นโยบาย
ในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของรัฐสภา

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา

รหัสเอกสาร : STD_PY_01
เวอร์ชั่น : 1.1
วันที่มีผลบังคับใช้ : 2565

ชั้นความลับของเอกสาร: ☐ลับมาก ☐ลับ ☐ปกปิด ☒ไม่ระบุ

จัดเตรียมเอกสารโดย : นายสุธี ยืนแน่นอน นักวิชาการคอมพิวเตอร์/สผ. ส.ค. 65
พิจารณาทบทวนโดย : คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของรัฐสภาระยะ 4 ปี (พ.ศ. 2562 - 2565)
เห็นชอบโดย : คณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ 5 ปี (พ.ศ. 2561 - 2565)

ประวัติการแก้ไขเอกสาร

เวอร์ชั่น	วันที่มีผลบังคับใช้	บทที่/หน้าที่แก้ไข	รายละเอียดการแก้ไข
1.0	30 ก.ย. 2563	ทั้งหมด	เอกสารใหม่
1.1	ก.ย. 2565	นิยามคำศัพท์	

(ยกเลิกข้อความทั้งหมด)

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) หมายถึง เลขาธิการรัฐสภา

(เพิ่มข้อความใหม่ทั้งหมด)

รัฐสภา หมายถึง สำนักงานเลขาธิการสภาผู้แทนราษฎรและ สำนักงานเลขาธิการวุฒิสภา

หมวดที่ 1 หน้า 9 1.1 วัตถุประสงค์

เพิ่มเป็น

2) เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของรัฐสภา

3) เพื่อเผยแพร่ให้ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของรัฐสภา ได้รับทราบและยอมรับและปฏิบัติตามนโยบาย นี้อย่างเคร่งครัด

4) เพื่อสร้างความตื่นตัวและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ ให้ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือหน่วยงานภายนอกที่ปฏิบัติงานให้กับรัฐสภา

หมวดที่ 2 หน้า 11 2.4 อุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล

ต้องมีการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล โดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติของรัฐสภา

แก้ไขเป็น

ต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึงของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล โดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติของรัฐสภา

หมวดที่ 8 หน้า 15 8.4 การสำรองข้อมูล

รัฐสภา ต้องจัดให้มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติรวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในรัฐสภา เพื่อป้องกันการสูญหายอันจะเกิดขึ้นจากภาวะคุกคามหรือจากการเกิดภัยพิบัติโดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้

แก้ไขเป็น
รัฐสภา ต้องจัดให้มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติรวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในรัฐสภา เพื่อป้องกันการสูญหายอันจะเกิดขึ้นจากภาวะคุกคามหรือจากการเกิดภัยพิบัติโดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้ ตามเอกสาร : SOC-BP-001 แผนสำรองข้อมูลของรัฐสภา (Backup Plan)

สารบัญ

นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา

รัฐสภา ได้ประกาศใช้แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562–2565) เป็นกรอบกำหนดทิศทางการดำเนินงานด้านการรักษาความปลอดภัย ให้เป็นไปตามสากล และมีการติดตามประเมินผลการดำเนินงาน อีกทั้งเพื่อให้เป็นตามความในมาตรา 5 มาตรา 6 และมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 ดังนั้นจึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยของสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีการดูแลการบริหารจัดการอย่างมีประสิทธิภาพตามหลักมาตรฐานสากล โดยให้ครอบคลุมด้านการรักษาความลับ ความถูกต้อง และสภาพพร้อมใช้ของสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นกรอบในการกำหนดมาตรฐาน ขั้นตอนปฏิบัติงาน ผู้รับผิดชอบ และใช้งานระบบรักษาความมั่นคงปลอดภัยของสารสนเทศรัฐสภา

2. เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม สามารถใช้งานได้เป็นปกติอย่างต่อเนื่องเหมาะสม และสอดคล้องตามภารกิจ

3. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

4. เพื่อส่งเสริมให้มีการเผยแพร่ความรู้แก่บุคลากรของรัฐสภา รวมถึงบุคคลที่เกี่ยวข้อง เพื่อสร้างความเข้าใจ ให้เกิดความตระหนัก และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

องค์ประกอบของนโยบาย

นโยบายนี้จัดทำขึ้นโดยอาศัยกรอบตามมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27000:2013 รวมทั้งข้อกำหนดตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศของรัฐสภา

จากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นจากภายในและภายนอกรัฐสภา โดยเจตนาหรือรู้เท่าไม่ถึงการณ์ ซึ่งเป็นแนวนโยบายในภาพรวมเพื่อการจัดการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ โดยจัดแบ่งสาระสำคัญออกเป็น 14 หมวด ประกอบด้วย

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

หมวดที่ 4 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

หมวดที่ 6 การเข้ารหัสข้อมูล(Cryptography)

หมวดที่ 7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

หมวดที่ 9 ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

หมวดที่ 10 การจัดหา พัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development And Maintenance)

หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

หมวดที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

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

หมวดที่ 14 การปฏิบัติตามข้อกำหนด (Compliance)

นิยามคำศัพท์

สารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

ระบบงาน หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้

ระบบปฏิบัติการ หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ เช่น การจัดสรรหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูลและอุปกรณ์แสดงผล

ระบบเครือข่าย หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของรัฐสภา

ความมั่นคงปลอดภัยของสารสนเทศ หมายถึงการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้อง (integrity) สภาพพร้อมใช้งาน (availability) ของสารสนเทศ

ความลับ (CONFIDENTIALITY) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั่นที่จะเข้าถึงข้อมูลเหล่านั้นได้

ความถูกต้อง (INTEGRITY) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ 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

รัฐสภา หมายถึง สำนักงานเลขาธิการสภาผู้แทนราษฎรและ สำนักงานเลขาธิการวุฒิสภา

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของหน่วยงานภายในรัฐสภา

ผู้ใช้งาน หมายถึง ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศและสินทรัพย์ต่าง ๆ ของรัฐสภา และได้รับอนุญาตให้เข้าใช้งานสารสนเทศของรัฐสภา

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการ ระบบคอมพิวเตอร์ลูกข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และระบบสารสนเทศของรัฐสภา

ผู้พัฒนาระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศของรัฐสภา

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

เจ้าของระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึงระบบงาน เช่น การให้สิทธิ การเพิ่มสิทธิ การลดสิทธิ การยกเลิกสิทธิ รวมทั้งการพัฒนา ปรับปรุงดูแลบำรุงรักษาระบบงาน

บัญชีผู้ใช้งาน หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศ ระบบปฏิบัติการ ระบบเครือข่าย รวมถึงโปรแกรมประยุกต์และสารสนเทศของรัฐสภา

สิทธิของผู้ใช้งาน หมายถึง สิทธิในการเข้าถึงระบบสารสนเทศ สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับโปรแกรมประยุกต์และสารสนเทศของรัฐสภา

ผู้ให้บริการภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของรัฐสภา โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล และผลกระทบต่อความเสียหายที่อาจเกิดขึ้นจากการปฏิบัติงาน

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1 วัตถุประสงค์

1) เพื่อกำหนดกรอบทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของรัฐสภา เพื่อให้เกิดการดำเนินการตามมาตรฐานสากล และสอดคล้องกับข้อกำหนดทางกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

2) เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของรัฐสภา

3) เพื่อเผยแพร่ให้ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของรัฐสภา ได้รับทราบและยอมรับและปฏิบัติตามนโยบาย นี้อย่างเคร่งครัด

4) เพื่อสร้างความตื่นตัวและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ ให้ข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือหน่วยงานภายนอกที่ปฏิบัติงานให้กับรัฐสภา

1.2 ข้อกำหนดตามกฎหมาย

ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศบางประเด็นอาจเกี่ยวข้องกับกฎหมายที่บัญญัติ เช่น

1) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

2) กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3) กฎหมายลิขสิทธิ์

1.3 ผู้ที่ได้รับผลกระทบจากนโยบาย

นโยบายฯ นี้มีผลบังคับใช้กับข้าราชการ สมาชิกรัฐสภา รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของรัฐสภา และได้รับอนุญาตให้เข้าใช้งานสารสนเทศของรัฐสภา

1.4 การใช้งาน

การใช้งานสารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องเป็นไปอย่างเหมาะสม โดยอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของผู้อื่น เคารพและปฏิบัติอย่างถูกต้องตามกฎหมายและไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใด ๆ

1.5 พื้นที่ที่มีผลบังคับใช้

มีผลบังคับใช้กับพื้นที่ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของรัฐสภา รวมถึงการเรียกใช้งานจากทางบ้าน หรือ การเข้าถึงจากระยะไกลและการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบสิทธิในการเข้าถึงทุกระบบฯ ต้องดำเนินการตามนโยบายฯ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจเกิดขึ้น

