององค์กรที่กำหนด หรือออกกฎระเบียบโดยอาศัยนโยบายดังกล่าวข้างต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

(๒) ซอฟต์แวร์ (Software) ที่องค์กรอนุญาตให้ใช้งาน หรือที่องค์กรมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และผู้ใช้งานต้องไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์องค์กรถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

(๓) ซอฟต์แวร์ (Software) ที่องค์กรได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการปฏิบัติงาน ผู้ใช้งานต้องไม่ติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๔) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยจัดเก็บไว้ในสื่อเก็บข้อมูล ที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง เป็นระยะเวลาอย่างน้อย ๙๐ วัน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องมีการกำหนดชั้นความลับในการเข้าถึง

(๕) ต้องควบคุมไม่ให้ผู้ดูแลระบบ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือบุคคลที่องค์กรมอบหมายเท่านั้น

(๖) ต้องควบคุมไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลในสื่อเก็บข้อมูลดังกล่าว และจำกัดสิทธิการเข้าถึงข้อมูลเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๖) นโยบายการป้องกันภัยคุกคามเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

(๖.๑) ด้านการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

(๑) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่องค์กร ได้จัดหาหรือได้ประกาศให้ใช้ เว้นแต่เครื่องคอมพิวเตอร์นั้น เป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

(๒) ข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

(๓) ต้องควบคุมให้มีการปรับปรุงข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

(๔) ต้องสร้างความตระหนักและพึงระวังเกี่ยวกับไวรัสและโปรแกรมไม่ประสงค์ดี และต้องแจ้งเหตุแก่ผู้ดูแลระบบ หากพบสิ่งผิดปกติ

(๕) ต้องควบคุมไม่ให้เชื่อมต่อเครื่องคอมพิวเตอร์ที่ติดไวรัสเข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

(๖) ต้องกำหนดให้ผู้ใช้งานไม่ลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินขององค์กร หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

(๗) ต้องควบคุมไม่ให้เผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สินขององค์กร

(๖.๒) ด้านการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

(๑) ต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุกเอาไว้ในตำแหน่งที่มีความเสี่ยงต่อการถูกโจมตี หรือบุกรุกได้

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

(๓) ต้องมีการตั้งระบบตรวจจับและป้องกันการบุกรุก ให้สามารถ Update Signature ได้โดยอัตโนมัติ หรือผู้ดูแลระบบเครือข่ายต้อง Update Signature ทุกสัปดาห์

(๔) ต้องตรวจสอบการทำงานของระบบตรวจจับและป้องกันการบุกรุก และตรวจสอบ Log พร้อมทดสอบการทำงานทุกเดือน

(๕) การเปลี่ยนแปลงใด ๆ ที่เกี่ยวกับระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการบันทึก และรายงานต่อผู้บริหารที่รับผิดชอบ

(๖) อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ และให้ติดตั้งในห้องที่มีการรักษาความปลอดภัย

(๖.๓) ด้านการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) ต้องกำหนดมีการแจ้งไปยังผู้ดูแลระบบ/ผู้เกี่ยวข้องโดยทันที เมื่อพบเห็นเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

(๒) หากพบจุดอ่อนช่องโหว่ในระบบสารสนเทศ จะต้องไม่เปิดเผย เผยแพร่ สนทนาหรือกระทำการใด ๆ อันเป็นการเผยแพร่ต่อผู้อื่น ต้องให้แจ้งต่อผู้ดูแลระบบโดยด่วนที่สุด

(๓) ต้องกำหนดให้มีคณะทำงานเพื่อทำหน้าที่ด้านความมั่นคง-ปลอดภัยสารสนเทศ ในการแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

(๔) เมื่อได้รับแจ้งเหตุการณ์ คณะทำงานจะต้องดำเนินการวิเคราะห์ความรุนแรงและผลกระทบของเหตุการณ์นั้น ๆ และร่วมกันหาวิธีการแก้ไข

(๕) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อการรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมาย ในกรณีที่จำเป็น

ข้อ ๕ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัลขององค์กร โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๖๕” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ข้อ ๖ ให้ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล เป็นผู้รับผิดชอบดำเนินการกำกับดูแลให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดขององค์กร (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ กันยายน พ.ศ. ๒๕๖๕

(ลงชื่อ) วิลาศ เฉลยสัตย์

(นายวิลาศ เฉลยสัตย์)

ผู้ว่าการ

เอกสารแนบท้ายประกาศ

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การไฟฟ้านครหลวง พ.ศ. ๒๕๖๕

คำนำ

ปัจจุบันมีการนำเทคโนโลยีดิจิทัลและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นใน การให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศ อันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบาย และแนวปฏิบัติ ด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

การไฟฟ้านครหลวงจึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัลของการไฟฟ้านครหลวง ประจำปี พ.ศ. ๒๕๖๕ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในการไฟฟ้านครหลวง เพื่อให้บุคลากรทุกคนในการไฟฟ้านครหลวง มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัลของการไฟฟ้านครหลวง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

การไฟฟ้านครหลวง

สารบัญ

หน้า

หน้า

บทนำ

๑. หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

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

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ จึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๒. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของการไฟฟ้านครหลวง ฉบับนี้มีวัตถุประสงค์เพื่อ

๑) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ การไฟฟ้านครหลวง ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๒) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ เทคโนโลยีดิจิทัล และการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของ การไฟฟ้านครหลวง มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศของการไฟฟ้านครหลวง และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีดิจิทัล ของการไฟฟ้านครหลวง

๓. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของการไฟฟ้านครหลวง โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ประกาศคณะกรรมการธุรกรรม ทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ โดยแนวปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีดิจิทัล ของการไฟฟ้านครหลวง

๔. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของการไฟฟ้านครหลวง บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยผู้ว่าการการไฟฟ้านครหลวง

กรณีข้อมูลหรือระบบสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ว่าการการไฟฟ้านครหลวงเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๕. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการไฟฟ้านครหลวง ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) ของการไฟฟ้านครหลวง จัดพิมพ์เผยแพร่เพื่อให้บุคลากรการไฟฟ้านครหลวงและบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

คำนิยาม

คำนิยาม ประกอบด้วย

(๑)	ผู้ใช้งาน	หมายถึง	ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป
(๒)	สิทธิ์ของผู้ใช้งาน	หมายถึง	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
(๓)	สินทรัพย์	หมายถึง	สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร
(๔)	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
(๕)	ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
(๖)	เหตุการณ์ด้านความมั่นคงปลอดภัย	หมายถึง	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
(๗)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	หมายถึง	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงถูกคุกคาม

(๘)	องค์กร	หมายถึง	การไฟฟ้านครหลวง
(๙)	ผู้บริหารระดับสูงสุด	หมายถึง	ผู้ว่าการการไฟฟ้านครหลวง (CEO)
(๑๐)	ผู้บริหาร	หมายถึง	ผู้ว่าการ รองผู้ว่าการ ผู้ช่วยผู้ว่าการ ผู้อำนวยการฝ่ายฯ ผู้อำนวยการไฟฟ้านครหลวงเขตฯ ผู้อำนวยการสำนักฯ
(๑๑)	ผู้ดูแลระบบ	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บริหารให้ทำหน้าที่ดูแลระบบสารสนเทศตามที่ผู้บริหารกำหนด
(๑๒)	พนักงาน	หมายถึง	พนักงานการไฟฟ้านครหลวง
(๑๓)	หัวหน้าหน่วยงาน	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
(๑๔)	หน่วยงานด้านเทคโนโลยีดิจิทัล	หมายถึง	หน่วยงานทั้งหมดที่อยู่ภายใต้สายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร
(๑๕)	เจ้าของข้อมูลและระบบงาน	หมายถึง	หน่วยงานที่เป็นเจ้าของข้อมูลและระบบงานที่ให้บริการกับผู้ใช้งาน โดยเจ้าของข้อมูลและระบบงานเป็นผู้รับผิดชอบข้อมูลและระบบงานนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลหรือระบบงานเหล่านั้นเกิดสูญหาย หรือไม่สามารถใช้งานได้
(๑๖)	ทรัพยากร	หมายถึง	ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และข้อมูลภายใต้การดูแลของสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร
(๑๗)	ระบบสารสนเทศ	หมายถึง	ระบบคอมพิวเตอร์และเครือข่าย ที่ให้บริการแก่พนักงานและผู้ใช้งาน
(๑๘)	ข้อมูล	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
(๑๙)	มาตรฐาน (Standard)	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
(๒๐)	การยืนยันตัวตน	หมายถึง	ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

ส่วนที่ ๑

นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม การไฟฟ้านครหลวง จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบ จากความจำเป็นและความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

ผู้รับผิดชอบ

๑) ฝ่ายจัดการทรัพย์สินและรักษาความปลอดภัย (ฝทภ.)
๒) ฝ่ายระบบโครงสร้างพื้นฐาน (ฝคฐ.)
๓) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)
๔) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑.๑ การจัดแบ่งพื้นที่

๑) ห้องควบคุมระบบ แบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๒) พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้ สำหรับการเยี่ยมชม หรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึง (Restricted Area) เป็นห้องที่มีระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายติดตั้งอยู่

๑.๒ ข้อกำหนดการป้องกันห้องควบคุมระบบและระบบเครือข่าย

๑.๒.๑ ข้อกำหนดทางด้านกายภาพของห้องควบคุมระบบ

๑) แยกอุปกรณ์ที่มีความสำคัญมาก ออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Server, Router, Network Switch ต่างๆ

๒) การติดตั้งอุปกรณ์ ควรติดตั้งภายในตู้ Rack ที่เหมาะสม เพื่อสะดวกในการบำรุงรักษา

๓) ตำแหน่งของการวางอุปกรณ์ต่างๆ ต้องไม่วางใกล้ประตูหน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ต้องไม่วางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรง เพื่อหลีกเลี่ยงความชื้น

๔) การจัดวางสายระบบเครือข่ายและสายไฟฟ้า ต้องจัดเก็บสายให้เรียบร้อย เพื่อป้องกันการเดินสะดุด อาจส่งผลเสียหายต่อระบบได้

๕) ติดประกาศบันทึกการบำรุงรักษา ชื่อ และหมายเลขโทรศัพท์ ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

๖) ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้องวงจรปิด (CCTV) ระบบการเข้า-ออกห้อง โดยระบบตรวจสอบลายนิ้วมือ (Fingerprint Scan) หรือบัตรผ่านเข้าออก (RFID)

๗) ต้องมีระบบป้องกันอัคคีภัย

๘) ต้องมีระบบไฟฟ้าสำรอง เพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง เป็นต้น

๙) ต้องมีระบบป้องกันไฟฟ้าจากฟ้าผ่า

๑๐) ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐ – ๘๐°F) และความชื้น (๒๐ – ๘๐%)

๑๑) ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและกำแพง

๑.๒.๒ ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๑) ตรวจสอบความพร้อมของระบบรักษาความปลอดภัย ทุก ๓ เดือน และรายงานให้ฝ่ายระบบโครงสร้างพื้นฐาน และฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล ทราบ

๒) จัดทำขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

๓) ต้องมีการซ้อมการปฏิบัติงานเมื่อเกิดกรณีฉุกเฉิน ทุก ๖ เดือน

๔) ต้องมีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

๒. การควบคุมการเข้า-ออกห้องควบคุมระบบและระบบเครือข่าย

๒.๑ ข้อกำหนดการเข้าไปในพื้นที่ควบคุม

๑) ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นพนักงานห้องควบคุมระบบ หัวหน้าหน่วยงาน หรือบุคคลที่หัวหน้าหน่วยงานนำเข้าเยี่ยมชม

๒) บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงาน หรือการเข้าเยี่ยมชมในพื้นที่ควบคุม ต้องได้รับอนุญาตจากรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร และต้องมีพนักงานนำเยี่ยมชมอยู่ด้วยตลอดเวลา

๓) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉิน อันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินขององค์กร จะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากหัวหน้าหน่วยงาน

๔) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๒.๒ ข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง

๑) ไม่อนุญาตให้บุคคลเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นพนักงานห้องควบคุมระบบ

๒) กรณีบุคคลอื่นมีความจำเป็นเข้าไปปฏิบัติงาน ต้องได้รับอนุญาตจากรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร และต้องมีพนักงานรับผิดชอบอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๓) กรณีบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าไปปฏิบัติหน้าที่ในพื้นที่ควบคุม ต้องมีพนักงานรับผิดชอบอย่างน้อย ๑ คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๔) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

๕) กรณีมีความจำเป็นเร่งด่วน หรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สิน จะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้ โดยได้รับความเห็นชอบจากหัวหน้าหน่วยงาน

๓. การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

๓.๑ ข้อกำหนดการควบคุมการเข้าถึงระบบสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ต้องคำนึงถึงการใช้งานและความมั่นคงปลอดภัยสารสนเทศ

๑) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกตามกลุ่มทรัพยากรของระบบ หรือระบบงาน โดยระบุถึงกลุ่มผู้ใช้งาน และสิทธิ์ของกลุ่มผู้ใช้งาน

