แนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของรัฐสภา

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา
ระยะ 4 ปี (พ.ศ. 2562 – 2565)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

รหัสเอกสาร : STD_PY_02

เวอร์ชั่น : 1.0

วันที่มีผลบังคับใช้ : 30 ก.ย. 2562

ชั้นความลับของเอกสาร: ☐ลับมาก ☐ลับ ☐ปกปิด ☐ไม่ระบุ

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา จัดทำขึ้นให้สอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศของรัฐสภาที่กำหนดไว้ โดยได้มีการกำหนดมาตรฐานแนวปฏิบัติ วิธีปฏิบัติ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ การกำหนดขั้นตอน กระบวนการที่เหมาะสมต่าง ๆ อาทิ ระบบสำรอง การเตรียมความพร้อมกรณีฉุกเฉิน การกำหนดหน้าที่ความรับผิดชอบให้เป็นไปตามหลักมาตรฐานสากล เพื่อสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ได้อย่างเหมาะสมและมีความน่าเชื่อถือ ซึ่งสามารถแบ่งสาระสำคัญออกเป็น 14 ส่วน ประกอบด้วย

ส่วนที่ 1 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security)
ส่วนที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)
ส่วนที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)
ส่วนที่ 4 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)
ส่วนที่ 5 การควบคุมการเข้าถึง (Access Control)
ส่วนที่ 6 การเข้ารหัสข้อมูล (Cryptographic)
ส่วนที่ 7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
ส่วนที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)
ส่วนที่ 9 ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)
ส่วนที่ 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development, and Maintenance)
ส่วนที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)
ส่วนที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
ส่วนที่ 13 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)
ส่วนที่ 14 การปฏิบัติตามข้อกำหนด (Compliance)

นิยามคำศัพท์

สารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

ระบบงาน หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้

ระบบปฏิบัติการ หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ เช่น การจัดสรรหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูลและอุปกรณ์แสดงผล

ระบบเครือข่าย หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของรัฐสภา

ความมั่นคงปลอดภัยของสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) สภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

ความลับ (CONFIDENTIALITY) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั่นที่จะเข้าถึงข้อมูลเหล่านั้นได้

ความถูกต้อง (INTEGRITY) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

สภาพพร้อมใช้งาน (AVAILABILITY) หมายถึง การรับรองว่าข้อมูล หรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

ความเสี่ยง หมายถึง โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการรักษาความปลอดภัย

การเข้ารหัส (ENCRYPTION) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

ช่องโหว่ หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบ ทำให้ประสิทธิภาพของการทำงานลดลง

สินทรัพย์ หมายถึง เครื่องคอมพิวเตอร์ของรัฐสภา เครือข่าย ข้อมูลและระบบสารสนเทศต่าง ๆ ที่รัฐสภาพัฒนาหรือจัดหาเพื่อใช้ในกิจการของรัฐสภา และบุคลากรของรัฐสภา

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) หมายถึง เลขาธิการรัฐสภา

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของหน่วยงานภายในรัฐสภา

ผู้ใช้งาน หมายถึง ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศและสินทรัพย์ต่าง ๆ ของรัฐสภา และได้รับอนุญาตให้เข้าใช้งานสารสนเทศของรัฐสภา

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการ ระบบคอมพิวเตอร์ลูกข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายและระบบ สารสนเทศของรัฐสภา

ผู้พัฒนาระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศของรัฐสภา

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

เจ้าของระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึงระบบงาน เช่น การให้สิทธิ การเพิ่มสิทธิ การลดสิทธิ การยกเลิกสิทธิ รวมทั้งการพัฒนา ปรับปรุงดูแลบำรุงรักษาระบบงาน

บัญชีผู้ใช้งาน หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศ ระบบปฏิบัติการ ระบบเครือข่าย รวมถึงโปรแกรมประยุกต์และสารสนเทศของรัฐสภา

สิทธิของผู้ใช้งาน หมายความว่า สิทธิในการเข้าถึงระบบสารสนเทศ สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับโปรแกรมประยุกต์และสารสนเทศของรัฐสภา

ผู้ให้บริการภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของรัฐสภา โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล และผลกระทบต่อความเสียหายที่อาจเกิดขึ้นจากการปฏิบัติงาน

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ส่วนที่ 1
แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ

1.1 แนวปฏิบัติทิศทางการบริหารจัดการความมั่นคงปลอดภัย (Management Directions for Information Security) เพื่อใช้เป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยสารสนเทศของรัฐสภาซึ่งจัดทำเป็นลายลักษณ์อักษรโดยผู้มีอำนาจเป็นผู้ลงนามอนุมัติและเผยแพร่ให้สมาชิกรัฐสภา ข้าราชการ ลูกจ้าง และผู้ที่เกี่ยวข้องกับวงงานรัฐสภาทุกคนได้รับทราบ

1.1.1 แนวปฏิบัติสำหรับความมั่นคงปลอดภัย (Information Security) เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของรัฐสภาทำให้การดำเนินกิจการของรัฐสภามีประสิทธิภาพและประสิทธิผล

(1) เพื่อสร้างความตื่นตัวให้สมาชิกรัฐสภา ข้าราชการ พนักงานและลูกจ้าง ผู้ดูแลระบบและหน่วยงานภายนอกที่ปฏิบัติงานให้กับรัฐสภาตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ

(2) เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัยที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

1.1.2 การสอบทานแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ (Review of the Policies for information Security) เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิ์ผล กำหนดให้มีการตรวจสอบและประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2
โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information security)

2.1 โครงสร้างภายในองค์กร (Internal Organization)

วัตถุประสงค์ เพื่อให้มีการกำหนดสิทธิของผู้ใช้งาน หน้าที่และความรับผิดชอบของบุคคล หน่วยงานที่มีส่วนเกี่ยวข้องในการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของรัฐสภา เพื่อเป็นการปกป้องสินทรัพย์ให้มีความมั่นคงปลอดภัย

2.1.1 บทบาทหน้าที่และความรับผิดชอบความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้ปฏิบัติหน้าที่ SOC Manager มีหน้าที่ความรับผิดชอบดังต่อไปนี้

(1) พิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศของฝ่ายรัฐสภา ถ้าเป็นการฝ่าฝืนระเบียบขั้นรุนแรงหรือกรณีที่ฝ่าฝืนแล้วก่อให้เกิดความเสียหายแก่รัฐสภาหรือต่อบุคคล ให้จัดทำบันทึกรายงานเกี่ยวกับการฝ่าฝืนแนวปฏิบัติดังกล่าวตามที่กำหนดไว้ในแนวปฏิบัติรัฐสภา

(2) ตักเตือนและชี้แจงผู้ละเมิดหรือฝ่าฝืน ในกรณีการละเมิดหรือฝ่าฝืนมีเจตนาไม่ชัดเจนพร้อมทั้งชี้แจงให้เข้าใจถึงข้อปฏิบัติที่ถูกต้องหากมีการกระทำการฝ่าฝืนนั้นอีก ให้พิจารณาเสนอแต่งตั้งคณะกรรมการพิจารณาตามที่กำหนดไว้ในแนวปฏิบัติรัฐสภา

(3) ป้องกันและแก้ไขปัญหาที่เกิดขึ้นทันทีเพื่อให้แน่ใจว่าการละเมิดหรือฝ่าฝืนเหล่านั้นจะไม่ลุกลามเป็นปัญหาใหญ่

(4) วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

(5) สืบสวนเหตุการณ์ต่าง ๆ ที่ไม่เป็นไปตามแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ

(6) สื่อสารให้คำแนะนำและสอดส่องดู เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องตามแนวปฏิบัติ และเอกสารต่าง ๆ ที่เกี่ยวข้องในระบบ ISMS รวมทั้งประสานงานในกรณีที่เกิดเหตุละเมิดความมั่นคงหรือเหตุฉุกเฉินใด ๆ

(7) ปรับปรุงกระบวนการการอนุมัติการใช้งานระบบสารสนเทศที่มีอยู่ให้สอดคล้องกับแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศของรัฐสภา

(8) ต้องพิจารณาให้ผู้ที่เกี่ยวข้องเท่าที่จำเป็น ลงนามในเอกสารสัญญารักษาความลับ (หรือสัญญาไม่เปิดเผยข้อมูล)

เจ้าของระบบ/ผู้ดูแลระบบ มีหน้าที่ความรับผิดชอบดังต่อไปนี้

(1) ปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ที่เจ้าของระบบกำหนดไว้

(2) สามารถยุติการทำงานของระบบสารสนเทศ ซึ่งพบว่าเป็นภัยต่อความมั่นคงปลอดภัยหรือสร้างภาระให้ระบบสารสนเทศของรัฐสภาโดยไม่จำเป็นต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้บังคับบัญชารับทราบ

(3) สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาตจากรัฐสภา โดยไม่ต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้น และทำรายงานให้ผู้บังคับบัญชารับทราบ

(4) แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบ เพื่อบำรุงรักษาปรับปรุงหรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉิน ผู้ดูแลระบบมีสิทธิปิดระบบทันทีและจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้บังคับบัญชารับทราบ

(5) สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และแจ้งให้ผู้บังคับบัญชารับทราบ เพื่อแจ้งไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม

(6) ดูแลให้ระบบสารสนเทศสามารถให้บริการได้สอดคล้องกับข้อกำหนดใน “แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และเอกสารที่เกี่ยวข้อง

(7) จะต้องรับผิดชอบในการปรับปรุงข้อมูลที่เกี่ยวข้องกับการดำเนินงานเมื่อมีการเปลี่ยนแปลงใด ๆ เกิดขึ้น

(8) ติดตาม กำชับการใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้ถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานของผู้ที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล

(9) ต้องติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

(10) ต้องขออนุญาตผู้บังคับบัญชาในกรณีที่มีการประเมิน ตรวจสอบ ทดสอบหาจุดอ่อน ช่องโหว่อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศและทำการแก้ไขอย่างรวดเร็ว

(11) ต้องรายงานผู้บังคับบัญชาในกรณีที่ตรวจพบหรือได้รับรายงานจากผู้ใช้งานหรือสงสัยว่าระบบ สารสนเทศที่รับผิดชอบโดยตรงหรือระบบที่เกี่ยวข้องอื่นใดของรัฐสภาถูกละเมิดทางด้านความมั่นคงปลอดภัย

(12) การเพิ่มหรือลดสิทธิในการเข้าถึงระบบใด ๆ ให้ปฏิบัติตามเอกสารกระบวนการที่เจ้าของระบบกำหนดอย่างเคร่งครัด พร้อมทั้งทบทวนความเหมาะสมของมาตรการที่นำมาใช้ในระบบอย่างสม่ำเสมอ

(13) ต้องสมัครเป็นสมาชิกเพื่อรับข่าวสารแจ้งเตือนเกี่ยวกับช่องโหว่ด้านความมั่นคงปลอดภัย และเข้าร่วมการประชุมหรือสัมมนาที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

เจ้าของข้อมูล มีสิทธิหน้าที่ความรับผิดชอบ ดังต่อไปนี้

(1) อนุมัติและตรวจทานเพื่อให้มั่นใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม

(2) กำหนดระดับชั้นความปลอดภัยให้กับข้อมูล

(3) ตรวจทานระดับชั้นความปลอดภัยของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงาน และมีความเหมาะสมและสอดคล้องกับระดับความปลอดภัยนั้น ๆ

(4) ตรวจสอบให้มั่นใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม

(5) กำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน

ผู้ใช้งาน มีสิทธิหน้าที่ความรับผิดชอบ ดังต่อไปนี้

(1) สามารถเข้าถึงข้อมูล ข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับของรัฐสภา ยกเว้น ในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรตามที่กำหนดไว้ในเอกสารระเบียบการปฏิบัติงาน เรื่อง การจัดระดับชั้นความลับข้อมูลและสารสนเทศ

(2) ต้องช่วยกันรักษาอุปกรณ์ต่าง ๆ ไม่ให้เกิดความเสียหายหากมีความเสียหายจากอุบัติเหตุหรือภัยต่าง ๆ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบ และผู้บังคับบัญชารับทราบทันที

(3) พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือกระจายส่งต่อไปรษณีย์อิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ ฯลฯ

(4) ต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)

(5) ต้องรับผิดชอบในการเลือกรหัสผ่าน (Password) ที่ปลอดภัยตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

(6) ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย ฯลฯ

(7) ต้องแจ้งต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันทีในกรณีตรวจพบ หรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต หรือใช้งานในทางมิชอบและพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

(8) ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

(9) ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

(10) ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิและไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น

(11) ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของรัฐสภาเพื่อทำธุรกิจส่วนตัว

(12) ต้องคืนสินทรัพย์ของรัฐสภาอันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ เช่น อุปกรณ์ระบบ สารสนเทศข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า - ออก ฯลฯ

(13) แจ้งให้ผู้ดูแลระบบและผู้บังคับบัญชาหน่วยงานทราบทันทีในกรณีที่มีการเคลื่อนย้ายถอดถอนอุปกรณ์ระบบสารสนเทศ

(14) แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยให้กับผู้ดูแลระบบทันที ในกรณีที่มีเหตุการณ์บุกรุกหรือเหตุการณ์ผิดปกติในการใช้งาน

(15) ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนการปฏิบัติงาน (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

(16) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์หรืออุปกรณ์ในเครื่องของรัฐสภา เพื่อป้องกันปัญหาด้านลิขสิทธิ์และปัญหาอื่น ๆ ที่จะเกิดขึ้นภายหลังการติดตั้ง เช่น การติดตั้ง Access Point ด้วยตนเองแล้วเกิดการ

เจาะระบบเข้ามาในระบบเครือข่ายของรัฐสภา หรือทำให้เกิดการแพร่กระจายของไวรัสและภัยคุกคามอื่น ๆ เป็นต้น

(17) หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่ามีผู้ใดกระทำการที่น่าสงสัย ให้แจ้งต่อผู้ดูแลระบบโดยทันที

(18) ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมาย ให้ทำการสืบสวนสอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของรัฐสภา

(19) ปกป้องข้อมูลและปฏิบัติตามข้อกำหนดในแนวปฏิบัติมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง

(20) รับผิดชอบการดำเนินการใด ๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลสารสนเทศ (Accountability)

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงาน (Segregation of dues) เพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต หรือการใช้งานผิดวัตถุประสงค

2.1.3 การติดต่อกับหน่วยงานที่เกี่ยวข้อง (Contact with authorities/ Contact with special interest groups)

(1) มีการจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เพื่อใช้ติดต่อในกรณีฉุกเฉิน หรือเกิดเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัย เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ ศูนย์ประสานงานความมั่นคงปลอดภัยด้านสารสนเทศคอมพิวเตอร์ประเทศไทย (ThaiCERT) กระทรวง หน่วยงานรัฐวิสาหกิจ สถานีตำรวจ สถานีดับเพลิง ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต เป็นต้น

(2) ควรสมัครเป็นสมาชิกเครือข่ายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ เพื่อพัฒนาความรู้ รวมถึงเพื่อการแลกเปลี่ยนข้อมูลด้านความปลอดภัยระหว่างองค์กร

(3) ต้องมีการทบทวนข้อมูลดังกล่าวให้ถูกต้องและเป็นปัจจุบันเสมอ

2.1.4 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

(1) การบริหารจัดการโครงการต่าง ๆ ต้องพิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

(2) เจ้าของโครงการ ผู้จัดการโครงการ ส่วนงานที่ดูแลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและส่วนงานอื่น ๆ ที่เกี่ยวข้องควรพิจารณาและดำเนินกิจกรรมต่อไปนี้ในแต่ละระยะ (Phrase) ของกระบวนการบริหารโครงการ

(2.1) การเริ่มต้นโครงการ (Initiating) กำหนดให้มีวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยสารสนเทศ (Security Objective) ในวัตถุประสงค์ของโครงการโดยรวม (Project Objective) และรวบรวมความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Requirement) โดยคำนึงถึงความเสี่ยงทางด้านความปลอดภัยความจำเป็นในการใช้งานกำหนดการและค่าใช้จ่าย แล้วนำเสนอให้ผู้ที่เกี่ยวข้องพิจารณาอนุมัติความต้องการดังกล่าว (Sign-off security requirements)

(2.2) การวางแผนงานโครงการ (Planning) กำหนดแผนการดำเนินงานและวิธีการดำเนินงาน เพื่อให้บรรลุวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยสารสนเทศ (Security Objective) และเป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Requirement) ที่กำหนดไว้ เช่น วิธีการควบคุมการเข้าถึง ขั้นตอนในการจัดหาและพัฒนาระบบงานอย่างมั่นคงปลอดภัย วิธีจัดเก็บและแลกเปลี่ยนข้อมูลของโครงการระหว่างผู้ที่เกี่ยวข้องอย่างมั่นคงปลอดภัย เป็นต้น นอกจากนี้ต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ทราบถึงภัยคุกคามและความเสี่ยงที่เกี่ยวข้องและกำหนดมาตรการในการป้องกันและควบคุมความเสี่ยงเหล่านั้น รวมถึงกำหนดความต้องการในการทบทวนความมั่นคงปลอดภัยของผลลัพธ์ของโครงการก่อนนำไปใช้งานจริง (เช่น การจัดทำ Source code Review, การทดสอบ Security Functions ของระบบ)

(2.3) การดำเนินงาน (Executing) ดำเนินการตามแผนงานของโครงการอย่างมั่นคงปลอดภัย เช่น ในการพัฒนาระบบงาน ควรใช้เครื่องมือหรือซอฟต์แวร์ในการพัฒนาที่ได้รับอนุญาตให้ใช้ภายในองค์กรรวมถึงจัดเก็บข้อมูลของโครงการอย่างมั่นคงปลอดภัย เป็นต้น

(2.4) การติดตามและกำกับดูแล (Monitoring and controlling) จัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศว่าได้ถูกพัฒนาหรือจัดให้มีขึ้นตามแผนการดำเนินงานหรือแผนการแก้ไขความเสี่ยงที่กำหนดไว้อย่างสอดคล้องกับแผนงานโครงการหรือไม่ รวมถึงกำกับดูแล และบริหารจัดการการเปลี่ยนแปลงฟังก์ชั่นการทำงานต่าง ๆ ที่อาจกระทบต่อความมั่นคงปลอดภัยโดยรวมของระบบงานอย่างเหมาะสม

(2.5) การสิ้นสุดโครงการ (Closing) ในขั้นตอนการตรวจรับโครงการหรือทดสอบเพื่อการยอมรับระบบ (System Acceptance Testing) ต้องดำเนินการทดสอบความถูกต้อง ครบถ้วน และประสิทธิผลของมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศว่าเป็นไปตามวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยสารสนเทศ (Security Objective) และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Requirement) หรือไม่ การอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ รวมถึงอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่นำมาใช้งานภายในกิจการของรัฐสภา จะต้องถูกอนุมัติให้นำมาใช้งานเพื่อให้มั่นใจว่าสินทรัพย์ดังกล่าวมีการระบุผู้เป็นเจ้าของ และรับผิดชอบในความมั่นคงปลอดภัยรวมถึงสามารถใช้งานรวมกับระบบเดิมที่มีอยู่ได้อย่างปลอดภัยและเหมาะสม

2.2 อุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากระยะไกล (Mobile Devices and Teleworking)

วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากระยะไกล

2.2.1 อุปกรณ์สื่อสารประเภทพกพา (Mobile Device) เพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น Notebook, Palm, Laptop , Smartphone, Tablet, Smartwatch, Netbook เป็นต้น) ควรพิจารณาดังต่อไปนี้

(1) อุปกรณ์สื่อสารประเภทพกพาต้องได้รับการอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศแล้วเท่านั้น จึงจะสามารถเข้าถึงข้อมูลสารสนเทศของรัฐสภาได้

(2) อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตาม แนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

(3) ไม่ควรเก็บข้อมูลสำคัญของรัฐสภาไว้บนอุปกรณ์สื่อสารประเภทพกพา แต่ถ้ามีความจำเป็นที่จัดเก็บบนอุปกรณ์สื่อสารประเภทพกพาจะต้องมีการเข้ารหัสข้อมูลตามแนวทางการเข้ารหัสของรัฐสภา

(4) ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

(5) ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพา หรือถูกส่งผ่านเครือข่ายไร้สายที่ต้องส่งออกไปนอกรัฐสภาต้องได้รับการอนุมัติจากเจ้าของข้อมูลและเข้ารหัสข้อมูลก่อนเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและจะต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

(6) ระบบคอมพิวเตอร์อื่นที่ต้องการเชื่อมต่อกับระบบของรัฐสภา จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ

(7) ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น จะต้องปิดห้องทำงานเมื่อไม่มีบุคคลที่ได้รับอนุญาตอยู่ประจำโต๊ะทำงาน และชั้นเก็บเอกสารต่าง ๆ จะต้องล๊อคอย่างดี เป็นต้น

(8) กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของรัฐสภา การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูลทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพาก่อนส่งซ่อม

(9) อุปกรณ์สื่อสารประเภทพกพา เช่น เครื่องคอมพิวเตอร์แบบพกพา (Notebook) หรือ Smart Device ควรมีกระบวนการเพื่ออัพเดท ระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามแนวปฏิบัติการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของรัฐสภา

(10) การเข้าถึงและใช้ข้อมูลสารสนเทศ ซึ่งรวมถึงชั้นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันที เมื่อผู้ใช้งานพ้นสภาพตามสิทธิของผู้ใช้งาน

(11) รัฐสภาอาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดการเข้าถึง ล่วงละเมิดใช้งานหรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิอันชอบ

2.2.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(1) ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอกรัฐสภา หน่วยงานที่รับผิดชอบต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และมีการตรวจสอบการใช้งานอย่างสม่ำเสมอ

(2) ไม่อนุญาตให้ใช้งาน Remote Access สำหรับการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เว้นแต่กรณีเกิดเหตุฉุกเฉินหรือเกิดเหตุการณ์ภัยพิบัติที่มีความจำเป็นต้องให้มีการปฏิบัติงานจากภายนอกเท่านั้น กรณีที่ต้องมีการเชื่อมต่อ Remote Access เพื่อปฏิบัติงานจากภายนอก ต้องปฏิบัติตามระเบียบการปฏิบัติงาน เรื่อง การขอเข้าใช้งานระบบ SSL VPN (SSL VPN Access Procedure) โดยได้รับการอนุมัติการเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ของรัฐสภาเท่านั้น

(3) การควบคุมโมเด็ม/เร้าเตอร์ ที่ผู้ดูแลระบบได้ติดตั้งไว้สำหรับการเข้าถึงจากภายนอก (Remote Diagnostic Port Protection) ผู้มีหน้าที่รับผิดชอบงานแต่ละสำนักงาน ต้องกำหนดให้มีการควบคุมการใช้งานโมเด็ม/เร้าเตอร์ ที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน Data Center เพื่อใช้ในการดูแลรักษาระบบจากภายนอก

(4) การเข้าสู่ข้อมูลของรัฐสภาจากระยะไกลได้นั้น ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศก่อนและผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติฯ ที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของรัฐสภาจากระยะไกล นอกจากนี้เจ้าของข้อมูลมีหน้าที่ดูแลรักษาและเปลี่ยนแปลงรายชื่อของผู้ใช้งานที่สามารถเข้าสู่ระบบจากระยะไกลให้ถูกต้องและเหมาะสมเพื่อให้หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศตรวจสอบความถูกต้องได้

(5) ต้องมีการกำหนดวิธีการพิสูจน์ตัวตน (Authentication Requirements)

(6) ก่อนจะกำหนดสิทธิของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นอย่างเพียงพอ และต้องได้รับอนุมัติจากหน่วยงานที่เป็นเจ้าของข้อมูลอย่างเป็นทางการเท่านั้น

(7) ต้องควบคุม Port ที่ใช้ในการเข้าสู่ระบบโดยการโทรเข้า/โทรออก (Dial-in/Dial-out) อย่างรัดกุม (ถ้ามี) ผู้ใช้งานที่มีความจำเป็นที่จะต้องใช้สาย Analog ในการเข้าสู่ระบบโดยวิธีการโทรเข้า/โทรออก ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ นอกจากนี้ สายที่ใช้ใน

การโทรออกต้องถูกตั้งค่าให้สามารถโทรออกได้เท่านั้น (ถ้าทำได้) การเข้าสู่ระบบโดยการโทรเข้านั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(8) ห้ามนำซอฟต์แวร์การควบคุมจากระยะไกล เช่น PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของรัฐสภา การใช้ซอฟต์แวร์ที่ไม่เหมาะสมดังกล่าวสามารถเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของรัฐสภา

(9) การอนุญาตให้ผู้จัดจำหน่ายระบบต่าง ๆ เข้าสู่ระบบข้อมูลของรัฐสภาจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และโมเด็มที่ใช้เพื่อการซ่อมบำรุงระบบจากระยะไกลทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรถูกปิดไม่ให้สามารถใช้การได้และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น เมื่อผู้จัดจำหน่ายระบบทำการซ่อมบำรุงเสร็จเรียบร้อยแล้ว Port ดังกล่าวจะต้องทำการปิดไม่ให้ใช้การได้อีกครั้ง

ส่วนที่ 3
ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

3.1 แนวปฏิบัติก่อนการจ้างงาน (Prior to Employment) เพื่อเป็นมาตรฐานในการควบคุมความปลอดภัยส่วนบุคคล โดยกำหนดเป็นมาตรฐานเกี่ยวกับข้าราชการ พนักงานลูกจ้าง และผู้ปฏิบัติงานตามสัญญาจ้างของรัฐสภา เริ่มตั้งแต่กระบวนการสรรหาข้าราชการ พนักงานและลูกจ้างใหม่ เพื่อให้มั่นใจว่ามีการพิจารณาคุณสมบัติอย่างเพียงพอ ก่อนที่จะมีการว่าจ้างและเพื่อให้มั่นใจว่าข้าราชการพนักงาน ลูกจ้างและผู้ปฏิบัติงานตามสัญญาจ้างมีความเข้าใจในบทบาทหน้าที่ความรับผิดชอบที่พึงปฏิบัติ

3.1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

(1) การคัดเลือกและการตรวจสอบคุณสมบัติต่าง ๆ ต้องเป็นไปตามกฎระเบียบและประกาศต่าง ๆ ที่กำหนดและต้องมีการจัดเก็บหลักฐานการตรวจสอบต่าง ๆ ให้ครบถ้วน

(2) ต้องมั่นใจว่าคุณสมบัติของผู้สมัครงานทุกคนถูกตรวจสอบก่อนที่จะบรรจุเป็นข้าราชการพนักงานและลูกจ้างโดยจะต้องไม่มีประวัติในการบุกรุกแก้ไขทำลายหรือโจรกรรมข้อมูลในระบบสารสนเทศของหน่วยงานใดมาก่อน

3.1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) สัญญาการว่าจ้างควรครอบคลุมหน้าที่ความรับผิดชอบของหนักงานและลูกจ้าง ดังนี้

(1) ข้าราชการ พนักงาน ลูกจ้าง และผู้ปฏิบัติงานตามสัญญาจ้างทุกคนมีหน้าที่ต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยของรัฐสภาและประกาศอื่นใดที่เกี่ยวข้อง

(2) กรณีที่มีการฝ่าฝืนหรือละเมิดแนวปฏิบัติหรือข้อกำหนดอันก่อให้เกิดความเสียหายแก่รัฐสภาหรือบุคคลหนึ่งบุคคลใด รัฐสภามีสิทธิในการดำเนินการทางวินัยและกฎหมายตามความเหมาะสม

3.2 แนวปฏิบัติระหว่างการจ้างงาน (During Employment) เพื่อให้เกิดความมั่นใจว่าข้าราชการ พนักงาน ลูกจ้าง และผู้ปฏิบัติงานตามสัญญาจ้างของรัฐสภาทุกคนเข้าใจและปฏิบัติตามบทบาทหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศที่ตัวเองรับผิดชอบ

3.2.1 ความรับผิดชอบของผู้บริหาร (Management Responsibilities) ผู้บริหารองค์กรมีหน้าที่บังคับใช้ มาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้ในแนวปฏิบัติและระเบียบปฏิบัติงานต่าง ๆ กับข้าราชการ พนักงาน ลูกจ้างและผู้ปฏิบัติงานตามสัญญาจ้างทุกคน ดังนี้

(1) สรุปหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้ทราบ ก่อนการอนุญาตให้มีการเข้าระบบหรือเข้าถึงข้อมูลที่เป็นความลับ

(2) กำหนดและสื่อสารความคาดหวังในบทบาทหน้าที่พึงปฏิบัติทราบ

(3) จัดอบรมหรือสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศตามความเหมาะสม

(4) สนับสนุนในการพัฒนาทักษะและความรู้อย่างสม่ำเสมอ

(5) แจ้งช่องทางในการรายงานการกระทำผิด หรือละเมิดกฎข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศโดยไม่ต้องเปิดเผยชื่อ

3.2.2 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information Security Awareness, Education and Training) ทุกคนต้องได้รับการอบรมด้านความมั่นคงปลอดภัยสารสนเทศตามความเหมาะสมกับหน้าที่งานที่ได้รับมอบหมาย

(1) รัฐสภาเป็นผู้จัดทำแผนการอบรมประจำปีเพื่อให้มีการอบรมให้ความรู้แก่ “ผู้ใช้” เกี่ยวกับวิธีปฏิบัติงานเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของศูนย์ปฏิบัติการ SOC โดยหลักสูตรการอบรมขึ้นอยู่กับหน้าที่ความรับผิดชอบของผู้ใช้ เช่น หลักสูตรสำหรับผู้บริหาร หลักสูตรสำหรับผู้ดูแลระบบ หลักสูตรสำหรับผู้ใช้ทั่วไป เป็นต้น

(2) รัฐสภาต้องเป็นผู้กำหนดให้มีการจัดอบรมเพื่อสร้างความตระหนักทางด้านความมั่นคงปลอดภัย หรือจัดให้มีการประเมินความตระหนักในเรื่องดังกล่าวอย่างน้อยปีละ 1 ครั้ง

3.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process) ในการจัดการกระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process) ให้ปฏิบัติแนวทางเดียวกับรัฐสภา “มาตรการดำเนินการกับผู้ฝ่าฝืนละเมิดแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของรัฐสภา” โดยมีข้อปฏิบัติดังนี้

(1) การฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจหรือบังเอิญ เช่น การเลือกรหัสผ่านที่ไม่เหมาะสมการสร้างกระบวนการที่กินกำลังระบบการใช้เนื้อที่ดิสค์เกินโควต้าโดยไม่ปฏิบัติตามคำเตือนการสั่งใช้

งานโปรแกรมที่ใช้ทรัพยากรจำนวนมากจนเกิดผลกระทบต่อการทำงานของระบบ เป็นต้น ให้ผู้ดูแลระบบแจ้งเตือนโดยวาจาหรือไปรษณีย์อิเล็กทรอนิกส์เป็นลายลักษณ์อักษร แต่หากเป็นการกระทำผิดซ้ำซ้อน ผู้ดูแลระบบอาจระงับสิทธิของผู้ใช้งานไว้ก่อน จนกว่าจะมีการตักเตือนอย่างเป็นลายลักษณ์อักษรโดยผู้บังคับบัญชาและมีการปรับปรุงแล้ว

(2) การฝ่าฝืนระเบียบขั้นรุนแรงเกิดจากการละเมิดกฎโดยเจตนา หรือจงใจสร้างความเสียหายให้แก่ระบบโดยไม่มีสิทธิและไม่ได้รับอนุญาต เช่น

(2.1) การจงใจสร้างความเสียหายแก่ซอฟต์แวร์หรือข้อมูลหรืออุปกรณ์ฮาร์ดแวร์

(2.2) การขโมยหรือพยายามขโมยสินทรัพย์หรือสิ่งที่ไม่มีสิทธิในการครอบครองมาไว้ในครอบครองซึ่งก่อให้เกิดความเสียหายแก่ผู้อื่น เช่น การลักลอบหรือใช้งานอุปกรณ์ระบบสื่อสารคอมพิวเตอร์ เป็นต้น

(2.3) การเข้าถึงระบบโดยมิชอบ (Unauthorized access) ทั้งในระดับกายภาพการเข้าถึงระบบสารสนเทศหรือข้อมูล และการเข้าถึงโดยผ่านเครือข่ายสาธารณะ เช่น การลักลอบดักฟังหรือดักเก็บข้อมูลที่มีชั้นความลับ ทั้งในส่วนของการติดตั้งซอฟท์แวร์และฮาร์ดแวร์ที่สามารถดักจับข้อมูล การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัสการตรวจสอบ Network Traffic โดยไม่ได้รับอนุญาตหรือมีเหตุอันสมควร เป็นต้น

(2.4) ประพฤติมิชอบในกิจกรรมใด ๆ ที่เกี่ยวข้องกับรัฐสภา เช่น การคดโกงคัดลอกผลงานหรือให้ข้อมูลที่ผิดแก่ทางรัฐสภาโดยเจตนา

(2.5) การสร้างโฮมเพจส่วนตัวที่แสดงออกในลักษณะที่ขัดต่อกฎหมายกฎระเบียบและศีลธรรม

(2.6) การก่อความวุ่นวายที่ขัดต่อกฎระเบียบของรัฐสภา หรือสร้างความเดือดร้อนรบกวนการทำงานของผู้ใช้งานอื่น ๆ ในระบบเครือข่าย

(3) กรณีที่ฝ่าฝืนหรือละเมิดข้อกำหนดในระเบียบนี้และก่อให้เกิดความเสียหายแก่รัฐสภาหรือบุคคลอื่นรัฐสภาจะพิจารณาดำเนินการทางวินัยและกฎหมายแก่ผู้ใช้งานนั้นตามความเหมาะสม ดังต่อไปนี้

(3.1) ผู้ดูแลระบบจะพิจารณาระงับการใช้งานและจะแจ้งชื่อผู้ใช้งานที่ทำผิดระเบียบไปยังหน่วยงานต้นสังกัดให้รับทราบ หรือแจ้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงรับทราบและพิจารณาตั้งกรรมการสอบสวนข้อเท็จจริงเพื่อพิจารณาจากความรุนแรงหรือความเสียหายที่เกิดขึ้นเป็นรายกรณีไป และรัฐสภาอาจพิจารณาดำเนินการทางวินัยหรือทางกฎหมายแก่ผู้นั้นตามความเหมาะสม

(3.2) ลงโทษทางวินัยต่อผู้ละเมิดตามความเหมาะสมเพื่อมิให้เกิดการละเมิดซ้ำและในกรณีที่ผู้ละเมิดเป็นหน่วยงานภายนอกให้ดำเนินการตามกฎหมายต่อไป

(3.3) หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อรัฐสภาอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมายให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป

(3.4) หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบสารสนเทศและต้องเสียค่าใช้จ่ายในการกู้คืน รัฐสภาสามารถเรียกร้องค่าเสียหายในส่วนนี้เพื่อเป็นค่าใช้จ่ายในการกู้คืน ข้อยกเว้น : กิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย เช่น การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัสการตรวจสอบ Network Traffic เป็นต้น หากปฏิบัติโดยหน่วยงานหรือบุคคลที่ได้รับอนุญาต หรือโดยหน่วยงานหรือบุคคลได้รับมอบหมายจากรัฐสภาแล้วจะไม่ถือว่าเป็นการฝ่าฝืนระเบียบนี้

3.3 แนวปฏิบัติการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and Change of Employment) เพื่อป้องกันความเสียหายด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดกับองค์กร ในกรณีทีเกิดการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงานของรัฐสภา

3.3.1 การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination or Change of Employment Responsibilities)

(1) ต้องทำการสื่อสารและแจ้งบทบาทและหน้าที่ความรับผิดชอบในด้านต่าง ๆ หลังสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานตามข้อกำหนดและเงื่อนไขในการจ้างงาน

(2) รัฐสภาต้องกำหนดเปลี่ยนแปลงหรือยกเลิกสิทธิของผู้ใช้งานที่เกี่ยวกับ User ID เพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

(3) เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของรัฐสภา เช่น อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า - ออก ฯลฯ ให้แก่รัฐสภาในทันทีที่พ้นหน้าที่

ส่วนที่ 4
การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

4.1 แนวปฏิบัติความรับผิดชอบต่อสินทรัพย์ (Responsibility for Asset) เพื่อเป็นการกำหนดมาตรฐานในการระบุสินทรัพย์ และกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่าง เหมาะสม สินทรัพย์ที่ใช้ในการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องทำบัญชี

สินทรัพย์ของหน่วยงาน เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ระบุผู้เป็นเจ้าของสารสนเทศแต่ละชนิด กำหนดการใช้สินทรัพย์ที่เหมาะสม และกำหนดแนวทางในการคืนสินทรัพย์ซึ่งมีแนวทางปฏิบัติ ดังนี้

4.1.1 การจัดทำบัญชีสินทรัพย์ (Inventory of Assets) กำหนดแนวทางการจัดทำและสอบทานบัญชีสินทรัพย์ด้านสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ดังต่อไปนี้

(1) จัดทำบัญชีสินทรัพย์ Data Center ของรัฐสภาทั้งหมด เช่น เครื่องคอมพิวเตอร์/คอมพิวเตอร์แบบพกพาอุปกรณ์เครือข่าย ซอฟต์แวร์ลิขสิทธิ์ เป็นต้น

(2) ต้องมีการทบทวนบัญชีสินทรัพย์ปีละ 1 ครั้งเพื่อตรวจสอบความถูกต้องครบถ้วนของบัญชีสินทรัพย์ Data Center ของรัฐสภา

(3) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ เช่น เดือนละครั้ง (สำหรับระบบสำคัญ) หรือปีละครั้ง (สำหรับระบบการใช้งานทั่วไป)

4.1.2 การระบุผู้เป็นเจ้าของสินทรัพย์ (Ownership of Assets) สินทรัพย์ทั้งหมดใน Data Center ของรัฐสภา จะต้องถูกกำหนดเจ้าของเพื่อให้มีผู้รับผิดชอบดูแลสินทรัพย์อย่างเหมาะสม โดยมีแนวทางปฏิบัติดังต่อไปนี้

(1) สินทรัพย์ทั้งหมดจะต้องกำหนดให้มีผู้ดูแลและเจ้าของอย่างชัดเจนโดยผู้เป็นเจ้าของสินทรัพย์ดังกล่าวอาจระบุเป็นชื่อบุคคลหรือชื่อหน่วยงานได้

(2) เจ้าของสินทรัพย์จะต้องกำหนดระดับชั้นความลับของข้อมูลในสินทรัพย์ที่ตนเองเป็นเจ้าของให้เป็นไปตามระเบียบการปฏิบัติงานเรื่องการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

(3) เจ้าของสินทรัพย์ต้องกำหนดผู้มีสิทธิใช้งานหรือเข้าถึงสินทรัพย์ของตนเอง (Access Control)

(4) เจ้าของสินทรัพย์จะต้องทบทวนความเหมาะสมของระดับชั้นความลับที่กำหนดไว้อย่างสม่ำเสมอ

(5) เจ้าของสินทรัพย์จะต้องกำหนดการบริหารจัดการสินทรัพย์ที่เหมาะสมเมื่อต้องมีการลบหรือทำลายสินทรัพย์

4.1.3 การใช้งานสินทรัพย์อย่างเหมาะสม (Acceptable Use of Asset)

(1) สินทรัพย์ทั้งหมดจะต้องถูกใช้ในกิจการของรัฐสภาเท่านั้น

(2) ข้อมูลหรือสารสนเทศทั้งหมดที่จัดเก็บอยู่ในระบบสารสนเทศใน Data Center ของรัฐสภา ถือเป็นสินทรัพย์ของรัฐสภา

(3) การใช้งานสินทรัพย์ต่าง ๆ ที่เป็น Data Center ของรัฐสภาจะต้องเป็นไปตามข้อกำหนดดังนี้:

(3.1) การใช้งานอินเทอร์เน็ต เครื่องโทรสารเครื่องพิมพ์ เครื่องถ่ายเอกสาร ฯลฯ จะจำกัดให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นไม่ครอบคลุมไปถึงบุคคลภายนอก ยกเว้น ได้รับการอนุญาต

(3.2) การใช้งานจะต้องไม่เป็นการขัดขวางประสิทธิภาพในการทำงานตามปกติ

(3.3) จะต้องไม่มีการส่งหรือรับไฟล์หรือเอกสารใด ๆ ซึ่งผิดกฎหมายหรือสร้างความเสื่อมเสีย

4.1.4 การคืนสินทรัพย์ (Return of Assets) เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของรัฐสภา เช่น อุปกรณ์ระบบสารสนเทศให้แก่รัฐสภาในทันทีที่พ้นหน้าที่

4.2 แนวปฏิบัติการจัดชั้นสารสนเทศ (Information Classification) เพื่อกำหนดมาตรฐานในการป้องกันสารสนเทศของรัฐสภา โดยมีการจัดชั้นความลับจัดทำป้ายชื่อ และบริหารจัดการสารสนเทศอย่างเหมาะสม การจัดชั้นความลับสารสนเทศที่ใช้ในการปฏิบัติงาน ภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องทำบัญชีสารสนเทศของหน่วยงานและระบุชั้นความลับให้ชัดเจนเพื่อใช้ในการกำหนดระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศแต่ละชนิด ซึ่งมีแนวทางปฏิบัติ ดังนี้