1.6 การตรวจสอบและทบทวน

รัฐสภาต้องกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่กำกับดูแลนโยบายฯ และรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบายฯ อย่างสม่ำเสมอและทันเหตุการณ์ โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์เปลี่ยนแปลงที่สำคัญ เพื่อความเหมาะสมและปกป้องผลประโยชน์ของรัฐสภา

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

2.1 วัตถุประสงค์

เพื่อให้การบริหารและการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับสารสนเทศของรัฐสภาดำเนินการได้อย่างชัดเจน และบุคลากรของรัฐสภาทุกคนได้ตระหนักถึงความสำคัญในเรื่องความมั่นคงปลอดภัยของสารสนเทศ มีความรู้ความเข้าใจ และมีความรับผิดชอบตามภาระหน้าที่ และร่วมกันในการจำกัดภาวะความเสี่ยงและภัยคุกคามซึ่งมีแนวโน้มของความซับซ้อนและความรุนแรงเพิ่มมากขึ้น

2.2 ผู้รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

2.2.1 ระดับสำนักงานฯ

ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบการบริหารจัดการและกำกับดูแลภาพรวมของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา โดยมอบหมายให้สำนักสารสนเทศทำหน้าที่รับผิดชอบในส่วนของนโยบายการรักษาความมั่นคงปลอดภัย ทั้งนี้ สำนัก/กลุ่มงาน ที่เป็นเจ้าของข้อมูลที่อยู่ในระบบส่วนกลางและในระบบที่สร้างขึ้นเอง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติของรัฐสภา

2.2.2 ระดับสำนัก/กลุ่มงาน

สำนัก/กลุ่มงาน ต้องกำหนดให้ผู้บริหารหรือเจ้าหน้าที่ประจำของหน่วยงานในฐานะเจ้าของข้อมูลเป็นผู้รับผิดชอบในการประสานความร่วมมือและกำกับดูแลให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติของรัฐสภา

2.3 ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

2.3.1 ผู้บริหาร

ผู้บริหารระดับสูง (Chief Executive Officer : CEO) และผู้บริหารของทุกสำนักฯ ภายใต้สังกัดรัฐสภา ต้องกำกับดูแลให้บุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศและปฏิบัติตามนโยบายและแนวปฏิบัติของรัฐสภา

2.3.2 ผู้ใช้งาน

ผู้ใช้งานทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของรัฐสภา และต้องรายงานต่อผู้บังคับบัญชา หากพบปัญหาหรือช่องโหว่ที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของรัฐสภา ใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยความลับของรัฐสภา โดยมิได้รับอนุญาต

2.3.3 ผู้พัฒนาและผู้ดูแลระบบ

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของรัฐสภา ต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และต้องมีภาระงานในเรื่องความมั่นคงปลอดภัยของสารสนเทศ ทั้งด้านเทคนิค การตรวจสอบ การเฝ้าระวัง การประเมินและรายงานความเสี่ยงต่อรัฐสภา

2.4 อุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล

ต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึงของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล โดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติของรัฐสภา

หมวดที่ 3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

3.1 วัตถุประสงค์

เพื่อให้บุคลากรของรัฐสภา และบุคลากรของผู้รับสัญญาว่าจ้างจากรัฐสภา ได้เข้าใจบทบาทและหน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง รวมทั้งการใช้สารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศอย่างไม่ถูกต้อง หรือผิดวัตถุประสงค์

3.2 ความมั่นคงปลอดภัยก่อนการจ้างงาน

รัฐสภาต้องกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการตรวจสอบคุณสมบัติของผู้สมัครตามระเบียบที่เกี่ยวข้อง โดยพิจารณาจากจดหมาย

รับรอง ประวัติการทำงาน และต้องมีการระบุเงื่อนไขการจ้างงาน ซึ่งรวมถึงความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

3.3 ความมั่นคงปลอดภัยระหว่างการจ้างงาน

บุคลากรของรัฐสภา หรือผู้ได้รับจ้างต้องปฏิบัติตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยของรัฐสภา โดยต้องมีการให้ความรู้และฝึกอบรมด้านความมั่นคงปลอดภัยแก่บุคลากร ในกรณีที่กระทำความผิดต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบของรัฐสภา

3.4 การสิ้นสุดหรือการเปลี่ยนการจ้าง

เมื่อสิ้นสุดการเป็นบุคลากรหรือมีการโยกย้ายสับเปลี่ยนหน้าที่ความรับผิดชอบหรือการเปลี่ยนสัญญาการจ้างงานต้องมีการคืนทรัพย์สินของรัฐสภา และถอดถอนหรือมอบสิทธิที่เหมาะสมในการเข้าถึงระบบสารสนเทศของบุคลากรนั้น

หมวดที่ 4 การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

4.1 วัตถุประสงค์

เพื่อป้องกันสินทรัพย์สารสนเทศของรัฐสภา และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสมโดยมีการจัดทำบัญชีสินทรัพย์ระบุผู้เป็นเจ้าของสินทรัพย์และกำหนดหลักเกณฑ์ในการใช้งาน และส่งการคืนสินทรัพย์รวมถึงการทำลายสื่อบันทึกข้อมูลที่เหมาะสมมีการจัดหมวดหมู่ตามระดับชั้นความลับและจัดทำป้ายชื่อเพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้

4.2 ความรับผิดชอบต่อสินทรัพย์สารสนเทศ

รัฐสภาต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำบัญชีสินทรัพย์สารสนเทศและปรับปรุงให้ถูกต้องอยู่เสมอและต้องจัดทำกฎ ระเบียบ หรือ หลักเกณฑ์ในการใช้สินทรัพย์อย่างเป็นลายลักษณ์อักษรเพื่อให้เกิดการใช้งานได้อย่างเหมาะสม และเพื่อป้องกันความเสียหายต่อสินทรัพย์เหล่านั้น

4.3 การจัดหมวดหมู่

รัฐสภาต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อรัฐสภา ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม รวมทั้งจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์สารสนเทศตามหมวดหมู่ที่กำหนดไว้

4.4 การจัดสื่อที่ใช้บันทึกข้อมูล

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต มีการป้องกันในการนำส่งหรือการขนย้าย หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัยเมื่อหมดความต้องการในการใช้งาน

หมวดที่ 5 การควบคุมการเข้าถึง
(Access Control)

5.1 วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการการเปิดเผยหรือขโมยสารสนเทศ และสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา จำเป็นต้องมีการกำหนดนโยบายการเข้าถึงระบบ การบริหารจัดการการเข้าถึงของผู้ใช้และการควบคุมการเข้าถึงเครือข่าย

5.2 การควบคุมการเข้าถึงระบบตามความต้องการทางธุรกิจ

รัฐสภา ต้องมีนโยบายควบคุมการเข้าถึงเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรและทบทวนตามระยะเวลาที่กำหนดไว้โดยพิจารณาให้สอดคล้องกับภารกิจของรัฐสภา และความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

5.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

รัฐสภา ต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้ การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่าน รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

5.4 หน้าที่ความรับผิดชอบของผู้ใช้งาน

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด

5.5 การควบคุมการเข้าถึงระบบ

การเข้าถึงระบบภายในรัฐสภา หรือการเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

หมวดที่ 6 การเข้ารหัสข้อมูล
(Cryptography)

6.1 วัตถุประสงค์

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลป้องกันความลับ การปลอมแปลงหรือความถูกต้องของสารสนเทศ

6.2 นโยบายการควบคุมการเข้ารหัสเพื่อป้องกันข้อมูลสารสนเทศ

นโยบายการควบคุมการเข้ารหัสมีการพิจารณาถึงการควบคุมการเข้ารหัส ผลของการประเมินความเสี่ยง เพื่อระบุระดับการป้องกัน

6.3 การบริหารจัดการกุญแจ

การบริหารจัดการการเข้ารหัส (key management) และมาตรฐานอื่น ๆ ที่มีประสิทธิภาพ การใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

หมวดที่ 7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

7.1 วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์ ป้องกันการถูกเปิดเผยโดยมิได้รับอนุญาต และป้องกันมิให้กิจกรรมการดำเนินงานด้านเทคโนโลยีสารสนเทศของรัฐสภาเกิดการติดขัดหรือหยุดชะงัก อาทิ การมีระบบไฟฟ้าสำรอง ระบบสื่อสารสำรอง

7.2 การรักษาความปลอดภัยทางกายภาพ

รัฐสภา ต้องกำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมีระบบป้องกันการเสียหายและการควบคุมการเข้าออกในการรักษาความมั่นคงปลอดภัย อาทิ ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของรัฐสภา ต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด

7.3 การควบคุมการเข้าถึงอุปกรณ์

อุปกรณ์ทุกชนิดต้องกำหนดให้มีผู้รับผิดชอบโดยตรง และผู้รับผิดชอบเท่านั้นที่ได้รับสิทธิในการเข้าถึง โดยต้องจัดให้มีระบบสำหรับจัดเก็บข้อมูลการเข้าถึงเพื่อใช้เป็นหลักฐานในการตรวจสอบ

7.4 การรักษาความปลอดภัยของอุปกรณ์

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ ต้องมีการจัดวางอย่างถูกต้อง มีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่ออุปกรณ์และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจนและต่อเนื่อง

7.5 การนำอุปกรณ์ออกนอกหน่วยงาน

การนำอุปกรณ์ทุกชิ้นออกนอกหน่วยงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของรัฐสภาและต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

8.1 วัตถุประสงค์

เพื่อให้การดำเนินการที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย ในแต่ละขั้นตอนของการปฏิบัติงานต้องมีการบันทึกและจัดเก็บเป็นลายลักษณ์อักษรเพื่อประโยชน์สำหรับการกู้คืนข้อมูลในกรณีที่เกิดการเสียหายรวมถึงการป้องกันและเฝ้าระวัง การบริหารจัดการช่องโหว่

8.2 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ

โครงสร้างพื้นฐานและสารสนเทศทุกระบบต้องมีผู้รับผิดชอบมีเอกสารขั้นตอนการปฏิบัติงานที่ได้บันทึกไว้เป็นลายลักษณ์อักษร ในกรณีที่มีการเปลี่ยนแปลงข้อมูล หรือการปรับเปลี่ยนเวอร์ชันของระบบ หรือโปรแกรมภายใน ต้องมีการบันทึกการจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จ มีการบริหารขีดความสามารถของโครงสร้างพื้นฐานและระบบสารสนเทศ

8.3 การป้องกันโปรแกรมที่ไม่พึงประสงค์

รัฐสภา ต้องจัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงานหรืออุปกรณ์หลักของรัฐสภา และกำหนดให้มีระเบียบและขั้นตอนวิธีปฏิบัติที่เหมาะสม และสนับสนุนให้หน่วยงานภายในที่มีการใช้งานผ่านระบบเครือข่ายของรัฐสภา ได้ยึดถือและปฏิบัติตาม

8.4 การสำรองข้อมูล

รัฐสภา ต้องจัดให้มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติรวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในรัฐสภา เพื่อป้องกันการสูญหายอันจะเกิดขึ้นจากภาวะคุกคามหรือจากการเกิดภัยพิบัติโดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตาม

รูปแบบและแผนการดำเนินการที่กำหนดไว้ ตามเอกสาร : SOC-BP-001 แผนสำรองข้อมูลของรัฐสภา (Backup Plan)

8.5 การบันทึกข้อมูลล็อกและการเฝ้าระวัง

รัฐสภา ต้องจัดให้มีการเฝ้าระวังระบบที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์และต้องกำหนดขั้นตอนวิธีปฏิบัติในการตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องที่ช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ของรัฐสภา

8.6 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

ต้องมีมาตรการในการรักษาความสมบูรณ์ของระบบปฏิบัติงานโดยมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานโดยก่อนการติดตั้งในระบบต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีไม่ก่อให้เกิดปัญหากับระบบ

8.7 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้สามารถทำงานได้เป็นปกติ ต้องปรับปรุงช่องโหว่ในระบบต่างๆ มีการประเมินความเสี่ยงของช่องโหว่เหล่านั้นตามระยะเวลาที่กำหนด กำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

8.8 สิ่งที่ต้องพิจารณาการตรวจประเมินระบบ

ต้องลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ โดยการกำหนดวิธีการปฏิบัติงานที่ชัดเจนในการใช้งานซอฟต์แวร์ที่ใช้ในการตรวจประเมินเพื่อป้องกันมิให้นำซอฟต์แวร์ไปใช้ในทางที่ผิด

หมวดที่ 9 ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

9.1 วัตถุประสงค์

เพื่อป้องกันข้อมูลบนเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ โดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย และการถ่ายโอนข้อมูลสารสนเทศรวมถึงข้อกำหนดในการรักษาความลับหรือการไม่เปิดเผยความลับ

9.2 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

ต้องจัดให้มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจจับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่รัฐสภาประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด และมีการบำรุงรักษาระบบให้ใช้งานได้ดีอยู่เสมอ