๒) สถานที่ตั้งของระบบสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลที่สำคัญ ต้องมีการควบคุมการเข้า-ออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๑.๒ การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง

๑) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบสารสนเทศ โดยผู้ขอใช้งานต้องทำการขออนุญาตเข้าระบบที่ต้องการอย่างเป็นลายลักษณ์อักษร ด้วยแบบฟอร์มเอกสารการขอสิทธิ์ในการเข้าสู่ระบบ ที่ต้องได้รับการลงนามอนุมัติ และมีการจัดเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน รวมทั้งต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒) เจ้าของข้อมูลและระบบงาน มีหน้าที่อนุมัติเพื่ออนุญาตให้ผู้ใช้งานเข้าสู่ระบบสารสนเทศตามที่ผู้ใช้งานร้องขอ แต่จะอนุญาตเฉพาะการเข้าถึงในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน อาจนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๓) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าของข้อมูลและระบบงาน ตามความจำเป็นต่อการใช้งานระบบสารสนเทศเท่านั้น

๔) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล และระบบสารสนเทศได้

๕) ผู้ดูแลระบบ มีหน้าที่ติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ และตรวจตราการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ที่มีผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศที่สำคัญได้

๖) ผู้ดูแลระบบ มีหน้าที่บันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาต และที่ไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓.๒ ข้อกำหนดการแบ่งประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๓.๒.๑ ประเภทของข้อมูล

๑) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่
   (๑) นโยบาย
   (๒) ข้อมูลยุทธศาสตร์
   (๓) ข้อมูลบุคลากร
   (๔) ข้อมูลงบประมาณการเงินและบัญชี
   (๕) ข้อมูลด้านการบริหารอื่นๆ

๒) ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน ได้แก่
   (๑) ข้อมูลการดำเนินงานตามภารกิจของ กฟน.
   (๒) ข้อมูลกฎระเบียบ และกฎหมายที่เกี่ยวข้องกับ กฟน.
   (๓) ข้อมูลการติดต่อสื่อสารภายใน กฟน.
   (๔) ข้อมูลติดตามการดำเนินงานตามภารกิจของ กฟน.
   (๕) ข้อมูลติดตามการใช้จ่ายงบประมาณ
   (๖) ข้อมูลรายงานผลการปฏิบัติงาน
   (๗) ข้อมูลด้านการจัดการและปฏิบัติงานอื่นๆ

๓) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่
   (๑) ข้อมูลด้านการใช้พลังงานไฟฟ้า
   (๒) ข้อมูลส่วนตัวของผู้ใช้ไฟฟ้า

(๓) ข้อมูลด้านการวิจัย

(๔) ข้อมูลด้านการให้บริการอื่นๆ

๓.๒.๒ การลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ ซึ่งกำหนดชั้นความลับของข้อมูลเป็น ๔ ระดับ ได้แก่

๑) ลับที่สุด ได้แก่ ข้อมูลที่มีความสำคัญที่สุดเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่ได้รับทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงปลอดภัยของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจ หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้อง อย่างร้ายแรงที่สุด

๒) ลับมาก ได้แก่ ข้อมูลที่มีความสำคัญมากเกี่ยวกับข่าวสาร วัตถุ หรือ บุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงปลอดภัยของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจ หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้อง อย่างร้ายแรง

๓) ลับ ได้แก่ ข้อมูลที่มีความสำคัญเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อธุรกิจ หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้อง

๔) ปกปิด ได้แก่ ข้อมูลซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจขององค์กรเท่านั้น

๓.๒.๓ การจัดแบ่งลำดับชั้นการเข้าถึงข้อมูล ได้แก่

๑) ระดับชั้นสำหรับผู้บริหาร คือระดับชั้นการเข้าถึงที่อนุญาตให้ผู้บริหาร หรือผู้ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการบริหาร ด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิ์ตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป คือระดับชั้นการเข้าถึงที่อนุญาตให้พนักงาน หรือเจ้าหน้าที่ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิ์ตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย คือระดับชั้นการเข้าถึงที่อนุญาตให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย เข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิ์ตามความจำเป็นต่อการดูและระบบ หรือปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

๓.๒.๔ การกำหนดเวลาที่ได้เข้าถึง ได้แก่

๑) การเข้าถึงสารสนเทศในเวลาทำการ (๗.๓๐–๑๕.๓๐ น.)

๒) การเข้าถึงสารสนเทศนอกเวลาทำการ (นอกช่วงเวลา ๗.๓๐–๑๕.๓๐น.)

๓) การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดทำการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

๔) การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลา จำนวนระยะเวลาการเข้าถึง และระยะเวลาการเข้าถึง ได้แก่

(๑) ๑-๓ วัน

(๒) ๑ สัปดาห์

(๓) ๑ เดือน

(๔) ๓ เดือน

(๕) ครึ่งปีงบประมาณ

(๖) ตามเวลาที่ร้องขอ

(๗) อื่นๆ (ถ้ามี)

๓.๒.๕ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง ได้แก่

๑) ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาทำการ)

๒) เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาทำการ)

๓) โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาทำการ)

๔) หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาทำการ)

๕) ระบบเครือข่ายภายใน (เข้าถึงได้ทั้งในและนอกเวลาทำการ)

๖) ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาทำการ)

๗) ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

๘) ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

๙) เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

๑๐) การเข้าถึงจากระยะไกล (เข้าถึงได้ในและนอกเวลาทำการ)

๑๑) การประชุมทางไกล (เข้าถึงได้ในและนอกเวลาทำการ)

๑๒) อื่นๆ (ถ้ามี)

๓.๓ การใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๓.๓.๑ การควบคุมการเข้าถึงสารสนเทศให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ

๑) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบงานให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ

๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการเข้าถึงข้อมูล หรือผ่านเข้าสู่ระบบให้กับผู้ใช้งาน โดยการอนุญาตเข้าสู่ระบบนั้น ต้องจัดทำเป็นเอกสาร เพื่อขอสิทธิ์ในการเข้าสู่ระบบและมีการลงนามอนุมัติเป็นลายลักษณ์อักษร รวมทั้งให้จัดเก็บเอกสารนั้นไว้ เพื่อเป็นหลักฐาน

๓) หัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าถึงข้อมูล หรือเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เพื่อป้องกันการให้สิทธิ์การใช้งานเกินความจำเป็น ซึ่งอาจนำไปสู่การใช้งานเกินอำนาจหน้าที่ การกำหนดสิทธิ์ในการเข้าถึงระบบงาน จึงต้องกำหนดตามความจำเป็นในการใช้งานตามภารกิจเท่านั้น

๓.๓.๒ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ

๑) ผู้ดูแลระบบ ต้องทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อปรับปรุงการให้สิทธิ์ให้สอดคล้องกับความต้องการทางธุรกิจ หรือข้อกำหนดการใช้งานตามภารกิจที่เปลี่ยนไป

๒) หัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงานของผู้ใช้งาน ต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำหนดสิทธิ์ตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน เมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิ์ต่างๆ ในการเข้าใช้ระบบสารสนเทศเมื่อมีผู้ใช้งานลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้ปฏิบัติอย่างน้อย ดังนี้

๓.๔.๑ การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) ให้ปฏิบัติ ดังนี้

๑) ผู้ใช้งานที่ได้รับอนุญาตให้มีสิทธิ์เข้าถึงระบบสารสนเทศ ต้องได้รับการอบรมหลักสูตรเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) ให้เกิดความรู้ความเข้าใจกับผู้ใช้งาน และเกิดความตระหนัก ความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒) หลักสูตรอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) ให้ดำเนินการตามแนวปฏิบัติด้านการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่อยู่ภายใต้นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๓.๔.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ให้ปฏิบัติอย่างน้อย ดังนี้

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานระบบสารสนเทศ

๒) ผู้ดูแลระบบ ตรวจสอบว่าผู้ใช้งานได้รับมอบหมายสิทธิ์จากเจ้าของข้อมูลและระบบงานสำหรับเข้าใช้งานระบบสารสนเทศอย่างถูกต้อง โดยต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงานเป็นลายลักษณ์อักษรเท่านั้น

๓) ผู้ดูแลระบบ ตรวจสอบบัญชีชื่อผู้ใช้งาน โดยต้องไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๔) ผู้ดูแลระบบ ตรวจสอบ และให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและความสอดคล้องกับความต้องการทางธุรกิจ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕) ผู้ดูแลระบบ สร้างบัญชีชื่อผู้ใช้งาน (Username) จากชื่อภาษาอังกฤษ และตามด้วยอักษรสองตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สาม หรือจนกว่าจะไม่ซ้ำกับบัญชีชื่อผู้ใช้งานคนอื่น และให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

๖) จัดทำเอกสารแสดงถึงสิทธิ์ และหน้าที่ความรับผิดชอบให้ผู้ใช้งานลงนามรับทราบ

๗) จัดทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศไว้เป็นหลักฐาน

๓.๔.๓ การยกเลิกสิทธิ์การใช้งานระบบสารสนเทศ

การยกเลิกเพิกถอนสิทธิ์การใช้งานระบบสารสนเทศ จะเกิดขึ้นในกรณีที่มีผู้ใช้งานลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง ซึ่งต้องปฏิบัติตามขั้นตอน ดังนี้

๑) หัวหน้างานหรือผู้บังคับบัญชาของผู้ร้องขอ กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำร้องขอกับหัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงาน

๒) ผู้ดูแลระบบ ยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบบัญชีชื่อผู้ใช้งานออกจากระบบที่เกี่ยวข้องทั้งหมด

๓.๔.๔ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ แต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ให้ปฏิบัติอย่างน้อย ดังนี้

๑) เจ้าของข้อมูลและระบบงาน ต้องเป็นผู้กำหนดสิทธิ์ในการเข้าถึงข้อมูล หรือเข้าใช้งานระบบสารสนเทศ โดยจัดทำเป็นเอกสารการกำหนดสิทธิ์เพื่อควบคุมการเข้าถึง (User Right Matrix) ซึ่งแบ่งแยกเป็นกลุ่มของผู้ใช้งานที่ต่างกัน และระดับสิทธิ์ พร้อมทั้งรายละเอียดสิทธิ์ที่ใช้เข้าถึงข้อมูล หรือเข้าใช้งานระบบในแต่ละระดับ เพื่อเป็นมาตรฐานสำหรับการกำหนดสิทธิ์ หรือมอบหมายสิทธิ์ในการเข้าถึงข้อมูล หรือเข้าใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม และตามความจำเป็นในการปฏิบัติหน้าที่

๒) หัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงาน ต้องเป็นผู้กำหนดสิทธิ์ หรือมอบหมายสิทธิ์ในการเข้าถึงข้อมูล หรือเข้าใช้งานระบบ กับหน่วยงานของผู้ร้องขอ โดยต้องจัดทำเป็นลายลักษณ์อักษร และต้องจัดทำบันทึกของการกำหนดสิทธิ์ หรือมอบหมายสิทธิ์ดังกล่าว เพื่อเก็บไว้เป็นหลักฐาน

๓) ในกรณีมีความจำเป็นต้องให้สิทธิ์จำเพาะ สิทธิ์พิเศษ หรือสิทธิ์อื่นๆ ที่ถูกกำหนดตามภาระหน้าที่ปกติกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน หรือผู้บังคับบัญชา โดยต้องมีการกำหนดระยะเวลาการให้ใช้งาน และต้องยกเลิกหรือเพิกถอนสิทธิ์การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากหน้าที่ หรือตำแหน่ง รวมถึงต้องระบุได้ว่าสิทธิ์พิเศษดังกล่าวนั้น สามารถเข้าถึงข้อมูลใด หรือเข้าใช้งานระบบส่วนใดได้บ้าง ทั้งนี้ผู้ดูแลระบบ ต้องสร้างบัญชีชื่อผู้ใช้งานขึ้นมาใหม่ที่ต่างจากบัญชีชื่อผู้ใช้งานปกติ

๓.๔.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

เพื่อให้การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานเป็นไปอย่างมีความรัดกุม ผู้ดูแลระบบต้องปฏิบัติตามอย่างน้อย ดังนี้

๑) นำแนวปฏิบัติเกี่ยวกับการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านมาจัดทำกลไกในการตรวจสอบและควบคุมการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน บนระบบสารสนเทศที่ตนเองรับผิดชอบอยู่

๒) เมื่อมีความจำเป็นต้องใช้รหัสผ่านชั่วคราว ต้องตั้งรหัสผ่านชั่วคราวให้ยากต่อการเดา และกรณีที่ต้องใช้รหัสผ่านชั่วคราวสำหรับบัญชีชื่อผู้ใช้งานหลายๆ บัญชีพร้อมกัน ต้องตั้งรหัสผ่านที่ไม่ซ้ำกัน

๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย และต้องไม่ส่งผ่านบุคคลอื่น หรือส่งผ่านช่องทางที่ไม่ปลอดภัย เช่น จดหมายอิเล็กทรอนิกส์ (Email)

๔) กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๕) กำหนดอายุการใช้งานของรหัสผ่าน และกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้

๖) การเปลี่ยนรหัสผ่านของบัญชีชื่อผู้ใช้งานใดๆ ต้องมีการตรวจสอบความถูกต้องของรหัสผ่านปัจจุบันก่อนที่จะอนุญาตให้เปลี่ยนรหัสผ่านใหม่

๗) กำหนดให้รหัสผ่านไม่ถูกบันทึก จัดเก็บไว้ในโปรแกรม หรือการตั้งค่าการเข้าใช้งานระบบ อย่างอัตโนมัติ

๘) ลบ หรือเปลี่ยนค่าเริ่มต้นรหัสผ่าน (Default Password) ทันทีหลังจากติดตั้งระบบ

๙) การพิมพ์ หรือแสดงค่า รหัสผ่าน ต้องอยู่ในรูปแบบที่ปกปิดจากการเห็นข้อมูลรหัสผ่านหรือที่ไม่สามารถอ่านได้

๑๐) การรับ-ส่ง ข้อมูลรหัสผ่าน ต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล และมีความปลอดภัย

๓.๔.๖ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

เพื่อให้สิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศสอดคล้องกับความจำเป็นในการปฏิบัติหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ ผู้ดูแลระบบต้องปฏิบัติอย่างน้อย ดังนี้

๑) เมื่อได้รับแจ้งถึงการเปลี่ยนแปลง ได้แก่ ผู้ใช้งานลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง ให้ดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศ และปรับปรุงบัญชีชื่อผู้ใช้งานและสิทธิ์ของผู้ใช้งานที่มีการเปลี่ยนแปลงนั้นโดยทันที หรืออย่างน้อยปีละ ๑ ครั้ง

๒) การทบทวนสิทธิ์การเข้าถึงจำเพาะ หรือสิทธิ์พิเศษ ต้องได้รับการทบทวน ดำเนินการโดยทันที หรืออย่างน้อยทุก ๖ เดือน

๓) จัดทำบันทึกหรือรายงานผลการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศเพื่อส่งให้ผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมายจากผู้บริหารรับทราบ ลงนาม และจัดเก็บไว้เป็นหลักฐาน

๓.๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้ปฏิบัติอย่างน้อย ดังนี้

๓.๕.๑ การใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน

เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน อย่างมีคุณภาพ ผู้ใช้งาน ต้องปฏิบัติอย่างน้อย ดังนี้

๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อเข้าใช้งานระบบครั้งแรก

๒) กำหนดรหัสผ่านที่ยากต่อการคาดเดา

๓) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๕) ไม่กำหนดรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๙) ไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล

๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อปฏิบัติหน้าที่แทน หลังจากการปฏิบัติหน้าที่นั้นเสร็จสิ้น ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑๒) เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรืออย่างน้อยทุก ๖ เดือน หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยใช้ไปแล้ว

๑๕) ผู้ใช้งานที่ได้รับสิทธิ์ให้เป็นผู้ดูแลระบบ ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

๓.๕.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ สามารถเข้าถึงอุปกรณ์ขององค์กร ผู้ดูแลระบบ หรือผู้ใช้งานต้องปฏิบัติอย่างน้อย ดังนี้

๑) ผู้ดูแลระบบ ต้องกำหนดให้ระบบ หรือเครื่องคอมพิวเตอร์ ป้องกันผู้อื่นเข้าใช้ระบบ ด้วยการใส่รหัสผ่านก่อนเข้าใช้งานทุกครั้ง

๒) ผู้ดูแลระบบ ต้องกำหนดให้ระบบตัดการใช้งานอย่างอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเป็นเวลาอย่างน้อย ๑๕ นาที

๓) ผู้ดูแลระบบ ต้องกำหนดให้เครื่องคอมพิวเตอร์ล็อคหน้าจออย่างอัตโนมัติ หรือกำหนดให้โปรแกรมถนอมหน้าจอทำงาน หลังจากที่ไม่ได้ใช้งานเป็นเวลาอย่างน้อย ๑๕ นาที และต้องให้ผู้ใช้งานใส่รหัสผ่านให้ถูกต้องทุกครั้ง จึงจะสามารถปลดล็อคหน้าจอได้

๔) ผู้ใช้งาน ต้องออกจากระบบสารสนเทศ โดยทันทีเมื่อเสร็จสิ้นการใช้งาน

๕) ผู้ใช้งาน ต้องล็อคอุปกรณ์ และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งาน

๓.๕.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

เพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึง โดยผู้ซึ่งไม่มีสิทธิ์ เพื่อกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ผู้ใช้งาน ต้องปฏิบัติอย่างน้อย ดังนี้

๑) เอกสาร และสื่อบันทึกต่างๆ ที่ใช้สำหรับการปฏิบัติงาน ต้องถูกจัดเก็บไว้ในตู้เอกสารที่สามารถล็อคได้ หรือสถานที่ที่มีความปลอดภัย หลังจากการใช้งาน

๒) ห้ามผู้ที่ไม่ได้รับอนุญาต ใช้งานอุปกรณ์บันทึกภาพและเสียง เครื่องพิมพ์เอกสาร เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร และเครื่องโทรสาร

๓) นำเอกสารออกจากเครื่องพิมพ์เอกสาร เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร และเครื่องโทรสาร ทันทีที่ใช้งานเสร็จ

๔) เมื่อสิ้นสุดระยะเวลาเก็บรักษาเอกสาร และสื่อบันทึกต่างๆ ที่ใช้สำหรับการปฏิบัติงาน ให้จัดการทำลายด้วยวิธีการที่ปลอดภัย เพื่อไม่ให้สามารถกู้คืนข้อมูลกลับมาใช้ใหม่ได้ ดังนี้

(๑) การทำลายเอกสาร หรือ สื่อบันทึกที่เป็นแผ่น CD/DVD ให้ใช้วิธีการหั่น ด้วยเครื่องหั่นทำลาย

(๒) การทำลายสื่อบันทึกที่เป็นเทป ให้ใช้วิธีทุบหรือบดให้เสียหาย หรือเผาทำลาย

(๓) การทำลายสื่อบันทึกประเภท Flash Drive หรือ ฮาร์ดดิสก์ ให้ใช้วิธีการทุบหรือบดให้เสียหาย หรือใช้วิธีการทำลายข้อมูลอิเล็กทรอนิกส์ตามมาตรฐานกระทรวงกลาโหมสหรัฐอเมริกา DOD

๕) ยืนยันตัวตนเพื่อเข้าถึงข้อมูล หรือเข้าใช้งานระบบสารสนเทศ ตามกลไกที่ผู้ดูแลระบบกำหนดก่อนการเข้าใช้งาน

๖) ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์ทันที หรือเครื่องคอมพิวเตอร์ต้องมีโปรแกรมถนอมหน้าจอพร้อมรหัสผ่านทุกครั้ง เมื่อผู้ใช้งานไม่ได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ เพื่อป้องกันไม่ให้ผู้อื่นลักลอบใช้งานเครื่องคอมพิวเตอร์ในเวลาดังกล่าว

๓.๕.๔ การเข้ารหัสข้อมูลที่เป็นความลับ

เพื่อรักษาความลับของข้อมูล ผู้ใช้งานสามารถใช้มาตรการการเข้ารหัสข้อมูล สำหรับข้อมูลที่ถูกจัดลำดับชั้นความลับตามข้อกำหนดเกี่ยวกับลำดับชั้นความลับของข้อมูล ที่กำหนดไว้ตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ หรือตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๑) เข้ารหัสข้อมูลที่เป็นความลับในระดับ ลับที่สุด ลับมาก และ ลับ ด้วยมาตรการเข้ารหัสที่มีความปลอดภัย และเป็นที่ยอมรับตามมาตรฐานสากล ได้แก่ กลไกการเข้ารหัสประเภท Symmetric แบบ AES 256 หรือ กลไกการเข้ารหัสประเภท Asymmetric แบบ RSA 1024 หรือแบบที่ให้ความปลอดภัยที่ดีกว่า

๒) หัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงาน ที่ต้องรักษาข้อมูลที่เป็นความลับ ต้องแต่งตั้งผู้ที่ทำหน้าที่ดูแล และเก็บรักษากุญแจที่ใช้เข้ารหัสข้อมูลที่เป็นความลับ ให้มีความปลอดภัย

๓.๖ การควบคุมการเข้าถึงและใช้งานบริการระบบเครือข่าย

เพื่อป้องกันการเข้าถึงบริการระบบเครือข่าย โดยไม่ได้รับอนุญาต ให้ปฏิบัติอย่างน้อย ดังนี้

๓.๖.๑ การใช้งานบริการระบบเครือข่าย

เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ต้องปฏิบัติอย่างน้อย ดังนี้

๑) หน่วยงานในสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร ต้องกำหนดนโยบายการใช้เครือข่ายและบริการต่างๆ บนระบบเครือข่ายอย่างชัดเจน โดยอย่างน้อยต้องระบุถึงเครือข่ายใด และบริการใด ที่อนุญาตให้หน่วยงานได้ใช้

๒) หน่วยงานผู้ดูแลระบบ ต้องนำนโยบายที่กำหนดไว้ จัดทำเป็นมาตรการเพื่อควบคุมการเข้าถึงและใช้งานบริการระบบเครือข่าย โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา/หัวหน้าหน่วยงาน เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์อย่างน้อยปีละ ๑ ครั้ง

๓.๖.๒ การยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

เพื่อยืนยันตัวตนก่อนที่อนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กร สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศได้ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) การเชื่อมต่อใดๆ จากภายนอกองค์กร ต้องมีการตรวจสอบผู้ใช้งาน (Identification) ด้วยบัญชีชื่อผู้ใช้งาน (Username) ทุกครั้ง ก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายและระบบสารสนเทศ

๒) การตรวจสอบผู้ใช้งานที่อนุญาตให้เข้าถึง ให้ใช้วิธีการยืนยันตัวตน (Authentication) เพื่อพิสูจน์ว่าเป็นผู้ใช้งานตัวจริง ด้วยการใช้รหัสผ่าน (Password) และสำหรับระบบที่มีความสำคัญสูงให้พิจารณาใช้วิธียืนยันตัวตนด้วยสมาร์ทการ์ด หรือการใช้ USB Token ที่ใช้การยืนยันตัวตนในแบบ ๒ ระดับ (Two-Factor Authentication) ซึ่งเป็นวิธีการที่ให้ความปลอดภัยสูงกว่าการใช้รหัสผ่านเพียงอย่างเดียว

๓) หน่วยงาน ในสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร ต้องควบคุมการเชื่อมต่อผ่านสายโทรศัพท์ สู่ระบบเครือข่ายภายในองค์กร

๓.๖.๓ การระบุอุปกรณ์บนระบบเครือข่าย (Equipment Identification in Networks)

เพื่อสามารถระบุอุปกรณ์บนระบบเครือข่ายได้ โดยการระบุอุปกรณ์บนระบบเครือข่าย ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ผู้ดูแลระบบ ต้องจัดทำบันทึกการขอเชื่อมต่อระบบเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ สถานที่ติดตั้ง รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ หมายเลขเครือข่ายทั้งในระดับ IP Address และ MAC Address

๒) ต้องสามารถตรวจสอบหมายเลขเครือข่ายของอุปกรณ์ระบบเครือข่าย ทั้งของต้นทางและปลายทางได้

๓) ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงหัวหน้าหน่วยงานผู้ดูแลระบบ เพื่อขอเชื่อมต่อระบบเครือข่าย และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๔) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบหรือผู้ที่ได้รับอนุญาตเท่านั้น

๕) ต้องใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายภายในองค์กรได้

๖) จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๗) ทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๓.๖.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ให้ปฏิบัติอย่างน้อย ดังนี้

๑) การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ดูแลระบบหรือผู้ที่ได้รับอนุญาตเท่านั้น

๒) ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยปิดพอร์ตที่เสี่ยงต่อการเกิดความเสียหายต่อระบบเครือข่าย และปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งาน

๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้ สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้ในระยะเวลาที่จำกัดเท่าที่จำเป็น และการขอใช้งานต้องได้รับการอนุญาตจากหัวหน้าหน่วยงานผู้ดูแลระบบ เป็นลายลักษณ์อักษร

๔) บุคคลภายนอกที่เข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบเครือข่ายจะต้องลงชื่อเข้า-ออก ในแบบฟอร์มการเข้า-ออกพื้นที่ ให้ถูกต้อง และได้รับการอนุมัติจากหัวหน้าหน่วยงานผู้ดูแลระบบ และต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๕) บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา หรือบริหารจัดการพอร์ต ของอุปกรณ์เครือข่ายผ่านทางระบบเครือข่าย ต้องทำหนังสือเป็นลายลักษณ์อักษรถึงหัวหน้าหน่วยงานผู้ดูแลระบบ เพื่อขอเชื่อมต่อระบบเครือข่าย

๓.๖.๕ การแบ่งแยกระบบเครือข่าย (Segregation in Networks)

เพื่อแบ่งแยกระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) แบ่งแยกระบบเครือข่ายเป็นระบบเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงระบบเครือข่าย โดยไม่ได้รับอนุญาต

๒) แบ่งแยกระบบเครือข่ายออกเป็น ระบบเครือข่ายภายใน และระบบเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๓) แบ่งแยกระบบเครือข่ายภายใน ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ

๔) ติดตั้งอุปกรณ์ควบคุมการเข้าถึงระบบเครือข่าย ได้แก่ ไฟร์วอลล์ (Firewall) เพื่อป้องกันทางเข้า-ออกระบบเครือข่าย ระหว่างระบบเครือข่ายภายใน และระบบเครือข่ายภายนอก และที่มีกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ ที่มีความสำคัญ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๖.๖ การควบคุมการเชื่อมต่อทางระบบเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ตรวจสอบการเชื่อมต่อระบบเครือข่าย เป็นประจำเพื่อตรวจหาการเชื่อมต่อที่ไม่ได้รับอนุญาต

๒) จำกัดสิทธิ์ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย และกลั่นกรองข้อมูลที่รับ-ส่ง โดยอาศัยกฎเกณฑ์ต่างๆ ที่กำหนดไว้ล่วงหน้า

๓) การเชื่อมต่อระหว่างระบบเครือข่ายภายในกับระบบเครือข่ายภายนอก ต้องกระทำผ่านไฟร์วอลล์ โดยกำหนดให้ไฟร์วอลล์อนุญาตเฉพาะการเชื่อมต่อจากภายในออกไปยังปลายทางภายนอกได้เท่านั้น หากระบบใดต้องการให้บุคคลภายนอกเรียกใช้ข้อมูลจากระบบภายใน ต้องผ่านการพิจารณาและเห็นชอบจากหัวหน้าหน่วยงานผู้ดูแลระบบ

๔) ตรวจจับการบุกรุก หรือการโจมตี ทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย จากผู้ไม่หวังดี ด้วยระบบตรวจจับผู้บุกรุก (Intrusion Detection/Prevention System – IDS/IPS) และตรวจทานผลการบุกรุกอย่างสม่ำเสมอ

๕) ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

๓.๖.๗ การควบคุมการจัดเส้นทางบนระบบเครือข่าย (Network Routing Control)

เพื่อควบคุมการจัดเส้นทางบนระบบเครือข่าย ให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ควบคุมไม่ให้มีการเปิดเผย แผนการใช้หมายเลขเครือข่าย (IP Address Schema)

๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย (Network Address Translation) เพื่อแยกระบบเครือข่ายย่อย

๓) กำหนดมาตรการการบังคับใช้เส้นทางบนระบบเครือข่าย โดยควบคุมให้เชื่อมต่อไปยังระบบเครือข่ายปลายทาง ผ่านช่องทางที่กำหนดไว้เท่านั้น หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่ายให้สำหรับผู้ใช้งานที่จำเป็นต้องใช้และได้รับสิทธิ์เท่านั้น

๓.๖.๘ การใช้งานอินเทอร์เน็ต

๑) ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่จำเป็นต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall หรือ IDS/IPS ซึ่งผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem เว้นแต่มีเหตุผลความจำเป็น และต้องขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์ประเภทพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

๓) ก่อนการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต ต้องมีการตรวจสอบไวรัส (Virus Scanning) ทุกครั้ง โดยโปรแกรมป้องกันไวรัส

๔) ผู้ใช้งานต้องไม่ใช้ระบบเครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่เนื้อหามีผลกระทบต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๕) ผู้ใช้งานถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

๖) ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสม ทางศีลธรรม ข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๗) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่มีการประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต

๘) ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย หรือภาพที่มีลักษณะลามก และไม่เผยแพร่ หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายอินเทอร์เน็ต

๙) ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัด ต่อเติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๐) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้อง และความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ ที่อยู่บนระบบเครือข่ายอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๑) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงโปรแกรมที่ใช้ปรับปรุงข้อมูลสำหรับโปรแกรมคอมพิวเตอร์ให้ทันสมัย (Patch) หรือโปรแกรมที่ใช้ซ่อมแซมจุดบกพร่องของโปรแกรมคอมพิวเตอร์ (Fixes) ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๒) ในการเสนอความคิดเห็น ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร รวมถึงการทำลายความสัมพันธ์ของพนักงานหน่วยงานอื่น ๆ

๑๓) ห้ามผู้ใช้งานใช้บริการอินเทอร์เน็ตที่มีการครอบครองแบรนด์วิดท์จำนวนมาก หรือเป็นเวลานาน

๑๔) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓.๖.๙ การใช้งานจดหมายอิเล็กทรอนิกส์

๑) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งานระบบ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้างเป็นต้น

๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์บัญชีชื่อผู้ใช้งานใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนของผู้เข้าใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

๓) ในการเข้าระบบจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานรายใหม่ จะได้รับรหัสผ่านค่าเริ่มต้น (Default Password) และเมื่อเข้าสู่ระบบครั้งแรกให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๔) การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในนโยบายการใช้ทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ (Acceptable Use Policy)

๕) การป้อนรหัสผ่านระบบจดหมายอิเล็กทรอนิกส์ ต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ให้แสดงในรูปแบบของสัญลักษณ์แทนตัวอักษร เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๖) ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ได้ไม่เกิน ๓ ครั้ง

๗) ผู้ดูแลระบบ ต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ มีการล็อกเอ้าท์ออกจากหน้าจอตัดการใช้งานของผู้ใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น อย่างน้อย ๑๕ นาที หากต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๘) ผู้ใช้งาน ต้องไม่ตั้งค่าการใช้โปรแกรม ช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๙) ผู้ใช้งาน ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านภายใน ๙๐ วัน

๑๐) ผู้ใช้งาน ต้องระมัดระวังในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กร หรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่ายขององค์กร

๑๑) ผู้ใช้งาน ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ ต้องรับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ที่ตนเป็นเจ้าของ

๑๒) ผู้ใช้งาน ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

๑๓) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑๔) ผู้ใช้งาน ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัสในการตรวจสอบ เพื่อป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น *.exe *.com เป็นต้น

๑๕) ผู้ใช้งาน ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๖) ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียง หรือเกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๑๗) หลีกเลี่ยงการส่งข้อมูลส่วนบุคคล เช่น รหัสผ่าน บัญชีชื่อผู้ใช้งาน หมายเลขบัตรประชาชน ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๘) กรณีต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑๙) ผู้ใช้งาน ต้องไม่ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อส่งจดหมายอิเล็กทรอนิกส์ที่ไม่ได้มีวัตถุประสงค์ในภารกิจขององค์กร หรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาเรื่องส่วนตัว หากผู้ใช้งานต้องการส่งจดหมายอิเล็กทรอนิกส์ดังกล่าว ขอให้ใช้จากบริการจดหมายอิเล็กทรอนิกส์ฟรี เช่น Hotmail Yahoo Gmail เป็นต้น

๒๐) ผู้ใช้งาน ต้องไม่นำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ซึ่งเป็นของการไฟฟ้านครหลวงไปเผยแพร่สู่บุคคลอื่นไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถาม หรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ขององค์กร หรือได้รับอนุญาตจากหัวหน้าหน่วยงานแล้วเท่านั้น

๒๑) ผู้ใช้งาน ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒๒) ผู้ใช้งาน ต้องลบจดหมายอิเล็กทรอนิกส์ ที่ไม่ต้องการออกจากตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเอง เพื่อลดปริมาณการใช้เนื้อที่เก็บข้อมูลจดหมายอิเล็กทรอนิกส์จากระบบ

๒๓) ผู้ใช้งาน ต้องโอนย้ายจดหมายอิเล็กทรอนิกส์ ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้เก็บจดหมายอิเล็กทรอนิกส์

๓.๖.๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ดูแลระบบ และผู้ใช้งาน ระบบเครือข่ายไร้สาย (Wireless Policy) ขององค์กร มีหน้าที่และความรับผิดชอบที่ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล และต้องมีการกำหนดรหัสผ่านในการเข้าใช้งาน

๒) ผู้ใช้งาน ต้องไม่นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานในองค์กร ไม่ว่าจะเป็น Access Point Wireless Routers Wireless USB Client หรือ Wireless Card

๓) ผู้ใช้งาน ต้องไม่เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (Ad-hoc) หรือ Peer-to-Peer Network

๔) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร ต้องลงทะเบียน กับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล อย่างเป็นลายลักษณ์อักษร

๕) ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งาน ในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๖) ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เชื่อมต่อระบบเครือข่ายไร้สาย

๗) ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์กระจายออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๘) ผู้ดูแลระบบ ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และสำรวจสัญญาณไม่ให้กระจายออกไปภายนอก โดยควรใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๙) ผู้ดูแลระบบ ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าตั้งต้น (Default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๑๐) ผู้ดูแลระบบ ต้องกำหนดชื่อล็อกอิน และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อล็อกอิน และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือเจาะรหัสได้โดยง่าย

๑๑) ผู้ดูแลระบบ ต้องกำหนดค่าให้ WEP หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Access Point และ Wireless LAN Client เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากยิ่งขึ้น

๑๒) ผู้ดูแลระบบ ต้องเลือกใช้วิธีการควบคุม MAC Address และบัญชีชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address บัญชีชื่อผู้ใช้งานและรหัสผ่านตามที่กำหนดไว้เท่านั้น ให้เข้าใช้ระบบเครือข่ายไร้สายได้

๑๓) ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สาย กับระบบเครือข่ายภายในองค์กร

๑๔) ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานระบบเครือข่ายไร้สาย ติดต่อสื่อสารข้อมูลองค์กรได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๑๕) ผู้ดูแลระบบ ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และรายงานให้รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร ทราบเป็นรายเดือน

๓.๗ การควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อควบคุม และป้องกันการเข้าถึงระบบสารสนเทศ โดยไม่ได้รับอนุญาต ให้ปฏิบัติอย่างน้อย ดังนี้

๓.๗.๑ กำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานที่มีความมั่นคงปลอดภัย โดยการเข้าถึงระบบปฏิบัติการ จะต้องมีการควบคุม โดยวิธีการยืนยันตัวตนที่มีความมั่นคงปลอดภัย ดังนี้

๑) ผู้ดูแลระบบ ต้องจัดการไม่ให้ระบบแสดงรายละเอียดสำคัญ หรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๒) ผู้ดูแลระบบ ต้องจัดการให้ระบบ สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓) ผู้ดูแลระบบ ต้องจัดการให้ระบบจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๔) ผู้ดูแลระบบ ต้องจำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๓.๗.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

เพื่อกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ผู้ใช้งาน ต้องมีบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศ

๒) หากอนุญาตให้ใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็น ทางด้านธุรกิจหรือด้านเทคนิคเท่านั้น

๓) บัญชีชื่อผู้ใช้งาน (Username) ทุกบัญชี ต้องมีรหัสผ่านและเจ้าของบัญชีชื่อผู้ใช้งานเท่านั้นที่ทราบรหัสผ่าน

๔) สำหรับระบบที่ต้องการความมั่นคงปลอดภัยสูง องค์กรสามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม หรือ การตรวจสอบลักษณะเฉพาะตัวของบุคคล (Biometric) ได้

๓.๗.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

เพื่อบริหารจัดการรหัสผ่าน ให้สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งส่งผลให้การกำหนดรหัสผ่านที่มีคุณภาพ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) เมื่อมีการเข้าสู่ระบบในครั้งแรก ระบบต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที และต้องตรวจสอบและยืนยันการกำหนดรหัสผ่านที่มีคุณภาพ และกำหนดรอบระยะเวลาให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

๒) การส่งรหัสผ่านผ่านทางเครือข่าย ต้องทำการเข้ารหัสข้อมูลของรหัสผ่าน เพื่อป้องกันรหัสผ่านถูกเปิดเผย

๓) ต้องทำการบันทึกประวัติการเปลี่ยนรหัสผ่าน เพื่อป้องกันการใช้รหัสผ่านซ้ำ

๔) ต้องป้องกันไม่ให้แสดงข้อมูลรหัสผ่านที่ผู้ใช้งานพิมพ์ลงไป หรือทำให้ไม่เห็นข้อมูลรหัสผ่านที่แท้จริงได้

๓.๗.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

เพื่อจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ปฏิบัติอย่างน้อย ดังนี้

๑) จำกัดสิทธิ์การเข้าถึงและกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๒) ผู้ดูแลระบบต้องจัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้

๓) ห้ามผู้ใช้งานติดตั้งหรือใช้งานโปรแกรมอรรถประโยชน์ที่ไม่อยู่ภายใต้บัญชีรายชื่อที่อนุญาตให้ใช้ และที่ละเมิดลิขสิทธิ์

๔) อนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๕) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่มีการใช้งานเป็นประจำ

๖) ต้องมีการเก็บบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์

๗) ต้องมีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๓.๗.๕ การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-out)

เพื่อป้องกันการเข้าใช้งานระบบ โดยไม่ได้รับอนุญาตผ่านการเชื่อมต่อ (Session) จากเครื่องปลายทางที่มีผู้ใช้งานเข้าใช้งานค้างไว้ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) กำหนดให้ระบบยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นระยะเวลาอย่างน้อย ๑๕ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นลง หรือเป็นระยะเวลาอย่างน้อย ๕ นาที เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒) ถ้าพบว่าไม่มีการใช้งานระบบเป็นระยะเวลาที่กำหนด ระบบต้องทำการยกเลิกการใช้แอปพลิเคชัน และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๓.๗.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

เพื่อลดความเสี่ยงจากการเชื่อมต่อ และเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศ หรือแอปพลิเคชัน ที่มีความเสี่ยงหรือมีความสำคัญสูง ให้ปฏิบัติอย่างน้อย ดังนี้

๑) กำหนดให้ระบบจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชัน ที่มีความเสี่ยงหรือมีความสำคัญสูง ให้ใช้งานได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง

๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๓) สำหรับระบบสารสนเทศที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) ให้ระบบจำกัดระยะเวลาการเชื่อมต่อ ให้มีระยะเวลาที่สั้นลง หรือเป็นระยะเวลาไม่เกิน ๒ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง

๓.๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน ของระบบสารสนเทศ

เพื่อควบคุม และป้องกันการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชัน ของระบบสารสนเทศ โดยไม่ได้รับอนุญาต ให้ปฏิบัติอย่างน้อย ดังนี้

๓.๘.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

เพื่อจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งาน ของผู้ใช้งานและบุคลากรฝ่ายที่สนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) เจ้าของข้อมูลและระบบงาน ต้องเป็นผู้กำหนดกลุ่มผู้ใช้งาน และสิทธิ์ของกลุ่มผู้ใช้งานในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน ของระบบสารสนเทศที่เกี่ยวข้อง

๒) การกำหนดสิทธิ์ให้เข้าใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชันนั้น ให้พิจารณาการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ตามแนวปฏิบัติด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓) โปรแกรมประยุกต์หรือแอปพลิเคชัน ที่ติดตั้งให้ผู้ใช้งานเข้าใช้งาน ต้องสามารถควบคุมให้มีฟังก์ชันการทำงานที่สอดคล้องกับสิทธิ์ที่ผู้ใช้งานได้รับ เพื่อป้องกันการเข้าถึงข้อมูล หรือฟังก์ชันที่เกินความจำเป็นต่อการปฏิบัติงาน

๔) ผู้ดูแลระบบ ต้องจัดหลักสูตรอบรมการใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชัน ตามกลุ่มผู้ใช้งาน ได้แก่ กลุ่มผู้ใช้งานทั่วไป และกลุ่มผู้ใช้งานระดับผู้บริหาร เป็นอย่างน้อย เพื่อป้องกันผู้ใช้งานทั่วไปล่วงรู้ถึงฟังก์ชันการทำงานที่เกินความจำเป็น

๕) ผู้ดูแลระบบ ต้องจัดการไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๖) ผู้ดูแลระบบ ต้องจัดการให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๗) ผู้ดูแลระบบ ต้องจัดการให้ระบบจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๘) กำหนดให้ระบบจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชัน ที่มีความเสี่ยงหรือมีความสำคัญสูง ให้ใช้งานได้เป็นระยะเวลาไม่เกิน ๔ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง เพื่อให้ผู้ใช้งานสามารถใช้งานได้ในช่วงเวลาทำการตามปกติ

๙) กำหนดให้ระบบยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นระยะเวลาอย่างน้อย ๑๕ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลง หรือเป็นระยะเวลาอย่างน้อย ๕ นาที เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๐) ถ้าพบว่าไม่มีการใช้งานระบบเป็นระยะเวลาที่กำหนด ระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์หรือแอปพลิเคชัน และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๓.๘.๒ การจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (Outsource)

เพื่อลดโอกาสที่ข้อมูลสำคัญอาจถูกเปิดเผยจากบุคคลภายนอก ที่รับจ้างพัฒนาระบบสารสนเทศ หรือจ้างเหมาดำเนินงาน (Outsource) ให้ปฏิบัติอย่างน้อย ดังนี้

๑) การประเมินความเสี่ยงของการเข้าถึงสารสนเทศ โดยหน่วยงานภายนอก

(๑) หน่วยงานหรือบุคคลภายนอกที่เกี่ยวข้องในการใช้ข้อมูลขององค์กร ต้องมีความรับผิดชอบต่อการปฏิบัติตามข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง ได้แก่ นโยบาย มาตรฐาน หรือคำสั่ง เช่นเดียวกับพนักงานขององค์กร

(๒) ก่อนที่จะอนุญาตให้หน่วยงานภายนอกเข้าใช้ข้อมูล หน่วยงานเจ้าของข้อมูลและระบบงานจะต้องพิจารณาถึงความจำเป็นทางธุรกิจเป็นหลัก และมีการประเมินความเสี่ยงของการเข้าถึง รวมถึงกำหนดความต้องการด้านความมั่นคงปลอดภัยที่เหมาะสมกับการเข้าถึงนั้น และร่วมกับผู้ดูแลระบบในการวางมาตรการควบคุมต่อไป

(๓) ในการจ้างหน่วยงานภายนอกเข้ามาทำงานให้องค์กรนั้น นอกจากจะคำนึงถึงเป้าหมายผลงานแล้ว องค์กรจะต้องพิจารณาถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรด้วย โดยในข้อตกลงการจ้างงานระหว่างหน่วยงานภายนอกกับองค์กรจะต้องประกอบด้วยความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่ได้มาจากการประเมินความเสี่ยง โดยอย่างน้อยต้องประกอบไปด้วย มาตรการควบคุม และกระบวนการการปฏิบัติให้เกิดความมั่นคงปลอดภัย รวมถึงข้อกำหนดในแง่ของการปฏิบัติงานและความรับผิดชอบของหน่วยงานภายนอกต่อข้อมูลขององค์กรอย่างปลอดภัย ตลอดจนสิทธิ์ต่างๆ ขององค์กรที่มีต่อการทำงานของหน่วยงานภายนอกในด้านความมั่นคงปลอดภัยสารสนเทศ

๒) การระบุและจัดทำข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศสำหรับหน่วยงานภายนอก

การอนุญาตให้หน่วยงาน หรือบุคคลภายนอกเข้าใช้ข้อมูลหรือระบบประมวลผลข้อมูลขององค์กร ต้องกระทำอยู่ในรูปแบบของข้อตกลงหรือสัญญาที่เป็นทางการที่ประกอบด้วยข้อกำหนดด้านความมั่นคงปลอดภัย เพื่อให้หน่วยงานหรือบุคคลภายนอกเข้าใจและปฏิบัติตาม ทั้งนี้ หากเป็นกรณีสัญญาการว่าจ้างจะต้องระบุถึงขอบเขตการใช้งานข้อมูลขององค์กรไว้อย่างชัดเจนในสัญญาการว่าจ้าง รวมทั้งการกำหนดให้ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลองค์กร ในกรณีที่มีความจำเป็นในการใช้ข้อมูลที่จัดอยู่ในชั้นความลับขึ้นไป

(๑) หน่วยงานภายนอกที่ทำงานในกับองค์กร ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงข้อบังคับและคำสั่งที่เกี่ยวข้องขององค์กร โดยองค์กรต้องให้บทสรุปของนโยบายและแนวปฏิบัติฯ ที่เกี่ยวข้องกับหน่วยงานภายนอกก่อนที่จะเริ่มทำงานให้กับองค์กร

(๒) กรณีหน่วยงานภายนอกที่ทำงานให้กับองค์กร มีความจำเป็นในการใช้ข้อมูลที่จัดอยู่ในชั้นความลับขึ้นไป หน่วยงานภายนอกจะต้องลงนามในสัญญาการไม่เปิดเผยข้อมูล ก่อนที่จะได้รับอนุญาตในการเข้าใช้ข้อมูล

(๓) หน่วยงานภายนอกต้องแจ้งหน่วยงานขององค์กรที่รับผิดชอบทันทีในกรณีที่เกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร

(๔) ห้ามหน่วยงานภายนอกนำอุปกรณ์ประมวลผลที่ไม่ใช่ขององค์กรมาเชื่อมต่อเข้ากับระบบเครือข่ายภายในขององค์กรเว้นแต่ได้รับอนุญาตจากองค์กร ทั้งนี้ให้ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล พิจารณาเป็นกรณีไป

(๕) หน่วยงานขององค์กรที่รับผิดชอบในการติดต่อกับหน่วยงานภายนอกที่ได้รับการว่าจ้างในการทำงานให้องค์กรจะต้องสื่อความกับหน่วยงานอื่นๆ ขององค์กรที่เกี่ยวข้องเพื่อให้ทราบถึงบทบาทหน้าที่และขอบเขตงานที่ชัดเจนของหน่วยงานภายนอก

(๖) องค์กรไม่อนุญาตให้หน่วยงานภายนอกนำข้อมูลและสื่อบันทึกข้อมูลที่จัดอยู่ในลำดับชั้นลับขึ้นไปออกจากองค์กรโดยไม่มีการควบคุมที่เหมาะสม

๓.๘.๓ การแยกระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง

เพื่อป้องกันความผิดพลาดที่เกิดจากระบบอื่นภายใต้สภาพแวดล้อมเดียวกัน ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ต้องปฏิบัติอย่างน้อย ดังนี้

๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ขององค์กร คือระบบ SAP ISU และ SAP ERP ซึ่งต้องได้รับการดูแลเป็นพิเศษ โดยให้แยกระบบดังกล่าว ให้ทำงานอยู่บนเครื่องแม่ข่าย หรือเครื่องคอมพิวเตอร์ที่ไม่ใช้ปะปนกับระบบอื่น

๒) ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น เข้าไปปฏิบัติงาน

๓) ต้องแยกสภาพการติดตั้งทางระบบเครือข่าย โดยใช้วิธีการทางเทคนิค VLAN (Virtual Local Area Network)

๔) ต้องควบคุมการเข้ามาใช้งานระบบดังกล่าวผ่านทางระบบเครือข่ายทั้งจากภายในและจากภายนอก ด้วยข้อกำหนดที่สามารถตั้งค่าได้บนตัวอุปกรณ์ไฟร์วอลล์

๕) อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่ลงทะเบียนและได้รับอนุมัติให้ใช้งานได้เท่านั้น ถึงจะสามารถใช้ปฏิบัติงานที่เกี่ยวข้องกับระบบดังกล่าวจากภายนอกสำนักงาน (Mobile Computing and Teleworking)

๓.๘.๔ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

เพื่อปกป้องสารสนเทศจากความเสี่ยง ของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ต้องมีวิธีการยืนยันตัวตนผู้เข้าใช้งานที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานจากระยะไกลผ่านทางอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และในกรณีที่เชื่อมต่ออุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ผ่านเครือข่ายไร้สายขององค์กร ให้ปฏิบัติตามข้อ ๓.๖.๑๐

๒) ต้องมีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่จะนำมาใช้งาน

๓) หน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เข้ามาปฏิบัติงานในพื้นที่ควบคุมที่กำหนด ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออกพื้นที่ให้ถูกต้องชัดเจน

และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

๓.๘.๕ การปฏิบัติงานจากภายนอกองค์กร (Teleworking)

เพื่อความมั่นคงปลอดภัยของการปฏิบัติงานจากภายนอกองค์กร ให้กำหนดแนวปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกองค์กร ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ผู้ดูแลระบบ ต้องให้สิทธิ์ตามที่ได้รับการขออนุมัติ การยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งาน เมื่อมีการยกเลิกการปฏิบัติงานจากระยะไกล

๒) การเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล เป็นลายลักษณ์อักษร

๓) ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชา หรือเจ้าของข้อมูลและระบบงาน เป็นลายลักษณ์อักษร และต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

๔) ผู้ใช้งานระบบจากระยะไกล ต้องทำการยืนยันตัวตนก่อนเข้าใช้งาน

๕) มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่หวังดี

๖) หากมีข้อมูลขององค์กรในการทำงานภายนอกองค์กร นโยบายขององค์กรทั้งหมดที่เกี่ยวกับการประมวลผลข้อมูล มีผลบังคับใช้กับการทำงานภายนอกองค์กร เช่นเดียวกับการทำงานภายในองค์กร

๗) ผู้ใช้งานต้องเพิ่มความระวังเป็นพิเศษ เมื่อมีการใช้ข้อมูลขององค์กรจากภายนอกองค์กร

๘) มีการทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกองค์กรอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒

นโยบายการบริหารจัดการระบบสารสนเทศและระบบสำรองของระบบสารสนเทศ

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อจัดทำระบบสำรองข้อมูล เพื่อให้มีข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย ให้สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความพร้อมใช้งาน (Availability Risk)

ผู้รับผิดชอบ

๑) ฝ่ายระบบโครงสร้างพื้นฐาน (ฝคฐ.)
๒) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การสำรองข้อมูลและการกู้คืนระบบ

๑.๑ การจัดให้มีระบบสำรองข้อมูล

๑) ผู้ดูแลระบบ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

๒) รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการดำเนินงานการบริหารจัดการ และการปรับปรุงกระบวนการที่ต้องใช้ข้อมูลสารสนเทศดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้ต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับการดำเนินงานตามวัตถุประสงค์ขององค์กร

๓) การสำรองข้อมูลภายในองค์กร หมายถึง การทำสำรองข้อมูลทั้งหมด (Full Backup) ผู้ดูแลระบบต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสม และกำหนดไว้ชัดเจน เช่น สำรองข้อมูลอย่างน้อย ๑ ครั้งในรอบสัปดาห์ เป็นต้น

๔) การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องจัดทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น และรายงานให้รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารทราบ

๕) การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๖) ผู้ดูแลระบบ ต้องมอบหมายหน้าที่การสำรองข้อมูลแก่พนักงานคนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบ ไม่สามารถปฏิบัติงานได้

๗) กรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา และรายงานต่อรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารทราบ

๘) ผู้ดูแลระบบ ต้องกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๙) การสำรองข้อมูลภายนอกองค์กร (Off-Site Backup) ผู้ดูแลระบบ ต้องจัดให้มีการสำรองข้อมูลภายนอกองค์กร ตามความเหมาะสมของหน่วยงาน เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็ว และป้องกันระบบจากการถูกโจมตี หรือความหายนะที่อาจเกิดขึ้น

๑๐) การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑๑) นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอน Backup Procedure โดยเคร่งครัด

๑.๒ ตัวอย่างการปฏิบัติเกี่ยวกับการสำรองข้อมูล

๑) ผู้ดูแลระบบ ต้องสำรองข้อมูลแต่ละรายการตามความถี่ ดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ็อกซ์	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๒	Web Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๓	Database Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๔	Firewall Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๕	Server อื่นๆ เช่น (ต้องกำหนดเองว่าเซิร์ฟเวอร์อื่นๆ ได้แก่อะไรบ้าง)	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบนเซิร์ฟเวอร์อื่นๆ	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
หมายเหตุ ทุกรายการที่ปรากฏในตารางใช้วิธี Full Backup			

๒) ผู้ดูแลระบบ ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การ Backup ตามรายละเอียดในตารางข้างต้นนั้น ถูกต้องสมบูรณ์หรือไม่

๓) กรณีสมบูรณ์ ผู้ดูแลระบบต้องนำสื่อบันทึกข้อมูล Backup ไปเก็บไว้นอกองค์กร ในสถานที่ปลอดภัย

๔) กรณีไม่สมบูรณ์ ผู้ดูแลระบบต้องแก้ไขให้ Backup สมบูรณ์และกลับไปตรวจสอบทั้งหมดใหม่อีกครั้ง

๑.๓ การกู้คืนระบบ

๑) ในกรณีพบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข รายงานผลการแก้ไข พร้อมทั้งบันทึก และให้รายงานสรุปผลการปฏิบัติงานต่อรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารทราบโดยเร็ว

๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้งานระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๒. การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

ในการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน (Business Continuity Management) รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร ต้องมอบหมายให้พนักงานที่เกี่ยวข้องดำเนินการ ดังนี้

๒.๑ การเตรียมรับมือภัยพิบัติ

๒.๑.๑ ความเสี่ยงและชนิดของภัยพิบัติ

ภัยพิบัติ หมายถึง เหตุการณ์ที่สร้างความเสียหายอย่างสิ้นเชิงกับระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสื่อสาร ภายใต้การดูแลของสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร การไฟฟ้านครหลวง โดยรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร กำหนดเหตุการณ์ที่เกิดขึ้นและจัดเป็นภัยพิบัติ ซึ่งจำเป็นต้องปฏิบัติตามแผน ชนิดของภัยพิบัติที่อาจเกิดขึ้นและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสื่อสาร ภายใต้การดูแลของสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร การไฟฟ้านครหลวง โดยเรียงลำดับตามความเป็นไปได้ที่จะเกิดจากมากไปหาน้อย ดังนี้

๑) การโจมตีของผู้บุกรุกคอมพิวเตอร์ ซึ่งมีผลทำให้ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสาร เกิดความเสียหายอย่างสิ้นเชิงทั้งหมด

๒) การเชื่อมโยงเครือข่ายล้มเหลว ซึ่งมีผลทำให้ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสาร ล้มเหลวอย่างสิ้นเชิงทั้งหมด

๓) อุปกรณ์จัดเก็บข้อมูลเสียหายอย่างสิ้นเชิงทั้งหมด และไม่สามารถกู้คืนได้

๔) เกิดอัคคีภัยที่ทำให้สร้างความเสียหายแก่ห้องควบคุมระบบ หรือระบบอื่น ที่กระทบต่อการให้บริการ

๕) โจรกรรมซึ่งเป็นเหตุการณ์ที่ทำให้ระบบไม่สามารถให้บริการได้เป็นจำนวนมาก

๖) การเกิดอุทกภัย หรือเกิดน้ำขัง อันเนื่องมาจากธรรมชาติหรือไม่ใช่เกิดจากธรรมชาติ เช่น ท่อส่งน้ำรั่วจนเป็นเหตุทำให้ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสาร เสียหายเป็นจำนวนมาก

๗) การเกิดแผ่นดินไหว จนเป็นเหตุทำให้เกิดความเสียหายจำนวนมากต่อระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสาร

๘) วาตภัยภัยที่เกิดขึ้นจากลม จนเป็นเหตุทำให้เกิดความเสียหายจำนวนมากต่อระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสาร

๒.๑.๒ การเตรียมแผนอุปกรณ์และเครื่องมือ

สายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร การไฟฟ้านครหลวง จัดให้มีการปฏิบัติการรับมือภัยพิบัติ โดยจัดตั้งศูนย์สำรองในกรณีเกิดภัยพิบัติขึ้นที่ศูนย์สำรองข้อมูลและจัดเตรียมกล่องฉุกเฉิน (Lock Box) จำนวน ๒ กล่อง จัดเก็บอยู่ที่ศูนย์สำรองข้อมูล ภายในกล่องฉุกเฉิน ประกอบด้วย

๑) รหัสผ่านสำหรับเข้าสู่ระบบคอมพิวเตอร์ที่มีสิทธิ์เท่าผู้ดูแลระบบ

๒) แผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติ

๓) ข้อมูลเกี่ยวกับการปรับตั้งค่าอุปกรณ์

๔) ซอฟต์แวร์ที่มีความสำคัญสูง

ผู้ที่สามารถเปิดกล่องฉุกเฉินได้ มีจำนวน ๕ คน คือ

๑) รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร

๒) ผู้ช่วยผู้ว่าการสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร

๓) ผู้อำนวยการฝ่ายระบบโครงสร้างพื้นฐาน

๔) ผู้อำนวยการฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

๕) ผู้อำนวยการฝ่ายพัฒนาระบบงานเทคโนโลยีดิจิทัล

๒.๑.๓ การสำรองข้อมูล

ผู้ดูแลระบบ มีหน้าที่สำรองข้อมูลเพื่อให้สามารถนำมาใช้ในการกู้คืนและติดตั้งระบบในกรณีที่เกิดภัยพิบัติ ทั้งนี้ให้ปฏิบัติตามนโยบายการสำรองข้อมูลและการกู้คืนระบบ ให้มีการสำรองข้อมูลที่มีความสำคัญสูงต่อการให้บริการการไฟฟ้านครหลวงไว้ที่ศูนย์คอมพิวเตอร์สำรองของการไฟฟ้านครหลวง เพื่อให้สามารถกู้คืนระบบได้อย่างรวดเร็ว สำหรับข้อมูลที่มีความสำคัญอื่น ๆ เช่น การติดตั้งระบบของอุปกรณ์เครือข่าย ซอฟต์แวร์ที่มีความสำคัญ ให้เก็บไว้ในกล่องฉุกเฉิน

๒.๒ การรับมือเร่งด่วนขณะเกิดภัยพิบัติ

๒.๒.๑ การรายงานเหตุการณ์

ผู้ที่ทราบเหตุการณ์ภัยพิบัติ มีหน้าที่รายงานเหตุการณ์การเกิดภัยพิบัติให้กับผู้ใดผู้หนึ่งตามข้อมูล ดังต่อไปนี้

ลำดับที่	ตำแหน่ง
๑.	รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร
๒.	ประธานอำนวยการประสานงานเหตุฉุกเฉิน
๓.	หัวหน้าหน่วยงาน ในสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร

๒.๒.๒ โครงสร้างและหน้าที่รับผิดชอบของผู้ปฏิบัติงาน

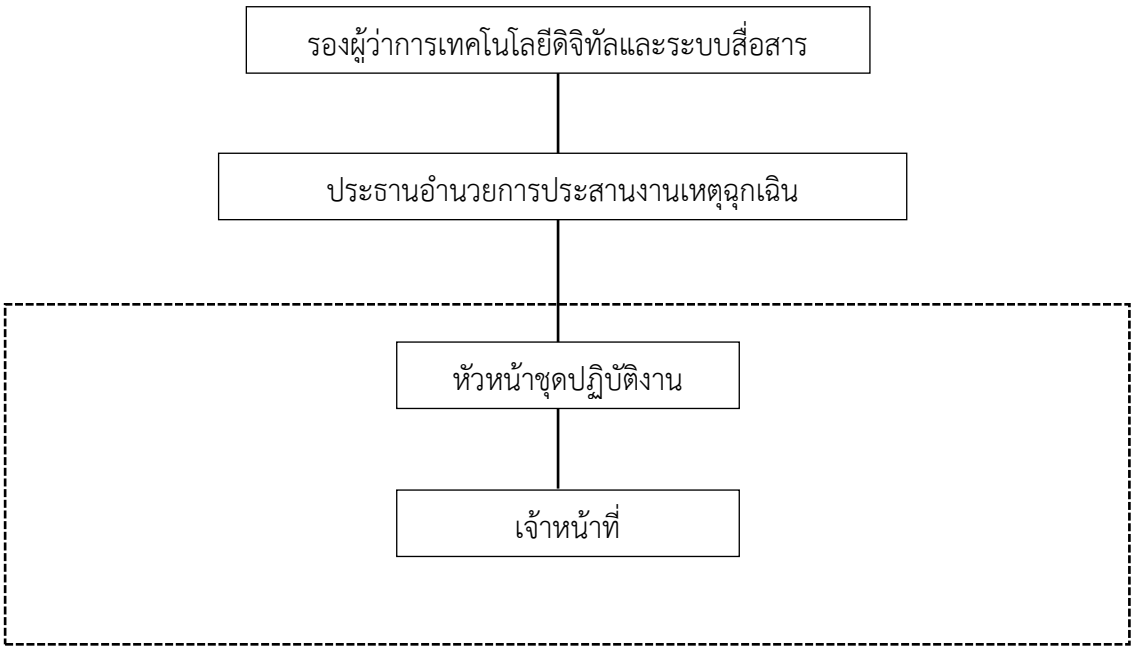
โครงสร้างสายงานการสั่งการของผู้ปฏิบัติงานกรณีเกิดภัยพิบัติแสดงได้ดังรูปที่ ๑ แต่ละตำแหน่งงาน มีรายละเอียดดังนี้

๑) รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร มีหน้าที่ติดตามผลการปฏิบัติงานขั้นสุดท้ายและตัดสินใจแก้ไขปัญหาที่ได้รับรายงานจากประธานอำนวยการประสานงานเหตุฉุกเฉิน

๒) ประธานอำนวยการประสานงานเหตุฉุกเฉิน ผู้ที่ได้รับการแต่งตั้งโดยรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร มีหน้าที่ประมวลผลการปฏิบัติงานในภาพรวม ให้เป็นไปอย่างถูกต้องสมบูรณ์

๓) หัวหน้าชุดปฏิบัติงาน ได้แก่ หัวหน้าส่วนที่ได้รับมอบหมาย มีหน้าที่วางแผนแบ่งหน้าที่รับผิดชอบให้แก่พนักงาน ควบคุมให้การปฏิบัติงานเป็นไปตามแผน และรายงานผลต่อประธานอำนวยการประสานงานเหตุฉุกเฉิน รวมทั้งทำหน้าที่ติดต่อประสานงานกับบุคคล หรือหน่วยงานอื่นทั้งภายนอกและภายในการไฟฟ้านครหลวง

๔) เจ้าหน้าที่ มีหน้าที่ในการปฏิบัติตามแผน รับผิดชอบงานตามที่ได้จัดแบ่งและรายงานผลปฏิบัติต่อหัวหน้าส่วนต่างๆ ที่ได้รับมอบหมาย



๒.๒.๓ ขั้นตอนการปฏิบัติงาน

๑) รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร สั่งการให้มีการปฏิบัติงาน เพื่อรับมือเร่งด่วนขณะเกิดภัยพิบัติ หากรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารไม่สามารถปฏิบัติงานได้ ให้ประธานอำนวยการประสานงานเหตุฉุกเฉินปฏิบัติงานแทน โดยสั่งการให้ผู้มีสิทธิ์ในการเปิดกล่องฉุกเฉิน หากไม่สามารถใช้กุญแจได้ ให้ทำลายกุญแจและเปิดโดยวิธีการใดก็ได้ และดำเนินการตามขั้นตอนการปฏิบัติงานที่เก็บในกล่อง

๒) ประธานอำนวยการประสานงานเหตุฉุกเฉิน สำรวจสถานะของพนักงานการไฟฟ้านครหลวง หรือผู้ที่อยู่ในเหตุการณ์ขณะเกิดภัยพิบัติ หากมีการบาดเจ็บ ให้โทรศัพท์แจ้งโรงพยาบาล สถานีตำรวจ หรือหน่วยกู้ภัย

๓) ประธานอำนวยการประสานงานเหตุฉุกเฉิน สำรวจจำนวนพนักงานในสายงานเทคโนโลยีดิจิทัลและระบบสื่อสาร หรือผู้ที่อยู่ในเหตุการณ์ขณะเกิดภัยพิบัติ เพื่อประชุมเร่งด่วน ชี้แจงหน้าที่ และการดำเนินการรับมือภัยพิบัติ หากพนักงานไม่ได้อยู่ในเหตุการณ์ให้โทรศัพท์ เพื่อเรียกตัวปฏิบัติงานโดยเร่งด่วนทั้งในและนอกเวลาทำการ โดยประกอบด้วย ชุดปฏิบัติงาน จำนวน ๔ ชุด ซึ่งแต่ละชุดจะมีหัวหน้าชุดปฏิบัติงานและพนักงานดังนี้

(๑) ชุดประสานงานเหตุการณ์ : มีหน้าที่ประสานงานการติดต่อทางโทรศัพท์ การช่วยเหลือผู้บาดเจ็บ การอำนวยความสะดวกด้านสถานที่ และการรับแจ้งข้อมูลข่าวสารกับผู้ใช้งานหรือผู้ที่เกี่ยวข้อง

(๒) ชุดงานการบริหาร : มีหน้าที่เก็บรวบรวมข้อมูลอุปกรณ์ด้านการบริหารงานทั่วไป และข้อมูลของหน่วยงาน โดยมีผู้ปฏิบัติงาน

(๓) ชุดโครงข่ายพื้นฐานและการสื่อสาร : มีหน้าที่จัดเตรียมเครื่องมืออุปกรณ์ และดำเนินการด้านเครือข่ายคอมพิวเตอร์ การสื่อสารต่าง ๆ ระบบไฟฟ้า และสายสัญญาณ

(๔) ชุดระบบคอมพิวเตอร์และระบบงานสารสนเทศ : มีหน้าที่จัดเตรียม เครื่องมืออุปกรณ์เพื่อดำเนินการด้านระบบคอมพิวเตอร์และระบบงานสารสนเทศ

๔) ประธานอำนวยการประสานงานเหตุฉุกเฉินสั่งการให้มีการตรวจสอบความเสียหายเบื้องต้น โดยชุดปฏิบัติงานแต่ละชุด ประเมินความจำเป็นต้องดำเนินการกู้ฟื้นภัยพิบัติทันทีหรือไม่ และดำเนินการโดยใช้สถานที่ใด หากมีความจำเป็นให้กำหนดฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล เป็นศูนย์ประสานงาน โดยให้ชุดประสานงานเหตุการณ์ดำเนินการเรื่องสถานที่จัดหาอุปกรณ์ เครื่องมือ และทำหน้าที่ประสานงานหลักในศูนย์ประสานงาน นอกจากนี้ ภายในศูนย์ประสานงาน ต้องประกอบด้วยเครื่องมือต่าง ๆ ดังนี้

ลำดับที่	อุปกรณ์หรือเครื่องมือ
๑.	โต๊ะและเก้าอี้
๒.	โทรศัพท์ทั่วไป
๓.	โทรศัพท์เคลื่อนที่
๔.	เครื่องคอมพิวเตอร์ส่วนบุคคล
๕.	เครื่องพิมพ์
๖.	เครื่องโทรสาร
๗.	เครื่องถ่ายเอกสาร
๘.	อุปกรณ์อื่น ๆ

๕) หัวหน้าชุดปฏิบัติงาน มอบหมายให้พนักงานเก็บรวบรวมอุปกรณ์หรือข้อมูลต่าง ๆ ที่มีความจำเป็นต่อการกู้ฟื้นภัยพิบัติตามรายละเอียด ดังนี้

ชุดงานการบริหาร

ลำดับที่	อุปกรณ์หรือสิ่งที่เก็บรวบรวม	ใช้งานในด้าน
๑.	ข้อมูลการเงินและบัญชี	การเงินและบัญชี
๒.	ข้อมูลพัสดุครุภัณฑ์	ครุภัณฑ์และจัดซื้อ
๓.	ข้อมูลพนักงาน	ข้อมูลส่วนบุคคล
๔.	ข้อมูลสารบรรณ	เอกสารหน่วยงาน

ชุดโครงข่ายพื้นฐานและการสื่อสาร

ลำดับที่	อุปกรณ์หรือสิ่งที่เก็บรวบรวม	ใช้งานในด้าน
๑.	อุปกรณ์และข้อมูล Router	เชื่อมต่อเครือข่าย
๒.	อุปกรณ์และข้อมูล Switch	เชื่อมต่อเครือข่าย
๓.	สายสัญญาณ LAN	เชื่อมต่อเครือข่าย

ชุดระบบคอมพิวเตอร์และระบบงานสารสนเทศ

ลำดับที่	อุปกรณ์หรือสิ่งที่เก็บรวบรวม	ใช้งานในด้าน
๑.	เซิร์ฟเวอร์ฐานข้อมูล	ให้บริการฐานข้อมูล
๒.	เซิร์ฟเวอร์ให้บริการหลัก	ให้บริการหลัก
๓.	แผ่นซีดีระบบปฏิบัติการ	ติดตั้งระบบ
๔.	แผ่นซีดีซอฟต์แวร์	ติดตั้งระบบ

๖) หัวหน้าชุดปฏิบัติงาน เรียกประชุมพนักงานในชุด เพื่อวิเคราะห์ความเสียหาย และกำหนดแผนปฏิบัติการกู้คืนระบบในแต่ละชุด แต่เนื่องจากการทำงานบางส่วนต้องมีความเกี่ยวพันกันจึงให้ประชุมร่วมกันทุกชุด เพื่อสร้างแผนปฏิบัติงานรวม และเสนอประธานอำนวยการประสานงานเหตุฉุกเฉิน ภายใน ๑ ชั่วโมงหลังจากระบบเกิดความเสียหาย และให้ใช้แผนปฏิบัติงานรวมเป็นแผนหลักในการดำเนินการ โดยต้องประกอบด้วยหลักเกณฑ์ต่าง ๆ ดังนี้

(๑) เก็บรวบรวมแหล่งเก็บข้อมูลสำรองทั้งหมดหรือที่มีความสำคัญ

(๒) ติดตั้งฮาร์ดแวร์/ซอฟต์แวร์สำหรับการใช้งานระบบ

(๓) ใช้ข้อมูลสำรอง เพื่อกู้ระบบหากไม่สามารถทำได้อาจต้องติดตั้งซอฟต์แวร์ระบบใหม่หลังจากนั้นจึงปรับแก้ค่าติดตั้ง

(๔) แก้ไขและปรับค่าข้อมูลของระบบงานต่าง ๆ ที่ทำงานบนระบบ

(๕) เปิดระบบและทดสอบ

(๖) เปิดระบบเพื่อทดสอบการทำงานพื้นฐาน

(๗) ให้ระบบทำงานให้เป็นปัจจุบันและเริ่มการทำงานอย่างสมบูรณ์

(๘) ให้ระบบทำงานเพื่อกลับสู่สถานะเดิมก่อนเกิดความเสียหาย หลังจากนั้นจึงเปิดให้ใช้งานได้อย่างสมบูรณ์

(๙) เฝ้าระวังระบบ

๒.๒.๔ การจัดเก็บและป้องกันทรัพย์สิน

ประธานอำนวยการประสานงานเหตุฉุกเฉิน กำหนดให้มีการจัดเก็บและป้องกันทรัพย์สินหลังจากเกิดภัยพิบัติแล้ว โดยป้องกันมิให้เกิดความเสียหายและสามารถนำมาใช้ เพื่อกู้คืนระบบได้ ทรัพย์สินแต่ละชนิดอาจมีการป้องกันด้วยวิธีต่างกัน ทั้งนี้ หากมีความจำเป็นให้นำทรัพย์สินต่าง ๆ จัดเก็บไว้ที่ศูนย์สำรองข้อมูลในกรณีเกิดภัยพิบัติ โดยศูนย์ดังกล่าวต้องมีพนักงานรักษาความปลอดภัยดูแลตลอด ๒๔ ชั่วโมง ทรัพย์สินต่าง ๆ ที่จัดเก็บมีดังนี้

๑) อุปกรณ์คอมพิวเตอร์หรือเครือข่ายที่มีความสำคัญ ให้เก็บรวบรวมไว้ในห้องที่มิดชิดและมีกุญแจปิดเพื่อป้องกันการเข้าออก และให้ผู้มีสิทธิ์ถือกุญแจกล่องฉุกเฉิน

๒) ห้องเก็บทรัพย์สินต้องหลีกเลี่ยงจากน้ำสารเคมีและวัตถุไวไฟทั้งหมด

๓) อุปกรณ์เก็บข้อมูลต้องจัดเก็บในตู้ที่มีกุญแจป้องกันการเปิดทุกครั้ง

๔) เอกสารที่มีความสำคัญต้องจัดเก็บแยกจากอุปกรณ์อื่น ๆ หากเป็นไปได้

๕) ให้เก็บในตู้ที่มีกุญแจป้องกันการเปิดทุกครั้ง

๒.๒.๕ การประเมินความเสียหาย

ประธานอำนวยการประสานงานเหตุฉุกเฉิน กำหนดให้หัวหน้าชุดปฏิบัติงานทุกชุด มีหน้าที่ต้องจัดทำรายงานประเมินความเสียหายจากการเกิดภัยพิบัติ โดยเสนอต่อรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร ในระหว่างการปฏิบัติงาน หรือหากไม่สามารถดำเนินการได้ให้เสนอรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารหลังจากการกู้ฟื้นระบบเสร็จสิ้นสมบูรณ์

๒.๒.๖ การจัดหาระบบทดแทนเร่งด่วน

ประธานอำนวยการประสานงานเหตุฉุกเฉิน กำหนดให้หัวหน้าชุดงานการบริหารประสานงานกับหัวหน้าชุดอื่น ๆ เพื่อจัดซื้อจัดหาระบบทดแทนเร่งด่วนหรือเร่งการจัดซื้อจัดหาระบบอย่างเร่งด่วนในกรณีที่มีความจำเป็นต่อการปฏิบัติงานกู้ฟื้นภัยพิบัติหรือการให้บริการที่มีความสำคัญ ทั้งนี้ให้อยู่ในดุลพินิจของรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร

๒.๓ การฟื้นฟูระบบหลังจากเกิดภัยพิบัติ

รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร สั่งการให้หัวหน้าหน่วยงานมีหน้าที่รับผิดชอบในการดำเนินการฟื้นฟูระบบอย่างสมบูรณ์หลังจากการรับมือเร่งด่วน โดยกำหนดขั้นตอนงบประมาณที่ใช้ และระยะเวลาในการฟื้นฟูระบบอย่างสมบูรณ์ในด้านต่าง ๆ

๒.๔ การทดสอบ/ประเมิน และการปรับปรุงแผน

คณะทำงานกรรมการด้านความปลอดภัยสารสนเทศการไฟฟ้านครหลวง มีหน้าที่ในการทดสอบ/ประเมิน และปรับปรุงแผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติเป็นประจำทุกปี ตามแผนบริหารความต่อเนื่องทางธุรกิจของการไฟฟ้านครหลวง (Business Continous Management : BCM) หากมีข้อมูลที่เปลี่ยนแปลงไปหลังจากที่มีการแก้ไขแล้ว ให้บันทึกการแก้ไขทุกครั้งในตารางบันทึกการปรับปรุงแผนและระบบให้รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารทราบ

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อแนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ พร้อมทั้งเป็นแนวปฏิบัติตามข้อบังคับขององค์กร โดยส่วนประกอบของแผนฯ มีรายละเอียดดังต่อไปนี้

ผู้รับผิดชอบ

๑) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)

๒) ฝ่ายตรวจสอบภายใน (ฝตส.)

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้ปฏิบัติอย่างน้อย ดังนี้

๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒) ตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในขององค์กร (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓) จัดทำแนวทางในการประเมินความเสี่ยง ที่ต้องคำนึงถึงอย่างน้อย ดังนี้

(๑) ระบุความเสี่ยง สาเหตุของความเสี่ยง และผลกระทบที่เกิดขึ้นจากความเสี่ยง

(๒) จัดลำดับความสำคัญของความเสี่ยง

(๓) จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

(๔) ให้จัดทำรายงานผลของมาตรการในการควบคุมความเสี่ยงประจำปี

(๕) หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยง เพื่อไม่ให้เกิดขึ้นซ้ำอีก เป็นการดำเนินการต่อเนื่องว่าแผนบริหารความเสี่ยง มีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนและพัฒนาระบบให้ดียิ่งขึ้น

(๖) การทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๔) มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ต้องกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบ ด้วยสิทธิ์ที่สามารถอ่านได้เท่านั้น (Read Only)

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องนำไปจัดเก็บรักษา

(๓) ต้องกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๔) ต้องกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึง

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจสอบประเมินระบบสารสนเทศ ต้องกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องดังกล่าว จากการเข้าถึงโดยไม่ได้รับอนุญาต

๕) จัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยงพร้อมข้อเสนอแนะ

๖) รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต่อรองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสาร อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔

นโยบายโครงสร้างความมั่นคงปลอดภัยและการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อจัดโครงสร้างของหน่วยงานภายในที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม และกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการกำกับดูแลกิจกรรมต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ และเพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้ใช้งานและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)

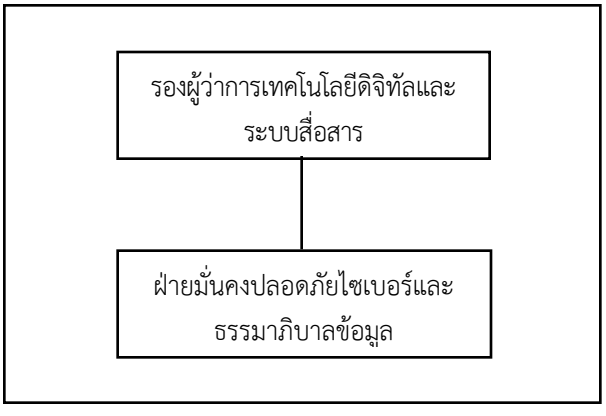
อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้ระบบเทคโนโลยีดิจิทัลและการสื่อสารขององค์กร มีความมั่นคงปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพ และน่าเชื่อถือ การไฟฟ้านครหลวงได้จัดตั้งฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล โดยมีบทบาทหน้าที่ ดังนี้



๑) ต้องรับผิดชอบในการวางแผนแม่บทความมั่นคงปลอดภัยสารสนเทศ

๒) กำหนดนโยบายและวิธีการตรวจสอบ (Audit)

๓) จัดทำแผนและมาตรฐานบริหารความปลอดภัยของระบบบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและติดตามประเมินผลการดำเนินงานตามแผน

๔) ประเมินความเสี่ยงของระบบงานและเทคโนโลยีที่นำมาใช้

๕) กำหนดนโยบายธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ เผยแพร่ให้คำแนะนำวิชาการด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

๖) ให้คำปรึกษา คำแนะนำ ในการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

๗) กำหนดนโยบายและแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และให้มีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

๒. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) ต้องมีการฝึกอบรมการใช้งานระบบสารสนเทศขององค์กร อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒) จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ให้รับทราบภายในองค์กร

๓) จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจเสริมเนื้อหา แนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรม ตามแผนการฝึกอบรมขององค์กร

๔) จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับพนักงานทุกภาคส่วน

๕) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

ส่วนที่ ๕

นโยบายการบริหารจัดการทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นโดยมีวัตถุประสงค์ เพื่อให้การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของการไฟฟ้านครหลวง เป็นไปอย่างมีระเบียบและถูกต้องทั้งในด้านจริยธรรมจรรยาบรรณ และด้านกฎหมาย รวมทั้งให้ผู้ใช้งานและบุคคลภายนอกที่เกี่ยวข้อง ใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพ โดยครอบคลุมหัวข้อ ดังต่อไปนี้

ผู้รับผิดชอบ

๑) ฝ่ายระบบโครงสร้างพื้นฐาน (ฝคฐ.)

๒) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การบริหารจัดการทรัพย์สิน

๑) ผู้ใช้งาน ต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ขององค์กร ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๒) ผู้ใช้งาน ต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๓) ผู้ใช้งาน ต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมต่อเข้าระบบเครือข่าย

๔) ผู้ใช้งาน ต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

๕) ผู้ใช้งาน ต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูล ที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

๖) ผู้ใช้งาน มีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่องค์กร มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งาน การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้ง โดยพนักงานที่องค์กรมอบหมาย

๗) ผู้ใช้งาน มีหน้าที่ต้องชดใช้ค่าเสียหาย หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน ไม่ว่าทรัพย์สินนั้น ชำรุดหรือสูญหาย ตามระเบียบขององค์กร

๘) ผู้ใช้งาน ต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือคอมพิวเตอร์ประเภทพกพา ไม่ว่าในกรณีใดๆ

๙) ผู้ใช้งาน ต้องไม่นำทรัพย์สินและระบบสารสนเทศต่างๆ ที่องค์กรจัดเตรียมไว้ให้ใช้งานไปใช้ในกิจกรรมที่องค์กรไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์กร

๑๐) ผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายใดๆ ที่เกิดขึ้นจากการละเมิดตามข้อ ๙ และให้ถือเป็นความผิดส่วนบุคคล

๒. การบริหารจัดการข้อมูลองค์กร

๑) ผู้ใช้งาน ต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นเป็นขององค์กร หรือบุคคลภายนอก

๒) ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินขององค์กร ถือเป็นทรัพย์สินขององค์กร ไม่ควรเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๓) ผู้ใช้งาน มีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลขององค์กร หรือข้อมูลของผู้ใช้งาน หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๔) ผู้ใช้งาน ต้องป้องกันดูแลรักษาไว้ ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๕) ผู้ใช้งาน มีสิทธิ์โดยชอบธรรมที่เก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามที่เห็นสมควร องค์กรให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่องค์กรต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรอาจแต่งตั้งให้มีบุคคลที่ทำหน้าที่ตรวจสอบสามารถตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๓. การบริหารจัดการระบบสารสนเทศ

๑) ผู้ใช้งาน มีสิทธิ์พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ก็ได้ ยกเว้นกรณีดังต่อไปนี้ ไม่ให้ดำเนินการ

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายกลไกการรักษาความปลอดภัยระบบสารสนเทศ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบ

(๒) ทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๓) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๔) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๕) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๖) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒) ต้องไม่เปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit Torrent) อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๓) ต้องไม่เปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น ดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

๔) ต้องไม่ใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดขององค์กรที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

๕) ต้องไม่ใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดขององค์กร เพื่อการรบกวนก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร

๖) ต้องไม่ใช้ทรัพยากรทุกประเภทที่เป็นขององค์กร เพื่อประโยชน์ทางการค้า

๗) ต้องไม่กระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

๘) ต้องไม่กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศขององค์กร ต้องหยุดชะงัก

๙) ต้องไม่ใช้ระบบสารสนเทศขององค์กร เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๐) ต้องไม่กระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งาน หรือรับรู้รหัสส่วนบุคคล ของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๑) ต้องไม่ติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อให้เข้าถึงระบบสารสนเทศขององค์กร โดยไม่ได้รับอนุญาตจากฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล

๔. การปฏิบัติตามข้อบังคับ

๔.๑ การปฏิบัติตามกฎหมายและข้อบังคับ

๑) บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบขององค์กรที่กำหนด หรือออกกฎระเบียบโดยอาศัยนโยบายดังกล่าวข้างต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔.๒ ซอฟต์แวร์และลิขสิทธิ์

๑) ซอฟต์แวร์ (Software) ที่องค์กร อนุญาตให้ใช้งาน หรือที่องค์กรมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และผู้ใช้งานต้องไม่ติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์องค์กร ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

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

๔.๓ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

เพื่อปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ และให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติอย่างน้อย ดังต่อไปนี้

๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูล ที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง เป็นระยะเวลาอย่างน้อย ๙๐ วัน ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องมีการกำหนดชั้นความลับในการเข้าถึง

๒) ห้ามผู้ดูแลระบบ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือบุคคลที่องค์กรมอบหมายเท่านั้น

๓) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลในสื่อเก็บข้อมูลดังกล่าว และจำกัดสิทธิ์การเข้าถึงข้อมูลเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๖
นโยบายการป้องกันภัยคุกคามเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นโดยมีวัตถุประสงค์ เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของการไฟฟ้านครหลวง และอาจสร้างความเสียหายและส่งผลกระทบต่อการใช้งานและการให้บริการของระบบสารสนเทศและต่อภาพลักษณ์ของการไฟฟ้านครหลวง โดยครอบคลุมหัวข้อ ดังต่อไปนี้

ผู้รับผิดชอบ

๑) ฝ่ายมั่นคงปลอดภัยไซเบอร์และธรรมาภิบาลข้อมูล (ฝมธ.)

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) เครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่องค์กร ได้จัดหาหรือได้ประกาศให้ใช้ เว้นแต่เครื่องคอมพิวเตอร์นั้น เป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

๒) ผู้ใช้งานที่ได้รับข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด จากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๓) ผู้ใช้งานต้องปรับปรุงข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๔) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา หากพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๕) ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ที่ติดไวรัสเข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

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

๗) ผู้ใช้งานไม่เผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สินขององค์กร

๒. การป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) องค์กรต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุกเอาไว้ในตำแหน่งที่มีการเชื่อมต่อกับภายนอกทุกจุด หรืออย่างน้อยต้องติดตั้งเอาไว้ในจุดที่ให้มีการให้บริการไปสู่ภายนอกองค์กร เช่น เครื่องคอมพิวเตอร์แม่ข่าย

๒) ในการติดตั้งระบบตรวจจับและป้องกันการบุกรุก ให้ติดตั้งไว้ที่ตำแหน่งหลังไฟร์วอลล์ และที่ด้านหน้าของกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server Farm)

๓) ต้องมีการปรับแต่ง (Tuning) การทำงานของระบบตรวจจับและป้องกันการบุกรุก โดยพนักงานขององค์กรที่ได้รับการอบรมหรือผู้เชี่ยวชาญ โดยให้ปรับแต่งให้ป้องกันได้มากที่สุด และเกิดการตรวจจับที่ผิดพลาด (False Positive) น้อยที่สุด ทุกครั้งที่มีการปรับแต่งต้องบันทึกข้อมูลทุกครั้ง

๔) ต้องมีการตั้งระบบตรวจจับและป้องกันการบุกรุก ให้สามารถ Update Signature ได้โดยอัตโนมัติ หรือผู้ดูแลระบบเครือข่ายต้อง Update Signature ทุกสัปดาห์

๕) หากมีการเพิ่มเติมหรือเปลี่ยนแปลงเส้นทางการสื่อสารคอมพิวเตอร์ ต้องได้รับการอนุญาตจากผู้ดูแลระบบเครือข่ายก่อน และต้องมีการตรวจสอบผลกระทบกับระบบตรวจจับและป้องกันการบุกรุก

๖) ต้องตรวจสอบการทำงานของระบบตรวจจับและป้องกันการบุกรุกและตรวจสอบ Log พร้อมทดสอบการทำงานทุกเดือน

๗) การเปลี่ยนแปลงใดๆ ที่เกี่ยวกับระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการบันทึก และรายงานให้รองผู้ว่าการเทคโนโลยีดิจิทัลและระบบสื่อสารทราบ

๘) อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุก ต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ และให้ติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อก โดยอนุญาตให้ผู้ดูแลระบบเครือข่ายเท่านั้น ที่สามารถเข้าถึงได้

๓. การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑) ผู้ใช้งาน แจ้งไปยังผู้ดูแลระบบ/ผู้เกี่ยวข้อง โดยทันที เมื่อพบเห็นเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

๒) ผู้ใช้งาน และผู้เกี่ยวข้องจากภายนอกทั้งหมด หากพบจุดอ่อนช่องโหว่ในระบบสารสนเทศ จะต้องไม่เปิดเผย เผยแพร่ สนทนาหรือกระทำการใดๆ อันเป็นการเผยแพร่ต่อผู้อื่น โดยให้ทำการแจ้งกับผู้ดูแลระบบ โดยด่วนที่สุด

๓) ต้องกำหนดคณะทำงานเพื่อทำหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศ ในการแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ โดยจะต้องได้รับการกำหนดและมอบหมายสิทธิ์อย่างชัดเจนในการดำเนินการแก้ไขปัญหา

๔) เมื่อผู้ดูแลระบบ/ผู้ที่เกี่ยวข้องได้รับแจ้งเหตุการณ์ คณะทำงานจะต้องดำเนินการวิเคราะห์ความรุนแรงและผลกระทบของเหตุการณ์นั้นๆ และร่วมกันหาวิธีการแก้ไข โดยมีขั้นตอนประกอบด้วย

(๑) การตรวจสอบหาสาเหตุของปัญหา

(๒) แผนงานในการลดผลกระทบ

(๓) ขั้นตอนในการแก้ไข

(๔) สื่อสารกับผู้ใช้งานที่เกี่ยวข้อง

(๕) ทำเอกสารบันทึกการดำเนินการดังกล่าว

๕) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศ โดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อการรักษาความถูกต้องทางด้านหลักฐาน และดำเนินการทางกฎหมาย ในกรณีที่จำเป็น ผู้บริหารที่ได้รับมอบหมายเท่านั้น ที่จะเป็นตัวแทนขององค์กร โดยความร่วมมือกับหน่วยงานด้านกฎหมายในการใช้ระเบียบปฏิบัติที่เกี่ยวกับการก่ออาชญากรรมในการดำเนินคดีต่อผู้ประสงค์ร้ายต่อองค์กร