4.2.1. การจัดชั้นความลับสารสนเทศ (Classification of Information)

(1) เจ้าของสารสนเทศมีหน้าที่ในการกำหนดชั้นความลับของสารสนเทศภายใต้รับความผิดชอบของตน

(2) การป้องกันสารสนเทศต้องพิจารณาทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้งาน

(3) ข้อมูลดิจิตอล (Digital Data) หรือสารสนเทศดิจิตอล (Digital Information) ให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้

(3.1) “ชั้นลับมาก”

(3.2) “ชั้นลับ”

(3.3) “ชั้นปกปิด”

(3.4) “ชั้นไม่ระบุ”หรือ “ชั้นเปิดเผย”

ทั้งนี้หากไม่ได้มีการกำหนดชั้นความลับที่ชัดเจนไว้สำหรับข้อมูลดิจิตอล หรือสารสนเทศดิจิตอล ให้ถือว่า ข้อมูลหรือสารสนเทศนั้นเป็น “ชั้นลับ” โดยปริยาย

(4) เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิตอลหรือสารสนเทศดิจิตอลซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิตอลหรือสารสนเทศดิจิตอลนั้นยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

(5) ต้องทำการจัดส่วนหมู่กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของรัฐสภาให้มีความปลอดภัยด้วยวิธีการที่เหมาะสมโดยให้ปฏิบัติตามระเบียบการปฏิบัติงานเรื่องการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

(6) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การเก็บรักษาจนถึงการทำลาย

4.2.2 การจัดทำป้ายชื่อสารสนเทศ (Labeling of Information)

(1) ข้าราชการ พนักงาน ลูกจ้างและผู้ปฏิบัติงานตามสัญญาจ้างทุกคน ต้องปฏิบัติตามขั้นตอนการปฏิบัติงานในการจัดทำป้ายชื่อสารสนเทศ

(2) การจัดทำป้ายชื่อต้องสอดคล้องกับระดับชั้นความลับที่กำหนดไว้ใน “การจัดชั้นความลับสารสนเทศ (Classification of Information)”

(3) การจัดทำป้ายชื่อสารสนเทศต้องครอบคลุมสารสนเทศทั้งในรูปแบบที่เป็นกายภาพ (physical) และ อิเล็กทรอนิกส์

(4) ต้องจัดให้มีวิธีการจัดทำ และจัดการป้ายชื่อสำหรับสารสนเทศ โดยแยกตามส่วนหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วยการถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย โดยมีแนวทางปฏิบัติ ดังนี้

(4.1) ข้อมูลที่ถูกจัดอยู่ใน “ชั้นลับมาก” ต้องใช้ระบบการนำส่งแบบใส่ 2 ซองซ้อนเช่นเดียวกัน โดยซองด้านในระบุถึงชื่อและประเภทของข้อมูลอย่างชัดเจน ส่วนซองด้านนอกจะระบุถึงชื่อและที่อยู่ของผู้รับเท่านั้น

(4.2) ข้อมูล “ชั้นลับมาก” ต้องส่งให้ถึงมือผู้รับที่ระบุเท่านั้นและต้องมีลายเซ็นของผู้รับระบุว่าได้รับเอกสารแล้ว

(4.3) การทำสำเนาเอกสารข้อมูลที่อยู่ “ชั้นลับมาก” ต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น

(4.4) ข้อมูลที่อยู่ “ชั้นลับมาก” ต้องถูกจัดพิมพ์จากเครื่องพิมพ์ที่เชื่อมโยงกับระบบเครือข่ายที่สามารถควบคุมการใช้ได้ เพื่อป้องกันการอ่าน เปลี่ยนแปลง หรือ ลบข้อมูลได้จากผู้ที่ไม่ได้รับอนุญาต

(4.5) เอกสารข้อมูล “ชั้นลับมาก” “ชั้นลับ” และ “ชั้นปกปิด” ที่ไม่ได้นำมาใช้แล้ว ต้องถูกรวบรวม ขีดฆ่า และ ทำเครื่องหมาย “ทำลายได้” และนำเอกสารไปทำลายเพื่อไม่ให้สามารถอ่านหรือนำมาใช้ได้อีกโดยการฉีกหรือเผาทำลาย

(5) กำหนดให้ข้อมูลทุกประเภทที่อยู่ในสื่อบันทึกเป็นข้อมูลประเภท “ลับ (Confidential)” และไม่จำเป็นจะต้องติดป้ายระดับชั้นความลับของข้อมูล

(6) หากมีความจำเป็นจะต้องกำหนดระดับชั้นความลับของข้อมูลในสื่อบันทึกดังกล่าวเป็นระดับอื่น จะต้องติดป้ายชื่อให้กับสื่อบันทึกดังกล่าว ให้สอดคล้องกับข้อมูลดังกล่าว

(7) ข้อมูลทุกระดับชั้น จะต้องถูกส่งผ่านระบบอีเมลของรัฐสภา เท่านั้น

4.2.3 การจัดการสินทรัพย์ (Handling of Assets)

(1) ขั้นตอนการปฏิบัติงานในการจัดการสินทรัพย์ต้องสอดคล้องและเป็นไปในทิศทางเดียวกับ “การจัดชั้นความลับสารสนเทศ (Classification of Information)”

(2) ให้ทำการจัดเก็บสินทรัพย์ตามรายละเอียดการจัดเก็บจากผู้ผลิต หากสินทรัพย์นั้นต้องการการจัดเก็บเป็นพิเศษ

4.3 แนวปฏิบัติการจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling) เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การขนย้าย การลบหรือการทำลายสินทรัพย์สารสนเทศ โดยไม่ได้รับอนุญาต

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้ (Management of Removable Media) เพื่อควบคุมและป้องกันสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้มีแนวทางการปฏิบัติ ดังนี้

(1) ข้อมูลที่มีชั้นความลับต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

(2) ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้วก่อนที่จะนำออกไปจากรัฐสภา ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

(3) ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากผู้ที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้ายเพื่อใช้ในการตรวจสอบ

(4) สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต เช่น อุณหภูมิสูงหรือต่ำเกินไป

(5) ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล เช่น มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิในการใช้งาน เป็นต้น

(6) ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูลควรจัดเก็บไว้ที่แหล่งอื่น เพื่อป้องกันการสูญหายของข้อมูล

(7) ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้เพื่อลดโอกาสการสูญหายของข้อมูล

(8) ตัวอ่านสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้จะต้องใช้เพื่อเหตุผลทางกิจการของรัฐสภาเท่านั้นการมอบอำนาจในระดับต่าง ๆ ควรทำเป็นเอกสารอย่างชัดเจน

4.3.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of Media) การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีก ต้องเป็นไปอย่างมั่นคงและปลอดภัย เพื่อลดความเสี่ยงของการรั่วไหลข้อมูลของรัฐสภาไปยังผู้อื่นที่ไม่ได้รับอนุญาต ซึ่งมีแนวทางปฏิบัติ ดังนี้

(1) สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย เช่น การเผาหรือแยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยซอฟต์แวร์อื่น ๆ ที่มีใช้ในรัฐสภา

(2) กระบวนการต่าง ๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจนเพื่อความปลอดภัยของข้อมูลเช่น ปฏิบัติตามแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

(3) เพื่อความสะดวกควรรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

(4) ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสารรวมทั้งอุปกรณ์ต่าง ๆ จากหน่วยงานภายนอกควรระวังในการเลือกใช้บริการต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดีและมีประสบการณ์

(5) ในการกำจัดสื่อบันทึกข้อมูลจะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ หมายเหตุ : ข้อมูลที่ไม่มีความสำคัญเมื่อมีการรวบรวมเป็นจำนวนมาก ๆ อาจจะกลายเป็นข้อมูลที่มีความสำคัญได้ ดังนั้นใน การกำจัดต้องคำนึงถึงข้อมูลที่มีการรวบรวมไว้ด้วย

4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer) เพื่อป้องกันสื่อบันทึกข้อมูลที่มีข้อมูลอาจถูกเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์และการทำให้ข้อมูลเกิดความเสียหายในระหว่างขนย้ายหรือนำส่งข้อมูลนั้นออกไปนอกรัฐสภาควรพิจารณาดัง ต่อไปนี้

(1) ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

(2) รายชื่อของพนักงานส่งของหรือบริษัทส่งของควรได้รับการอนุมัติจากผู้มีอำนาจ

(3) กระบวนการตรวจสอบพนักงานส่งของต้องมีการปรับปรุงอย่างสม่ำเสมอ

(4) การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่งโดยเป็นไปตามข้อกำหนดของผู้ผลิตตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล เช่น ความร้อนความชื้นและสนามแม่เหล็ก

(5) การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

(5.1) ใช้ตู้ที่มีกุญแจล๊อค

(5.2) ส่งด้วยมือตนเองและลงบันทึกการรับ - ส่งเพื่อสามารถตรวจสอบได้

(5.3) บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลาย ๆ ส่วนและหลาย ๆ เส้นทาง เพื่อกระจายความเสี่ยง

4.3.4 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ มีแนวทางปฏิบัติ ดังนี้

(1) ติดป้ายชื่อของสื่อบันทึกข้อมูลทั้งหมดเพื่อระบุประเภท

(2) จำกัดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ที่ไม่ได้รับอนุญาต

(3) ทำบันทึกข้อมูลเกี่ยวกับผู้ที่มีสิทธิได้รับข้อมูล

(4) ข้อมูลที่ป้อนเข้าสู่ระบบและในระหว่างการประมวลผลต้องมีครบถ้วนและต้องตรวจสอบผลลัพธ์ที่ออกมาด้วย

(5) ต้องมีการปกป้องข้อมูลที่อยู่ในระหว่างการแสดงผลลัพธ์ออกมาตามระดับความสำคัญ

(6) เก็บรักษาสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต

(7) กระจายข้อมูลให้น้อยที่สุด

(8) ลบเครื่องหมายของสำเนาสื่อบันทึกข้อมูลทั้งหมดเพื่อไม่ให้เป็นที่สังเกตของผู้ที่มีสิทธิได้รับข้อมูล

(9) ทบทวนการกระจายข้อมูลและรายชื่อของผู้ที่มีสิทธิได้รับข้อมูลอย่างต่อเนื่อง หมายเหตุ : กระบวนการเหล่านี้คลอบคลุมทั้งสื่อที่เป็นเอกสารระบบคอมพิวเตอร์ระบบเครือข่ายโทรศัพท์เคลื่อนที่ ไปรษณีย์อิเล็กทรอนิกส์ การสื่อสารด้วยเสียงมัลติมีเดีย การบริการของไปรษณีย์ เครื่องถ่ายเอกสารรวมไปถึงเช็คเปล่าและใบเรียกเก็บเงิน

4.3.5 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System documentations) มาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาตมีแนวทางปฏิบัติ ดังนี้

(1) จัดเก็บอย่างมั่นคงปลอดภัย

(2) รายการเกี่ยวกับการเข้าถึงเอกสารระบบควรเก็บไว้ให้น้อยที่สุด และต้องได้รับการอนุมัติจากเจ้าของระบบงาน

(3) เอกสารระบบที่จัดเก็บไว้ในเครือข่ายสาธารณะ หรือมีการใช้งานผ่านเครือข่ายสาธารณะจะต้องมีระบบการป้องกันที่เหมาะสม

(4) ไม่ควรจัดเก็บเอกสารระบบที่มีการระบุ Username และ Password เช่น เอกสารคู่มือการใช้งานระบบ ไว้ในเครือข่ายสาธารณะเพราะอาจทำให้ผู้ไม่มีสิทธิสามารถนำข้อมูลดังกล่าวไปใช้ในการเข้าถึงระบบได้

ส่วนที่ 5
การควบคุมการเข้าถึง (Access Control)

5.1 แนวปฏิบัติการควบคุมการเข้าถึงตามความต้องการทางธุรกิจ (Business Requirements of Access Control) เพื่อควบคุมการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของรัฐสภา เพื่อให้มีความมั่นคงปลอดภัย และป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบได้

5.1.1 การจัดทำแนวปฏิบัติการควบคุมการเข้าถึง (Access Control)

(1) สถานที่ตั้งของระบบสารสนเทศที่สำคัญ ต้องมีการควบคุมการเข้า - ออกอย่างเคร่งครัด และให้เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นเท่านั้น สามารถเข้าใช้งานได้เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึง

(2) ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ

(3) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงบริการได้

(4) ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของรัฐสภา และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่สำคัญ ทั้งนี้ ผู้ที่สามารถใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจตรา และเฝ้าระวังในระบบเครือข่ายหรือระบบงานใด ๆ ต้องเป็นผู้ที่ได้รับอนุญาตจากหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศของรัฐสภาเท่านั้น

(5) ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า – ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

(6) ในการขออนุญาตเข้าสู่ระบบงานต่าง ๆ จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบกำหนดให้มีการลงนามอนุมัติและเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

(7) เจ้าของข้อมูลและเจ้าของระบบงานนั้น ๆ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น ต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(8) ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชา เจ้าของข้อมูลและเจ้าของระบบงานก่อนตามความจำเป็นในการใช้งานตามภารกิจของรัฐสภา

5.1.2 การเข้าถึงระบบเครือข่ายและการให้บริการเครือข่าย (Access to Network and Network Services) ต้องจัดทำข้อกำหนดหรือสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างรัฐสภากับผู้ใช้งาน ซึ่งมีแนวทางปฏิบัติ ดังนี้

(1) ในกรณีที่อนุญาตให้ Protocol บางประเภทสามารถเข้าถึงระบบเครือข่ายของรัฐสภา จะต้องมีมาตรการการป้องกันล่วงหน้าและขั้นตอนการปฏิบัติงานโดยเฉพาะ

(2) แม้จะติดตั้ง Router และ Firewall อย่างปลอดภัยแล้วก็ตาม การแก้ไขในภายหลังอาจก่อให้เกิดความเสี่ยงต่อระบบงานได้ เพื่อลดความเสี่ยงต่าง ๆ ทุกครั้งที่มีการเปลี่ยนแปลง Router และ Firewall จะต้องปฏิบัติตามแนวปฏิบัติการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

(3) ห้ามทำ Packet Forwarding หรือ Re-routing สำหรับ Server ที่มีการติดตั้ง Protocol ที่สามารถทำได้ เช่น กำหนดให้ FTP ไม่สามารถทำ IP Forwarding หรือ Passive mode ได้

(4) หมายเลขเครือข่ายภายใน (Internal Network Address) ของรัฐสภา จำเป็นต้องมีการป้องกันมิให้ส่วนงานที่เชื่อมต่อจากภายนอกสามารถมองเห็นได้ เพื่อป้องกันไม่ให้ Hackers หรือหน่วยงานภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบงานเครือข่ายและส่วนประกอบของคอมพิวเตอร์ของรัฐสภาได้โดยง่าย

(5) เพื่อลดความเสี่ยงจากการใช้ TCP/IP ดังนั้น Router และ Firewall จะต้องปฏิเสธการเชื่อมต่อใด ๆจากระบบภายนอกซึ่งมี IP Address เหมือนกับ IP Address ที่ใช้ในเครือข่ายภายในของรัฐสภา

(6) สำหรับข้อมูลที่ผ่านเข้าและส่งออกจากระบบเครือข่ายรัฐสภา ต้องส่งข้อมูลผ่าน Firewall เพื่อป้องกันการเชื่อมต่อจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้อนุมัติการเชื่อมต่อระบบเครือข่ายจากภายนอกของรัฐสภา

(7) การเข้าสู่ระบบเครือข่ายของรัฐสภาผ่านอินเทอร์เน็ตจะต้องมีการ Log on เพื่อพิสูจน์ตัวตนและได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศก่อน

(8) ระบบเครือข่ายทั้งหมดของรัฐสภาที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกรัฐสภา ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

(9) ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังรัฐสภา และการเชื่อมต่อนี้ต้องเข้ามายังเครื่องคอมพิวเตอร์หรือระบบงานที่กำหนดไว้เท่านั้น ควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของรัฐสภา ทั้งด้าน Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายรัฐสภาได้โดยอิสระ

(10) ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย

(11) ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์บนเครือข่าย สามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อบนเครือข่ายมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว เพื่อจำกัดสิทธิในการใช้งานระบบสารสนเทศของรัฐสภา

5.2 แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบของผู้ใช้งาน และป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบได้เพื่อสร้างความมั่นใจในส่วนของการรักษาความลับและการรักษาความสมบูรณ์

5.2.1 การลงทะเบียนและการถอดถอนผู้ใช้งาน (User Registration and De-registration)

(1) มีการจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้งานใหม่

(2) มีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงานภายในรัฐสภา

(3) ผู้ใช้งานแต่ละคนต้องมี User Account ที่ไม่ซ้ำกัน

(4) ไม่อนุญาตให้ใช้ User account ร่วมกัน

(5) การใช้ Share Account อนุญาตให้เฉพาะกับบางระบบที่จำเป็นเท่านั้น

5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

(1) ผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อนจึงจะสามารถเข้าใช้งานระบบได้

(2) ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน เช่น กำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานตามความจำเป็นขั้นต่ำเท่านั้น

(3) ต้องมีการพิจารณาในส่วนของการกำหนดสิทธิเพื่อให้เกิดการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) อย่างเหมาะสม

(4) มีการบันทึกรวบรวมสิทธิทั้งหมดที่ผู้ใช้งานแต่ละคนได้รับ และทำการสอบทานสิทธิเหล่านี้อย่างสม่ำเสมอ

5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิพิเศษ (Management of Privileged Access Rights)

(1) การกำหนดสิทธิในการเข้าถึงระดับพิเศษ (เช่น Power User, Root หรือ Administrator) ต้องได้รับการควบคุมเป็นพิเศษ และพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นเท่านั้น

(2) มีการจัดทำรายชื่อบัญชีผู้ใช้งานในระดับ System (เช่น root หรือ administrator เป็นต้น) และสิทธิการเข้าถึงในระดับพิเศษ (เช่น Power User)

(3) สำหรับ User Account ในระดับ System ผู้ใช้งานต้องใช้ User Account ดังกล่าวเพื่อทำงานที่เกี่ยวข้องกับการดูแลระบบเท่านั้น ส่วนการทำงานทั่วไปอื่น ๆ ให้ใช้ User Account ที่มีสิทธิในระดับปกติ

(4) ควรมีการกำหนดระยะเวลาในการใช้งาน (expiration date) ของ User Account ที่ได้รับสิทธิการเข้าถึงในระดับพิเศษ

5.2.4 การบริหารจัดการรหัสผ่านของผู้ใช้งาน (Management of Secret Authentication Information of Users) เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศผู้ใช้งานควรปฏิบัติตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ผู้ดูแลระบบเจ้าของข้อมูลและเจ้าของระบบงานต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.2.6 การถอนหรือเปลี่ยนแปลงสิทธิผู้ใช้งาน (Removal or Adjustment of Access Rights)

(1) ต้องกำหนดเปลี่ยนแปลงหรือยกเลิกสิทธิของผู้ใช้งานที่เกี่ยวกับ User ID เพื่อให้สอดคล้องกับการ เปลี่ยนแปลงสถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

(2) ผู้ดูแลระบบต้องลบ Username และ Password ของผู้ปฏิบัติงานชั่วคราวทันทีเมื่อครบกำหนดสิ้นสุดการขอใช้งาน

5.2.7 การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกรัฐสภา (User Authentication for External Connections) ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกรัฐสภาสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของรัฐสภาได้

(1) ผู้ใช้งานทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบเสียก่อน

(2) การเข้าสู่ระบบของรัฐสภาต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี เช่น รหัสผ่าน

(3) ต้องแจ้งเป็นลายลักษณ์อักษรให้กับบุคคลที่ใช้บริการด้านสารสนเทศ ตามสัญญาถึงความสำคัญที่มีต่อการรักษาความปลอดภัยของข้อมูลสารสนเทศ ซึ่งแต่ละบุคคลต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของรัฐสภาและจัดเก็บเอกสารไว้ในแฟ้มสัญญา การเข้าสู่ระบบของรัฐสภาจากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ เช่น รหัสผ่านและเพื่อเพิ่มความปลอดภัยการพิสูจน์ตัวตนต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

5.2.8 ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องมีการพิสูจน์ตัวตน ก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ มีแนวทางปฏิบัติดังนี้

(1) ควรบังคับใช้สำหรับผู้ใช้งานทุกประเภท

(2) User ID ของผู้ใช้งานต้องสามารถตรวจสอบร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ในภายหลัง

(3) กิจกรรมงานประจำไม่ควรดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

(4) กรณีที่จำเป็นต้องมีการใช้งาน User ID ร่วมสำหรับกลุ่มของผู้ใช้งานหรือในเฉพาะบางงานในกรณีดังกล่าวควรมีการจัดทำ เอกสารอนุมัติรับรองจากผู้บริหาร

(5) ต้องกำหนดตัวควบคุมอื่นเพิ่มเติม เพื่อให้รับผิดชอบต่อข้อมูลในกรณีใช้ User ID ร่วมกัน

(6) การใช้ User ID ร่วมดังกล่าวควรถูกใช้เฉพาะกรณีที่การใช้งานนั้นไม่จำเป็นต้องบันทึกประวัติการใช้งาน (เช่นการดูอย่างเดียว เป็นต้น) หรือในกรณีที่มีการควบคุมอื่นควบคู่ไปด้วย เช่น อนุญาตให้เข้าใช้เพียงครั้งเดียว

(7) กรณีที่จำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มงวดอาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ เช่น วิธีการเข้ารหัสเพื่อรักษาความลับสมาร์ทการ์ด Token หรือ วิธีการทางไบโอเมตริก

5.3 แนวปฏิบัติความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานในการป้องกันและรักษาสารสนเทศส่วนตัวในการเข้าระบบที่สำคัญ เช่น User Account และรหัสผ่าน เป็นต้น

5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นความลับ (Use of Secret Authentication Information) ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

5.4 แนวปฏิบัติด้านการควบคุมการเข้าถึงระบบและแอปพลิเคชัน (System and Application Access Control) เพื่อกำหนดแนวทางการป้องกันการเข้าถึงระบบและแอปพลิเคชัน โดยมิชอบจากผู้ที่ไม่ได้รับอนุญาต

5.4.1 ข้อกำหนดการเข้าถึงสารสนเทศ (Information Access Restriction)

(1) ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอปพลิเคชันตามแนวปฏิบัติการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยต้องแยกตามประเภทของผู้ใช้งานการจำกัดสิทธิของผู้ใช้งาน ควรพิจารณาอยู่บนพื้นฐานความจำเป็นของระบบซอฟต์แวร์แต่ละระบบโดยมีแนวทางปฏิบัติ ดังนี้

(1.1) เตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

(1.2) ควบคุมสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน

(1.3) ควบคุมสิทธิการเข้าถึงข้อมูลของระบบซอฟต์แวร์อื่น

(1.4) สร้างความมั่นใจว่าข้อมูลที่สำคัญจะถูกแสดงในหน้าจอที่ปลอดภัยและเหมาะสม

(2) เจ้าของระบบงานต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะซึ่งมีแนวทางปฏิบัติ ดังนี้

(2.1) ความสำคัญ (Sensitivity) ของระบบซอฟต์แวร์ประยุกต์ควรมีการระบุอย่างชัดเจนและจัดทำเป็นเอกสารโดยเจ้าของระบบ

(2.2) เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่นจะต้องมีการระบุความเสี่ยงและมีการยอมรับโดยเจ้าของระบบนั้น

5.4.2 ขั้นตอนในการปฏิบัติ Log-on อย่างปลอดภัย (Secure Log-on Procedures)

(1) ไม่แสดงรุ่น (Version) ของซอฟต์แวร์จนกว่าจะ Log On เสร็จสิ้นสมบูรณ์

(2) แสดงข้อความเตือนว่าคอมพิวเตอร์ควรถูกใช้งานโดยผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

(3) ไม่ควรแสดง Help ระหว่าง Log On ซึ่งอาจช่วยให้ Hacker ค้นหาช่องทางเข้าได้

(4) ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการนำเข้าเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาดระบบไม่ควรแสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

(5) จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง เป็นต้นและควรพิจารณาเพิ่มเติมประเด็น ต่อไปนี้

(5.1) บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ

(5.2) หลังจาก Log On ผิดพลาดบังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้ทำต่อไป

(5.3) ตัดการเชื่อมโยงเครือข่าย

(5.4) ส่งข้อความเตือนไปยังหน้าจอของระบบถ้าความพยายามในการ Log On หลายครั้งเกินจำนวนครั้งมากที่สุดที่ยอมรับได้

(5.5) กำหนดรหัสผ่านให้เหมาะสมกับความยาวของรหัสผ่านและมูลค่าของระบบที่จะต้องได้รับการป้องกัน

(6) ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกันและต้องมีการพิสูจน์ตัวตน ก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

(7) จำกัดจำนวนครั้งสูงสุดและต่ำสุดถ้าเกินกว่านั้นระบบควรหยุดการให้ Log On

(8) แสดงข้อมูลต่อไปนี้หลังจากที่ Log On สำเร็จ

(8.1) วันที่และเวลาของการ Log On ครั้งที่แล้ว

(8.2) รายละเอียดของการพยายาม Log On ที่ไม่สำเร็จ ตั้งแต่การ Log On ครั้งที่แล้ว

(9) ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้งาน เมื่อไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้มีแนวทางปฏิบัติดังนี้

(9.1) มีกลไกในการเคลียร์ Session เมื่อไม่ได้ใช้งานมาเป็นระยะเวลาที่กำหนด (Time-out)

(9.2) Time-out ควรกำหนดให้เหมาะสมกับความเสี่ยงนั้น ประเภทข้อมูลที่เกี่ยวข้อง และระบบซอฟต์แวร์นั้น ๆ

(10) ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง มีแนวทางปฏิบัติดังนี้

(10.1) ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่งซึ่งได้กำหนดไว้ล่วงหน้า

(10.2) จำกัดการเชื่อมต่อเครือข่ายให้เฉพาะภายในระยะเวลาทำการ

(10.3) ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System) ต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับตั้งรหัสผ่านที่มีคุณภาพและต้องสามารถรองรับและสนับสนุนแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

5.4.4 การใช้งานซอฟต์แวร์ประเภทอรรถประโยชน์ (Use of Privileged Utility Programs)

(1) ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานซอฟต์แวร์ประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยง มาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

(2) การใช้ซอฟต์แวร์ประเภทอรรถประโยชน์ควรมีการระบุตัวตนตรวจสอบยืนยัน และการควบคุมสิทธิของผู้ใช้งาน

(3) ทำการแยกซอฟต์แวร์ประเภทอรรถประโยชน์ออกจากซอฟต์แวร์ประยุกต์

(4) จำกัดการใช้งานของระบบยูทิลิตี้ให้เฉพาะสำหรับผู้ใช้งานที่จำเป็น

(5) การขอใช้งานซอฟต์แวร์ประเภทอรรถประโยชน์ แบบเฉพาะกิจ (ad hoc) ต้องได้รับการอนุมัติก่อนเสมอ

(6) มีการจำกัดสิทธิในการใช้งานซอฟต์แวร์ประเภทอรรถประโยชน์ตามความเหมาะสม

(7) มีการบันทึกประวัติการใช้งานของซอฟต์แวร์ประเภทอรรถประโยชน์

(8) จัดทำเอกสารระดับการให้สิทธิในการเข้าถึงซอฟต์แวร์ประเภทอรรถประโยชน์

(9) ทำการยกเลิกซอฟต์แวร์ประเภทอรรถประโยชน์ที่ไม่ได้ใช้งานหรือไม่จำเป็น

(10) ไม่ควรให้สิทธิการใช้ซอฟต์แวร์ประเภทอรรถประโยชน์กับผู้ใช้งานที่มีสิทธิเข้าถึงระบบซอฟต์แวร์ประยุกต์

5.4.5 การควบคุมการเข้าถึงโปรแกรม Source Code (Access Control to Program Source Code) ต้องมีการควบคุมการใช้งานไลบรารีซึ่งประกอบด้วย Source Code ของระบบที่ใช้งานจริงหรือระบบที่ให้บริการ โดยมีแนวทางปฏิบัติดังนี้

(1) ห้ามเก็บ Source Code Library ไว้ในระบบที่ใช้งานจริง (Production System)

(2) หน่วยงานที่รับผิดชอบต้องแต่งตั้งผู้มีอำนาจในการดูแลและปรับปรุงไลบรารี่

(3) ระหว่างทดสอบต้องไม่เก็บ Source Code ที่ใช้ทดสอบรวมกับไลบรารี่ที่ใช้งานจริง

(4) ไม่ควรให้สิทธิการเข้าถึงแบบไม่มีข้อจำกัด (unlimited access) แก่ผู้ดูแลระบบ

(5) การเปลี่ยนแปลงหรือแก้ไข Source Code ของโปรแกรมต้องได้รับการอนุมัติก่อนเสมอ

(6) มีการบันทึกประวัติการเข้าถึงไลบรารี่

แนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

1.วัตถุประสงค์เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

2. การบริหารจัดการรหัสผ่าน

2.1 รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบข้อมูลของรัฐสภาจริง

2.2 ผู้ใช้งานระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน

2.3 ผู้ใช้งานรายใหม่จะได้รับรหัสผ่านเริ่มแรกในการผ่านเข้าระบบและเมื่อเข้าสู่ระบบในครั้งแรกจะต้องเปลี่ยนรหัสผ่านโดยทันทีและควรเปลี่ยนรหัสผ่านตามระยะเวลา เช่น 3 เดือนต่อครั้ง

2.4 รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้งานที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้งานที่มีสิทธิใช้งานระบบจริง รหัสผ่านดังกล่าวควรใช้อย่างระมัดระวังและจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

2.5 ไม่ควรส่งรหัสผ่าน ผ่านระบบเครือข่ายโดยไม่เข้ารหัสเพื่อรักษาความลับก่อน

2.6 ต้องกำหนดให้ผู้ใช้งานมีการพิสูจน์ตัวตน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

2.7 กำหนดให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนรหัสผ่านเพื่อป้องกันความผิดพลาด

2.8 ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ เช่น มีการแนะนำว่ารหัสผ่านที่ผู้ใช้งานกำหนดนั้นอยู่ในระดับอ่อนปานกลางหรือแข็งแกร่ง เป็นต้น

2.9 บันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

2.10 ต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไปหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

3. การใช้งานรหัสผ่าน

3.1 เก็บรหัสผ่านไว้เป็นความลับ

3.2 ต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้หรือไม่ควรเก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย เช่น บนเครื่องคอมพิวเตอร์บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

3.3 ไม่พิมพ์รหัสผ่านในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

3.4 ไม่ทำการใด ๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

3.5 เปลี่ยนรหัสผ่านส่วนของตนเองในครั้งแรกของการใช้งานไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตามและไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

3.6 หากมีเหตุที่น่าเชื่อถือได้ ผู้ใช้งานควรรายงานเหตุการณ์ที่สงสัยว่ามีการเปิดเผยรหัสผ่านไปยังผู้ดูแลระบบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

3.7 ถ้าพบว่ารหัสผ่านของตนถูกล็อคโดยไม่ทราบสาเหตุ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

3.8 ในกรณีที่ได้รับความช่วยเหลือในการแก้ไขปัญหา และต้องการให้ใส่รหัสผ่านผู้ใช้งานไม่ควรให้รหัสผ่านแก่ผู้ช่วยเหลือ แต่ควรใส่รหัสผ่านด้วยตนเอง

4. การกำหนดรหัสผ่าน

4.1 การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม ชื่อหนังชื่อ สถานที่ หรือชื่อสิ่งลึกลับ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับรัฐสภา หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา

4.2 ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า 3 ตัวหรือเรียงกันตามลำดับ เช่น aaaabbbb, 11111111, abcdefg

4.3 รหัสผ่านที่ดีควรมีลักษณะดังนี้

4.3.1 ควรมีความยาวอย่างน้อย 8 ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด

4.3.2 ควรมีส่วนประกอบของอักษรอักขระพิเศษหรือตัวเลขประสมกันตามลักษณะ ดังนี้

(1) ตัวอักษรใหญ่เช่น A, B, C, ...

(2) ตัวอักษรเล็กเช่น a, b, c, ...

(3) ตัวเลขเช่น 0, 1, 2, ...

(4) สัญลักษณ์พิเศษเช่น !, @, # , $, ...

5. การเปลี่ยนรหัสผ่าน

5.1 รหัสผ่านเข้าสู่ระบบ (เช่น root, NT Admin ฯลฯ) ต้องเปลี่ยนอย่างน้อยทุก 3 เดือน

5.2 รหัสผ่านของผู้ใช้งานต้องเปลี่ยนอย่างน้อยทุก 6 เดือน

แนวทางการปฏิบัติ : การกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน : กำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดเช่น 30 วัน 60 วัน 90 วัน เป็นต้น

6. การยกเลิกรหัสผ่าน รหัสผ่านของผู้ใช้งานที่ลาออกสิ้นสุดการจ้างงาน หรือย้าย ต้องทำการยกเลิกสิทธิของผู้ใช้งานในระบบทันทีและลบชื่อผู้ใช้งานนั้นออกจากระบบภายใน 30 วันนับจากวันที่ได้รับการอนุมัติให้ลาออกสิ้นสุดการจ้าง หรือย้าย

ส่วนที่ 6
การเข้ารหัสข้อมูล (Cryptographic)

6.1 แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล (Cryptographic Controls) เพื่อกำหนดแนวทางในการจัดทำการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และป้องกันความลับการปลอมแปลง เพื่อให้ได้มาซึ่งความน่าเชื่อถือถูกต้องและความสมบูรณ์ของสารสนเทศ

6.1.1 มาตรการการเข้ารหัสข้อมูล (policy on the Use of Cryptographic Controls)

(1) เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล เช่น อัลกอริทึม RSA, DES, 3DES เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศเพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

(2) อัลกอริทึมที่เรียกใช้ต้องรองรับซอฟต์แวร์ประยุกต์ที่นำไปใช้งานได้ เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

(3) ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า 56 บิตสำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบไม่สมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

(4) เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุก ๆ ปีเพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของเครื่องที่ดำเนินงาน

(5) กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติมให้ติดต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและแนวปฏิบัติฯ

6.1.2 การบริหารจัดการกุญแจ (Key Management)

(1) ข้อมูลที่มีการเข้ารหัสต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพโดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่งและการเปลี่ยนควรกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

(2) กุญแจส่วนตัวที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและจัดเก็บอย่างมั่นคงปลอดภัยเสมอ

(3) การส่งกุญแจถึงผู้รับกุญแจต้องส่งผ่านในช่องทางที่มีความมั่นคงปลอดภัยเสมอ

(4) กุญแจต้องได้รับการเพิกถอนทันทีเมื่อทราบว่ากุญแจมีความเสี่ยงที่จะก่อให้เกิดการล่วงละเมิดทางด้านความมั่นคงปลอดภัย เช่น เมื่อกุญแจส่วนตัว (private key) รั่วไหลไปยังบุคคลอื่น เป็นต้น

(5) การเพิกถอนการใช้งานกุญแจต้องมีการแจ้งให้ผู้เกี่ยวข้องกับกุญแจหรือผู้ที่ใช้งานกุญแจทราบ โดยต้องรวมถึงรหัสกุญแจเหตุผลของการเพิกถอนวันที่และเวลาที่กุญแจถูกเพิกถอน

(6) การทำ Archive กุญแจเมื่อไม่มีการใช้งานกุญแจเป็นระยะเวลานาน ต้องใช้วิธีการ Archive ที่มีความมั่นคงปลอดภัยโดยต้องมีการเข้ารหัสกุญแจที่ถูก Archive ด้วยเสมอ

(7) การทำลายกุญแจต้องทำด้วยความระมัดระวังเป็นพิเศษโดยต้องทำลายด้วยวิธีการทำลายกุญแจแบบมั่นคงปลอดภัย (Secure Deletion) และต้องแน่ใจว่ากุญแจนั้นจะไม่มีความต้องการในการใช้งานถอดรหัสข้อมูลอีกในอนาคต

(8) การกระทำใด ๆ ที่เกี่ยวข้องกับกุญแจต้องได้รับการจัดเก็บบันทึกอย่างมั่นคงปลอดภัยเสมอเพื่อให้สามารถตรวจสอบได้ในภายหลัง

ส่วนที่ 7
ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

7.1 แนวปฏิบัติการกำหนดพื้นที่ที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Areas) เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบสารสนเทศตลอดจนอุปกรณ์คอมพิวเตอร์ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของรัฐสภา โดยแนวปฏิบัตินี้มีผลบังคับใช้กับผู้ใช้งานและผู้ดูแลระบบซึ่งมีส่วนเกี่ยวข้องกับการใช้ระบบสารสนเทศของรัฐสภา

7.1.1 พื้นที่ใช้งานระบบสารสนเทศ (Physical Security Perimeter)

(1) ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวังควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้และประกาศให้รับทราบทั่วกัน

(2) ต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับส่วนหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

(3) หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก เป็นต้น ในพื้นที่ใช้งานระบบสารสนเทศของรัฐสภา ได้แก่ ศูนย์ปฏิบัติการ SOC

ห้อง Server/Data Center ห้อง Network Control หรือห้อง Network Center ห้องเก็บข้อมูลสำรองเพื่อให้เป็นไปตามมาตรฐานสากลที่กำหนดไว้

(4) ไม่อนุญาตให้ถ่ายภาพ บันทึกวิดีโอหรือเสียง ภายในบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Areas) เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

7.1.2 การควบคุมการเข้าออก (Physical Entry Controls) ต้องกำหนดมาตรการการควบคุมการเข้าออกในบริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้าออกได้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น ซึ่งมีแนวทางปฏิบัติดังนี้

(1) ระบุตัวผู้ใช้งานและช่วงเวลาที่มีสิทธิผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

(2) ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

(3) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบ เหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวที่รัฐสภาออกให้ หรือบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

(4) การขออนุญาตเข้ามาปฏิบัติงานในพื้นที่ให้ปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการขออนุญาตเข้าสู่พื้นที่

7.1.3 ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

(1) ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า - ออกของบุคคลเป็นจำนวนมาก

(2) สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

(3) ประตูหน้าต่างของสำนักงานต้องใส่กุญแจเมื่อไม่มีคนอยู่หรือมีการควบคุมการเข้าถึงรูปแบบอื่น ๆ

(4) เครื่องโทรสารหรือเครื่องถ่ายเอกสารควรแยกออกมาจากบริเวณดังกล่าว

(5) แนวทางปฏิบัติสำหรับพื้นที่สำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ เช่น กั้นพื้นที่อย่างรอบด้าน ติดตั้งผนังติดตั้งเหล็กดัดล็อคประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม เช่น ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น

7.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(1) ห้องคอมพิวเตอร์จะต้องมีการควบคุมการเข้า - ออกอย่างเข้มงวด และตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น แผ่นดินไหว หรือน้ำท่วม เป็นต้น

(2) สถานที่ปฏิบัติงานควรจะมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม ทั้งนี้ ในพื้นที่ที่ต้องมีการรักษาความปลอดภัยควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติด้วย

(3) ควรดูแลเรื่องความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอ เพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

7.1.5 การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

(1) ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณควบคุม เป็นต้น

(2) ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

7.1.6 การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Delivery and Loading Areas) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของรัฐสภาโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมาต่างหาก

7.2 แนวปฏิบัติความมั่นคงปลอดภัยของอุปกรณ์ (Equipment) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศในการป้องกันอุปกรณ์จากการสูญหาย ถูกขโมย หรือเสียหายซึ่งอาจส่งผลต่อการดำเนินงาน

7.2.1 การจัดวางและป้องกันอุปกรณ์ (Equipment Siting and Protection)

(1) ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

(2) มีการจัดวางอุปกรณ์ที่ไม่เกี่ยวข้องกับการปฏิบัติงานไว้ภายนอกพื้นที่ปฏิบัติงาน เพื่อป้องกันการเข้าถึงพื้นที่ปฏิบัติงานของผู้ไม่มีส่วนเกี่ยวข้องโดยไม่จำเป็น

(3) มีการจัดเตรียมพื้นที่จัดเก็บอุปกรณ์ที่ปลอดภัย และไม่สามารถเข้าถึงได้โดยง่าย เช่น ตู้หรือลิ้นชักที่มีกุญแจล็อค

(4) ห้ามมิให้มีการสูบบุหรี่ รับประทานอาหารและน้ำดื่ม ในพื้นที่จัดวางอุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศ

(5) ห้ามนำสสารวัตถุอาวุธ และเครื่องมือที่อาจก่อให้เกิดอันตรายกับอุปกรณ์เข้ามาในบริเวณพื้นที่ปฏิบัติงาน นอกจากได้รับการพิจารณาอนุญาตและตรวจสอบความเหมาะสมแล้วเท่านั้น

(6) ทำการติดตั้งระบบป้องกันฟ้าผ่ากับอาคารอย่างเหมาะสม

7.2.2 ระบบสาธารณูปโภคพื้นฐาน (Supporting Utilities) สาธารณูปโภคพื้นฐานในที่นี้หมายถึง สาธารณูปโภคจำพวก น้ำประปา ไฟฟ้า การติดต่อสื่อสาร เครื่องปรับอากาศ ระบบบำบัดของเสีย เป็นต้น โดยต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรองสำหรับระบบที่สำคัญ เช่น ระบบ Security ระบบ SIEM (security information event management) เป็นต้น โดยมีแนวทางปฏิบัติดังนี้

(1) ต้องมีระบบไฟฟ้าสำรองอัตโนมัติเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่องและต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 2 ครั้ง

(2) ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

(3) ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัยพิบัติ เช่น อัคคีภัย อย่างน้อยปีละ 2 ครั้ง

(4) ไม่ควรกระทำการใด ๆ ให้เกิดมีประกายไฟหรือเปลวไฟ

(5) ระบบที่สำคัญของรัฐสภาจะต้องมีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อลดความสูญเสียที่อาจเกิดขึ้นจากผลกระทบจากเหตุการณ์ภัยพิบัติหรือเหตุการณ์ไม่คาดคิด

7.2.3 การเดินสายไฟฟ้าหลัก (Main Power Cable) และสายเคเบิลหลัก(Backbone Cable)(Cabling Security)

(1) ต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดินผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย ซึ่งมีแนวทางปฏิบัติ เช่น บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงานและมีการติดตั้งตู้พักสายต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

(2) ควรจัดเก็บสายเคเบิลทั้งหมดที่ใช้ในการรับ – ส่งข้อมูลไว้ในรางหรืออุปกรณ์ป้องกัน เพื่อป้องกันการดักจับข้อมูลหรืออุบัติเหตุที่อาจทำให้สายขาดหรือชำรุดได้

(3) ควรแยกสายไฟทั้งหมดออกจากสายเคเบิลในการรับ - ส่งข้อมูล เพื่อป้องกันสัญญาณรบกวน

7.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(1) ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ 1 ครั้งหรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุก 3 เดือน เป็นต้น

(2) ทุกครั้งที่ต้องมีการซ่อมแซมอุปกรณ์ใด ๆ จะต้องทำการบันทึกรายการซ่อมบำรุงรักษาอุปกรณ์ดังกล่าวทุกครั้ง

(3) ควรบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่าง ๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้

(4) กำหนดให้บุคลากรที่ผ่านการฝึกอบรมและได้รับอนุญาตเท่านั้น ที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่าง ๆ ในกรณีที่ใช้บริการซ่อมบำรุงจากผู้ผลิตหรือผู้จัดจำหน่าย จะต้องกำหนดเงื่อนไขในการบำรุงรักษาอย่างละเอียด

7.2.5 การนำสินทรัพย์ออกนอกสถานที่ (Removal of Assets)

(1) การเคลื่อนย้ายสินทรัพย์ของรัฐสภา ต้องทำเป็นบันทึกและขออนุญาตอย่างถูกต้องในการเคลื่อนย้ายซึ่งมีแนวทางปฏิบัติดังนี้

(1.1) ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และสินทรัพย์ด้วย การย้ายสถานที่ทำงาน เป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของรัฐสภาได้

(1.2) ข้อมูลที่มีความสำคัญมากรวมถึงข้อมูลในคอมพิวเตอร์แบบพกพา (Notebook) ควรมีการเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูลเว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

(1.3) ผู้ใช้งานจะต้องแน่ใจว่าข้อมูลสำคัญใด ๆ ต้องมีการเข้ารหัสเมื่อถูกจัดเก็บอยู่ในฮาร์ดดิสก์

(1.4) ผู้ที่มีส่วนร่วมในการเคลื่อนย้ายสถานที่ทำงาน จะต้องมีการตรวจตราสถานที่ซึ่งย้ายสินทรัพย์ออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ มีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร เช่น ตู้เก็บแฟ้มเอกสาร ห้องเก็บรักษาแฟ้มข้อมูล ห้องนิรภัย เป็นต้น

(1.5) ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้าย เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของรัฐสภา

(2) เมื่อมีการนำอุปกรณ์และสื่อที่เคลื่อนย้ายได้ออกไปใช้นอกสถานที่ ผู้ที่รับผิดชอบควรมีการป้องกันการสูญหาย

(3) การเคลื่อนย้ายทรัพย์สินใด ๆ ของรัฐสภา จะต้องได้รับการอนุญาตอย่างเป็นลายลักษณ์อักษรและควรจะมีการเก็บบันทึกการอนุญาตดังกล่าว

(4) ต้องกำหนดระยะเวลาที่ต้องการยืมทรัพย์สิน หรือเวลาที่จะทำการเคลื่อนย้ายทรัพย์สินและต้องบันทึกการเคลื่อนย้ายทรัพย์สินทุกครั้ง

7.2.6 การป้องกันอุปกรณ์และสินทรัพย์ภายนอกสถานที่ (Security of Equipment and Assets Off - Premises)

(1) ปฏิบัติตามคำแนะนำในการใช้งานจากเจ้าของผลิตภัณฑ์ของอุปกรณ์และสินทรัพย์อย่างเคร่งครัด เช่น ไม่วางตากแดด หรือใกล้ความร้อน

(2) ไม่วางอุปกรณ์และสินทรัพย์ไว้ในที่สาธารณะ โดยขาดการดูแลหรือเฝ้าระวัง

(3) ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของรัฐสภา เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน

7.2.7 การทำลายหรือนำกลับมาใช้งานของอุปกรณ์ (Secure Disposal or Reuse of Equipment)

(1) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ (Secure Disposal of Reuse of Equipment) ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

(2) การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่จะต้องถูกกำหนดขั้นตอนการดำเนินงาน ในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้แน่ใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งโดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

(3) จะต้องกำหนดขั้นตอนการดำเนินงาน ในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้แน่ใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งไปแล้ว โดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

(4) การทำลายหรือนำกลับมาใช้ใหม่ของอุปกรณ์ต้องได้รับอนุญาตจากเจ้าของอุปกรณ์ก่อนเสมอ

7.2.8 อุปกรณ์ที่ไม่อยู่ระหว่างการใช้งาน (Unattended User Equipment)

(1) ควรใช้งานซอฟต์แวร์รักษาจอภาพ (Screen Saver) โดยตั้งเวลาให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน

(2) ทำการ log out ออกจากโปรแกรมใช้งาน หรือ บริการระบบเครือข่ายเมื่อไม่ใช้งาน

7.2.9 (Clear Desk and Clear Screen)

(1) ข้าราชการ พนักงานและลูกจ้างต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็น “ชั้นลับมาก” ไว้ในที่สามารถพบเห็นได้ง่าย (Clear Desk) โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

(2) เมื่อสั่งพิมพ์งานเอกสารที่มีข้อมูลสำคัญ ผู้สั่งพิมพ์ต้องทำการจัดเก็บเอกสารโดยทันที

ส่วนที่ 8
ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

8.1 แนวปฏิบัติด้านขั้นตอนและความรับผิดชอบในการปฏิบัติงาน (Operational Procedures and Responsibilities) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการบริหารจัดการอุปกรณ์ประมวลผลสารสนเทศให้มีความถูกต้องและปลอดภัย

8.1.1 ขั้นตอนการปฏิบัติงานของระบบงาน (Documented Operating Procedures)

(1) ต้องกำหนดให้มีการจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานที่จำเป็นในการปฏิบัติงาน

(2) จัดทำคู่มือการแก้ปัญหาระบบเพื่อการแก้ไขปัญหาที่รวดเร็วขึ้น

(3) จัดทำคู่มือในการเฝ้าระวังระบบ

(4) จัดทำรายชื่อผู้ติดต่อทั้งภายในและภายนอกที่เกี่ยวข้องของแต่ละระบบ ในกรณีที่ต้องแก้ไขระบบในกรณีเร่งด่วน

8.1.2 การเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Change Management)

(1) ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Change management) ผู้ดูแลระบบสารสนเทศนั้น ต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้ผู้ที่เกี่ยวข้องทราบ

(2) สำหรับการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศระบบเครือข่ายจะต้อง ปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง (Change Management Procedure)

(3) ก่อนทำการเปลี่ยนแปลงแก้ไขบนเครื่องให้บริการจริง (Production Machine) ต้องมีการวางแผน ทดสอบ และได้รับการอนุมัติก่อนเสมอ

(4) ต้องมีการจัดทำและทดสอบขั้นตอนในการย้อนกลับ (fallback procedure) ระบบในกรณีที่การเปลี่ยนแปลงไม่สมบูรณ์หรือเกิดปัญหา

(5) ต้องมีการพิจารณาวิเคราะห์ผลกระทบจากการขอเปลี่ยนแปลงแก้ไขระบบ และหาแนวทางในการบริหารจัดการผลกระทบนั้น ๆ

(6) มีการจัดทำกระบวนการขอเปลี่ยนแปลงเร่งด่วน ในกรณีที่เกิดเหตุการณ์ที่ต้องการการแก้ไขเปลี่ยนแปลงอย่างเร่งด่วน

8.1.3 การบริหารจัดการความต้องการทรัพยากรสารสนเทศ (Capacity Management)

โดยมีการกำหนดแนวทางในการเฝ้าระวังทรัพยากรระบบที่มีความสำคัญอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าทรัพยากรระบบมีเพียงพอต่อความต้องการใช้งาน

(1) มีการกำหนดแนวทางในการเฝ้าระวังและปรับค่าระบบ (Tuning) ตามความเหมาะสม เพื่อเพิ่มประสิทธิภาพในการทำงานของระบบ

(2) มีการจัดทำแผนความต้องการทรัพยากร (Capacity Plan) สำหรับระบบที่มีความสำคัญ เพื่อให้มั่นใจว่าระบบจะมีทรัพยากรเพียงพอต่อการใช้งานเสมอ

8.1.4 การแยกเครื่องเพื่อการพัฒนา ทดสอบ และใช้งานจริง (Separation of Development, Testing and Operational Environments)

(1) ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

(2) ในขั้นตอนการทดสอบระบบ ต้องไม่ใช้ข้อมูลจริงที่มีความสำคัญในการทดสอบ

8.2 แนวปฏิบัติด้านการป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection from Malware) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากซอฟต์แวร์ไม่ประสงค์ดี

การป้องกันซอฟต์แวร์และสารสนเทศของรัฐสภา ให้ปลอดภัยจากการถูกทำลายจากซอฟต์แวร์ที่ไม่ประสงค์ดี (Controls against Malware)

ต้องจัดให้มีการติดตั้งและใช้งานซอฟต์แวร์ป้องกันไวรัส เพื่อป้องกันความเสียหายและการรั่วไหลของข้อมูลโดยมีแนวทางปฏิบัติ ดังนี้

8.2.1 ห้ามนำเครื่องคอมพิวเตอร์ซอฟต์แวร์หรือข้อมูลที่ไม่มั่นใจว่าติด malware มาติดตั้งใช้งาน

8.2.2 ควรสำรองข้อมูลสำคัญเก็บไว้ในที่ที่ปลอดภัย เช่น สื่อจัดเก็บข้อมูลแบบพกพาหรือบนเนื้อที่ Server ที่รัฐสภาจัดสรรไว้ให้ เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัส

8.2.3 ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัส ที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่รัฐสภาจัดหาให้

8.2.4 ผู้ใช้งานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอและแจ้งให้ผู้ดูแลระบบทราบ หากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

8.2.5 ผู้ใช้งานควรแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติหรือเมื่อสงสัยว่ามีการติดไวรัส

8.3 แนวปฏิบัติด้านการสำรองข้อมูล (Backup) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภาในการป้องกันการสูญเสียข้อมูล

การสำรองข้อมูล (Information Backup) มีแนวปฏิบัติ ดังนี้

8.3.1 ผู้ดูแลระบบสารสนเทศที่สำคัญนั้น ๆ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

8.3.2 ผู้ดูแลระบบต้องบันทึกรายละเอียดการสำรองข้อมูล โดยมีรายละเอียดเวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูลและชนิดของข้อมูลที่บันทึก

8.3.3 กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

8.3.4 ผู้ดูแลระบบต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสม เพื่อให้สามารถกู้ข้อมูลกลับคืนได้ป้องกันระบบจากการถูกโจมตีหรือความเสียหายที่อาจเกิดขึ้น

8.3.5 ผู้ดูแลระบบต้องควบคุมความปลอดภัยของข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

8.4 แนวปฏิบัติด้านการเฝ้าระวังและบันทึกเหตุการณ์ (Logging and Monitoring) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการบันทึกเหตุการณ์และรวบรวมหลักฐานที่เกี่ยวข้อง เพื่อใช้ในการตรวจสอบและวิเคราะห์หาสาเหตุเพื่อหามาตรการในการป้องกันในอนาคต

8.4.1 การบันทึกเหตุการณ์ (Event Logging)

(1) ให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบและเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ ตามระยะเวลาที่กำหนดไว้ซึ่งประกอบด้วย

(1.1) User ID

(1.2) วันเวลาและรายละเอียดที่สำคัญ เช่น การเข้าระบบและการออกจากระบบ

(1.3) ระบุเครื่องปลายทางหรือที่ตั้ง (ถ้ามี)

(1.4) บันทึกของการพยายามเข้าสู่ระบบทั้งสำเร็จและไม่สำเร็จหรือล้มเหลว

(1.5) บันทึกของการพยายามเข้าสู่ข้อมูลและทรัพยากรทั้งสำเร็จและไม่สำเร็จหรือล้มเหลว

(1.6) การเปลี่ยนค่า Configuration ของระบบ

(1.7) การใช้สิทธิพิเศษ เช่น Administrator หรือ Root

(1.8) การใช้ยูทิลิตี้และซอฟต์แวร์ประยุกต์ของระบบ

(1.9) การเข้าถึงไฟล์และชนิดของการเข้าถึง

(1.10) Network Address และ Protocol

(1.11) สัญญาณเตือนที่เพิ่มขึ้นโดยระบบการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(1.12) การทำงานและไม่ทำงานของระบบการป้องกัน เช่น ระบบป้องกันไวรัส และ IDS

(2) การตรวจสอบการใช้งานระบบ (Monitoring System Use) เพื่อตรวจสอบการใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอโดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด มีแนวทางปฏิบัติดังนี้

(2.1) การระบุตัวตนในการเข้าถึงประกอบด้วย

1) User ID

2) วันเวลาและรายละเอียดที่สำคัญ

3) ชนิดของเหตุการณ์

4) การเข้าถึงไฟล์

5) ซอฟต์แวร์หรือยูทิลิตี้ที่ใช้

(2.2) การดำเนินการเกี่ยวกับสิทธิของผู้ใช้งาน

1) การใช้บัญชีผู้ใช้งานแบบสิทธิพิเศษ เช่น Administrator, Root หรือ Supervisor

2) การเริ่มต้นและหยุดของระบบ

3) อุปกรณ์ที่นำมาเชื่อมต่อ

(2.3) การพยายามเข้าถึงของผู้ที่ไม่มีสิทธิ

1) การล้มเหลวหรือยกเลิกของผู้ใช้งาน

2) การล้มเหลวหรือยกเลิกการกระทำที่เกี่ยวกับข้อมูลหรือทรัพยากรอื่น ๆ

3) การฝ่าฝืนแนวปฏิบัติการเข้าถึงและการแจ้งเตือนของ Network Gateway และ Firewall

4) การแจ้งเตือนของ IDS

(2.4) ระบบแจ้งเตือนหรือความล้มเหลว

1) ศูนย์แจ้งเตือนหรือข้อความ

2) Log ของระบบที่มีการยกเว้น

3) การแจ้งเตือนของ Network Management

4) สัญญาณเตือนที่เพิ่มขึ้นโดยระบบการควบคุมการเข้าถึงหรือควบคุมการใช้งาน

(2.5) การเปลี่ยนแปลงหรือพยายามเปลี่ยนแปลงการตั้งค่าและการควบคุมระบบรักษาความปลอดภัย

(3) การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging) การบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้นและดำเนินการแก้ไขตามสมควร ดังนี้

(3.1) ทบทวน Log ที่ผิดพลาดเพื่อความมั่นใจว่าความผิดพลาดนั้นได้มีการตัดสินใจที่ดีแล้ว

(3.2) ทบทวนปริมาณ Log ที่มีการแก้ไขเพื่อความมั่นใจว่ามีการควบคุมที่เข้มงวดและกระทำไปตามสิทธิที่ได้รับ

8.4.2 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information) เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาตจึงควรพิจารณาเรื่องดังต่อไปนี้

(1) การเปลี่ยนแปลงชนิดของข้อความที่ถูกบันทึก

(2) Log ที่ถูกแก้ไขหรือถูกลบ

(3) ความจุของพื้นที่ในการจัดเก็บ Log ที่ไม่เพียงพอทำให้ไม่สามารถจัดเก็บ Log ได้

(4) ระยะเวลาในการจัดเก็บและการ Backup Log

8.4.3 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs) กิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบควรมีการเก็บ Log โดย Log เหล่านี้ควรมีมาตรการในการป้องกัน และมีการสอบทานอย่างสม่ำเสมอ Log ที่จะบันทึกประกอบด้วย

(1) เวลาที่เกิดเหตุการณ์ทั้งที่สำเร็จและล้มเหลว

(2) ข้อมูลที่เกี่ยวกับเหตุการณ์ (เช่นไฟล์ที่เกี่ยวข้อง) หรือการล้มเหลว (เช่นความผิดพลาดที่เกิดขึ้นและการแก้ไขต่าง ๆ)

(3) บัญชีผู้ใช้งานและผู้ดูแลระบบหรือผู้ปฏิบัติการที่เกี่ยวข้อง

(4) กระบวนการที่เกี่ยวข้อง

8.4.4 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock Synchronization) การตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานโดยการตั้งเวลาด้วย Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลา หากเครื่องคอมพิวเตอร์ของรัฐสภา ถูกบุกรุกโดยสามารถอ้างอิงผู้ให้บริการดังต่อไปนี้

ภายในฝ่ายรัฐสภา การตั้งเวลาของเครื่อง Server และเครื่องคอมพิวเตอร์ทุกเครื่องในรัฐสภา ให้ตั้งเวลาด้วย Network Time Protocol (NTP) ไปยัง Server ที่ให้บริการข้อมูลเวลา คือ

(1) clock1.cattelecom.com หรือ 10.9.1.19

(2) clock2.cattelecom.com หรือ 172.16.9.91

8.5 แนวปฏิบัติด้านควบคุมซอฟต์แวร์ปฏิบัติงาน (Control of Operational Software) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการรักษาความสมบูรณ์ (Integrity) ของระบบปฏิบัติงาน

8.5.1 การควบคุมการติดตั้งซอฟต์แวร์ (Installation of Software on Operational Systems)

(1) ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

(2) มีการบริหารจัดการเวอร์ชั่นของซอฟต์แวร์ และมีการจัดเก็บซอฟต์แวร์เวอร์ชั่นก่อนหน้าไว้ในกรณีที่มีความจำเป็นต้องทำการถอยกลับไปใช้เวอร์ชั่นก่อนหน้านี้

8.6 แนวปฏิบัติด้านการบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการป้องกันการใช้ช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์เพื่อหาผลประโยชน์หรือสร้างความเสียหายให้องค์กร

8.6.1 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์(Management of Technical Vulnerability) ต้องดำเนินการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว ซึ่งมีแนวทางปฏิบัติดังต่อไปนี้

(1) ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน เช่น การเฝ้าระวังภัยคุกคามการประเมินความเสี่ยงของภัยคุกคาม การ Patch ปิดช่องโหว่ในระบบการตรวจสอบสินทรัพย์ที่ได้จัดส่วนหมู่ไว้ เป็นต้น

(2) ต้องร่วมกันวิเคราะห์ความเสี่ยงและประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก 6 เดือน

(3) ในกรณีที่จะทำการ Update Patch ของระบบสำคัญ ๆ ต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายต่อระบบ แต่ถ้าไม่สามารถ Update Patch ได้ก็ให้พิจารณาดังต่อไปนี้

(3.1) ปิด Service หรือการทำงานที่เกี่ยวข้องกับช่องโหว่

(3.2) ปรับปรุงหรือเพิ่มระดับ Security ในการเข้าถึงที่บริเวณรอบนอกเครือข่าย เช่น เพิ่ม Firewall หรือ IPS (Intrusion Prevention System) เป็นต้น

(3.3) เพิ่มการเฝ้าระวังเพื่อตรวจจับหรือป้องกันการโจมตีเครือข่าย

(3.4) สร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

(3.5) เก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

(3.6) กระบวนการบริหารจัดการช่องโหว่ที่มีการดำเนินการ เช่น การเฝ้าระวังต้องมั่นใจว่ามีประสิทธิภาพและประสิทธิผล

(3.7) ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญ

8.6.2 การจำกัดสิทธิในการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

(1) ต้องจัดทำรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เช่น PC, Laptop เป็นต้น

(2) SOC Manager ต้องทำการตรวจสอบและอนุมัติรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เพื่อจัดทำเป็นรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานในองค์กร (Baseline) สำหรับเครื่องผู้ใช้งานทั่วไป

(3) ห้ามผู้ใช้งานทำการติดตั้งซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์ รวมถึงซอฟต์แวร์อื่น ๆ ที่ไม่ได้รับอนุญาตให้ใช้งานในองค์กร

(4) หากผู้ใช้งานต้องการติดตั้งซอฟต์แวร์ที่อยู่นอกเหนือรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานในองค์กร (Baseline) จะต้องทำการขออนุมัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง (Change Management Procedure)

(5) การติดตั้งซอฟต์แวร์บนเครื่องผู้ใช้งานจะต้องกระทำโดยผู้ดูแลระบบเท่านั้น โดยผู้ดูแลระบบต้องทำการจำกัดสิทธิในการติดตั้งซอฟต์แวร์บนเครื่องของผู้ใช้งานอย่างเหมาะสม

(6) ผู้ดูแลระบบจะต้องทำการตรวจสอบการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตตามขั้นตอนที่กำหนดในระเบียบการปฏิบัติงาน เรื่อง การตรวจสอบซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน (Review of Disallow Software Usage Procedure) อย่างน้อยปีละ 1 ครั้ง

8.7 แนวปฏิบัติด้านการประเมินระบบสารสนเทศ (Information Systems Audit Considerations) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการบรรเทาผลกระทบต่อระบบปฏิบัติการอันเนื่องมาจากกิจกรรมต่าง ๆ ที่เกิดจากกระบวนการตรวจสอบระบบ

8.7.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls)

(1) ระบบงานสำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของรัฐสภา ต้องวางแผนการตรวจประเมินระบบทั้งหมด โดยการตรวจประเมินที่จะดำเนินการจะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของรัฐสภาน้อยที่สุด

(2) การตรวจสอบระบบสารสนเทศ จะต้องได้รับการอนุมัติให้ดำเนินการอย่างเป็นลายลักษณ์อักษร โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่องการจัดการช่องโหว่ (Vulnerability Management Procedure)

8.7.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of Information Systems Audit Tools) ต้องมีการกำหนดวิธีการปฏิบัติงานที่ชัดเจนในการใช้งานซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ เพื่อป้องกันมิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ

ส่วนที่ 9
ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

9.1 แนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการป้องกันสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศบนระบบเครือข่ายให้มีความมั่นคงปลอดภัย

9.1.1 การป้องกันการใช้งานเครือข่าย (Network Controls)

(1) ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

(1.1) ระบบเครือข่ายภายใน อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายในรัฐสภา ได้แก่ Router, Switch และ HUB มีข้อปฏิบัติดังนี้

• อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่ายต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password

• การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาต

• ผู้ดูแลระบบต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ

• ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ซอฟต์แวร์ระบบ การเข้ารหัสข้อมูลอัตโนมัติ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

• ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลลับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

(1.2) ระบบ Remote Access อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS), Remote VPN, Remote Router มีข้อปฏิบัติดังนี้

• อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

• เมื่อเสร็จสิ้นการทดสอบการใช้งานอุปกรณ์ RAS แล้วให้ลบ User/Password ที่ใช้ในงานทดสอบทันที

• อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่า Default Community, Default Username และ Default Password

(1.3) อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายในรัฐสภา มีข้อปฏิบัติดังนี้

• ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password

• ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

• ให้เปิด Service Port ที่จำเป็นเท่านั้นส่วน Port ที่ไม่ใช้งานให้ปิดทั้งหมด และต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง

• ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

• เมื่อจบการใช้งานที่ Console ต้อง Log - off User นั้นโดยทันที

• ผู้ดูแลระบบต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้งโดยสอดคล้องกับความสำคัญของระบบ

(1.4) อุปกรณ์ PC Terminal มีข้อปฏิบัติดังนี้

• ให้เปิด Service Port ที่จำเป็นเท่านั้นส่วน port ที่ไม่ใช้งานให้ทำการปิดให้หมดและต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง

• ต้องติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น

• การ Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

(2) การป้องกันการใช้งานเครือข่าย

(2.1) ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของรัฐสภา โดยไม่ได้รับอนุญาต

(2.2) ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย เช่น การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของรัฐสภาเอง

9.1.2 ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย (Security of Network Services) ต้องจัดทำข้อกำหนดหรือข้อตกลงของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกัน ซึ่งมีแนวทางปฏิบัติ ดังนี้

(1) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งาน เพื่อควบคุมให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับ อนุญาตเท่านั้น

(2) ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(3) ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย

(4) ระบบเครือข่ายทั้งหมดของรัฐสภา ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกรัฐสภา ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

(5) ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังรัฐสภา และต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะ และติดต่อกับระบบงานที่กำหนดไว้เท่านั้น หากเป็นไปได้ควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ รัฐสภา ทั้งทาง Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายรัฐสภาได้โดยอิสระ

9.1.3 การแบ่งแยกเครือข่าย (Segregation in Networks) ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย

9.2 แนวปฏิบัติด้านการแลกเปลี่ยนสารสนเทศ (Information Transfer) ในการรักษาไว้ซึ่งความมั่นคงปลอดภัยในการแลกเปลี่ยนสารสนเทศทั้งภายในองค์กร และกับหน่วยงานภายนอก

9.2.1 ขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Transfer Policies and Procedures) ขั้นตอนปฏิบัติและมาตรการสำหรับการถ่ายโอนสารสนเทศ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร โดยผ่านทางช่องทางการสื่อสารทุกชนิด ควรพิจารณาดังต่อไปนี้

(1) การป้องกันจากการถูกดักจับคัดลอกแก้ไขส่งผิดเส้นทางและการทำลายข้อมูล

(2) การตรวจจับและป้องกัน Source Code ที่ไม่พึงประสงค์ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

(3) การป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File)

(4) แนวทางปฏิบัติต้องสอดคล้องกับแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

(5) การสื่อสารไร้สายต้องคำนึงถึงความเสี่ยงจะที่เกิดขึ้นด้วย

(6) ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนแนวปฏิบัติหรือกฎระเบียบของรัฐสภา เช่น การหมิ่นประมาท การข่มขู่หรือ ก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ เป็นต้น

(7) เทคนิคการเข้ารหัสเพื่อปกป้องความลับความสมบูรณ์และความถูกต้องของสารสนเทศ

(8) แนวทางในการเก็บรักษาและทำลายจดหมายธุรกิจต้องเป็นไปตามที่กฎหมายกำหนด

(9) ไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

(10) ควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่อ mail อัตโนมัติไปนอกรัฐสภา

(11) เตือนผู้ใช้งานให้มีความระมัดระวัง เช่น ข้อมูลสำคัญต้องไม่รั่วไหลโดยการดักฟังหรือได้ยินแบบไม่ตั้งใจในขณะใช้โทรศัพท์ ได้แก่

(11.1) คนที่อยู่บริเวณใกล้ ๆ ในขณะที่ใช้โทรศัพท์เคลื่อนที่

(11.2) การดักฟังหรือการแอบฟังทางสายโทรศัพท์

(11.3) คนที่อยู่ฝั่งตรงข้าม

(12) เตือนผู้ใช้งานเกี่ยวกับปัญหาในการใช้เครื่องโทรสาร เช่น

(12.1) การเข้าถึงของผู้ที่ไม่ได้รับอนุญาตเพื่อดึงข้อมูลภายในเครื่องที่จัดเก็บไว้

(12.2) การตั้งโปรแกรมในการส่งไปยังเลขหมายปลายทางโดยตั้งใจและไม่ตั้งใจ

(12.3) การส่งเอกสารหรือข้อความผิดเลขหมายโดยการโทรที่ผิดพลาดหรือบันทึกเลขหมายผิด

(12.4) เครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่จะมีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งที่ผิดพลาดซึ่งจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

9.2.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Agreements on Information Transfer) ในการแลกเปลี่ยนสารสนเทศ ควรคำนึงถึงความปลอดภัยในการแลกเปลี่ยน ดังต่อไปนี้

(1) การบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสารการส่งและการรับ

(2) การแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสารการส่งและการรับ

(3) กระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

(4) มาตรฐานทางเทคนิคขั้นต่ำในการบรรจุและส่งออก

(5) สัญญาข้อตกลง

(6) มาตรฐานในการระบุตัวผู้ส่งเอกสาร

(7) ใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญเพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและเป็นการปกป้องสารสนเทศอย่างเหมาะสม

(8) ความเป็นเจ้าของและความรับผิดชอบสำหรับการปกป้องข้อมูลลิขสิทธิ์ การปฏิบัติตามใบอนุญาตการใช้งานซอฟต์แวร์และค่าตอบแทนต่าง ๆ

(9) การควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น กุญแจรหัส

9.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) การป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์ควรพิจารณา ดังต่อไปนี้

(1) ปกป้องข้อความจากผู้ที่ไม่ได้รับอนุญาตไม่ให้มีการแก้ไขข้อความหรือปฏิเสธบริการ (Denial of Service)

(2) ต้องมั่นใจว่าที่อยู่ปลายทางและการส่งข้อความถูกต้อง

(3) มีความน่าเชื่อถือและสามารถใช้บริการได้

(4) ข้อกำหนดทางกฎหมาย เช่น การใช้ลายมืออิเล็กทรอนิกส์

(5) การใช้บริการแบบสาธารณะ ต้องระวังในการรับ - ส่งข้อมูลที่เป็นความลับของรัฐสภา เช่น การ Chat การแชร์ไฟล์ เป็นต้น

(6) การระบุตัวตนในการควบคุมการเข้าถึงจากระบบเครือข่ายสาธารณะจะต้องเข้มงวด

9.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-disclosure Agreements) ต้องจัดให้มีการลงนามในสัญญาระหว่างผู้ใช้งานและรัฐสภา ว่าจะไม่เปิดเผยความลับของรัฐสภา ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 3 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว ข้าราชการ พนักงาน ลูกจ้าง และบุคลากรจากหน่วยงานภายนอก รวมถึงนักศึกษาฝึกงานทุกคน จะต้องลงนามในสัญญารักษาความลับ (หรือสัญญาไม่เปิดเผยข้อมูล) ซึ่งเป็นส่วนหนึ่งของเงื่อนไขและข้อกำหนดในการจ้างหรือการฝึกงาน โดยให้จัดเก็บหลักฐานการลงนาม เพื่อพร้อมรับการตรวจสอบ

ส่วนที่ 10

การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

10.1 แนวปฏิบัติด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Requirements of Information Systems) เพื่อเป็นส่วนประกอบสำคัญในการบริหารจัดการระบบสารสนเทศตลอดวงจรของชีวิตของการพัฒนาระบบ ทั้งนี้ รวมถึงระบบสารสนเทศที่ให้บริการบนเครือข่ายสาธารณะด้วย

10.1.1 การจัดทำข้อกำหนดด้านความมั่นคงปลอดภัย (Information Security Requirements Analysis and Specification)

(1) ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศจะต้องถูกระบุไว้ในข้อกำหนดในการพัฒนาระบบใหม่หรือการปรับปรุงระบบที่มีอยู่เดิม โดยข้อกำหนดควรครอบคลุมหัวข้อต่อไปนี้

(1.1) การพิสูจน์ตัวตนและการกำหนดสิทธิของผู้ใช้งานระบบ

(1.2) บทบาทหน้าที่ของผู้ใช้งานระบบและเจ้าหน้าที่ดูแลระบบ

(1.3) แนวทางในการป้องกันสินทรัพย์ที่เกี่ยวข้อง โดยเฉพาะในด้านการรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้

(2) ข้อกำหนดด้านความมั่นคงปลอดภัยจะต้องถูกระบุไว้ในเอกสารข้อกำหนด (Terms of Reference (TOR)) และ/หรือในขั้นตอนการเก็บข้อมูลความต้องการของผู้ใช้ในระหว่างการพัฒนาหรือการปรับปรุงระบบ

(3) ในการจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการจัดซื้อจัดจ้างทรัพยากรสารสนเทศนั้น ควรครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

(3.1) มีระบบในการการระบุและพิสูจน์ตัวตน (User Identification and authentication)

(3.2) มีระบบควบคุมและตรวจสอบสิทธิ์ในการเข้าถึง (Access control and authorization)

(3.3) มีกระบวนการหรือการป้องกันข้อมูลให้มีความครบถ้วนสมบูรณ์ (Integrity Protection)

(3.4) สามารถรองรับการตั้งค่าเพื่อใช้ในการตรวจสอบระบบ (Audit Requirements)

(3.5) สามารถกำหนดค่าต่าง ๆ ในระบบให้สอดคล้องกับข้อกำหนดในแนวปฏิบัติของศูนย์ปฏิบัติการ SOC (System Configuration)

(3.6) สามารถรองรับการปฏิบัติตามข้อกำหนดเชิงกฎหมาย และระเบียบปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

(3.7) สามารถรองรับหรือสนับสนุนการกู้คืนระบบในกรณีเกิดเหตุการณ์ภัยพิบัติ (Disaster Recovery)

(3.8) การรักษาความลับในการพัฒนาระบบสารสนเทศ เพื่อไม่ให้บุคคลภายนอกทราบ (Need for development confidentiality) เป็นต้น

(4) กำหนดให้มีการตรวจสอบความถูกต้องในการติดตั้งระบบ และความถูกต้องในการทำงานของฟังก์ชั่นต่าง ๆ ในแต่ละขั้นตอนของการพัฒนาระบบ (The development lifecycle) โดยจากทีมพัฒนาระบบและ/หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Security Specialist) เพื่อให้แน่ใจว่ามาตรการด้านความมั่นคงปลอดภัยที่ได้กำหนดขึ้นมานั้น ได้ถูกนำไปออกแบบ พัฒนา และทดสอบ ตามที่กำหนดไว้

(5) ข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้ข้างต้น จะต้องถูกนำมาใช้ในการประเมินก่อนการจัดซื้อซอฟต์แวร์สำเร็จรูปมาใช้ในการให้บริการของฝ่ายรัฐสภาด้วยเช่นกัน

(6) การจัดซื้อจัดจ้างภายในขอบเขตการดำเนินงานของเอกสารแนวปฏิบัติฉบับนี้ ให้มีการดำเนินงานตามกระบวนการจัดซื้อ จัดจ้างของรัฐสภา

10.1.2 การป้องกันบริการแอปพลิเคชันบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks) สารสนเทศของบริการแอปพลิเคชันต่าง ๆ ที่มีการส่งผ่านทางเครือข่ายสาธารณะต้องมีการป้องกันจากการฉ้อโกง การปฏิเสธ การเปิดเผยและการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต โดยต้องมีการพิจารณาส่วนต่อไปนี้

(1) สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available Information) การป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะครอบคลุมถึงซอฟต์แวร์ ข้อมูล และสารสนเทศอื่น ๆ ที่ต้องการความถูกต้องในระดับสูง ที่จะถูกเผยแพร่ออกสู่สาธารณะ จะต้องมีการป้องกันที่ดีเช่น ลายมือชื่ออิเล็กทรอนิกส์ การเข้าถึงจากเครือข่ายสาธารณะควรจะตรวจสอบความผิดพลาดต่าง ๆ และได้รับการอนุมัติก่อนควรมีการควบคุม ดังต่อไปนี้

(1.1) สารสนเทศนั้นต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล

(1.2) สารสนเทศที่นำเข้าและประมวลผลโดยระบบจะต้องสมบูรณ์และถูกต้องตามสภาวะกาล

(1.3) สารสนเทศสำคัญจะต้องถูกปกป้องในระหว่างที่มีการรวบรวมประมวลผลและจัดเก็บ

(1.4) การป้องกันการโจมตีจากหน้าเว็บไซต์เพื่อไม่ให้มีการเข้าถึงเครือข่ายของรัฐสภา

10.1.3 การป้องกันธุรกรรมของบริการแอปพลิเคชัน(Protecting Application Services Transactions)

(1) เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ – ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศการเปิดเผยสารสนเทศ หรือการสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

(2) เส้นทางการสื่อสารระหว่างคู่ค้ามีการเข้ารหัส

(3) ข้อตกลงที่ใช้ในการสื่อสารระหว่างคู่ค้ามีความมั่นคงปลอดภัย

(4) ต้องมั่นใจว่าข้อมูลที่เกี่ยวกับรายละเอียดในการทำธุรกรรมไม่สามารถเข้าถึงได้จากเครือข่ายสาธารณะ เช่น เก็บไว้ใน Intranet และไม่สามารถเข้าถึงโดยผ่าน Internet ได้

(5) เมื่อมีการใช้อำนาจที่เชื่อถือได้ เช่น ลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรองอิเล็กทรอนิกส์จะถือได้ว่ากระบวนการจัดการนั้นมีความมั่นคงปลอดภัย

10.2 แนวปฏิบัติด้านความมั่นคงปลอดภัยในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and Support Processes) เป็นองค์ประกอบสำคัญในการออกแบบและพัฒนาระบบสารสนเทศ

10.2.1 แนวปฏิบัติการพัฒนาระบบอย่างปลอดภัย (Secure Development)

(1) ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย เป็นต้น

(2) ในการพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์ (Software Development Lifecycle) โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งาน ตลอดไปจนถึงการยกเลิกการใช้งานระบบ

(3) ในขั้นตอนการพัฒนาระบบสารสนเทศต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ โดยคำนึงถึงความต้องการในด้านต่าง ๆ ดังต่อไปนี้

(3.1) การป้องกันข้อมูลจากการถูกเปิดเผยโดยไม่ได้รับอนุญาต (Protection from disclosure)

(3.2) การป้องกันข้อมูลจากการถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต (Protection from alteration)

(3.3) ความต้องการด้านความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

(3.4) การพิสูจน์ตัวตนของผู้ใช้งานและผู้ดูแลระบบ (Authentication)

(3.5) การจัดการสิทธิในการใช้งานระบบ (Authorization)

(3.6) ความต้องการในการตรวจสอบและจัดเก็บประวัติการใช้งาน (Auditing/Logging)

(3.7) การป้องกันการปฏิเสธการทำรายการ (Non-repudiation)

(3.8) การบริหารจัดการค่าการปรับแต่ง (Configuration), เซสชั่น (Session) และการจัดการกับข้อผิดพลาดที่เกิดขึ้น (Exceptions handling)

(3.9) ความต้องการด้านสมรรถนะ (Capacity) ของระบบสารสนเทศ

(3.10) ความต้องการด้านความมั่นคงปลอดภัยอื่น ๆ ที่สอดคล้องกับข้อกำหนดกฎหมาย หรือกฎระเบียบที่องค์กรต้องปฏิบัติตาม

(4) ต้องกำหนดจุดทบทวนด้านความมั่นคงปลอดภัย (Security Checkpoint) ในแต่ละระยะ (Phrase) การดำเนินงานของโครงการ เช่น มีการกำหนดให้มีการสอบทานด้านความมั่นคงปลอดภัยในขั้นตอนการออกแบบ การพัฒนา การทดสอบ และก่อนการใช้งานจริง เป็นต้น

(5) ต้องรักษาความปลอดภัยของพื้นที่ที่ใช้ในการจัดเก็บข้อมูล (Repositories) อย่างเหมาะสม เช่น มีการกำหนดและจำกัดสิทธิในการเข้าถึงฐานข้อมูล เป็นต้น

(6) ผู้พัฒนาระบบสารสนเทศต้องได้รับการอบรมความรู้ด้านการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เช่น Secure Coding เป็นต้น รวมถึงความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุกปี

10.2.2 ขั้นตอนการปฏิบัติงานในการควบคุมการเปลี่ยนแปลง (System Change Control Procedures) การเปลี่ยนแปลงระบบงานใด ๆ จะต้องมีการควบคุมเพื่อไม่ให้มีผลกระทบต่อซอฟต์แวร์ประยุกต์ (Application Software) ซอฟต์แวร์ระบบ (System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่น ๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน เช่น การพัฒนาระบบการทดสอบระบบ จะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้น ๆ สามารถทำงานเข้ากันได้ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ การเปลี่ยนแปลงแก้ไขควรมีคำขอการเปลี่ยนแปลงอย่างเป็นทางการซึ่งมีการอนุมัติในส่วนที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้น ๆ

(1) ความต้องการในการขอให้มีการเปลี่ยนแปลง

(1.1) ผู้ร้องขอ ต้องดำเนินการตามกระบวนการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือใช้งานอยู่แล้ว โดยทำหนังสือแจ้งไปยังหน่วยงานเจ้าของข้อมูล หน่วยงานเจ้าของระบบงาน และหรือหน่วยงานที่เกี่ยวข้องทุกส่วนให้รับทราบก่อนทำการแก้ไขซอฟต์แวร์นั้น และต้องมี

การอนุมัติโดยผู้เป็นเจ้าของซอฟต์แวร์ดังกล่าว และปฏิบัติตามระเบียบการปฏิบัติงาน เรื่อง การจัดการกับการแก้ไขเปลี่ยนแปลง

(1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน จะต้องมีการจัดเตรียมและปรับปรุงคู่มือในการใช้งานระบบงานและคู่มือในการอบรมให้กับผู้ใช้งาน ต้องมีการจัดทำและปรับปรุงให้สอดคล้องกับการเปลี่ยนแปลงระบบงานอยู่เสมอ

(2) การกำหนดบทบาทและหน้าที่การเปลี่ยนแปลง

(2.1) ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน เพื่อการควบคุมที่ดีไม่ควรจะทำโดยบุคคลเดียวกัน

(2.2) ซอฟต์แวร์ที่ใช้งานจริงสำหรับระบบงานนั้น ๆ ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการโอนย้ายซอฟต์แวร์ที่พร้อมใช้งานไปยังส่วนที่ใช้งานจริง

(2.3) ควรแบ่งแยกส่วนที่ใช้สำหรับงานต่อไปนี้ออกจากกัน เช่น ส่วนการพัฒนาระบบงานส่วนที่ใช้สำหรับโอนย้าย ซอฟต์แวร์ก่อนการย้ายเข้าส่วนที่ใช้งานจริงส่วนที่ใช้ทดสอบระบบสำหรับผู้ใช้งานและส่วนที่ใช้งานจริงในแต่ละส่วน ต้องมีการควบคุมการเข้าใช้งานที่ดี หมายเหตุ ถ้าไม่สามารถแบ่งแยกส่วนที่ใช้สำหรับทดสอบระบบงาน ให้แยกส่วนที่ใช้สำหรับการทดสอบระบบโดยผู้ใช้งานออกจากส่วนที่ใช้พัฒนาระบบงาน

(3) การเปลี่ยนแปลงระบบคอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์และสื่อที่ใช้ในการจัดเก็บข้อมูล

(3.1) การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์อุปกรณ์และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และการแก้ไขโดยไม่ได้ตั้งใจ

(3.2) การเปลี่ยนแปลงระบบงานใด ๆ ต้องไม่รบกวนหรือขัดขวางการปฏิบัติงานของระบบงานปัจจุบันและการเปลี่ยนแปลงดังกล่าวนั้นจะต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานที่มีการใช้อยู่ในปัจจุบันได้ด้วย

(3.3) การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลที่ไม่ใช้งานแล้วทั้งหมดของรัฐสภาอย่างถาวร ออกจากอุปกรณ์หรือสื่อที่ใช้สำหรับเก็บข้อมูลที่มีการเปลี่ยนแปลง

(4) การเปลี่ยนแปลงระบบเครือข่าย เช่น Network, Firewalls และ Router เป็นต้น

(4.1) ผู้ร้องขอต้องปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ

(4.2) การเปลี่ยนแปลงใด ๆ ของระบบเครือข่ายของรัฐสภา ต้องปฏิบัติตามคู่มือที่กำหนดไว้ เช่น การเปลี่ยนแปลงระบบเครือข่าย รวมถึงการเพิ่มซอฟต์แวร์ของระบบเครือข่าย การ

เปลี่ยนแปลงหมายเลขของเครือข่ายการกำหนดค่าของ Routers ใหม่การเพิ่มเติมคู่สายเพื่อใช้ในการเชื่อมต่อระบบ เป็นต้น

(4.3) ผู้ดูแลระบบจะต้องทำการบันทึกข้อมูลของระบบเก่าเก็บไว้ เพื่อใช้แก้ปัญหาในการนำระบบเก่ามาใช้ในกรณีที่ระบบใหม่เกิดปัญหา โดยพิจารณาว่าข้อมูลใดมีความสำคัญต่อระบบ เช่น บัญชีผู้ใช้งานและรหัสผ่านค่า Configuration ของระบบ เป็นต้น

(4.4) ผู้ดูแลระบบจะต้องเก็บข้อมูลต่าง ๆ รวมทั้งคู่มือที่มาพร้อมกับระบบใหม่ไว้อย่างดีเพื่อใช้ในการแก้ปัญหาในครั้งต่อไป

(4.5) ผู้ดูแลระบบจะต้องบันทึกข้อมูลที่มีการเปลี่ยนแปลงต่าง ๆ ไว้ในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form)

(5) การเปลี่ยนแปลง Source Code

(5.1) สำหรับ Source Code ที่ใช้งานจริงต้องมั่นใจว่า Source Code ทั้งหมดมีการจัดเก็บไว้ในที่เดียวกันซึ่งการเปลี่ยนแปลงจะต้องได้รับอนุมัติให้ทำการแก้ไขแล้วเท่านั้น เมื่อมีการแก้ไขซอฟต์แวร์จะมีการนำเอา Source Code จากที่จัดเก็บไปทำการแก้ไขการเปลี่ยนแปลงแก้ไข Source Code ที่ใช้งานจริงต้องมีการควบคุม Version ของ Source Code อย่างเคร่งครัด

(5.2) ผู้ทำหน้าที่ในการเปลี่ยนแปลงแก้ไขต้องถูกจำกัดสิทธิในการเข้าถึงส่วนระบบงานที่ใช้จริงผู้ทำการแก้ไขจะได้รับอนุญาตให้ทำการคัดสำเนา Source Code เพื่อใช้ในการแก้ไขพัฒนาซอฟต์แวร์ในส่วนที่ใช้สำหรับการพัฒนาระบบงาน และทำการย้ายซอฟต์แวร์ที่แก้ไขเสร็จเข้าสู่ส่วนที่ใช้สำหรับโอนย้ายซอฟต์แวร์ก่อนการย้ายเข้าส่วนที่ใช้งานจริงเท่านั้น

(6) แนวทางปฏิบัติของการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบและผู้ใช้งาน) ให้ปฏิบัติตามระเบียบการปฏิบัติงาน เรื่องการจัดการกับการแก้ไขเปลี่ยนแปลง

10.2.3 การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง (Technical Review of Applications after Operating Platform Changes)

(1) การจ้างพัฒนาระบบต้องตรวจสอบระบบสารสนเทศที่เกี่ยวข้อง ภายหลังที่ได้ติดตั้งระบบใหม่เพื่อให้ทราบถึงผลกระทบจากการพัฒนาระบบและเป็นไปตามเงื่อนไขในการว่าจ้าง พร้อมทั้งมีการตรวจสอบจาก หน่วยงานที่เกี่ยวข้องหลังจากการติดตั้งระบบใหม่หรือการปรับปรุง

(2) ทำการสอบทานและทดสอบการปฏิบัติงานของระบบปฏิบัติการทางธุรกิจที่เกี่ยวข้องโดยเฉพาะระบบที่มีความสำคัญทุกครั้งที่มีการเปลี่ยนแปลงของแพลตฟอร์ม การควบคุมการทำงานของคอมพิวเตอร์ (Operating Platform) เพื่อให้มั่นใจว่าระบบยังปฏิบัติงานได้ตรงตามวัตถุประสงค์ เช่น การเข้าถึงระบบ และความสมบูรณ์ถูกต้องในการปฏิบัติงานของระบบ โดยมีข้อควรปฏิบัติทุกครั้งที่จะเกิดการเปลี่ยนแปลง ดังนี้

(2.1) จัดทำแผนในการขอเปลี่ยนแปลงและประกาศให้ผู้ที่มีส่วนเกี่ยวข้องได้ทราบล่วงหน้า

(2.2) ทำการปรับปรุงแผนความต่อเนื่องทางธุรกิจที่เกี่ยวข้องอย่างเหมาะสม เพื่อให้เกิดความสอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้น

10.2.4 การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ (Restrictions on Changes to Software Packages) ผู้ดูแลระบบหรือหน่วยงานที่ดูแลระบบต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อ โดยมีแนวทางปฏิบัติดังนี้

(1) หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

(2) ในกรณีที่หลีกเลี่ยงไม่ได้ในการเปลี่ยนแปลงแก้ไข ให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไขหรือมอบให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

(3) ในการเปลี่ยนแปลงซอฟต์แวร์แพ็กเกจ ให้ผู้ที่รับผิดชอบเก็บตัวซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

(4) ตัวซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการตรวจสอบเป็นอย่างดีว่าจะไม่มีผลกระทบต่อระบบ

10.2.5 ทฤษฎีด้านความปลอดภัยวิศวกรรมระบบ (Secure System Engineering Principles) หลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure System Engineering Principles) กำหนดขึ้นเพื่อให้ระบบสารสนเทศมีระดับของการรักษาความมั่นคงปลอดภัยที่เหมาะสม และสามารถตอบสนองต่อความต้องการขององค์กรได้โดยหลักการดังกล่าว ต้องได้รับการนำไปใช้งานร่วมกับวงจรการพัฒนาระบบสารสนเทศขององค์กรและประกอบด้วย ประเด็นพื้นฐานที่ต้องได้รับการพิจารณาในระหว่างการออกแบบสร้างหรือพัฒนาระบบสารสนเทศ ดังต่อไปนี้

(1) มาตรการรักษาความมั่นคงปลอดภัยของระบบต้องได้รับการออกแบบให้สอดคล้องกับข้อกำหนดของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนขั้นตอนปฏิบัติงาน มาตรฐานหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องขององค์กร

(2) พิจารณาและกำหนดมาตรการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการระบุความต้องการในการพัฒนาระบบสารสนเทศ (Requirements Development Phase) และถือเป็นส่วนหนึ่งของการออกแบบระบบในภาพรวม

(3) ในกรณีที่มีการปรับเปลี่ยนความต้องการของระบบ ต้องมีการพิจารณาปรับเปลี่ยนหรือเพิ่มเติมมาตรการด้านความมั่นคงปลอดภัยให้มีความสอดคล้องกับความต้องการที่เปลี่ยนแปลงไปเสมอ

(4) มาตรการด้านความมั่นคงปลอดภัยที่เลือกใช้ ต้องมีระดับความเข้มงวดที่เหมาะสมกับความเสี่ยงค่าใช้จ่ายวัตถุประสงค์ทางธุรกิจ และประสิทธิผลของการใช้งานระบบสารสนเทศโดยมาตรการที่ใช้ต้องสามารถลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(5) ระบบต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็น ข้อผิดพลาดที่อาจเกิดขึ้น และโอกาสในการถูกโจมตีโดยผู้ไม่ประสงค์ดี

(6) มีการวางมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้หลายชั้น (Layered Security) โดยครอบคลุมทั้งทาง Physical และ Logical ทั้งในระดับระบบปฏิบัติการฐานข้อมูลแอพลิเคชันและระบบเครือข่าย

(7) ระบบต้องได้รับการออกแบบให้มีความสามารถในการต้านทานภัยคุกคาม (เช่น เมื่อมาตรการรักษาความมั่นคงปลอดภัยทำงานผิดพลาดหรือถูกข้ามผ่าน ระบบต้องจำกัดหรือปฏิเสธการเข้าใช้งาน ไม่ยอมให้เข้าใช้งานได้) และมีความสามารถในการฟื้นสภาพ (Recoverability) (โดยอัตโนมัติหรือโดยการสร้างกระบวนการกู้คืน) ภายในระยะเวลาที่เหมาะสมกับความต้องการของรัฐสภา

(8) มีการสร้างมาตรการด้านความมั่นคงปลอดภัยเพื่อปกป้องในส่วนของการรักษาความลับของข้อมูล การรักษาความถูกต้อง ครบถ้วนของข้อมูล และความพร้อมใช้ของข้อมูลทั้งในระหว่างการประมวลผลการแลกเปลี่ยน และการจัดเก็บ

(9) กำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานไม่ซ้ำกัน (Unique Identification)

(10) ต้องมีการออกแบบมาตรการรักษาความมั่นคงปลอดภัยเชิงป้องกันการโจมตีต่าง ๆ (Attack) โดยพิจารณาในมุมมองของผู้ไม่ประสงค์ดีที่ไม่ได้อยู่ภายใต้กรอบของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร หรือพยายามข้ามผ่านมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่และต้องสร้างมาตรการรักษาความมั่นคงปลอดภัยในกรณีที่จำเป็นต้องใช้งานระบบในสภาพแวดล้อมที่ไม่พึงประสงค์ (เช่น การใช้งานระบบในระหว่างเกิดเหตุฉุกเฉินหรือภัยพิบัติ)

(11) ออกแบบสิทธิในการใช้ระบบโดยอาศัยหลักการสิทธิที่น้อยที่สุด (Least Privilege) ตามหน้าที่การทำงานและ/หรือความจำเป็นในการใช้งาน

(12) ออกแบบระบบให้มีกลไกในการตรวจสอบการใช้งาน (Audit Mechanism) สำหรับฟังก์ชั่นการทำงานที่สำคัญเพื่อตรวจจับการใช้งานระบบโดยไม่ได้รับอนุญาตและเพื่อใช้สนับสนุนการตรวจสอบเหตุการณ์ผิดปกติต่าง ๆ

10.2.6 สภาพแวดล้อมสำหรับการพัฒนาระบบ (Secure Development Environment) มีการจัดเตรียมและปกป้องสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยโดยครอบคลุมถึงประเด็นต่าง ๆ ดังต่อไปนี้

(1) แบ่งแยกสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศออกจากระบบสารสนเทศที่ใช้งานจริง

(2) ควบคุมให้มีเฉพาะผู้ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศขององค์กร

(3) จัดให้มีการปกป้องข้อมูลที่จัดเก็บและประมวลผลในสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศและข้อมูลที่ส่งผ่าน ระหว่างสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศและระบบสารสนเทศที่ใช้งานจริง

(4) ทำการตรวจสอบและควบคุมการเคลื่อนย้ายข้อมูลเข้าและออกจากสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศอย่างเข้มงวด เช่น การจ้างพัฒนาระบบโดยหน่วยงานภายนอก (Outsourced Development)

(5) ข้อกำหนดสำหรับ Secure Coding จะต้องถูกระบุไว้ใน TOR

(6) เมื่อมีการจ้างพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกจะต้องกำหนดมาตรการป้องกันให้ครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้

(6.1) จัดทำข้อกำหนดเกี่ยวกับการอนุญาตให้ใช้สิทธิ์ (Licensing arrangements) รูปแบบความเป็นเจ้าของโค้ด (code ownership) และสิทธิ์ในทรัพย์สินทางปัญญา

(6.2) จะต้องมีการรับรองคุณภาพและความถูกต้องผลงาน

(6.3) ผู้ว่าจ้างจะต้องได้รับสิทธิ์ในการเป็นเจ้าของ source code และเอกสารอื่น ๆ ที่เกี่ยวข้องกับระบบที่ว่าจ้างให้พัฒนา

(6.4) ผู้ว่าจ้างจะต้องสามารถตรวจสอบคุณภาพและความถูกต้องของงานที่จะส่งมอบได้

(6.5) จัดทำกระบวนการในการตรวจสอบคุณภาพและความถูกต้องในการทำงานของฟังก์ชั่นต่าง ๆ ที่ถูกพัฒนาขึ้นว่ามีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้

(6.6) จะต้องมีการทดสอบหา Trojan ที่อาจแฝงอยู่ใน code ที่ถูกเขียนขึ้นก่อนที่จะนำมาติดตั้งเพื่อใช้งานจริง

(6.7) จัดทำข้อกำหนดในสัญญาบำรุงรักษาซอฟต์แวร์ให้มีการแก้ไข หากพบปัญหาที่เกิดจากการใช้งานในภายหลัง

10.2.8 การทดสอบด้านความมั่นคงปลอดภัยระบบ (System Security Testing)

(1) ระบบสารสนเทศที่ได้รับการพัฒนาขึ้นหรือได้รับการปรับปรุงแก้ไข ต้องได้รับการทดสอบก่อนนำไปใช้งานจริง โดยผู้ใช้งานต้องร่วมทดสอบการทำงานของระบบด้วย

(2) ต้องมีการทดสอบการทำงานทางด้านความมั่นคงปลอดภัยของระบบ (Security Functionality) ในขั้นตอนการพัฒนาระบบงาน

(3) ข้อมูลที่ใช้ในการทดสอบระบบสารสนเทศ ควรเป็นข้อมูลที่จัดเตรียมไว้เพื่อการทดสอบโดยเฉพาะ หากจำเป็นต้องใช้ข้อมูลที่มีความสำคัญสูงในการทดสอบ ต้องได้รับอนุญาตจากเจ้าของข้อมูล และทำการปิดบัง เปลี่ยนแปลง หรือลบ ข้อมูลสำคัญออกตามความเหมาะสม

10.2.9 เกณฑ์ในการตรวจรับระบบสารสนเทศ (System Acceptance Testing) รัฐสภาต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ (System acceptance) รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน เช่น การตรวจรับระบบตาม TOR ที่ได้กำหนดไว้

10.3 แนวปฏิบัติด้านข้อมูลในการทดสอบระบบ (Test Data) เพื่อใช้ในการป้องกันข้อมูลที่ใช้ระหว่างการทดสอบระบบ

10.3.1 หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protection of Test Data) ข้อมูลจริงที่จะนำใช้ทดสอบระบบต้องได้รับอนุญาตจากหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องลบข้อมูลจริงออกจากระบบทดสอบทันที และบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ทดสอบอะไรบ้าง รวมถึงวันเวลาและหน่วยงานที่ทดสอบแจ้งไปยังหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

ส่วนที่ 11
ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

11.1 แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศต่อผู้ให้บริการภายนอก (Information Security in Supplier Relationships) เพื่อใช้ในการป้องกันสินทรัพย์องค์กรจากการเข้าถึงโดยผู้ให้บริการภายนอก

11.1.1 แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก (Information Security for Supplier Relationships)

(1) กำหนดมาตรการควบคุมการเข้าถึงสารสนเทศขององค์กร โดยผู้ให้บริการภายนอกอย่างเหมาะสม

(2) กำหนดประเภทของสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้และกำหนดมาตรการเฝ้าระวังและสอบทานอย่างเหมาะสม

(3) ให้ความรู้แก่ผู้ที่มีส่วนเกี่ยวข้องกับผู้ให้บริการภายนอก เพื่อช่วยในการเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.2 กำหนดความมั่นคงปลอดภัยในข้อตกลงกับผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ด้วยการจัดทำและลงนามยอมรับข้อตกลงกับผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร โดยข้อตกลงควรครอบคลุมเนื้อหา ดังต่อไปนี้

(1) แนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องที่ต้องปฏิบัติตาม

(2) การมีส่วนร่วมของผู้ให้บริการภายนอกในการแก้ไขเหตุการณ์ (Incident) ที่เกี่ยวข้อง

(3) ข้อกำหนดต่าง ๆ ที่เกี่ยวข้องในกรณีที่ผู้ให้บริการภายนอกมีการว่าจ้างผู้รับจ้างช่วง (Subcontract)

(4) รายชื่อทีมงานที่เกี่ยวข้อง รวมถึงผู้ที่สามารถติดต่อได้ในกรณีที่เกิดประเด็นด้านความมั่นคงปลอดภัยสารสนเทศ

(5) กระบวนการในการแก้ไขข้อผิดพลาด หรือข้อขัดแย้ง

11.1.3 ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

(1) ในกรณีที่มีการใช้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารจากผู้ให้บริการภายนอก และผู้ให้บริการภายนอกมีการจ้างผู้รับจ้างช่วง (Subcontractor) ผู้ให้บริการภายนอกต้องกำหนดให้ผู้รับจ้างช่วง ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของรัฐสภาด้วย

(2) ในกรณีที่มีการจัดซื้อสินค้าด้านเทคโนโลยีสารสนเทศและการสื่อสารจากผู้ให้บริการภายนอกและผู้ให้บริการภายนอกมีการรับชิ้นส่วนจากผู้ให้บริการรายอื่น ผู้ให้บริการภายนอกต้องกำหนดให้ผู้ให้บริการภายนอกรายอื่นที่เกี่ยวข้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยของรัฐสภาด้วย

(3) ต้องเฝ้าระวัง และตรวจรับสินค้าและบริการด้านเทคโนโลยีสารสนเทศและการสื่อสารตามข้อกำหนดด้านความมั่นคงปลอดภัยของรัฐสภา

(4) ต้องบริหารจัดการความเสี่ยงในกรณีที่ผู้ให้บริการภายนอกยุติการให้บริการจากผลของการปิดกิจการ หรือจากการเปลี่ยนแปลงของเทคโนโลยี

11.2 แนวปฏิบัติด้านการบริหารจัดการการส่งมอบงานของผู้ให้บริการภายนอก (Supplier Service Delivery Management) การรักษาระดับความสัมพันธ์กับผู้ให้บริการภายนอกในด้านความมั่นคงปลอดภัยสารสนเทศและการส่งมอบงานตามข้อตกลงที่ทำไว้

11.2.1 การเฝ้าระวังและสอบทานการให้บริการ (Monitoring and Review of Supplier Services)

(1) กำหนดมาตรการในการเฝ้าระวัง สอบทาน และตรวจสอบการให้บริการของผู้ให้บริการภายนอก

(2) เฝ้าระวังระดับของบริการให้เป็นไปตามข้อตกลงที่ทำไว้

(3) สอบทานรายงานของผู้ให้บริการภายนอก และกำหนดการประชุมเพื่อตรวจสอบความคืบหน้าของงานอย่างสม่ำเสมอตามความเหมาะสม

(4) กำหนดให้ผู้ให้บริการภายนอกต้องมีส่วนร่วมในการประชุมเพื่อทบทวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องเพื่อการป้องกันและแก้ไข

11.2.2 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการต่อหน่วยงานภายนอก (Managing Changes to Supplier Services) ต้องปรับปรุงเงื่อนไขการให้บริการต่อหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่การปรับปรุงแนวปฏิบัติและขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก โดยต้องได้รับการอนุมัติก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัยเมื่อมีการเปลี่ยนแปลงสารสนเทศ

ส่วนที่ 12
การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 แนวปฏิบัติการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements) เพื่อให้มีวิธีการที่สอดคล้องและได้ผล สำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของรัฐสภา

12.1.1 กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผลและมีความเป็นระบบระเบียบที่ดี

12.1.2 การรายงานเหตุการณ์น่าสงสัย/จุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Events/Reporting Information Security Weaknesses)

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

(2) ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้ทำแจ้งต่อผู้ดูแลระบบหรือผู้รับผิดชอบทันทีเช่น เหตุการณ์ต่อไปนี้

(2.1) พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อคโดยไม่ทราบสาเหตุ

(2.2) เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

(2.3) พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ

(2.4) มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

(2.5) พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

(2.6) พบหรือคาดว่าข้อมูลในระบบจะถูกทำลายแก้ไขหรือลบทิ้ง

(2.7) มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธีไม่ว่าจะสำเร็จหรือไม่

(2.8) การให้บริการของระบบเกิดการชะงักหรือไม่สามารถให้บริการ

(2.9) เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

(2.10) การแก้ไขค่าความปลอดภัยในระบบเช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

12.1.3 การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events) ผู้ดูแลระบบต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหาหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้างรุนแรงหรือมีผลต่อชื่อเสียงจะต้องรายงานให้ผู้บังคับบัญชาทราบโดยด่วนเพื่อหาแนวทางแก้ไข และป้องกันไม่ให้เกิดในครั้งต่อไปควรมีการแบ่งประเภทของปัญหาอย่างเหมาะสม โดยกำหนดให้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศเป็นอีกหนึ่งประเภท

12.1.4 การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ (Response to Information Security Incidents) เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก เป็นต้น และให้บุคลากรในรัฐสภาได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว มีแนวทางปฏิบัติดังนี้

(1) หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events) และ/หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses) และ/หรือการทำงานที่บกพร่องหรือการทำงานผิดปกติของซอฟต์แวร์ (Reporting Software Malfunctions) ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

(2) ในกรณีที่ไม่สามารถติดต่อผู้ดูแลระบบได้ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น

(3) ในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้ปฏิบัติตามระเบียบการปฏิบัติงานเรื่องการจัดการ เหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยภายในศูนย์ปฏิบัติการ SOC (Incident Management Procedure)

12.1.5 การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Learning from Information Security Incidents)

(1) ผู้ดูแลระบบต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อนช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศรวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

(2) ผู้ดูแลระบบต้องจัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้รับทราบอย่างน้อยเดือนละ 1 ครั้ง

12.1.6 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

(1) ต้องกำหนดให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐาน ในกระบวนการทางศาลที่เกี่ยวข้องเมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

(2) ส่วนงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลระเบียบรัฐสภาและกฎหมาย (เช่น 90 วัน หรือ 1 ปี เป็นต้น)

(3) ผู้ดูแลระบบต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพเพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

ส่วนที่ 13
ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ
(Information Security Aspects of Business Continuity Management)

13.1 แนวปฏิบัติความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการกำหนดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยเป็นส่วนหนึ่งของระบบบริหารจัดการความต่อเนื่อง

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)

(1) กำหนดแนวทางในการสร้างความต่อเนื่องด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ เช่น เหตุฉุกเฉิน หรือวิกฤต

(2) จัดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของกระบวนการในการบริหารจัดการความต่อเนื่องทางธุรกิจ หรือกระบวนการในการกู้คืนระบบในภาวะวิกฤต

(3) พิจารณาด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างการวางแผนความต่อเนื่องทางธุรกิจ หรือการกู้คืนระบบในภาวะวิกฤต

13.1.2 แนวทางปฏิบัติของแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

(1) รัฐสภาต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศซึ่งประกอบไปด้วยตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน และหน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

(2) คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษร

(3) กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องประกอบด้วยหัวข้อหลักดังนี้

(3.1) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)

(3.2) การประเมินความเสี่ยงและการควบคุม (Risk Analysis & Control)

(3.3) การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Strategy Development)

(3.4) การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Development)

(3.5) การประชาสัมพันธ์และการฝึกอบรม

(3.6) การทดสอบปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ควรพิจารณาดังนี้

(3.7) การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินภารกิจและการให้บริการของรัฐสภา

(3.8) การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น

(3.9) การดำเนินการเพื่อให้สามารถดำเนินภารกิจได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น

(3.10) การกลับคืนสู่การทำงานปกติเพื่อให้ภารกิจของรัฐสภากลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

(4) แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศผู้ใช้งานควรปฏิบัติตามแนวปฏิบัติการสำรองข้อมูลการกู้คืนและรักษาความลับของข้อมูล

(4.1) เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS) ซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้น กำหนดจำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ ด้วย

(4.2) ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

(4.3) ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก (Host) และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

(4.4) ข้อมูลและสารสนเทศที่มีความสำคัญมาก รัฐสภาจะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

(4.5) ระบบข้อมูลที่สำคัญทั้งหมดของรัฐสภา ควรมีระบบการประมวลผลสำรอง ระบบเครือข่ายสำรองเพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้ สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ภารกิจหลักของรัฐสภาดำเนินต่อไปได้

(4.6) ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดาซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการของรัฐสภา จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูลและข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

(5) แนวทางปฏิบัติของการเก็บข้อมูลสำรองนอกสถานที่

(5.1) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่ใช้ในการจัดเก็บข้อมูลสำรองควรตั้งอยู่ไกลจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะแน่ใจได้ว่าเหตุการณ์หรือภัยธรรมชาติชนิดเดียวกัน เช่น ไฟไหม้ หรือเหตุจลาจลต่าง ๆ จะไม่เกิดขึ้นกับศูนย์คอมพิวเตอร์ทั้งสองแห่งพร้อมกัน

(5.2) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่จัดเก็บข้อมูลสำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก ต้องมีการรักษาความปลอดภัยทั้งในด้านกายภาพและสภาพแวดล้อมการควบคุมเช่นเดียวกันกับศูนย์คอมพิวเตอร์หลัก หรือปรับเปลี่ยนตามความเหมาะสม

(6) การตรวจสอบ สอบทาน และวัดผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity) คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษรโดยต้องมีการสอบทานและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

13.2 แนวปฏิบัติด้านการทดแทนของอุปกรณ์เพื่อความพร้อมใช้งาน (Redundancies) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของรัฐสภา ในการสร้างความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

13.2.1 ความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

(1) มีการออกแบบอุปกรณ์ประมวลผลสารสนเทศให้สามารถใช้งานทดแทนกันได้เพื่อให้ระบบมีความพร้อมในการใช้งานอยู่เสมอ

(2) ในการออกแบบการทำงานของอุปกรณ์ที่สามารถทดแทนกันได้ต้องคำนึงถึงความเสี่ยงทางด้านความลับของข้อมูลและความถูกต้องของข้อมูลด้วย โดยควรมีมาตรการให้มั่นใจว่าระดับความลับและความถูกต้องของข้อมูลยังถูกรักษาไว้อย่างเหมาะสม

(3) ทำการทดสอบการใช้งานทดแทนของอุปกรณ์เพื่อให้มั่นใจว่าอุปกรณ์สามารถทำงานทดแทนกันได้จริงเวลาเกิดเหตุการณ์

ส่วนที่ 14
การปฏิบัติตามข้อกำหนด (Compliance)

14.1 แนวปฏิบัติด้านการปฏิบัติตามข้อกำหนดของสัญญาและกฎหมาย (Compliance with Legal and Contractual Requirements) เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ ซึ่งมีการนำมาใช้ภายในรัฐสภารวมถึงเรื่องของการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายและข้อกำหนดในการใช้ซอฟต์แวร์ของผู้ใช้งานและผู้ที่เกี่ยวข้องกับรัฐสภา

14.1.1 การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย (Identification of Applicable Legislation and Contractual Requirements)

โดยการปฏิบัติตามข้อกำหนดของกฎหมาย ดังต่อไปนี้

(1) เจ้าของระบบต้องมั่นใจว่าระบบของตนได้มีการดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมายและระเบียบ หรือคำสั่งของรัฐสภา

(2) เจ้าของระบบต้องปฏิบัติตามข้อกำหนดในสัญญาและข้อตกลงในสัญญาการให้บริการ

14.1.2 การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานสินทรัพย์ทางปัญญา (Intellectual Property Rights)

(1) การจัดซื้อและการนำซอฟต์แวร์ของบุคคลที่สามมาใช้ในรัฐสภา ต้องเป็นไปตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมาย (Licensing Agreement) ที่ได้ทำไว้กับเจ้าของลิขสิทธิ์

(2) ผู้ใช้งานซอฟต์แวร์บนระบบสารสนเทศของรัฐสภา ต้องยึดถือและปฏิบัติตามกฎหมาย ลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

(3) ต้องควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์โดยการลงทะเบียนเพื่อใช้งานและเก็บเป็นหลักฐานมีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

(4) ซอฟต์แวร์ที่พัฒนาขึ้นโดย/หรือเพื่อรัฐสภาถือเป็นสินทรัพย์ของรัฐสภาซึ่งครอบคลุมถึงซอฟต์แวร์หรือระบบงานที่พัฒนาโดยบุคคลภายนอกเพื่อให้กับรัฐสภา ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิ์ของซอฟต์แวร์ที่อาจเกิดขึ้นหลังจากเสร็จสิ้นโครงการ

(5) ซอฟต์แวร์ที่ถูกพัฒนาโดยข้าราชการ พนักงานและลูกจ้าง ในระหว่างเวลาทำงานถือเป็นสินทรัพย์ของรัฐสภา

(6) ผู้ดูแลระบบต้องคอยตรวจสอบซอฟต์แวร์ทั้งหมดถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องทำการยกเลิกการติดตั้งหรือลบทิ้งทันที

(7) แชร์แวร์ทั้งหมดที่ได้รับอนุญาตให้นำมาใช้ได้และต้องการใช้ต่อหลังจากสิ้นสุดระยะเวลาการทดลองใช้จะต้องได้รับอนุญาตและมีการลงทะเบียนขอสิทธิ์ในการใช้งานอย่างถูกต้องและผู้ใช้ซอฟต์แวร์ดังกล่าวต้องยึดถือและปฏิบัติตาม กฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

(8) การใช้แชร์แวร์และฟรีแวร์จะมีทั้งสามารถทำงานได้อย่างมีประสิทธิภาพและไม่มีประสิทธิภาพหรือไม่มีความปลอดภัย หรือบางครั้งมีชุดคำสั่งที่ไม่พึงประสงค์แอบแฝงมาด้วยซึ่งอาจก่อให้เกิดอันตรายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายได้ ซึ่งผู้ใช้งานส่วนใหญ่ไม่สามารถประเมินการทำงานและความเสียหายที่เกิดขึ้นจากซอฟต์แวร์ได้ ดังนั้นจึงควรขอรับคำปรึกษากับผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และต้องได้รับการพิจารณาอนุมัติจากผู้ดูแลระบบในการนำแชร์แวร์และฟรีแวร์มาใช้กับระบบสารสนเทศของรัฐสภา

(9) ข้อควรระวัง ในบางครั้งข้อมูลหรือซอฟต์แวร์ที่ดาวน์โหลดจากอินเทอร์เน็ตเป็นแฟ้มข้อมูลที่สามารถประมวลผลเองได้ (Executable files) เช่น แฟ้มข้อมูลที่มีนามสกุล .exe, .com, .bat และ .dll เป็นต้น ซึ่งอาจมีชุดคำสั่งที่ไม่พึงประสงค์ฝังอยู่ ชุดคำสั่งดังกล่าวไม่เพียงแต่ส่งผลร้ายต่อเครื่องคอมพิวเตอร์เท่านั้น แต่อาจมีผลกระทบถึงระบบเครือข่ายทั้งหมดของรัฐสภาด้วย

(10) การ Download ซอฟต์แวร์ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จาก Vendor ต้องเป็นไปโดยไม่ละเมิดสินทรัพย์ทางปัญญา

(11) การติดตั้งซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์ระบบงาน (Operating System and Application Software) ต้องกระทำโดยบุคคลที่ได้รับอนุญาตเท่านั้น ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ใน

เครื่องคอมพิวเตอร์ของรัฐสภาโดยไม่ได้รับอนุญาต แล้วเกิดข้อพิพาทเกี่ยวกับกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์นั้น ๆ ทาง “รัฐสภา จะไม่ขอรับผิดชอบไม่ว่ากรณีใด ๆ”

(12) ซอฟต์แวร์ที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของรัฐสภา เป็นซอฟต์แวร์ที่รัฐสภาได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

14.1.3 การป้องกันข้อมูลของรัฐสภา (Protection of Records) เพื่อเป็นการป้องกันข้อมูลสำคัญของรัฐสภาหน่วยงานต่าง ๆ ต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของรัฐสภา

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนตัว มีแนวทางการปฏิบัติดังนี้ (Privacy and Protection of Personally Identifiable Information)

(1) ผู้ดูแลระบบต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัว เช่น ข้อมูลในไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

(2) ผู้ดูแลระบบต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศเกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายข้อมูลที่เข้ารหัสไว้หรืออุปกรณ์หรือเครื่องมือหรือระบบที่ใช้ในการเข้ารหัสข้อมูลไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศนั้นด้วย

14.1.5 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls) ต้องใช้มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) ตามที่ได้กำหนดในแนวปฏิบัติการพัฒนาระบบสารสนเทศ

14.2 แนวปฏิบัติการสอบทานด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Reviews) เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสารสนเทศได้ถูกนำไปใช้และปฏิบัติตามอย่างถูกต้อง ตามวัตถุประสงค์และแนวปฏิบัติขององค์กร

14.2.1 การตรวจสอบด้านความมั่นคงปลอดภัยของข้อมูลโดยหน่วยงานอิสระ (Independent Review of Information Security)

(1) ต้องจัดให้มีการตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Scope Statement) อย่างน้อยปีละ 1 ครั้ง

(2) ผู้ตรวจสอบที่ได้รับมอบหมายจะต้องเป็นบุคคลที่ไม่เกี่ยวข้องกับการดำเนินงานในส่วนงานที่จะได้รับการตรวจสอบ

14.2.2 การปฏิบัติตามแนวปฏิบัติและมาตรฐานความมั่นคงปลอดภัย (Compliance with Security Policies and Standards) ปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามแนวปฏิบัติและมาตรฐานความมั่นคงปลอดภัยของรัฐสภา

14.2.3 การสอบทานการปฏิบัติตามมาตรฐานทางเทคนิคของรัฐสภา (Technical Compliance Review) เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคของรัฐสภา จึงควรปฏิบัติตามแนวทางดังต่อไปนี้

(1) ผู้ดูแลระบบต้องดูแลรักษาตรวจสอบแก้ไขและเสนอผู้บังคับบัญชาให้ปรับปรุงระบบสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดีมีเสถียรภาพมีความมั่นคงปลอดภัยและมีประสิทธิภาพอยู่เสมอ

(2) ผู้ดูแลระบบต้องขออนุญาตหัวหน้าหน่วยงานในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและแนวปฏิบัติฯ ในการประเมินตรวจสอบทดสอบหาจุดอ่อนช่องโหว่อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศและทำการแก้ไขอย่างรวดเร็ว

(3) รัฐสภาต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบและแก้ไขปัญหาช่องโหว่ที่เกิดขึ้น

(4) รัฐสภาต้องกำหนดให้มีการตรวจสอบระบบไฟฟ้าสำรอง อย่างน้อยปีละ 2 ครั้ง

(5) ในกรณีที่มีการเคลื่อนย้าย ผู้ที่รับผิดชอบในการย้าย ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และสินทรัพย์ด้วย การย้ายสถานที่ทำงานเป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของรัฐสภาได้

(6) ผู้ใช้งานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้โดยตรวจสอบ การอัพเดตซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถอัพเดตซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

(7) ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากไปรษณีย์อิเล็กทรอนิกส์ก่อนทำการเปิด เช่น การตรวจสอบไฟล์โดยใช้ซอฟต์แวร์ป้องกันไวรัส หลีกเลี่ยงในการเปิดไฟล์ที่เป็น Executable file เช่น .EXE, .COM

(8) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thump Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(9) ต้องมีการตรวจสอบการใช้งานระบบ (Monitoring System Use) อย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานสินทรัพย์สารสนเทศ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด

(10) การเข้าสู่ระบบของรัฐสภาจากอินเทอร์เน็ตหรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ เช่น รหัสผ่านและเพื่อเพิ่มความปลอดภัยการพิสูจน์ตนต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

(11) ต้องมีการตรวจทานสาย Dial–up ที่ไม่ได้รับอนุญาตอย่างสม่ำเสมอเป็นประจำ ทั้งนี้ รวมไปถึงการตรวจสอบบันทึกการใช้โทรศัพท์ของรัฐสภา และการทำ “War-dialing” เพื่อค้นหาโมเด็มที่อาจติดตั้งอยู่ในระบบเครือข่ายคอมพิวเตอร์ของรัฐสภาโดยไม่ได้รับอนุญาต

(12) ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอกรัฐสภา หน่วยงานที่รับผิดชอบต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

14.2.4 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities) มีแนวทางปฏิบัติดังนี้

(1) อุปกรณ์ประมวลผลสารสนเทศของรัฐสภา มีไว้เพื่อใช้ในกิจการของรัฐสภาเท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากรัฐสภา

(2) อุปกรณ์ประมวลผลสารสนเทศที่รัฐสภาเช่ามาใช้งาน หน่วยงานที่เช่าจะต้องจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของรัฐสภา

(3) รัฐสภาต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของรัฐสภา เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน

(4) ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงเพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของรัฐสภา

(5) ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลงหรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไขเปลี่ยนแปลงซอฟต์แวร์หรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

(6) ไม่อนุญาตให้ผู้ใช้งานติดตั้งซอฟต์แวร์หรืออุปกรณ์ในเครื่องของรัฐสภา การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ฮาร์ดแวร์อุปกรณ์และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากส่วนที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

(7) อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

(8) อุปกรณ์ประมวลผลสารสนเทศควรมีกระบวนการเพื่ออัพเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ ตามแนวปฏิบัติการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของรัฐสภา

จัดเตรียมเอกสารโดย : นายสุธี ยืนแน่นอน	นักวิชาการคอมพิวเตอร์/สผ.	22 มี.ค. 62	_____
พิจารณา/ทบทวนโดย : _____	_____	_____	_____
อนุมัติโดย : _____	เลขาธิการรัฐสภา	_____	_____
ชื่อ	ตำแหน่ง/สังกัด	วันที่	ลงนาม

ประวัติการแก้ไขเอกสาร

เวอร์ชั่น	วันที่มีผลบังคับใช้	บทที่/หน้าที่แก้ไข	รายละเอียดการแก้ไข
1.0	30 ก.ย. 62	ทั้งหมด	เอกสารใหม่