9.3 การถ่ายโอนสารสนเทศ

ในการถ่ายโอนหรือแลกเปลี่ยนสารสนเทศ จากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอรวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อรัฐสภา

หมวดที่ 10 การจัดหา พัฒนา และการบำรุงรักษาระบบ
(Systems Acquisition, Development, and Maintenance)

10.1 วัตถุประสงค์

เพื่อให้การจัดหา พัฒนาระบบสารสนเทศและการบำรุงรักษาระบบสารสนเทศ ได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญในทุกขั้นตอนตลอดวงจรชีวิตการพัฒนาระบบ ซึ่งครอบคลุมถึงกระบวนในการพัฒนา การทดสอบ และข้อมูลสำหรับใช้ทดสอบ

10.2 ความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศ

การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศบนเครือข่ายสาธารณะรวมถึงธุรกรรมของบริการสารสนเทศ

10.3 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน

การพัฒนาระบบสารสนเทศต้องมีความมั่นคงปลอดภัยมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนา การกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการ เพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานหลังการเปลี่ยนแปลงนั้นๆ

10.4 ข้อมูลสำหรับการทดสอบระบบ

ต้องมีมาตรการควบคุมการใช้ข้อมูลสำหรับการทดสอบระบบและการป้องกันข้อมูลรั่วไหล เมื่อใช้งานเสร็จต้องลบข้อมูลจริงออกจากระบบทดสอบทันที

หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier Relationships)

11.1 วัตถุประสงค์

เพื่อป้องกันสินทรัพย์องค์กรที่สามารถเข้าถึงโดยผู้ให้บริการภายนอก มีข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอก ในส่วนของการเข้าถึงระบบ การประมวลผล การจัดเก็บ และการสื่อสารสารสนเทศ ที่ผู้ให้บริการภายนอกพึงปฏิบัติ และการบริหารจัดการด้านการเปลี่ยนแปลง ในการให้บริการผู้ให้บริการภายนอก

11.2 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์ต่อผู้ให้บริการภายนอก

การรับบริการจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอรวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อรัฐสภา

11.3 กาบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

ติดตามทบทวนบริการของผู้ให้บริการภายนอก มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจรับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่รัฐสภาประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

หมวดที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Management)

12.1 วัตถุประสงค์

เพื่อให้มีระบบการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศ ได้รับการสื่อสารและและดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของรัฐสภา

12.2 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง

ต้องมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการณ์ความมั่นคงปลอดภัยสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ จุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศให้รับทราบ

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

13.1 วัตถุประสงค์

เพื่อมิให้การดำเนินงานตามภารกิจของรัฐสภา ไม่เกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานได้รับผลกระทบหรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และสามารถกู้ระบบคืนได้ในระยะเวลาที่เหมาะสม โดยมีการวางแผน จัดทำเอกสาร นำไปปฏิบัติ บำรุงรักษา ตรวจสอบ ควบคุม และประเมินผลในส่วนของความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าระดับความมั่นคงปลอดภัยสารสนเทศอยู่ในเกณฑ์ที่ยอมรับได้ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ รวมถึงการเตรียมการเพื่อสร้างความต่อเนื่องของอุปกรณ์ในการประเมินผลสารสนเทศให้พร้อมใช้งานอยู่เสมอ

13.2 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุงกระบวนการ ขั้นตอนปฏิบัติ มีการมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนด

13.3 การเตรียมการอุปกรณ์ประมวลผลสำรอง

จัดเตรียมสภาพความพร้อมใช้อุปกรณ์ประมวลผลสารสนเทศไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

หมวดที่ 14 การปฏิบัติตามข้อกำหนด (Compliance)

14.1 วัตถุประสงค์

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยๆ และให้มั่นใจว่าความมั่นคงปลอดภัยสารสนเทศถูกนำไปปฏิบัติ และใช้งานตามนโยบายและระเบียบปฏิบัติของรัฐสภา

14.2 การปฏิบัติตามข้อกำหนดของสัญญาและกฎหมาย

รัฐสภา ต้องมีการศึกษา กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา เพื่อให้บุคลากรได้รับทราบทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

14.3 การทบทวนความมั่นคงปลอดภัยสารสนเทศ

รัฐสภา ต้องจัดให้มีการทบทวน มาตรการ นโยบาย กระบวนการ ขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสารสนเทศ อย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ โดยเทียบกับนโยบายมาตรฐาน ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง