สภากาชาดไทย
THAI RED CROSS SOCIETY

นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

โครงการจ้างที่ปรึกษาปรับปรุงนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ของสภากาชาดไทย

สารบัญ

สภากาชาดไทย
THAI RED CROSS SOCIETY

ประกาศสภากาชาดไทย

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสภากาชาดไทย พ.ศ. 2566

ตามที่สภากาชาดไทยได้มีการประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของสภากาชาดไทย พ.ศ. 2561 เพื่อสร้างความเชื่อมั่นต่อการทำธุรกรรมอิเล็กทรอนิกส์ในทุกรูปแบบ รักษาความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ และสอดคล้องเป็นไปตามความในมาตรา 5 มาตรา 6 และมาตรา 7 ของพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแล้วนั้น

ปัจจุบันประเทศไทยได้ตรากฎที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพิ่มเติม คือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมทั้งมาตรฐานสากล ISO/IEC 27001 ที่นำมาใช้เป็นแนวทางในการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้มีการเปลี่ยนแปลงเวอร์ชัน โดยเพิ่มมาตรการควบคุมความเสี่ยงให้มีความทันสมัยสอดคล้องกับการใช้งานเทคโนโลยีสารสนเทศในปัจจุบัน จึงเห็นควรให้มีการปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของสภากาชาดไทย พ.ศ. 2561 ให้สอดคล้องกับพระราชบัญญัติ และมาตรฐานสากลดังกล่าวข้างต้น

สภากาชาดไทย จึงออกประกาศดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสภากาชาดไทย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย พ.ศ. 2566”

ข้อ 2 ในประกาศนี้

2.1 **“ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)”** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

2.2 **“ความเสี่ยง (Risk)”** หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบ หรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ เป้าประสงค์ และเป้าหมายของสภากาชาดไทย

2.3 **“ประเมินความเสี่ยง (Risk Assessment)”** หมายถึง กระบวนการวิเคราะห์ภัย และความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

ข้อ 3 หน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุดของหน่วยงาน ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ ผู้บริหาร หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ ดังนี้

3.1 **“ระดับนโยบาย”** ผู้รับผิดชอบ ได้แก่ ผู้บริหารระดับสูงสุดของหน่วยงาน ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ

(1) กำกับให้มีการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับดูแล

(2) มอบหมาย หน้าที่ อำนาจ ให้ผู้ดูแล ควบคุมและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

(3) ติดตามการบริหารความเสี่ยง และระบบรักษาความมั่นคงปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ

3.2 **“ระดับบริหาร”** ผู้รับผิดชอบ ได้แก่ ผู้บริหาร หัวหน้า

(1) กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความมั่นคงปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ

(2) รับผิดชอบในการควบคุม ดูแล รักษาความมั่นคงปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

(3) จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

(4) ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

3.3 **“ระดับปฏิบัติ”** ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

(1) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(2) ประสานการปฏิบัติงานตามแผนป้องกัน และแก้ไขปัญหาด้านความมั่นคงปลอดภัยด้านสารสนเทศ

(3) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย

ข้อ 4 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

4.1 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.2 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 5 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี 2 ส่วน ดังนี้

5.1 ส่วนที่ว่าด้วยการจัดทำนโยบาย

(1) ผู้บริหารระดับสูงสุดของหน่วยงาน ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ ผู้บริหาร หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย

(2) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้บุคลากร และผู้เกี่ยวข้องทั้งหมดทราบ และสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสภากาชาดไทย และช่องทางอื่น ๆ

(3) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง

5.2 ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(1) การใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัย มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน และประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึง และใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และรวมถึงการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัย

(2) การควบคุมการเข้าถึงระบบสารสนเทศ และระบบเครือข่าย มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศ และระบบเครือข่ายของสภากาชาดไทย โดยการกำหนดสิทธิ์ในการเข้าถึงตามความเหมาะสม หรือหน้าที่ความรับผิดชอบ

(3) การบริหารจัดการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ข้อมูลส่วนบุคคล ต้องกำหนดการแบ่งระดับชั้นความลับของข้อมูล และการไม่จัดเก็บข้อมูลส่วนบุคคล รวมถึงกำหนดมาตรการป้องกันในการถ่ายโอนข้อมูล

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม มีการกำหนดคุณลักษณะของศูนย์ข้อมูลคอมพิวเตอร์ การควบคุมการเข้าถึงพื้นที่ดังกล่าวให้มีความมั่นคงปลอดภัย และรวมถึงการบำรุงรักษาระบบสนับสนุนต่าง ๆ

(5) กำหนดหน้าที่ และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น

(6) มีการกำหนดให้ทำการสำรองข้อมูล และระบบคอมพิวเตอร์ที่สำคัญ ให้มีสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(7) การตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ประเมินความเสี่ยง และกำหนดมาตรการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง

(8) การสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศ หรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยจัดทำคู่มือการฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศ และระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน

ข้อ 6 ต้องประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติ ดังนี้

6.1 หนังสือเวียนภายในสภากาชาดไทย

6.2 ประกาศบนเว็บไซต์ภายในสภากาชาดไทย

6.3 ช่องทางอื่น ๆ ตามเหมาะสม

ข้อ 7 หน่วยงานภายในสภากาชาดไทยที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศ สามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สภากาชาดไทย พ.ศ. 2566

ข้อ 8 องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สภากาชาดไทย พ.ศ. 2566” ซึ่งบุคลากรของสภากาชาดไทย และบุคคลภายนอกต้องถือปฏิบัติอย่างเคร่งครัดต่อไป

ข้อ 9 หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สภากาชาดไทย หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 10 ให้สำนักงานเทคโนโลยีสารสนเทศและดิจิทัล เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และกำหนดให้ทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

ข้อ 11 บรรดาประกาศ ระเบียบ และคำสั่งอื่นใดที่ได้กำหนดไว้แล้วซึ่งขัดกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศ เป็นต้นไป

ประกาศ ณ วันที่ 1 เดือน ตุลาคม - พฤศจิกายน พ.ศ. 2566

(ลงชื่อ) .....

(นายเตช บุนนาค)

เลขาธิการสภากาชาดไทย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย (Information Security Policy)

1. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐ ต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัยเชื่อถือได้ สภากาชาดไทยได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสภากาชาดไทยเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัย ให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่าง ๆ สภากาชาดไทยจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

2. วัตถุประสงค์

2.1 เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของสภากาชาดไทยเป็นไปตามกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อให้เกิดความเชื่อมั่นด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของสภากาชาดไทย และทำให้การดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

2.3 เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้บุคลากรสภากาชาดไทยทุกระดับ และบุคคลภายนอกที่ปฏิบัติงานให้กับสภากาชาดไทย มีความรู้ ความเข้าใจ ตระหนักถึงความสำคัญ และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 เพื่อให้มีระบบตรวจสอบ และประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

3. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ 1 นโยบายการใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัย

1. การบริหารจัดการทรัพย์สิน (Assets Management)
2. การบริหารจัดการโปรแกรมและลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Program Licensing and Intellectual Property and Preventing Malware)
3. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

4. การใช้งานอินเทอร์เน็ต (Use of the Internet)
5. การใช้งานและการควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)
6. การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server Management)
7. การใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Computer Desktop Used)
8. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Computer Notebook Used)
9. การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)
10. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log)
11. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)
12. การใช้งานระบบเครือข่ายสังคมออนไลน์ (Social Network)
13. การใช้งานการเข้ารหัสลับ (Cryptography)
14. การใช้บริการคลาวด์ (Use of Cloud Service)

ส่วนที่ 2 นโยบายการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

1. การควบคุมการเข้าถึงสารสนเทศ (Access Control)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
4. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
5. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ส่วนที่ 3 นโยบายการบริหารจัดการและการรักษาความมั่นคงปลอดภัยข้อมูลและข้อมูลส่วนบุคคล

ส่วนที่ 4 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ส่วนที่ 5 นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนที่ 6 นโยบายการจัดทำระบบสำรองสารสนเทศและแผนเตรียมพร้อมกรณีฉุกเฉิน

ส่วนที่ 7 นโยบายการตรวจสอบ และประเมินความเสี่ยงสารสนเทศ

ส่วนที่ 8 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้

“หน่วยงาน (Agency)” หมายถึง สำนักงาน ศูนย์ชำนัญการ กลุ่มงาน สำนักหรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่นในสังกัดสภากาชาดไทย

“ผู้บังคับบัญชา (Commander)” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสภากาชาดไทย

“ผู้บริหารระดับสูงสุดของสภากาชาดไทย (Chief Executive Officer: CEO)” หมายถึง เลขาธิการสภากาชาดไทย

“ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer: CIO)” หมายถึง ผู้ช่วยเลขาธิการที่ได้รับมอบหมาย ให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสภากาชาดไทย

“ผู้บริหาร (Top Management)” หมายถึง เลขาธิการ ผู้ช่วยเลขาธิการ เลขาธิการและกรรมการอำนวยการมูลนิธิ เหรัญญิก ผู้ช่วยเหรัญญิก ผู้อำนวยการสำนักงาน รองผู้อำนวยการสำนักงาน ผู้ช่วยผู้อำนวยการสำนักงาน ผู้อำนวยการศูนย์ชำนัญการ รองผู้อำนวยการศูนย์ชำนัญการ ผู้ช่วยผู้อำนวยการศูนย์ชำนัญการ ผู้อำนวยการกลุ่มงาน รองผู้อำนวยการกลุ่มงาน ผู้ช่วยผู้อำนวยการกลุ่มงาน ผู้อำนวยการสำนัก รองผู้อำนวยการสำนัก ผู้ช่วยผู้อำนวยการสำนัก

“สำนักงานเทคโนโลยีสารสนเทศและดิจิทัล (Information Technology and Digital Bureau)” หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบงานสารสนเทศภายในสภากาชาดไทย

“ผู้อำนวยการสำนักงานเทคโนโลยีสารสนเทศและดิจิทัล (Director of Information Technology and Digital Bureau)” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของสภากาชาดไทย ซึ่งมีบทบาทหน้าที่ และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

“นโยบาย (Policy)” หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“ผู้ใช้งาน (User)” หมายถึง บุคลากรของสภากาชาดไทยและให้หมายความรวมถึงบุคคลอื่นที่สภากาชาดไทยว่าจ้าง หรือให้มาปฏิบัติงานให้แก่สภากาชาดไทย รวมทั้งบุคลากรที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ และบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวข้องกับระบบสารสนเทศของสภากาชาดไทย หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

“ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บุคลากร (Personnel)” หมายถึง เจ้าหน้าที่ประจำ เจ้าหน้าที่วิสามัญ ลูกจ้างประจำ และลูกจ้างชั่วคราว

“เจ้าของข้อมูล (Data Owners)” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิของผู้ใช้งาน (User Access Rights)” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

“บุคคลภายนอก (External Parties)” หมายถึง บุคคลที่ไม่ได้สังกัดอยู่ในสภากาชาดไทย แต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสภากาชาดไทย โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“ผู้ให้บริการภายนอก (Service provider/Outsource/Supplier/Vendor)” หมายถึง บริษัท นิติบุคคล หรือบุคคลอื่น ที่สภากาชาดไทยทำสัญญา หรือข้อตกลงในการใช้บริการ

“ทรัพย์สิน (Asset)” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่ายฮาร์ดแวร์ และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)” หมายถึง พื้นที่ที่สภากาชาดไทยอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสาร โดยแบ่งเป็น

(1) พื้นที่ทำงานทั่วไป หมายถึง พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน และอุปกรณ์ต่อพ่วงต่าง ๆ
(2) พื้นที่ทำงานของผู้ดูแลระบบ
(3) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย
(4) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

ส่วนที่ 1
นโยบายการใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัย

วัตถุประสงค์

1. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. เพื่อให้ผู้ใช้งานปฏิบัติตามแนวทางการควบคุมทรัพย์สินสารสนเทศสำคัญไว้ในที่ ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน
3. เพื่อให้ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544
4. การใช้งานรหัสผ่าน ต้องกำหนดแนวทางปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน
5. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดแนวทางปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานได้ในขณะที่มีผู้ดูแล

แนวปฏิบัติ

1. การบริหารจัดการทรัพย์สิน (Assets Management)

1.1 ผู้รับผิดชอบมีหน้าที่จัดทำรายการทรัพย์สินทางด้านสารสนเทศ (Asset Inventory) ที่หน่วยงานตนเองถือครองโดยรายการทรัพย์สินสารสนเทศ ประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลสารสนเทศ เป็นอย่างน้อย

1.2 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งาน เสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สินที่ผู้ใช้งานต้องรับผิดชอบการรับ หรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

1.3 มีการตรวจสอบ ปรับปรุง ทบทวน รายการทรัพย์สินอย่างน้อยปีละ 1 ครั้ง

1.4 กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของหน่วยงานที่ได้รับมอบหมาย

1.5 ผู้รับผิดชอบต้องไม่ทำการแก้ไข เปลี่ยนแปลงการตั้งค่าระบบต่าง ๆ ของเครื่องคอมพิวเตอร์หรือทรัพย์สินของหน่วยงานโดยไม่ได้รับอนุญาต เช่น การตั้งค่าระบบ (System Configuration) การตั้งค่าโปรแกรม (Program Configuration) เป็นต้น

1.6 ผู้ใช้งานต้องไม่ทำการติดตั้งโปรแกรมเพิ่มเติมนอกเหนือจากที่ได้รับอนุญาตให้ติดตั้ง กรณีที่มีความจำเป็น ผู้ใช้งานต้องขออนุญาตผู้บังคับบัญชาในการติดตั้งโปรแกรมอรรถประโยชน์ โดยชี้แจงเหตุผลและความจำเป็นก่อนดำเนินการติดตั้ง

1.7 ต้องไม่ถอนการติดตั้งโปรแกรมรักษาความมั่นคงปลอดภัย ที่ติดตั้งในเครื่องคอมพิวเตอร์ออกโดยไม่ได้รับอนุญาต เช่น โปรแกรม Antivirus เป็นต้น

1.8 ต้องไม่ปล่อยทิ้งเครื่องคอมพิวเตอร์ไว้ในที่สาธารณะโดยไม่มีผู้ดูแล ที่อาจก่อให้เกิดการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

1.9 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าระบบเครือข่าย เพื่อการประกอบธุรกิจส่วนบุคคล

1.10 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหาย ตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

1.11 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา

1.12 ผู้ใช้งานมีสิทธิ์ใช้ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สิน และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อสภากาชาดไทย

1.13 ความเสียหายใด ๆ ที่เกิดจากการละเมิดตาม ข้อ1.12 ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

2. การบริหารจัดการโปรแกรมลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Program Licensing and Intellectual Property and Preventing Malware)

2.1 สภากาชาดไทยได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา และไม่สนับสนุนการใช้โปรแกรมที่ละเมิดลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ สภากาชาดไทยถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

2.2 เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรม Antivirus ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

2.3 ข้อมูล ไฟล์ โปรแกรม หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

2.4 ผู้ใช้งานต้องทำการปรับปรุงฐานข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

2.5 ผู้ใช้งานต้องพึงระวังไวรัส และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

2.6 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

2.7 ผู้ใช้งานห้ามทำการเผยแพร่ชุดคำสั่งไม่พึงประสงค์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความมั่นคงปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์ และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับโปรแกรมเรียกค่าไถ่ (Ransomware) หรือไวรัสคอมพิวเตอร์ (Virus computer)

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้โปรแกรม (License)

(5) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนระบบเครือข่ายคอมพิวเตอร์

2.8 การพัฒนาโปรแกรมโดยหน่วยงานภายนอก (Outsourced Program Development)

(1) จัดให้มีการควบคุมโครงการพัฒนาโปรแกรมโดยผู้ให้บริการจากภายนอก

(2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาโปรแกรมโดยผู้ให้บริการภายนอก

(3) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพ และความถูกต้องของโปรแกรมที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีต่าง ๆ ก่อนที่จะดำเนินการติดตั้ง

(5) หลังจากการส่งมอบการพัฒนาโปรแกรมจากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

3. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

3.1 ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพ สำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

3.2 ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัย สำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะปฏิบัติงานจากระยะไกล และระบบงานภายในสภากาชาดไทย ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล เช่น SSL VPN เป็นต้น

3.3 ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัว หรือเพื่อนของตนเองเข้าถึงระบบเทคโนโลยีสารสนเทศภายในสภากาชาดไทย

3.4 ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้งานระบบเครือข่ายจากที่บ้าน หรือระบบเครือข่ายสาธารณะ เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสภากาชาดไทย รวมทั้งมาตรการควบคุมการใช้บริการระบบเครือข่ายไร้สายที่บ้านหรือที่สาธารณะ

3.5 ต้องมีการตรวจสอบว่าอุปกรณ์คอมพิวเตอร์ส่วนตัว ซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัส และการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

3.6 ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

3.7 ผู้ใช้งานจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนแบบ Multi-Factor Authentication เพื่อเพิ่มความมมั่นคงปลอดภัย

3.8 การใช้งานอุปกรณ์คอมพิวเตอร์ส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน อุปกรณ์ดังกล่าว ต้องลงทะเบียนเพื่อควบคุมดูแลตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

3.9 หน่วยงานต้องกำหนดมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอกหน่วยงาน ระยะเวลาที่สามารถเชื่อมต่อได้ และระดับชั้นความลับของข้อมูล

3.10 หน่วยงานต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ และการขอยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

4. การใช้งานอินเทอร์เน็ต (Use of the Internet)

4.1 ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์ เพื่อเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความมั่นคงปลอดภัยที่สภากาชาดไทยจัดสรรไว้ตามสิทธิ์ที่ได้รับ

4.2 ห้ามใช้อินเทอร์เน็ตของสภากาชาดไทย เพื่อหาผลประโยชน์เชิงพาณิชย์เป็นการส่วนบุคคล

4.3 ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา และพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสภากาชาดไทย เป็นต้น

4.4 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

5. การใช้งานและการควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

5.1 ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ โดยยื่นคำขอกับหน่วยงานที่รับผิดชอบของสภากาชาดไทย

5.2 ขณะใส่รหัสผ่านต้องไม่ปรากฏ หรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “*” หรือ “•” ในการพิมพ์แต่ละตัวอักษร

5.3 เมื่อได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นให้เปลี่ยนรหัสผ่านโดยทันที

5.4 ผู้ดูแลระบบต้องกำหนดให้ใช้การพิสูจน์ตัวตนแบบ Multi-Factor Authentication เพื่อเพิ่มความมั่นคงปลอดภัยต้องในการเข้าใช้งาน

5.5 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน 3 ครั้ง หากเกินให้ทำการกำหนดมาตรการป้องกันการสุ่มเดารหัสผ่าน เช่น หน่วงเวลาไม่ให้ใส่รหัสผ่านตามแต่ละหน่วยงานกำหนด หรือเป็นระยะเวลาอย่างน้อย 15 นาที หรือล็อกบัญชีผู้ใช้งานชั่วคราว เป็นต้น

5.6 เมื่อบัญชีผู้ใช้งานไม่สามารถใช้งานได้จากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ให้ดำเนินการแจ้งผู้ดูแลระบบเพื่อทำการปลดล็อกต่อไป

5.7 ไม่บันทึกหรือเก็บรหัสผ่านไว้ในที่สาธารณะ หรือในสถานที่ที่เข้าถึงได้โดยง่าย

5.8 ทบทวนรหัสผ่านอย่างน้อยปีละ 1 ครั้ง

5.9 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ ของผู้อื่น เพื่ออ่าน รับ หรือส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

5.10 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

5.11 การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ เว้นเสียแต่ว่า จะใช้วิธีการเข้ารหัสข้อมูลอีเมลที่หน่วยงานกำหนดไว้ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิดตัวผู้รับ

5.12 ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

5.13 ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

5.14 ห้ามส่งอีเมลที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

5.15 ห้ามส่งอีเมลที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

5.16 ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

5.17 ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

5.18 ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์ โดยใช้โปรแกรม Antivirus เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

5.19 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

5.20 ผู้ใช้งานต้องไม่เปิดจดหมายอิเล็กทรอนิกส์บนระบบเครือข่ายสาธารณะ ที่ไม่มีการเข้ารหัสลับของข้อมูล

5.21 ผู้ใช้งานต้องใช้ข้อความที่สุภาพหรือไม่ รับ-ส่ง จดหมายอิเล็กทรอนิกส์ที่มีข้อมูลไม่เหมาะสม ซึ่งอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

5.22 ผู้ใช้งานต้องตรวจสอบกล่องข้อความอิเล็กทรอนิกส์ (Mail box) ของตนเองอย่างสม่ำเสมอ และควรจัดเก็บข้อความอิเล็กทรอนิกส์ (Mail box) เท่าที่จำเป็นเพื่อความสะดวกและความรวดเร็วในการใช้งาน

5.23 ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของสภากาชาดไทยสำหรับใช้ รับ-ส่ง ข้อมูลติดต่อกับหน่วยงานของสภากาชาดไทย หรือหน่วยงานอื่น ๆ ภายนอก

6. การใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Computer Desktop Used)

6.1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นทรัพย์สินของหน่วยงาน เพื่อใช้ในงานของสภากาชาดไทย

(2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้ง และแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบตั้งโต๊ะของหน่วยงาน

(4) การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์แบบตั้งโต๊ะตรวจซ่อม ต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงาน หรือผู้ให้บริการภายนอกบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ได้ทำสัญญากับสภากาชาดไทยเท่านั้น

(5) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม Antivirus

(6) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์

(7) ปิดเครื่องคอมพิวเตอร์แบบตั้งโต๊ะที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง หรือเมื่อสิ้นสุดการใช้งาน

(8) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะที่ตนเองรับผิดชอบ ให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 30 นาที เพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

(9) ห้ามนำอุปกรณ์คอมพิวเตอร์ส่วนตัว มาใช้งานกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน เว้นแต่จะได้รับการตรวจสอบจากผู้ดูแลระบบ หรือปฏิบัติตามนโยบายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

6.2 การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่าน ที่ระบุไว้ในหัวข้อ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)”

6.3 การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(1) ผู้ใช้งานต้องตรวจสอบไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(2) ผู้ใช้งานต้องตรวจสอบไวรัสของข้อมูลที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนใช้งาน

(3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6.4 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนสื่อบันทึกข้อมูล ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากสื่อบันทึกข้อมูลเสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

7. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Computer Notebook Used)

7.1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นทรัพย์สินของหน่วยงาน เพื่อใช้ในงานของสภากาชาดไทย

(2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ผู้ใช้งานต้องศึกษา และปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างมั่นคงปลอดภัยและมีประสิทธิภาพ

(4) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ และรักษาสภาพของเครื่องคอมพิวเตอร์ให้มีสภาพเดิม

(5) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

(6) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกากดสัมผัสหน้าจอภาพ ให้เป็นรอยขีดข่วนหรือทำให้จอภาพ ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้ เป็นต้น

(7) ไม่วางของทับบนหน้าจอ และแป้นพิมพ์

(8) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(9) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่ง ก่อนเปิดใช้งานใหม่อีกครั้ง

(10) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

7.2 ความมั่นคงปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

(2) ผู้ใช้งานไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น และฝุ่นละอองสูง โดยต้องระวังป้องกันการตกกระทบ

7.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(2) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดี และเป็นไปตามที่ระบุไว้ในหัวข้อ“การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)”

(3) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาไม่เกิน 30 นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(4) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

7.4 การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในหัวข้อ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)”

7.5 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการบันทึกลงบนสื่อสำรองข้อมูลต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(2) ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(3) สื่อบันทึกข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้ ต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(4) สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(5) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนสื่อบันทึกข้อมูล ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากสื่อบันทึกข้อมูลเสียไปก็ไม่กระทบต่อกาดำเนินการของหน่วยงาน

8. การใช้งานระบบเครือข่ายสังคมออนไลน์ (Social Network)

8.1 การใช้งาน หรือใช้บริการเว็บไซต์ระบบเครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของสภากาชาดไทยเป็นสำคัญ

8.2 ในการใช้งานระบบเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของสภากาชาดไทย

8.3 ในการใช้ระบบเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความเห็น หรือใช้ข้อความยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสภากาชาดไทย

8.4 หากผู้ใช้งานทราบ และรู้สึกในภายหลังว่าการใช้งานระบบเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับสภากาชาดไทย ผู้ใช้งานต้องแจ้งหน่วยงานต้นสังกัดโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

9. การบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server Management)

9.1 กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

9.2 ต้องกำหนดกระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ ต้องดำเนินการแก้ไข และบันทึกรายงานการแก้ไขโดยทันที

9.3 ต้องตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (1.ntp.redcross.or.th และ 2.ntp.redcross.or.th) ตามที่สภากาชาดไทยกำหนด

9.4 เครื่องคอมพิวเตอร์แม่ข่ายต้องเปิดใช้ Port และ Service ที่จำเป็นเท่านั้น และต้องกำหนดมาตรการป้องกันเพิ่มเติมเพื่อลดความเสี่ยงสำหรับการเปิดใช้ Port และ Service ที่มีความเสี่ยงหากยังมีความจำเป็นที่ต้องใช้งาน

9.5 ต้องปรับปรุงโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นปัจจุบันอยู่เสมอ เพื่อป้องกันช่องโหว่ต่าง ๆ

9.6 ต้องทดสอบการรักษาความมั่นคงปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษาระบบเทคโนโลยีสารเทศ

9.7 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

10. การติดตั้ง และกำหนดค่าของระบบ (System Installation and Configuration)

10.1 การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(1) ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ระบบ

(2) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งานตามที่หน่วยงานกำหนด

(3) กำหนดชื่อ รหัสผ่านผู้ดูแลระบบ และชื่อผู้ใช้งาน โดยใช้ชื่อของผู้ใช้งาน จุด (มหัพภาค) และตามด้วยนามสกุลตัวอักษรแรก โดยเป็นภาษาอังกฤษ หรือหากระบบใดที่ไม่สามารถกำหนดเป็นตัวอักษรได้ ให้กำหนดเป็นตัวเลข โดยใช้รหัสเจ้าหน้าที่ หรือตามความเหมาะสม โดยต้องระบุถึงผู้ถือครองหรือผู้รับผิดชอบได้

(4) กำหนดค่าติดตั้ง Computer Name และ IP Address

(5) ปรับปรุง กำหนดค่าระดับความมั่นคงปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(6) ติดตั้งโปรแกรม Antivirus ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

(7) ต้องบันทึกข้อมูลกิจกรรม (Log) ให้เป็นไปตามที่กฎหมายกำหนด โดยสามารถตรวจสอบข้อมูลย้อนหลังได้ไม่น้อยกว่า 90 วัน

10.2 การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึง และการใช้งานระบบ (User Account Management)

(1) กำหนดชื่อ และรหัสผ่านผู้ดูแลระบบ

(2) กำหนดชื่อผู้ใช้งาน และรหัสผ่าน โดยใช้ชื่อของผู้ใช้งาน จุด (มหัพภาค) และตามด้วยนามสกุลตัวอักษรแรก โดยเป็นภาษาอังกฤษ หรือหากระบบใดที่ไม่สามารถกำหนดเป็นตัวอักษรได้ ให้กำหนดเป็นตัวเลข โดยใช้รหัสเจ้าหน้าที่ หรือตามความเหมาะสม โดยต้องระบุถึงผู้ถือครองหรือผู้รับผิดชอบได้

(3) กำหนดสิทธิ์การเข้าใช้งานตามบทบาทหน้าที่ ความรับผิดชอบเท่าที่จำเป็นเท่านั้น

(4) บันทึกบัญชีผู้ใช้งาน และสิทธิ์การเข้าใช้ระบบ

10.3 การปรับปรุงการรักษาความมั่นคงปลอดภัยของ Antivirus (System Security & Antivirus Update)

(1) ติดตามเฝ้าระวังระบบการทำงานของเครื่องคอมพิวเตอร์การเข้าใช้ระบบ

(2) ตรวจสอบประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัย อย่างน้อยสัปดาห์ละ 1 ครั้ง

(3) ปรับปรุง และกำหนดค่าระบบความมั่นคงปลอดภัยให้เหมาะสมกับปัญหา

(4) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(5) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ สัปดาห์ละครั้งเป็นอย่างน้อย

10.4 ติดตั้ง ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(1) ติดตั้งระบบจัดการฐานข้อมูลตามความต้องการของระบบงานที่หน่วยงานใช้งาน

(2) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพตามระบบฐานข้อมูลนั้นกำหนด

(3) สร้างและกำหนดรายชื่อผู้จัดการฐานข้อมูล (Database Manager) ชื่อผู้ใช้งานอื่น และสิทธิ์การใช้งาน

(4) ปรับปรุง กำหนดค่าระบบให้เหมาะสมทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

(5) บันทึกข้อมูลกิจกรรม (Log) ของฐานข้อมูลตามที่หน่วยงานกำหนด โดยต้องระบุถึงผู้ใช้งาน ช่วงเวลาการใช้งานเป็นอย่างน้อย และต้องจัดเก็บไว้ไม่น้อยกว่า 90 วัน

10.5 ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ กำหนดค่าระบบของโปรแกรม และกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการหรือเข้าถึงฐานข้อมูล

(1) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนา

(2) กำหนดค่าโปรแกรม หรือบริการที่ทำงานร่วมกับระบบปฏิบัติการ ให้เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้อง และมีประสิทธิภาพ

(3) การติดตั้งฐานข้อมูล การเชื่อมต่อระบบงาน หรือทำการทดสอบการให้บริการตามที่ระบบงานกำหนด

(4) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อรหัสผ่าน และสิทธิ์การเข้าใช้ระบบ และฐานข้อมูลตามที่กำหนดไว้

(5) กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน

(6) บันทึกข้อกำหนดค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

11. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log)

11.1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง โดยการระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

(1) กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงานหรือตามที่หน่วยงานกำหนด

(2) ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่เก็บรักษาไว้

(3) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการ เข้า-ออก ระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลงโดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกข้อมูลต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

12. หน้าที่ และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)

12.1 ผู้ดูแลระบบ แบ่งออกเป็น 3 กลุ่ม

(1) ผู้ดูแลระบบเครือข่าย (Network Administrator)

(2) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (System Administrator)

(3) ผู้ดูแลระบบสารสนเทศ (Application Administrator)

12.2 ผู้ดูแลระบบเครือข่าย มีหน้าที่ และความรับผิดชอบดังนี้

(1) ดูแลรักษา และตรวจสอบอุปกรณ์ระบบเครือข่าย และช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(2) เก็บรักษาข้อมูลจราจรเครื่องคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาไม่น้อยกว่า 90 วัน หรือตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังนี้

(2.1) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนสมบูรณ์ถูกต้อง และความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บไว้ เว้นแต่ ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

(2.2) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(2.3) หากมีการเปลี่ยนแปลงใด ๆ ต้องดำเนินการตามขั้นตอนการเปลี่ยนแปลงตามที่หน่วยงานกำหนด

12.3 ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่ และความรับผิดชอบดังนี้

(1) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานนั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

(2) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์ สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งาน ให้เป็นเวอร์ชันล่าสุดหรือเวอร์ชันใหม่ที่สุดเท่าที่เครื่องคอมพิวเตอร์แม่ข่ายสามารถรองรับได้

(3) ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

(4) ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

(5) ดูแลรักษา และปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้อง และเป็นประจำอย่างน้อย 3 เดือนครั้ง

(6) หากมีการเปลี่ยนแปลงใด ๆ ต้องดำเนินการตามขั้นตอนการเปลี่ยนแปลงตามที่หน่วยงานกำหนด

12.4 ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

(1) ดูแลรักษา และปรับปรุงระบบบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้อง และเป็นประจำอย่างน้อย 3 เดือนครั้ง

(2) ปรับปรุงรายการระบบสารสนเทศ และรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นประจำอย่างน้อย 3 เดือนครั้ง

(3) หากมีการเปลี่ยนแปลงใด ๆ ต้องดำเนินการตามขั้นตอนการเปลี่ยนแปลงตามที่หน่วยงานกำหนด

12.5 หลักธรรมาภิบาลของผู้ดูแลระบบ

(1) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

(2) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งาน หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(3) ไม่เปิดเผยข้อมูลที่ได้จากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

13. การใช้งานการเข้ารหัสลับ (Cryptography)

13.1 หน่วยงานกำหนดประเภท ความแข็งแรง และคุณภาพของอัลกอริทึมในการเข้ารหัสลับที่เป็นมาตรฐาน และน่าเชื่อถือ ได้รับการยอมรับในระดับสากล และเหมาะสม อย่างน้อยต้องใช้ AES-256, RSA หรือ IDEA ตามการระบุระดับการป้องกัน และการกำหนดชั้นความลับของข้อมูลสารสนเทศ

13.2 การใช้โปรแกรมการเข้ารหัสลับ ต้องใช้ตามที่หน่วยงานกำหนดเท่านั้น

13.3 ต้องดำเนินการเข้ารหัสข้อมูลด้วยอัลกอริทึมที่มีความมั่นคงปลอดภัยทุกครั้ง เมื่อมีการดำเนินการดังต่อไปนี้

(1) การส่งข้อมูลที่มีการกำหนดชั้นความลับ ได้แก่ ลับ (Confidential) ลับมาก (Secret) และลับที่สุด (Top Secret) ผ่านระบบเครือข่าย

(2) การจัดเก็บข้อมูลที่มีการกำหนดชั้นความลับ ได้แก่ ลับ (Confidential) ลับมาก (Secret) และลับที่สุด (Top Secret) ในสื่อจัดเก็บข้อมูลที่เคลื่อนย้ายได้

(3) การจัดเก็บข้อมูลที่มีการกำหนดชั้นความลับ ได้แก่ ลับ (Confidential) ลับมาก (Secret) และลับที่สุด (Top Secret) ในระบบสารสนเทศที่ไม่มีการจำกัดสิทธิการเข้าถึง

13.4 หน่วยงานกำหนดให้มีการตรวจสอบ และปรับปรุงการเข้ารหัสลับ ให้เหมาะสมตามเทคโนโลยีปัจจุบัน และทำการติดตามช่องโหว่หรือจุดอ่อนของอัลกอริทึมอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

13.5 กรณีที่มีการใช้บริการจากผู้ให้บริการภายนอก และมีการเข้ารหัสลับของข้อมูลรวมอยู่ด้วย หน่วยงานต้องระบุเนื้อหารายละเอียดข้อตกลง หรือสัญญา ที่ครอบคลุมปัญหาด้านความรับผิดชอบ ความน่าเชื่อถือของบริการ และเวลาการตอบสนองของการให้บริการให้ชัดเจน

13.6 กรณีที่มีความจำเป็น หรือมีข้อยกเว้น ที่ไม่สามารถดำเนินการตามข้อกำหนดการเข้ารหัสลับของข้อมูลได้ ต้องได้รับการอนุมัติจากผู้บริหารเท่านั้น

14. การใช้บริการคลาวด์ (Use of cloud service)

14.1 หน่วยงานต้องกำหนดกระบวนการสำหรับการใช้บริการคลาวด์ เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งต้องระบุเรื่องดังต่อไปนี้

(1) การประเมิน และคัดเลือกผู้ให้บริการคลาวด์ (Due Diligence)

(2) การทำสัญญา และข้อตกลงการให้บริการคลาวด์ (Engage)

(3) การให้บริการของผู้ให้บริการคลาวด์ (Operate)

(4) การทบทวนบริการคลาวด์ในรอบระยะเวลาที่ผ่านมา (Review)

(5) การยกเลิก หรือสิ้นสุดการใช้บริการคลาวด์ (Exit)

14.2 การใช้บริการคลาวด์พิจารณาจากการประเมินมาตรฐานของผู้ให้บริการ ประเมินความรู้และความสามารถของผู้ให้บริการ ตลอดจนคัดเลือกผู้ให้บริการที่มีคุณสมบัติเหมาะสมที่สุด

14.3 หน่วยงานพิจารณาประเมินความเสี่ยงที่เกี่ยวข้องกับการยกเลิกหรือการสิ้นสุดการใช้บริการคลาวด์ เช่น

(1) ความเสี่ยงด้านการหยุดชะงักของระบบ อันเกิดจากการสิ้นสุดการใช้บริการ

(2) ความเสี่ยงเรื่องของการถ่ายโอนข้อมูลจากผู้ให้บริการรายปัจจุบัน ไปสู่ผู้ให้บริการรายใหม่

(3) ความเสี่ยงเรื่องของการลบทำลายข้อมูลที่อยู่บนระบบของผู้ให้บริการรายปัจจุบัน

14.4 ผลจากการประเมินความเสี่ยง และผลการประเมินด้านอื่น ๆ ของการใช้บริการคลาวด์ ต้องรายงานแก่หัวหน้างานเพื่อพิจารณา และรับทราบต่อไป

ส่วนที่ 2
นโยบายการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูล และอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัย
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงาน
3. เพื่อกำหนดวิธีการบริหารจัดการเข้าถึงข้อมูล และระบบสารสนเทศของผู้ใช้งานแต่ละประเภทที่เหมาะสม และตรวจสอบได้ เพื่อป้องกันการเข้าถึงของผู้ไม่ได้รับอนุญาต
4. เพื่อควบคุมการเข้าถึงระบบเครือข่าย และการใช้บริการผ่านระบบเครือข่าย รวมทั้งการเชื่อมต่อระบบเครือข่ายทั้งจากภายในสภากาชาดไทย และจากภายนอกสภากาชาดไทย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
5. เพื่อควบคุมการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต
6. เพื่อควบคุมการเข้าถึงโปรแกรม และระบบสารสนเทศโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

1. การควบคุมการเข้าถึงสารสนเทศ (Access Control)

1.1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ ตามความจำเป็นต่อการใช้งานเท่านั้น

1.2 บุคคลจากหน่วยงานภายนอก หรือหน่วยงานอื่นในสังกัดสภากาชาดไทย ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชา

1.3 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ดังนี้

(1) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจดังนี้

(1.1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- เพิ่มข้อมูล
- แก้ไขข้อมูล
- ลบข้อมูล
- อนุมัติ

- ไม่มีสิทธิ์

(1.2) กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(1.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชา หรือผู้ดูแลระบบที่ได้รับมอบหมาย

1.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ โดยตรวจสอบทุก 90 วัน หรือเมื่อมีการเปลี่ยนแปลง

1.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ และสามารถตรวจสอบย้อนหลังได้ 90 วัน เป็นอย่างน้อย หรือตามที่หน่วยงานกำหนด

1.6 ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่าน เข้า-ออก สถานที่ตั้งของระบบสารสนเทศ เพื่อเป็นหลักฐานในการตรวจสอบ และสามารถตรวจสอบย้อนหลังได้ 90 วัน เป็นอย่างน้อย หรือตามที่หน่วยงานกำหนด

1.7 เวลาการเข้าถึงระบบสารสนเทศดังนี้

(1) การเข้าถึงสารสนเทศในเวลาปฏิบัติงาน (08.30 น. – 16.30 น.)

(2) การเข้าถึงสารสนเทศนอกเวลาปฏิบัติงาน (นอกช่วงเวลา 08.30 น. – 16.30 น.)

(3) การเข้าถึงสารสนเทศในช่วงวันหยุด (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

(4) การเข้าถึงสารสนเทศตามที่หน่วยงานกำหนด

1.8 ช่องทางการเข้าถึงระบบสารสนเทศ

(1) ระบบเครือข่ายภายในสภากาชาดไทย

(2) ระบบเครือข่ายภายนอกสภากาชาดไทย

(3) เข้าถึงโดยผ่าน VPN

(4) ระบบอื่นตามที่หน่วยงานกำหนด

1.9 ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

(1) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

(2) มีการทบทวน และปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลง

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

2.1 การลงทะเบียนผู้ใช้

(1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของสภากาชาดไทย หรือตามที่หน่วยงานกำหนด

(2) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(3) ผู้ดูแลระบบต้องตรวจสอบ และให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย

(4) ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากได้ทำความเข้าใจ

(5) ผู้ดูแลระบบต้องทำข้อตกลงการใช้งานระบบ (AUP) กับผู้ใช้งานที่มีสิทธิ High Privilege User เพื่อแสดงถึงสิทธิ และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากได้ทำความเข้าใจ

(6) ผู้ดูแลระบบต้องแจ้งผู้ใช้งานให้ทราบถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย

(7) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

(8) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาตอย่างน้อยปีละ 1 ครั้ง หรือตามที่หน่วยงานกำหนด

(9) การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

(9.1) บุคลากรของสภากาชาดไทย อาจารย์พิเศษ นักวิจัย และบุคคลภายนอกของหน่วยงาน ผู้ดูแลระบบหรือผู้ที่รับผิดชอบ จะสร้างบัญชีเจ้าหน้าที่ใหม่โดยทันทีที่สำนักงานบริหารทรัพยากรบุคคล ป้อนข้อมูลบุคลากรเข้าระบบสารสนเทศทรัพยากรบุคคล

(9.2) บุคคลอื่น ๆ ที่สภากาชาดไทยมอบสิทธิ์ให้ เช่น อาสาสมัครที่ทำงานในหน่วยงาน บุคคลที่ทำงานในหน่วยงานอิสระ บุคคลที่สภากาชาดไทยมอบสิทธิ์ให้สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อหน่วยงานที่รับผิดชอบและมีหนังสือรับรองจากผู้บริหารระดับสำนักงาน/หน่วยงานขึ้นไป และแสดงบัตรประชาชน หรือหนังสือเดินทาง พร้อมสำเนาที่รับรองสำเนาถูกต้อง 1 ฉบับ

(10) การจัดการสิทธิ์ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

(10.1) เมื่อบุคลากรของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์การใช้งานไว้ ผู้รับผิดชอบต้องแจ้งผู้ดูแลระบบ ล่วงหน้าอย่างน้อย 7 วัน ก่อนวันที่มีผลในการลาออกหรือเปลี่ยนแปลงหน้าที่ และให้ผู้ดูแลดำเนินการเปลี่ยนสิทธิ์ หรือถอดถอนสิทธิ์ออกจากระบบตามวันที่มีผลในการลาออกโดยทันที

(10.2) การแจ้งขอใช้สิทธิ์หรือเปลี่ยนแปลงสิทธิ์ในการเข้าถึง การใช้งานข้อมูล และสารสนเทศและระบบสารสนเทศต้องทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

- ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้
- ส่งถึงผู้บริหารของหน่วยงานหลัก
- เก็บเอกสารไว้เป็นหลักฐานอ้างอิง
- หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ
- ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึง และควบคุมการใช้งานสารสนเทศ

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากผู้มีอำนาจในการอนุมัติ

2.3 การทบทวนสิทธิ์การเข้าถึง

(1) ต้องมีกระบวนการทบทวนบัญชีผู้ใช้ และสิทธิ์การใช้งานระบบสารสนเทศ และปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ 1 ครั้ง

(2) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน

(2.1) กรณีบุคลากร เมื่อพ้นสภาพการเป็นบุคลากรของสภากาชาดไทย ต้องดำเนินการผู้รับผิดชอบต้องแจ้งผู้ดูแลระบบ ล่วงหน้าอย่างน้อย 7 วัน ก่อนวันที่มีผลในการลาออก และให้ผู้ดูแลดำเนินการถอดถอนสิทธิ์ออกจากระบบ ตามวันที่มีผลในการลาออกโดยทันที

(2.2) กรณีบุคลากร เมื่อมีการเปลี่ยนแปลงตำแหน่งงานภายในสภากาชาดไทย ต้องผู้รับผิดชอบต้องแจ้งผู้ดูแลระบบ ล่วงหน้าอย่างน้อย 7 วัน ก่อนวันที่มีผลในการเปลี่ยนแปลงหน้าที่ และให้ผู้ดูแลดำเนินการเปลี่ยนแปลงสิทธิ์ตามวันที่มีผลในการเปลี่ยนแปลงหน้าที่โดยทันที

(2.3) กรณีที่ไม่ใช่บุคลากรของสภากาชาดไทย จะหมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี

2.4 การบริหารจัดการสิทธิ์การใช้งาน และรหัสผ่าน

(1) ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

(2) กำหนดการเปลี่ยนแปลง และการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(4) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่มั่นคงปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(5) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน

(6) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง หากเกินให้ทำการกำหนดมาตรการป้องกันการสุ่มเดารหัสผ่าน เช่น หน่วงเวลาไม่ให้ใส่รหัสผ่านตามแต่ละหน่วยงานกำหนด หรือเป็นระยะเวลาอย่างน้อย 15 นาที หรือล็อกบัญชีผู้ใช้งานชั่วคราว เป็นต้น

(7) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(8) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษหรือผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง ต้องกำหนดให้รหัสผ่านผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ และต้องทบทวนทุก 30 วัน

2.5 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(1) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การ รับ-ส่ง ข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(5) ต้องกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำทรัพย์สินออกนอกหน่วยงาน เช่น บำรุงรักษาตรวจซ่อมให้ดำเนินการสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2.6 ระบบงานสารสนเทศที่ต้องเชื่อมโยงกัน ให้ผู้บังคับบัญชาพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน โดยหน่วยงานจะต้องดำเนินการดังต่อไปนี้

(1) กำหนดนโยบาย และมาตรการเพื่อควบคุมป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(2) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(3) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(4) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(5) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกัน ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

3.1 การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(2) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษรซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

(3) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อ นามสกุลของตนเอง หรือบุคคลในครอบครัว

(4) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

(5) ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ที่ไม่มั่นคงปลอดภัยหรือไม่ได้มาตรฐาน สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(6) ไม่จดและไม่บันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(7) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(8) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

3.2 การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับผู้ใช้งานต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากลที่ทันสมัยล่าสุด ณ ขณะนั้น

3.3 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

3.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สิน หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อก หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทาง ดังนี้

(1) ต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนการเข้าถึงระบบปฏิบัติการ

(2) การใช้งานระบบคอมพิวเตอร์อื่นในระบบเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานอินเทอร์เน็ตต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) ไว้ไม่เกิน 30 นาที หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(6) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.5 ผู้ใช้งานต้องตระหนัก และระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของสภากาชาดไทย หรือเป็นข้อมูลของบุคคลภายนอก

3.6 ข้อมูลที่เป็นความลับ หรือมีระดับความสำคัญที่อยู่ในการครอบครองของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

3.7 ผู้ใช้งานมีส่วนในการรับผิดชอบต่อข้อมูลของสภากาชาดไทย และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย ถูกนำไปใช้ในทางที่ผิด หรือการเผยแพร่โดยไม่ได้รับอนุญาต

3.8 ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

3.9 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษาใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สภากาชาดไทยจะให้การสนับสนุน และเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่หน่วยงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับหน่วยงาน ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

3.10 ห้ามใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิตทอร์เรนต์ (BitTorrent), อีมูล (eMule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

3.11 ห้ามใช้งานโปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

3.12 ห้ามใช้ทรัพย์สินของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูลข้อความรูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสภากาชาดไทย

3.13 ห้ามใช้ทรัพย์สินของหน่วยงานอันที่จะก่อให้เกิดความเสียหาย หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม

3.14 ห้ามใช้ทรัพย์สินของสภากาชาดไทยเพื่อประโยชน์ทางการค้า

3.15 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่ายระบบสารสนเทศของสภากาชาดไทยโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

3.16 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

3.17 ห้ามใช้ระบบสารสนเทศของสภากาชาดไทย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3.18 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งาน หรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

3.19 ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของสภากาชาดไทยโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ดูแลระบบที่ได้รับมอบหมาย

4. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

4.1 ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

4.2 การใช้งานอุปกรณ์คอมพิวเตอร์ส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน อุปกรณ์ดังกล่าวต้องลงทะเบียนเพื่อควบคุมดูแล ตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

4.3 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง เช่น อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

4.4 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนได้รับอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของหน่วยงานได้ ดังนี้

(1) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องพิสูจน์ตัวตนผู้ใช้ด้วยบัญชีผู้ใช้งานทุกครั้ง

(2) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง ด้วยการใช้รหัสผ่านหรือการใช้สมาร์ทการ์ด

(3) ต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบเทคโนโลยีสารสนเทศของหน่วยงานแบบ Multi-Factor Authentication เพื่อเพิ่มความมั่นคงปลอดภัย หรืออย่างน้อย 2 วิธี

(4) ผู้ดูแลระบบต้องตรวจสอบผู้ใช้งาน เมื่อมีการเข้าสู่ระบบเทคโนโลยีสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

4.5 การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนระบบเครือข่าย

(1) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อระบบเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

(2) ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(3) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากระบบเครือข่ายภายนอกต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับระบบเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

(4) อุปกรณ์ระบบเครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทาง และปลายทางได้

(5) การเข้าใช้งานอุปกรณ์บนระบบเครือข่ายต้องทำการพิสูจน์ตัวตนของผู้ใช้ทุกครั้ง

(6) อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

(7) ผู้ดูแลระบบจะต้องบันทึกข้อมูล Mac Address เพื่อประโยชน์ในการบริหารจัดการอุปกรณ์ต่าง ๆ

4.6 การป้องกัน Port ที่ใช้สำหรับทดสอบ และปรับแต่งระบบ

(1) ต้องควบคุม Port และหมายเลข IP Address ที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้เข้าถึงอุปกรณ์ระบบเครือข่ายอย่างรัดกุม

(2) ต้องกำหนดรหัสผ่านสำหรับตรวจสอบ และปรับปรุงอุปกรณ์ระบบเครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

(3) ไม่อนุญาตให้เชื่อมต่อ Port โดยตรงจากระบบเครือข่ายภายนอกสภากาชาดไทย แต่ให้เชื่อมต่อโดยตรงบนตัวอุปกรณ์

(4) อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์ระบบเครือข่ายที่ควบคุมความมั่นคงปลอดภัย

(5) ต้องปิด Port หรือปิด Service บนอุปกรณ์ระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(6) ต้องตรวจสอบ และปิด Port ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานทันที

(7) ต้องตรวจสอบ และยกเลิกการใช้งานอุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานทันทีหลังจากทดสอบเสร็จสิ้น

4.7 กำหนดให้มีการแบ่งแยกระบบเครือข่าย ดังต่อไปนี้

(1) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายใน และระบบเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(2) แบ่งแยกระบบเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้งาน และระบบงานต่าง ๆ ของสภากาชาดไทย

(3) ต้องแบ่งแยกระบบเครือข่ายภายในออกเป็นระบบเครือข่ายย่อย ๆ

(4) ต้องใช้ Gateway เพื่อควบคุมการเข้าถึงระบบเครือข่ายภายใน และระบบเครือข่ายภายนอกหน่วยงานซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึง และนโยบายการใช้งานบริการระบบเครือข่ายของหน่วยงาน

4.8 ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสภากาชาดไทย ต้องเชื่อมต่อผ่านอุปกรณ์ไฟร์วอลล์ และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี และอนุญาตการเชื่อมต่อเฉพาะหมายเลข IP Address ที่กำหนดให้เท่านั้น

4.9 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

4.10 IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

4.11 การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

4.12 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องกำหนดวิธีการจำกัดเส้นทางเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(3) ต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(4) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของสภากาชาดไทย

(5) ต้องกำหนดการป้องกันระบบเครือข่าย และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 2 ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

4.13 กำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย เพื่อดูแลรักษาความมั่นคงปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บังคับบัญชาของหน่วยงานหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

(2) ผู้ดูแลระบบต้องควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม โดยต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติ และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

(3) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บังคับบัญชาของหน่วยงานหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

(4) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(5) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

(6) การเข้าสู่ระบบต้องมีการใช้มาตรการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น การใช้ VPN SSL เป็นต้น

(7) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเชื่อมต่อกับระบบระยะไกลได้เพียงหนึ่งการเชื่อมต่อในขณะเวลาเดียวกัน

(8) ผู้ดูแลระบบต้องกำหนด Port ที่ใช้ในการเข้าสู่ระบบ และต้องตรวจสอบ และติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

4.14 การควบคุมการจัดการเส้นทางบนระบบเครือข่าย

(1) อนุญาตเส้นทางระบบเครือข่ายเฉพาะกลุ่มหมายเลข IP Address ที่กำหนด

(2) มี Gateway เพื่อกรองข้อมูลที่ผ่านระบบเครือข่าย และต้องควบคุมการไหลของข้อมูลผ่านระบบเครือข่าย

(3) ต้องกำหนดเส้นทางการ รับ-ส่ง ของข้อมูลบนระบบเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึง และการใช้บริการบนระบบเครือข่าย

(4) ต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

(5) ต้องตรวจสอบหมายเลข IP Address ของต้นทางและปลายทาง

5. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

5.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสภากาชาดไทยต้องทำการลงทะเบียนกับผู้ดูแลระบบ และได้รับพิจารณาอนุญาตจากผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

5.2 ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(1) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(2) ต้องทำการลงทะเบียนอุปกรณ์กระจายสัญญาณไร้สายทุกตัวที่ใช้ในระบบเครือข่ายไร้สาย

(3) ต้องควบคุม ป้องกันสัญญาณของอุปกรณ์กระจายสัญญาณไร้สาย ไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

(4) ต้องทำการเปลี่ยนค่าชื่อระบบเครือข่ายไร้สาย ที่ถูกกำหนดเป็นค่าตั้งต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

(5) ต้องทำการเปลี่ยนค่าชื่อบัญชีผู้ใช้ และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อ และรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(6) ต้องเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณไร้สายด้วยวิธีที่มีประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 เพื่อให้ยากต่อการดักจับข้อมูล และทำให้มั่นคงปลอดภัยมากขึ้น

(7) ควรเลือกใช้วิธีการควบคุม MAC Address และ/หรือชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และ/หรือชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(8) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

(9) ต้องติดตั้งไฟร์วอลล์ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในสภากาชาดไทย

(10) ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างน้อย 90 วัน เพื่อตรวจสอบ และบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบโดยทันที หรือภายใน 4 ชั่วโมง

6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

6.1 ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

6.2 กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติดังนี้

(1) ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(2) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(3) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

6.3 ระบุ และยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงที่สามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

(1) การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

(2) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุ และยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

(3) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(4) ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

6.4 การบริหารจัดการรหัสผ่าน (Password Management System)

(1) ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

(2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

(3) มีระบบให้ผู้ใช้งานสามารถเปลี่ยน และยืนยันรหัสผ่านได้ด้วยตนเอง

(4) ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

(5) ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

(6) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

6.5 การใช้งานโปรแกรมประเภทยูทิลิตี้ต้องจำกัด และควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(1) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้เพื่อจำกัด และควบคุมการใช้งาน

(2) โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่สภากาชาดไทยได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

(3) ต้องจัดเก็บโปรแกรมยูทิลิตี้แยกออกจากโปรแกรมสำหรับระบบงาน

(4) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(5) ต้องยกเลิกหรือลบโปรแกรมยูทิลิตี้ และโปรแกรมที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

(6) ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

6.6 การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Timeout)

(1) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน 30 นาที หากเป็นระบบที่มีความเสี่ยงสูงหรือมีความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งาน เมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน 15 นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(2) ถ้าไม่มีการใช้ระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(3) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูง ต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

6.7 การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

(1) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศที่มีความเสี่ยงสูง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ 3 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง เป็นต้น และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาทำการตามปกติของหน่วยงานเท่านั้น

(2) กำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(3) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน ที่มีการจำกัดช่วงเวลาการเชื่อมต่อ

7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

7.1 ให้หน่วยงาน กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อดูแลรักษาความมั่นคงปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอก หรือบุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงาน ต้องขออนุญาตจากผู้บังคับบัญชาหรือจากผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

7.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยทุก 90 วัน

7.3 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความมั่นคงปลอดภัยที่มีต่อระบบข้อมูล

7.4 ผู้ดูแลระบบ จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่าน เข้า-ออก สถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาต และไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบย้อนหลังได้ 1 ปีเป็นอย่างน้อย

7.5 ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสภากาชาดไทย ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

7.6 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยทุก 90 วัน

7.7 ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน 15 นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งานอีกครั้ง

7.8 ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบ และรหัสผ่านของบุคลากร ดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลง และการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดชื่อผู้ใช้งานในระบบต้องไม่ซ้ำกัน

(4) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับการอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง โดยมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

7.9 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การ รับ-ส่ง ข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากลเช่น SSL, VPN หรือ XML Encryption เป็นต้น

(5) กำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลนั้นก่อน เป็นต้น

7.10 ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อสภากาชาดไทย ต้องดำเนินการดังนี้

(1) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสภากาชาดไทย เช่น ระบบสารสนเทศการเงินสภากาชาดไทย จะได้รับการแยกระบบเครือข่ายออกจากระบบงานอื่น ๆ ของหน่วยงาน

(2) ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีพื้นที่ปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น เข้าปฏิบัติงานในพื้นที่ควบคุมดังกล่าว

7.11 การใช้งานอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ต้องปฏิบัติ ดังต่อไปนี้

(1) ตรวจสอบความพร้อมของเครื่องคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งาน ว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนด้วย

(5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(6) การใช้อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารเคลื่อนที่ของสภากาชาดไทยต้องดำเนินการดังต่อไปนี้

(6.1) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่ กรณีนำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(6.2) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(6.3) ผู้ใช้งานต้องตั้งรหัสผ่านเพื่อพิสูจน์ตัวตนก่อนเข้าใช้งาน

(6.4) ไม่ใช้งานอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ร่วมกับบุคคลอื่น

(6.5) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าว ต้องเข้ารหัสข้อมูลทุกครั้ง

(6.6) ห้ามใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ เป็นอุปกรณ์กระจายสัญญาณระบบเครือข่ายไร้สายภายในสภากาชาดไทย

(6.7) อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ ที่สามารถติดตั้งโปรแกรม Antivirus ได้ ต้องทำการปรับปรุงโปรแกรม Antivirus นั้น ให้มีความทันสมัยเป็นปัจจุบัน ถูกต้องตามกฎหมาย

(6.8) มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์เคลื่อนที่เกิดการสูญหาย หรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

(7) การสำรองข้อมูล และการกู้คืน

(7.1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูล จากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลสำรอง (Backup Media) เช่น ฮาร์ดดิสก์ภายนอก (External Hard Disk) เป็นต้น

(7.2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.12 การควบคุมผู้ให้บริการภายนอก กรณีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

(1) มีกระบวนการคัดเลือกผู้ให้บริการภายนอก โดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้ให้บริการภายนอกที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการให้บริการทั้งในส่วนของ ฮาร์ดแวร์ และซอฟท์แวร์ รวมถึงระบบสนับสนุนอื่น ๆ เพื่อให้ได้ผู้ให้บริการภายนอก ที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

(2) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้ให้บริการภายนอก และต้องกำหนดขอบเขตและระดับการให้บริการอย่างชัดเจน และผู้ให้บริการภายนอกต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

(3) หน่วยงานต้องเข้าตรวจสอบรายละเอียดการปฏิบัติงานของผู้ให้บริการภายนอก ได้ เช่น ร่วมกำหนดวิธีทำงาน การตรวจติดตามคุณภาพของผู้ให้บริการภายนอก เป็นระยะ ๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้ให้บริการภายนอก ใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้ให้บริการภายนอก ในการกระทำตามข้อกำหนดของหน่วยงาน

(4) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

(5) มีหลักเกณฑ์ และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้ให้บริการภายนอก ที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

ส่วนที่ 3
นโยบายการบริหารจัดการและการรักษาความมั่นคงปลอดภัยข้อมูลและข้อมูลส่วนบุคคล

วัตถุประสงค์

1. เพื่อกำหนดเกณฑ์การแบ่งระดับชั้นความลับของข้อมูล และข้อมูลส่วนบุคคล
2. เพื่อกำหนดมาตรการในการป้องกันการเข้าถึงข้อมูล และข้อมูลส่วนบุคคลตามการจัดระดับชั้นความลับของข้อมูล

แนวปฏิบัติ

1. การแบ่งประเภทของข้อมูล และการจัดลำดับชั้นความลับของข้อมูล (Information Classification)

1.1 การแบ่งประเภทของข้อมูล และการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ใช้แนวทางปฏิบัติชั้นความลับตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบครอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความมั่นคงปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

(1) จัดแบ่งประเภทของข้อมูลออกเป็น

(1.1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงิน และบัญชี เป็นต้น

(1.2) ข้อมูลสารสนเทศด้านการแพทย์ และการสาธารณสุข ได้แก่ ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(2) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น 3 ระดับ คือ

(2.1) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(2.2) ข้อมูลที่มีระดับความสำคัญปานกลาง

(2.3) ข้อมูลที่มีระดับความสำคัญน้อย

(3) จัดแบ่งลำดับชั้นความลับของข้อมูล

(3.1) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(3.2) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(3.3) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(3.4) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(4) จัดแบ่งระดับชั้นการเข้าถึง

(4.1) ระดับชั้นสำหรับผู้บริหาร

(4.2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(4.3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(5) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

(5.1) รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นโปรแกรมปกติ เมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์ และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format) เป็นต้น

(5.2) รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นโปรแกรมมีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format เป็นต้น

1.2 การรักษาข้อมูลส่วนบุคคล และการปกป้องข้อมูลที่สามารถระบุตัวตนได้อย่างมั่นคงปลอดภัย หรือข้อมูลอ่อนไหว ต้องอ้างอิงตามระเบียบสภากาชาดไทย ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564, ประกาศสภากาชาดไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2564, ประกาศสภากาชาดไทย เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2565 และประกาศสภากาชาดไทย เรื่อง กรอบแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล สภากาชาดไทย พ.ศ. 2565

1.3 กำหนดหมวดหมู่ของรายการข้อมูลทั้งหมดที่ต้องการควบคุมการรั่วไหล โดยข้อมูลแต่ละรายการควรจะมีการจัดเก็บไว้เป็นหมวดหมู่ เพื่อให้ง่ายในการบริหารจัดการ การสืบค้น และการใช้งาน

1.4 กำหนดผู้รับผิดชอบข้อมูลสารสนเทศ พร้อมทั้งผู้ใช้งานข้อมูลสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูลสำคัญให้เป็นไปตามที่ได้รับอนุญาตเท่านั้น

1.5 กำหนดสถานที่สำหรับจัดเก็บข้อมูลสารสนเทศแต่ละรายการ เช่น ระบบสำหรับการจัดเก็บข้อมูล File Server อุปกรณ์จัดเก็บข้อมูล เป็นต้น โดยสามารถพิจารณาการนำโปรแกรมมาใช้กำหนดเกณฑ์หรือใช้ในการตรวจสอบข้อมูล เพื่อควบคุมการนำข้อมูลเข้ามาจัดเก็บในสถานที่สำหรับจัดเก็บข้อมูล

1.6 หน่วยงานต้องจัดเก็บ และรักษาข้อมูลที่เป็นเอกสารหรือที่เป็นไฟล์อิเล็กทรอนิกส์ ไว้ในสถานที่และสภาพแวดล้อมที่มีความมั่นคงปลอดภัย และควบคุมการเข้าถึงตามสิทธิ์ที่ได้รับเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1.7 หน่วยงานต้องกำหนดระยะเวลาขั้นต่ำ สำหรับการจัดเก็บข้อมูลแต่ละประเภทโดยคำนึงถึง

(1) ความสอดคล้องกับกฎหมาย ระเบียบ หรือข้อบังคับที่หน่วยงานต้องปฏิบัติตาม

(2) ข้อกำหนดในสัญญาจ้างที่ต้องปฏิบัติตาม

1.8 เมื่อพ้นระยะเวลาการจัดเก็บที่กำหนดไว้ หน่วยงานสามารถพิจารณาขยายระยะเวลาการจัดเก็บข้อมูลเพิ่มเติมได้ โดยให้พิจารณาจากข้อกำหนดทั้ง 2 ข้อที่ได้กล่าวถึงในหัวข้อที่แล้วนั้น

1.9 ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล ต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

2. ข้อตกลงในการถ่ายโอนข้อมูลสารสนเทศ (Information Transfer Agreement)

2.1. การทำข้อตกลงในการถ่ายโอนข้อมูลสารสนเทศ และลงนามในเอกสารข้อตกลงไม่เปิดเผยความลับในการถ่ายโอนข้อมูลสารสนเทศ

2.2. มีการกำหนดวิธีการ หรือช่องทางการถ่ายโอนข้อมูลสารสนเทศ และมีการแจ้งให้ผู้ รับ-ส่ง ทราบ

2.3. มีการบันทึกข้อมูลการติดต่อในการถ่ายโอนข้อมูลสารสนเทศ ที่สามารถติดตามและตอบกลับได้

2.4. มีการระบุชั้นความลับของข้อมูลสารสนเทศที่จะมีการถ่ายโอน

3. การถ่ายโอนข้อมูลสารสนเทศทางอิเล็กทรอนิกส์ (Electronic Data Transfer)

3.1 มีมาตรการป้องกันทางเทคนิคจากการถูกดักจับ คัดลอก แก้ไข และการทำลายข้อมูลสารสนเทศระหว่างถ่ายโอนข้อมูล เช่น ประยุกต์ใช้การเข้ารหัสข้อมูลในการถ่ายโอนข้อมูลที่เป็นความลับ รวมถึงการตรวจจับและป้องกันมัลแวร์

3.2 ต้องมีการยืนยันการ รับ-ส่ง ข้อมูลสารสนเทศกับผู้รับปลายทางทุกครั้ง

3.3 กรณีที่มีการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องระมัดระวังด้านการรักษาความมั่นคงปลอดภัย เช่น ตรวจสอบความถูกต้องของจดหมายอิเล็กทรอนิกส์ ผู้รับเพื่อป้องกันการส่งผิด หรือการส่งข้อมูลที่เป็นความลับต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อของจดหมายอิเล็กทรอนิกส์ เว้นแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมลที่หน่วยงานกำหนด

3.4 กรณีที่มีการใช้เครื่องโทรสาร ผู้ใช้งานต้องมีความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องดำเนินการอย่างน้อย ดังต่อไปนี้

(1) ใช้เครื่องโทรสารที่อยู่ในพื้นที่ควบคุม เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

(2) ตรวจสอบเลขหมายปลายทางให้ชัดเจนก่อนส่งทุกครั้ง

(3) ตรวจสอบความครบถ้วนของเอกสารที่พิมพ์ออกมาทุกครั้ง

(4) ยืนยันการ รับ-ส่ง ข้อมูลสารสนเทศกับผู้รับปลายทางทุกครั้ง

3.5 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

3.6 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้งซึ่งข้อมูลข้อความเอกสารหรือสิ่งใด ๆ ที่เป็นทรัพย์สินของหน่วยงานหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

4. การลบหรือทำลายข้อมูล (Data Deletion or Destruction)

4.1 การลบหรือทำลายข้อมูล ต้องอ้างอิงตาม ระเบียบสภากาชาดไทยว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564, ประกาศสภากาชาดไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2564, ประกาศสภากาชาดไทย เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2565 และประกาศสภากาชาดไทย เรื่อง กรอบแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล สภากาชาดไทย พ.ศ. 2565

4.2 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย ดำเนินการลบหรือทำลายข้อมูลตามกระบวนการเมื่อถึงระยะเวลาที่กำหนด ขออนุมัติทำลายข้อมูลที่พ้นระยะเวลาการจัดเก็บ หน่วยงานต้องพิจารณาการลบทำลายข้อมูลบนระบบ แอปพลิเคชัน หรือบริการต่าง ๆ

4.3 วิธีการลบข้อมูลที่มีความอ่อนไหว เมื่อไม่มีความจำเป็น หรือไม่มีความต้องการอีกต่อไป โดยใช้โปรแกรมการลบข้อมูลที่มีความน่าเชื่อถือ ปลอดภัย และมั่นใจว่าไม่สามารถกู้คืนข้อมูลที่ลบกลับมาได้ เลือกวิธีการลบ ทำลายที่เหมาะสมกับระดับชั้นความลับของข้อมูล

4.4 กรณีที่จะนำอุปกรณ์ สื่อบันทึกต่าง ๆ ที่มีข้อมูลออกไปนอกพื้นที่ หรือส่งซ่อมควรตรวจสอบพิจารณามาตรการป้องกันข้อมูลสารสนเทศที่มีความอ่อนไหว เพื่อป้องกันข้อมูลถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต

4.5 ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	– ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ – ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์ / SSD / Storage	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ หรือใช้วิธีการทุบหรือบดให้เสียหาย

5. ปิดบังข้อมูล (Data Masking)

5.1 กำหนดให้หน่วยงานพิจารณาการใช้เทคนิคสำหรับการปิดบังข้อมูล เพื่อป้องกันข้อมูลที่มีความอ่อนไหว ข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ข้อมูลลับ หรือข้อมูลอื่น ๆ ที่มีความสำคัญถูกมองเห็นหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

5.2 พิจารณาการใช้เทคนิคการปิดบังข้อมูล ที่เหมาะสมกับลักษณะของข้อมูล หรือความสำคัญของข้อมูล เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ด้วยวิธีการดังต่อไปนี้

(1) การเข้ารหัสข้อมูล ซึ่งเทคนิคนี้จำเป็นต้องใช้กุญแจ (Key) ในการเข้าและถอดรหัสข้อมูล

(2) การ Hash ในการเปลี่ยนค่าต่าง ๆ ไปเป็นอีกค่าที่ต่างออกไป เพื่อให้ยากต่อการเปลี่ยนข้อมูลกลับได้ ซึ่งผู้ที่จะสามารถเข้าจริงได้นั้นต้องเป็นผู้ที่สามารถเข้าถึงข้อมูลที่ถูกเทียบเคียงไว้กับข้อมูลที่ถูกเปลี่ยนแปลงโดยการ Hash ไว้เท่านั้น

(3) พิจารณาการใช้ Salt ร่วมกับการ Hash เพื่อเพิ่มความมั่นคงปลอดภัยข้อมูล

(4) การเปลี่ยนข้อมูลตั้งต้นบางส่วนให้เป็นตัวอักษร หรือสัญลักษณ์ (Masking Out) เช่น ข้อมูลเลขบัตรประจำตัวประชาชนเปลี่ยนเป็น 123 XXXX XXX 567 หรือเบอร์โทรศัพท์เปลี่ยนเป็น 081 XXX XX78 เป็นต้น หน่วยงานเป็นผู้พิจารณาความสำคัญของตำแหน่งการ Masking ข้อมูล

(5) การปกปิดข้อความที่สำคัญ หรือรูปภาพที่มีความอ่อนไหว บนเอกสารประเภทกระดาษ หรือเอกสารอิเล็กทรอนิกส์ เช่น การคาดสีดำ หรือวิธีการที่เหมาะสมที่ไม่สามารถ Reverse ข้อมูลกลับมาได้

5.3 พิจารณาการใช้เทคนิคการแฝงข้อมูล (Pseudonymization) เป็นวิธีการแปลงข้อมูลส่วนบุคคลตั้งต้นให้ไปเป็นชื่ออื่น หรือการทำให้ไม่สามารถระบุได้ว่าใครเป็นเจ้าของข้อมูลส่วนบุคคลที่แท้จริง โดยสามารถเลือกใช้เทคนิคการปิดบังข้อมูลในข้างต้นมาประกอบการดำเนินการ เช่น เทคนิคการเปลี่ยนข้อมูลตั้งต้นบางส่วนให้เป็นตัวอักษร หรือสัญลักษณ์ (Masking Out) เป็นต้น

5.4 พิจารณาการใช้เทคนิคการปิดบังข้อมูล การแปลงข้อมูลให้เป็นนามแฝง ต้องเป็นไปตามกฎหมายระเบียบ หรือข้อบังคับที่เกี่ยวข้องที่สภากาชาดไทยต้องปฏิบัติตาม เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งกำหนดให้ต้องป้องกันข้อมูลส่วนบุคคลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 4
นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

1. เพื่อกำหนดมาตรการในการป้องกันการบุกรุกทางกายภาพ และระบบสนับสนุนเพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย

แนวปฏิบัติ

1. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม (Physical and Environmental Security)

1.1 อาคารสถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่ายหรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์ และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และแบบพกพา และอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

1.2 ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ต้องมีลักษณะ ดังนี้

(1) กำหนดเป็นเขตหวงห้ามเด็ดขาดหรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(2) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่าน เข้า-ออก ของบุคคลเป็นจำนวนมาก

(3) ต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(4) ต้องปิดล็อกหรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(5) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสารให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(6) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงาน

(7) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

1.3 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(1) มีการจำแนก และกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(2) กำหนด และแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้ง

อุปกรณ์ระบบเทคโนโลยีสารสนเทศ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ และพื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

1.4 การควบคุมการ เข้า-ออก อาคารสถานที่

(1) กำหนดให้มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูดการใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ

(2) กำหนดสิทธิ์ผู้ใช้งานที่มีสิทธิ์ผ่าน เข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่าน เข้า-ออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(3) ห้ามไม่ให้ผู้ที่ไม่มีสิทธิ์ หรือไม่มีส่วนเกี่ยวข้อง เข้า-ออก พื้นที่เขตหวงห้าม

(4) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย ต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอร์มการเข้า-ออก พร้อมกับบัตรผู้ติดต่อ

(5) ให้มีการบันทึกวัน และเวลาการ เข้า-ออก พื้นที่สำคัญของผู้ที่มาติดต่อ

(6) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(7) หน่วยงานภายนอกที่ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(8) จัดเก็บบันทึกการ เข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น Data Center เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(9) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ และจากไป เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(10) มีกลไกการอนุญาตการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(11) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่ หรือบริเวณที่มีความสำคัญ

(12) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(13) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต

(14) จัดให้มีการดูแล และเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(15) จัดให้มีการทบทวนหรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญทุก 3 เดือน

1.5 ระบบ และอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(1) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ดังต่อไปนี้

(1.1) ระบบสำรองกระแสไฟฟ้า

(1.2) เครื่องกำเนิดกระแสไฟฟ้า

(1.3) ระบบควบคุมอุณหภูมิและความชื้น

(1.4) ระบบแจ้งเตือนและระบบดับเพลิง

(1.5) ระบบส่องสว่างฉุกเฉิน

(2) กำหนดให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(3) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องคอมพิวเตอร์แม่ข่ายทำงานผิดปกติหรือหยุดการทำงาน

1.6 การติดตั้งสายไฟ สายสื่อสารและสายเคเบิลอื่น ๆ (Cabling Security)

(1) หลีกเลี่ยงการติดตั้งสายสัญญาณระบบเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(2) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(3) ให้ติดตั้งสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(4) ต้องทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(5) จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วน และถูกต้อง

(6) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องมีการป้องกันการเข้าถึงจากบุคคลภายนอก

(7) พิจารณาใช้งานสายใยแก้วนำแสงแทนสายสัญญาณสื่อสารแบบเดิม สำหรับระบบสารสนเทศที่สำคัญ

(8) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดีอย่างน้อยปีละ 1 ครั้ง

1.7 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(1) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยสามารถตรวจสอบย้อนหลังได้ 1 ปี เป็นอย่างน้อย

(4) จัดเก็บบันทึกปัญหา และข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมิน และปรับปรุงอุปกรณ์ดังกล่าว โดยสามารถตรวจสอบย้อนหลังได้ 1 ปี เป็นอย่างน้อย

(5) ควบคุม และสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(6) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้ให้บริการภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

1.8 การนำทรัพย์สินสารสนเทศของหน่วยงานออกนอกหน่วยงาน (Removal of Assets)

(1) ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินสารสนเทศนั้นออกไปใช้งานนอกหน่วยงาน

(2) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงานเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(3) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(4) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(5) ต้องลบข้อมูลที่สำคัญก่อนนำส่งคืน

(6) ต้องตรวจสอบการชำรุดเสียหายของอุปกรณ์ เมื่อมีการนำอุปกรณ์นั้นมาส่งคืน

1.9 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

(1) กำหนดมาตรการความมั่นคงปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(2) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(3) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

1.10 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

(1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(2) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ 5
นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อกำหนดมาตรการในการป้องกันการบุกรุก และการโจมตีหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

1. การรับมือกับเหตุการณ์ (Incident Response)

1.1 มีการกำหนดวิธีปฏิบัติอย่างชัดเจน เมื่อมีเหตุการณ์ที่จะก่อให้เกิดความไม่ปลอดภัยสารสนเทศ

1.2 มีการกำหนดผู้รับผิดชอบ และหน้าที่รับผิดชอบอย่างชัดเจน

1.3 กำหนดเกณฑ์ของเหตุการณ์เพื่อให้สามารถตอบสนองกับเหตุการณ์ได้ทันท่วงที

1.4 มีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ

1.5 กำหนดให้มีการเฝ้าระวัง และป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติ และการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์ และหาสาเหตุของการบุกรุก ในระบบสารสนเทศเพื่อเป็นเครื่องมือสืบสวน หาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด

1.6 ผู้ดูแลระบบต้องมีการบริหารจัดการ เหตุการณ์ไม่ปกติ โดยต้องจัดลำดับความสำคัญของ Incident จากผลกระทบที่เกิดขึ้น และจัดทำวิธีปฏิบัติที่ถูกต้อง ให้กับหน่วยงานเพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

1.7 การเก็บหลักฐานด้านสารสนเทศในสถานที่ปลอดภัย มีข้อกำหนด และควบคุมการนำมาใช้เพื่อไม่ให้เกิดการสูญหาย

1.8 ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตี เพื่อใช้เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความมั่นคงปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น และเพื่อเป็นการปรับปรุง ป้องกันระบบเครือข่ายภายในจากอันตราย ที่มาจากระบบเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือผู้ไม่ประสงค์ดี รวมทั้งไวรัสประเภทต่าง ๆ และสามารถตรวจสอบย้อนหลังได้ 1 ปี เป็นอย่างน้อย

1.9 เมื่อเกิดสถานการณ์ที่ไม่ปลอดภัยหรือมีจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย ให้มีการรายงานต่อผู้ดูแลระบบ และผู้บังคับบัญชาให้ทราบทุกครั้ง ไม่เกิน 1 ชั่วโมง หรือตามที่หน่วยงานกำหนดโดยขึ้นอยู่กับระดับผลกระทบที่ได้รับ

1.10 กำหนดแหล่งข้อมูลข่าวสารที่เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีความน่าเชื่อถือ เพื่อใช้เป็นช่องทางในการติดตาม และเรียนรู้ภัยคุกคามทางไซเบอร์ใหม่ ๆ เช่น เว็บไซต์ต่าง ๆ ที่น่าเชื่อถือบริษัทเจ้าของผลิตภัณฑ์ที่หน่วยงานมีการใช้งาน

1.11 ทบทวน และปรับปรุงแหล่งข้อมูลข่าวสารที่เกี่ยวกับภัยคุกคามทางไซเบอร์ตามระยะเวลาที่กำหนด หรืออย่างน้อยทุก 6 เดือน หรือเมื่อมีเหตุการณ์เปลี่ยนแปลง

1.12 วิเคราะห์และประเมินข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ได้รับ เพื่อนำไปวางแผนและดำเนินการตามความจำเป็น

1.13 สื่อสารและแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ได้ทำการคัดกรองแล้วว่ามีความน่าเชื่อถือ หรือมีความเป็นไปได้สูง ตลอดจนเหตุการณ์ด้านความมั่นคงปลอดภัยที่หน่วยงานทราบไปยังหน่วยงานที่เกี่ยวข้อง หรือเป็นพันธมิตร เพื่อให้สามารถระมัดระวังและป้องกันหน่วยงานของตนเองได้อย่างเหมาะสม

2. เครื่องมือสนับสนุนการรับมือเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ (Incident Response Tool)

2.1 ระบบป้องกันผู้บุกรุก (IPS/IDS System)

(1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง

(2) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุกสิ่งที่ทำการตรวจสอบ มีดังต่อไปนี้

(2.1) มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด

(2.2) ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

(2.3) ระดับความรุนแรงมากน้อยเพียงใด

(2.4) หมายเลขไอพีของระบบเครือข่ายที่เป็นผู้โจมตี

2.2 ระบบไฟร์วอลล์ (Firewall System)

(1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง

(2) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

(2.1) Packet ที่ไฟร์วอลล์ได้ทำการ Block

(2.2) ลักษณะของ Packet ที่ถูก Block

(2.3) Packet ของหมายเลข IP Address ของระบบเครือข่ายใดถูก Block เป็นจำนวนมาก

(3) กรณีตรวจพบการโจมตีระบบ หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

(4) เฝ้าระวังช่องทาง และข้อมูลที่อ่อนไหวซึ่งเสี่ยงต่อการถูกเปิดเผยโดยไม่ได้รับอนุญาตหรือรั่วไหล อย่างน้อยเดือนละ 1 ครั้ง

2.3 ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต หรือชุดคำสั่งไม่พึงประสงค์ (Malware)

(1) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตสิ่งที่ต้องตรวจสอบ มีดังนี้

(1.1) ชุดคำสั่งไม่พึงประสงค์ประเภทใดถูกพบเป็นจำนวนมาก

(1.2) ชุดคำสั่งไม่พึงประสงค์ถูกส่งมาจากระบบเครือข่ายใด และถูกส่งไปยังที่ใด

(1.3) มีการส่งชุดคำสั่งไม่พึงประสงค์จากระบบเครือข่ายภายในสภากาชาดไทยไปยังภายนอกหรือไม่

(2) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในระบบเครือข่ายของสภากาชาดไทย

(3) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในระบบเครือข่ายถูกติดตั้งชุดคำสั่งไม่พึงประสงค์หรือส่งชุดคำสั่งไม่พึงประสงค์ออกไปนอกระบบเครือข่าย โดยต้องยุติการเชื่อมต่อของเครื่องที่ถูกติดตั้งชุดคำสั่งไม่พึงประสงค์และดำเนินการกับเครื่องคอมพิวเตอร์นั้นทันที

(4) กำหนด ทบทวน และปรับปรุงประเภทของเว็บไซต์ที่หน่วยงานไม่อนุญาตให้เข้าถึงอย่างสม่ำเสมอ เช่น

(4.1) เว็บไซต์ที่ขัดต่อศีลธรรม ลามก อนาจาร การพนัน การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา พระมหากษัตริย์ และสิ่งที่ขัดต่อศีลธรรม กฎหมาย ความมั่นคงของประเทศ

(4.2) เว็บไซต์ที่มีมัลแวร์หรือโปรแกรมที่เป็นอันตรายฝังอยู่ จัดอยู่ในกลุ่มเว็บไซต์อันตราย

(4.3) เว็บไซต์ปลอม (Phishing)

(4.4) เว็บไซต์ที่จัดเก็บข้อมูล หรือเนื้อหาที่ผิดกฎหมาย หรือจัดเก็บโปรแกรมที่ละเมิดลิขสิทธิ์

(5) กรณีที่หน่วยงาน หรือผู้ใช้งานมีความจำเป็นต้องเข้าถึงเว็บไซต์ที่ไม่ได้รับอนุญาตดังกล่าว ต้องขออนุญาตผู้มีอำนาจ โดยระบุชื่อผู้ใช้ หรือหน่วยงานที่มีความจำเป็นต้องใช้ พร้อมทั้งระบุเหตุผล และความจำเป็นของการเข้าถึงนั้น

(6) ตั้งค่าระบบให้มีการคัดกรองเว็บไซต์ เพื่อป้องกันผู้ใช้งานเข้าถึงเว็บไซต์ที่ไม่ได้รับอนุญาต เช่น ระบบสำหรับการคัดกรองเว็บไซต์ หรือโปรแกรมป้องกันมัลแวร์ หรือใช้ความสามารถของเว็บเบราว์เซอร์ เป็นต้น

ส่วนที่ 6
นโยบายการจัดทำระบบสำรองสารสนเทศ และแผนเตรียมพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของสภากาชาดไทยมีสภาพพร้อมใช้ และสามารถให้บริการได้อย่างต่อเนื่อง
2. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย และผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูล และสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

แนวปฏิบัติ

1. ศูนย์ข้อมูลคอมพิวเตอร์สำรอง (Disaster Recovery Site: DR Site)

1.1 จัดทำบัญชีระบบเครือข่าย ระบบสารสนเทศที่สำคัญ และจำเป็นต้องมีระบบสำรอง รวมทั้งทบทวนบัญชีอย่างน้อยปีละ 1 ครั้ง เช่น ระบบบริการแปลงชื่อเป็นหมายเลข IP Address ระบบสารสนเทศทางการเงิน การบัญชี และการพัสดุ ระบบบริหารงานทรัพยากรบุคคล ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น

1.2 ศูนย์ข้อมูลคอมพิวเตอร์สำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากศูนย์ข้อมูลคอมพิวเตอร์หลัก และมีการควบคุม ดังนี้

(1) มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง
(2) มีระบบไฟฟ้าสำรอง
(3) มีระบบปรับอากาศ และความชื้นที่เหมาะสม
(4) มีระบบป้องกันอัคคีภัย
(5) มีระบบส่องสว่างที่เหมาะสม
(6) มีระบบสื่อสารหรือระบบเครือข่ายสำรอง
(7) มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

1.3 มีแผนบำรุงรักษาศูนย์ข้อมูลคอมพิวเตอร์สำรองทุกระบบอย่างต่อเนื่อง

2. การสำรองข้อมูล (Data Backup)

2.1 จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูล และทบทวนบัญชีปีละ 1 ครั้ง เช่น ระบบบริการแปลงชื่อเป็นหมายเลข IP Address ระบบสารสนเทศทางการเงิน การบัญชี และการพัสดุ ระบบบริหารงานทรัพยากรบุคคล ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น

2.2 กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

2.3 กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

2.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน เวลา ชื่อข้อมูลที่สำรอง สถานการณ์ทำงานที่สำเร็จหรือไม่สำเร็จ เป็นต้น

2.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น โปรแกรมต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบ และอุปกรณ์ต่าง ๆ เป็นต้น

2.6 จัดเก็บข้อมูลสำรองไว้ในศูนย์ข้อมูลคอมพิวเตอร์สำรอง

2.7 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อศูนย์ข้อมูลคอมพิวเตอร์สำรองที่ใช้จัดเก็บข้อมูลสำรอง

3. แผนเตรียมความพร้อมกรณีฉุกเฉิน (Business Continuity Plan)

มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

3.1 ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

3.2 มีการจัดลำดับความสำคัญของระบบงาน กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน ระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง และการประเมินผลกระทบของกระบวนงานหลัก

3.3 ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

3.4 ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

3.5 ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลสำรองไว้

3.6 ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

4. การกู้คืนข้อมูล (Data Recovery)

4.1 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

4.2 ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

4.3 ให้ใช้ข้อมูลทันสมัยที่สุด (Last Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

4.4 ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5. การทดสอบสภาพพร้อมใช้งาน (Availability testing)

ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ศูนย์ข้อมูลคอมพิวเตอร์สำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 7
นโยบายการตรวจสอบ และประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบ และประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
2. เพื่อเป็นการป้องกัน และลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

1. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศโดยผู้ดูแลระบบ และผู้ที่ได้รับมอบหมายอย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวทางการประเมินความเสี่ยงต้องคำนึงถึง ดังนี้

1.1 จัดลำดับความสำคัญของความเสี่ยง

1.2 ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

1.3 ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

1.4 สรุปผลข้อเสนอแนะ และแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

2. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ (Risks that Harm the Information Technology System)

จากการประเมินความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศสามารถแยกเป็นภัยต่าง ๆ ได้ 4 ประเภท ดังนี้

2.1 ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่ หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้เกิดการชะงักงันหรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ เป็นต้น ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(1) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ และซอฟต์แวร์เบื้องต้นเพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุดทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้ และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้ง

ทางด้านฮาร์ดแวร์ และซอฟต์แวร์ได้มีประสิทธิภาพยิ่งขึ้นทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(2) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลาง และส่วนภูมิภาคเรื่องการใช้ และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์ และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

2.2 ประเภทที่ 2 ภัยที่เกิดจากโปรแกรม ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวกโปรแกรมเหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากซอฟต์แวร์ดังนี้

(1) ติดตั้งไฟร์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(2) ติดตั้งโปรแกรม Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

2.3 ประเภทที่ 3 ภัยจากไฟไหม้หรือระบบไฟฟ้าจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องคอมพิวเตอร์แม่ข่าย ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และสำรองข้อมูลไว้อย่างมั่นคงปลอดภัย

(2) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่ายอุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(3) ติดตั้งอุปกรณ์ดับเพลิงสำหรับใช้งานในห้องควบคุมระบบคอมพิวเตอร์หรือระบบเครือข่ายเพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

2.4 ประเภทที่ 4 ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(2) จัดเก็บข้อมูลเทป Backup ไว้ในที่มั่นคงปลอดภัย

(3) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุมโดยปิดเบรกเกอร์เครื่องปรับอากาศเพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(4) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ระบบเครือข่ายไว้ในที่สูง

(5) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมระบบเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ระบบเครือข่าย

(6) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ระบบเครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบเครือข่ายว่าสามารถเชื่อมต่อ และให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(7) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้บริการได้ตามปกติ

3. การตรวจสอบ (Audit)

การตรวจสอบ หรือทวนสอบด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีมาตรการ หรือแนวทางในตรวจสอบที่ต้องคำนึงถึง ดังนี้

3.1 กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

3.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลาย หรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

3.3 กำหนดให้มีการระบุ และจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

3.4 กำหนดให้มีการเฝ้าระวัง การเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้นซึ่งรวมถึงวัน และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

3.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

3.6 จัดทำรายงานพร้อมข้อเสนอแนะเสนอต่อผู้บริหารรับทราบ และพิจารณา

4. ข้อยกเว้นในการไม่ปฏิบัติตามนโยบาย (Exceptions to Non-Compliance)

ข้อยกเว้นในการไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย ฉบับนี้ ให้หน่วยงานพิจารณาตามความเหมาะสม โดยไม่ขัดกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยระบุเหตุผลให้ชัดเจน เสนอต่อผู้บริหารเพื่อพิจารณาอนุมัติในการยกเว้นต่อไป

ส่วนที่ 8
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ และระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน
2. เพื่อให้การใช้งานระบบสารสนเทศ และระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
3. เพื่อป้องกัน และลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศ และระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

1. กำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
3. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอโดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
4. จัดสัมมนาหรือจัดให้มีการสร้างความตระหนักด้วยวิธีอื่น ๆ ตามความเหมาะสม เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรโดยการจัดสัมมนา มีแผนการดำเนินงาน ปีละไม่น้อยกว่า 1 ครั้ง โดยจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
5. ระดมการมีส่วนร่วม และลงสู่ภาคปฏิบัติด้วยการกำกับติดตามประเมินผล และสำรวจความต้องการของผู้ใช้งาน
6. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
7. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดเพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
8. ผู้ใช้งานต้องตระหนัก และปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของสภากาชาดไทย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้ หากผู้ใช้งานไม่

9. ปฏิบัติตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งาน ต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง
10. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่ายโดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ดัชนี

ภาคผนวก ก.

<u>คำศัพท์ทางเทคนิคที่ใช้ในนโยบายนี้</u>

“เพียร์ทูเพียร์ (Peer-to-Peer)” หมายถึง รูปแบบของระบบเครือข่ายรูปแบบหนึ่ง โดยในระบบเครือข่ายรูปแบบนี้ มีการกำหนดให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายทุกเครื่องเท่าเทียมกัน โดยไม่มีคอมพิวเตอร์ส่วนกลางที่ทำหน้าที่นี้ เรียกได้ว่าต่างคนต่างเก็บ ต่างคนต่างใช้ แต่ผู้ใช้งานในระบบเครือข่ายสามารถเรียกใช้ไฟล์จากคอมพิวเตอร์เครื่องอื่นได้ ถ้าคอมพิวเตอร์เครื่องนั้นทำการแชร์ไฟล์เหล่านั้นไว้

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของสภากาชาดไทยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สภากาชาดไทยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนในการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

“ระบบคอมพิวเตอร์ (Computer System)” หมายถึง เครื่องคอมพิวเตอร์ เครื่องบริการ และอุปกรณ์อื่น ๆ ที่เชื่อมการทำงานเข้าด้วยกัน เพื่อให้สามารถทำงาน ประมวลผล หรือติดต่อสื่อสารข้อมูลร่วมกัน หรือระหว่างกันได้โดยอัตโนมัติผ่านทางระบบสื่อสาร (Communication System)

“ระบบสื่อสาร (Communication System)” หมายถึง ระบบที่ประกอบด้วย ผู้รับ ผู้ส่ง เช่น โทรศัพท์มือถือ คอมพิวเตอร์ เครื่องแม่ข่าย เป็นต้น และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล (ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจรทางสาย เช่น สายเคเบิล (Cable) สายโคแอกเชียล (Coaxial Cable) สายใยแก้วนำแสง (Fiber Optic) และระบบไร้สาย เช่น คลื่นไมโครเวฟ (Microwave) ดาวเทียม (Satellite) คลื่นสัญญาณวิทยุ (เช่น 3G, 4G, 5G) บลูทูธ (Bluetooth)

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลให้มีความหมายโดยผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลขข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจและอื่น ๆ

“ระบบเครือข่าย (Network System)” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

“ระบบเครือข่ายเสมือน (Virtual Private Network: VPN)” หมายถึง เครือข่ายส่วนตัวเสมือน ซึ่งในการ รับ-ส่ง ข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้ว รับ-ส่ง ผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นจากต้นทางไปจนถึงปลายทาง

“อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)” หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในระบบเครือข่ายไร้สาย

“ชื่อระบบเครือข่ายไร้สาย (Service Set Identifier: SSID)” หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

“รูปแบบการเข้ารหัสความปลอดภัยของระบบเครือข่ายไร้สาย (Wire Equivalent Privacy: WEP)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้ในการเข้ารหัสข้อมูล ดังนั้นทุกเครื่องในระบบเครือข่ายที่ รับ-ส่ง ข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“รูปแบบการเข้ารหัสความปลอดภัยของระบบเครือข่ายไร้สาย (Wi-Fi Protected Access: WPA)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาให้มีความปลอดภัยมากกว่า WEP

“ไฟร์วอลล์ (Firewall)” หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูล และทรัพยากรในระบบเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์ และซอฟต์แวร์ในการรักษาความปลอดภัย

“อินเทอร์เน็ต (Internet)” หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเชื่อมโยง

“ข้อมูลจราจรทางคอมพิวเตอร์ (Log File)” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์หรืออุปกรณ์เครือข่าย ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทางวันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“เครื่องแม่ข่ายศูนย์กลางจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Centralized Log Server)” หมายถึง เครื่องแม่ข่ายคอมพิวเตอร์สำหรับการจัดเก็บข้อมูล log ของอุปกรณ์เครือข่ายต่าง ๆ รวมถึงเครื่องแม่ข่ายอื่น ๆ ไว้ที่เครื่องแม่ข่ายศูนย์กลาง เพื่อควบคุมการเข้าถึงให้เฉพาะผู้ที่มีสิทธิ์และเพื่อง่ายต่อการรักษาความมั่นคงปลอดภัย

“เครื่องคอมพิวเตอร์ (Computer)” หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา

“ข้อมูลคอมพิวเตอร์ (Computer Data)” หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ระบบจดหมายอิเล็กทรอนิกส์ (E-mail System)” หมายถึง ระบบที่บุคคลใช้ในการ รับ-ส่ง ข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน

“เครือข่ายสังคมออนไลน์ (Social Network)” หมายถึง เว็บไซต์หรือแอปพลิเคชันที่ผู้ใช้งานสามารถนำเสนอ และเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ

“รหัสผ่าน (Password)” หมายถึง ชุดตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

“บัญชีผู้ใช้ (Account)” หมายถึง เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกันมีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกันเพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชีหรือกลุ่มคนที่สามารถเข้าถึงระบบได้บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

“ชุดคำสั่งไม่พึงประสงค์ (Malware)” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น โปรแกรมเรียกค่าไถ่ (Ransomware), ไวรัสคอมพิวเตอร์ (Virus computer) เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)” หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)” หมายถึง การเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“ข้อมูลที่กำหนดชั้นความลับ (Information classification)” หมายถึง ข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหา จำกัดการเข้าถึง และหรือจำกัดให้ทราบเท่าที่จำเป็นและรวมถึงรหัสผ่านที่กำลังใช้อยู่หรือเตรียมจะใช้ ตลอดจนวัสดุหรือเอกสารทุกอย่างที่บันทึกข้อมูลดังกล่าว

“ภัยคุกคาม (Threat)” หมายถึง อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศโดยคน (Person) สิ่งต่าง ๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนา และไม่เจตนาอันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงานหรือการกระทำอื่น ๆ ตามความต้องการของภัยนั้น

“ความอ่อนแอ (Vulnerability)” หมายถึง จุดอ่อนหรือข้อบกพร่องใด ๆ ก็ตามของระบบสารสนเทศที่เป็นภัยในรูปแบบที่เหมาะกันสามารถนำไปใช้ประโยชน์เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้น ๆ ได้ ความอ่อนแอที่มีอยู่ของระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากันในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศแต่ละแห่ง ควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด

“ศูนย์ข้อมูลคอมพิวเตอร์หลัก (Data Center)” หมายถึง โครงสร้างพื้นฐานทางกายภาพ หรือพื้นที่สถานที่ ที่ใช้ในการวางระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงระบบสนับสนุน ที่ให้บริการระบบเทคโนโลยีสารสนเทศหลักแก่หน่วยงาน

“ศูนย์ข้อมูลคอมพิวเตอร์สำรอง (Disaster Recovery Site: DR Site)” หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็นที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

“ระบบสนับสนุน (Facility Supporting)” หมายถึง ระบบสนับสนุนศูนย์ข้อมูลคอมพิวเตอร์ ซึ่งประกอบด้วยระบบทำความเย็น ระบบไฟฟ้าสำรอง ระบบไฟฟ้าฉุกเฉิน ระบบดับเพลิงอัตโนมัติ เป็นต้น ที่สนับสนุนการทำงานของศูนย์ข้อมูลคอมพิวเตอร์หลัก และศูนย์ข้อมูลคอมพิวเตอร์สำรอง ให้สามารถทำงานได้อย่างต่อเนื่อง

“ซอร์สโค้ด (Source Code)” หมายถึง รหัสคำสั่งหรือโค้ดโปรแกรม ซึ่งถูกเขียนขึ้นโดยภาษาคอมพิวเตอร์ เช่น ภาษาซี (C) ภาษาจาวา (Java) ภาษาพีเอชพี (PHP) ภาษาไพทอน (Python) และอื่น ๆ เพื่อสร้างโปรแกรมสำหรับควบคุมการทำงานของคอมพิวเตอร์หรือใช้งานทั่วไป ตลอดจนงานเฉพาะด้าน

“สื่อบันทึกข้อมูลพกพา (Removable Media)” หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Flash Drive, External Hard disk, SSD หรืออุปกรณ์จัดเก็บข้อมูลที่เคลื่อนย้ายได้ เป็นต้น

“อุปกรณ์คอมพิวเตอร์ส่วนตัว (Bring Your Own Device: BYOD)” หมายถึง การนำอุปกรณ์คอมพิวเตอร์ส่วนตัว เช่น สมาร์ทโฟน แท็บเล็ต หรือคอมพิวเตอร์โน้ตบุ๊ค มาเชื่อมต่อระบบงานเทคโนโลยีสารสนเทศของสภากาชาดไทย

“โปรแกรมยูทิลิตี้ (Utility Program)” หมายถึง โปรแกรมอรรถประโยชน์ประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ ถูกออกแบบมาเพื่อทำหน้าที่เฉพาะอย่าง เช่น การวิเคราะห์ การปรับปรุงให้ระบบคอมพิวเตอร์ทำงานได้ดีขึ้น รวมถึงการบำรุงรักษาคอมพิวเตอร์ ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่ม

ประสิทธิภาพการทำงานของคอมพิวเตอร์ เช่น โปรแกรมสำรองและกู้คืนข้อมูล (Backup and Restore) โปรแกรมตรวจสอบดิสก์ (Check Disk) โปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) เป็นต้น

“เอสเอสแอล วีพีเอ็น (Secure Sockets Layer + Virtual Private Network: SSL VPN)” หมายถึง บริการระบบเครือข่ายเฉพาะภายในองค์กร ที่สามารถใช้งานผ่านระบบเครือข่ายสาธารณะ (Public Network) หรือ Internet มาใช้เป็นสื่อในการส่งข้อมูลระหว่างหน่วยงานภายในองค์กรโดยใช้การเข้ารหัสข้อมูลสร้างเป็นระบบเครือข่ายเสมือน เพื่อให้ข้อมูลที่ส่งผ่านกันยังคงปลอดภัยและยังคงรักษาความลับของข้อมูลได้เสมือนกับเป็นการส่งกันเองภายในองค์กร โดยที่บุคคลภายนอกองค์กรไม่สามารถเข้าถึงได้ เพราะระบบจะทำการตรวจสอบความมีตัวตนก่อนให้บริการ มีการทำงานโดยอาศัย Cryptographic system ที่จะต้องมีกุญแจที่สำคัญของการเข้ารหัส 2 อันคือ Public Key และ Private Key การเข้ารหัสที่เป็น SSL ที่เราเห็นกันทั่วไปมักใช้ในรูปแบบของ https:

“ไฟล์สั่งทำการ (Executable file: exe)” หมายถึง ไฟล์ที่มีคำสั่งให้เครื่องคอมพิวเตอร์ทำงานตามคำสั่ง โดยทำงานบนระบบปฏิบัติการ Microsoft Windows เช่น โปรแกรม Microsoft Excel จะประกอบด้วยแฟ้มข้อมูลหลายสิบแฟ้ม แต่แฟ้มที่เป็นตัวกระทำการคือแฟ้ม Excel.exe ถ้ากดเมาส์สองทีที่แฟ้มข้อมูลนี้ก็จะเท่ากับเป็นการสั่งให้โปรแกรมนั้นเริ่มทำงาน แฟ้มประเภทนี้จะใช้นามสกุล (file type) คือ .exe

“การเข้ารหัสลับ (Encryption)” หมายถึง กระบวนการเปลี่ยนแปลงข้อมูลทั่วไปให้เป็นรหัส () H*@HF)NOUBNPIFJ ที่ไม่สามารถอ่านออก เพื่อให้ข้อมูลสามารถเปิดอ่านข้อมูลต่าง ๆ ได้เฉพาะผู้ที่มีกุญแจสำหรับถอดรหัสเท่านั้น เป็นการทำงานแบบสองทาง โดยจะใช้อัลกอริทึมในการกำหนดวิธีการเข้ารหัส (Encryption) และการถอดรหัส (Decryption) เช่น AES-256, RSA, IDES เป็นต้น

“แฮช (Hash)” หมายถึง การเข้ารหัสข้อมูล โดยใช้หลักอัลกอริทึมมาสร้างแผนที่ข้อมูลที่มีความยาวคงที่ขึ้นมา โดยจะเรียกว่า "Hash Value" (อาจจะเรียกว่า Hash Code, Hash Sum หรือ Hash Digest ก็ได้เช่นกัน) มีคุณสมบัติในการทำงานเพียงทางเดียว จะไม่สามารถถอดรหัส หรือกระทำการใดๆ เพื่อที่จะ Reverse ให้ออกมาเป็นข้อความต้นฉบับได้ ซึ่งในปัจจุบันมีวิธีการ Hash มากมาย เช่น MD5, SHA1, SHA256, SHA512, RipeMD, WHIRLPOOL, SHA3 เป็นต้น ใช้ในการตรวจสอบว่าไฟล์ หรือข้อมูลนั้น ไม่ถูกเปลี่ยนแปลง แก้ไข ปลอมแปลง หรือจะกล่าวว่าเป็นการ CheckSum (การตรวจสอบความถูกต้องของข้อมูล) ก็ว่าได้

“ซอลท์ (Salt)” หมายถึง เทคนิคสำหรับเพิ่มความปลอดภัยสำหรับข้อมูล ซึ่งทำให้ใช้เวลาในการถอดรหัสมากขึ้น เช่น ข้อความที่ต้องการเข้ารหัสตั้งต้นคือ “RedCross” และเมื่อรวมเข้ากับ Salt (ซึ่งอาจมาจากข้อความที่สุ่มขึ้นมา) คือ “46jg!hnbZ8d” จะได้เป็น “RedCross46jg!hnbZ8d” จากนั้นนำข้อความนี้ไป Hashing ซึ่งถ้าคำนวนความน่าจะเป็นของข้อความ กรณีที่เป็นตัวอักษรตัวเล็ก ตัวใหญ่ และตัวเลข มีความเป็นไปได้ 62 แบบ จะเท่ากับว่าถ้ารหัสผ่านที่เราเก็บมีความยาว 16 ตัวอักษร ก็ต้อง Hash ถึง 16x62 แบบ แต่ถ้าเป็นข้อความที่รวมกับSalt แล้วข้างต้น เป็นความยาว 27 ตัวอักษร ผู้ไม่ประสงค์ดีต้อง Hash ถึง 27x62 ถึงจะได้ข้อความที่ถูกต้อง ซึ่งต้องใช้เวลามากกว่าเดิม

“พอร์ต (Port)” หมายถึง ช่องเสียบในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่าย เป็นต้น เพื่อการทำงานร่วมกัน เช่น เมื่อต้องการใช้เมาส์เชื่อมต่อกับโน้ตบุ๊ก เมาส์จะมีหัวสำหรับเสียบที่เรียกว่า USB สามารถเสียบเข้ากับช่องเสียบที่เรียกว่า USB Port หรือต่อจอภาพเข้ากับเครื่องคอมพิวเตอร์ สามารถเสียบสายสัญญาณเข้ากับช่องเสียบที่เรียกว่า VGA Port หรือ HDMI Port เป็นต้น

“โปรแกรมรักษาจอภาพ (Screen Saver)” หมายถึง โปรแกรมที่จัดให้หน้าจอมีภาพที่เคลื่อนไหว เพราะการปล่อยให้จอภาพแสดงภาพใดภาพหนึ่งนานเกินไป จอจะมีรอยไหม้ลบออกไม่ได้ และบางทีอาจทำให้จอมืด หากมีขยับเมาส์ หรือแตะที่แป้นพิมพ์แป้นใดแป้นหนึ่ง ข้อความหรือภาพบนจอที่เคลื่อนไหวอยู่ก็จะหายไป

“บริการคลาวด์ (Cloud Service)” หมายถึง บริการที่ครอบคลุมถึงการให้ใช้กำลังประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่าง ๆ จากผู้ให้บริการ เพื่อลดความยุ่งยากในการติดตั้ง ดูแลระบบ ประหยัดเวลา และลดต้นทุนในการสร้างระบบคอมพิวเตอร์และเครือข่ายเอง โดยจะมีการคิดค่าใช้จ่ายแบบ pay per use หรือใช้เท่าไหร่จ่ายเท่านั้น

“ไอพีแอดเดรส (Internet Protocol Address: IP Address)” หมายถึง หมายเลขเฉพาะที่กำหนดให้กับอุปกรณ์ทั้งหมด เช่น เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่าย แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP สามารถบอกสถานที่ตั้งว่าอยู่ที่ไหน ซึ่งหมายเลขประจำเครื่องคอมพิวเตอร์จะไม่ซ้ำกัน หากมีการแจกจ่ายด้วย DHCP Server

“แมคแอดเดรส (Media Access Control Address: Mac Address)” หมายถึง ตัวเลขเฉพาะประจำตัวของอุปกรณ์ที่ประกอบด้วยตัวเลขฐาน 16 มี 12 ตัว เช่น "2C:54:91:88:C9:E3" ซึ่งรหัสเหล่านี้จะถูกติดตั้งมาพร้อมกับฮาร์ดแวร์เน็ตเวิร์คการ์ด หรือ NIC (Network Interface Card) ที่อุปกรณ์ต่าง ๆ ใช้เชื่อมต่อระบบเครือข่าย Ethernet (LAN), Wi-Fi และ บลูทูธ (Bluetooth) นั่นเอง โดยอุปกรณ์เหล่านี้จะมีตัวเลข MAC Address เฉพาะมาจากโรงงาน ที่ไม่ซ้ำกัน และไม่สามารถเปลี่ยนแปลงได้

“การยืนยันตัวตน (Authentication)” หมายถึง กระบวนการยืนยันตัวบุคคล ว่าผู้เข้ารหัสหรือผู้ใช้บริการนั้นเป็น “ตัวจริง” หรือการ Log- in เช่น การเข้าสู่ระบบ Email, การเข้าสู่ระบบ Internet Banking และการเข้าสู่ระบบ social media ต่างๆ เพื่อเป็นการยืนยันตัวตนว่าเราคือคน ๆ นี้และกำลังจะใช้บริการต่าง ๆ ในฐานะคนนี้ พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบนั้นมีสิทธิ์ใช้ได้และเป็นเจ้าของข้อมูลเหล่านั้นจริง ๆ โดยการยืนยันนั้นจะมีการใส่ Username และ Password ไม่ว่าจะเป็นแบบที่เรากำหนดตั้งเองหรือแบบที่ระบบกำหนดมาให้เราใช้ตาม

“การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication: MFA)” หมายถึง การใช้ปัจจัยหลาย ๆ อย่างในการตรวจสอบและยืนยันตัวบุคคล เพื่ออนุญาตให้เข้าใช้งานระบบ หรือข้อมูลต่าง ๆ โดยทั่วไประบบ MFA จะเป็นการใช้เครื่องมือตั้งแต่ 2 อย่างขึ้นไปในการตรวจสอบและยืนยันความถูกต้อง ดังนี้

(1) สิ่งที่คุณรู้ (What you know) เช่น รหัสผ่าน (password) หรือ รหัสประจำตัว

(2) สิ่งที่คุณมี (What you have) เช่น OTP หรือ authenticator device อื่นๆ

(3) สิ่งที่คุณเป็น (Who you are) เช่น ลายนิ้วมือ หรือ ระบบจดจำใบหน้า

(4) สิ่งที่คุณทำ หรือ ที่ที่คุณอยู่ (What you do and where you are) เช่น การระบุที่อยู่ โดยใช้ GPS, IP Address หรือ Integrated Windows Authentication (IWA)

“เราเตอร์ (Router)” หมายถึง อุปกรณ์เครือข่ายที่หาเส้นทางหรือการกำหนดเส้นทาง และ รับ-ส่ง Data Packet ระหว่างเครือข่ายคอมพิวเตอร์ โดย Router จะพิเศษตรงที่ใช้งานกับ Traffic บน Internet โดยข้อมูลปกติจะถูกส่งต่อระหว่าง Router ด้วยกันผ่านระบบเครือข่ายไปเรื่อยๆจนกว่าจะถึงปลายทาง ซึ่ง Router สามารถต่อเข้ากับระบบเครือข่ายได้หลาย ระบบเครือข่ายและจะมีการเก็บข้อมูลที่เรียกว่า Routing Table หรือ Routing Policy ไว้ใช้ในการเลือกเส้นทางที่จะส่งข้อมูลข้ามเครือข่าย

“สวิตช์ (Switch)” หมายถึง อุปกรณ์เครือข่ายแบบมีสายต่อสัญญาณในเชื่อมต่อกับอุปกรณ์อื่นโดยใช้สายแลนแบบอีเทอร์เน็ต (Ethernet) ประกอบด้วย Port เชื่อมต่อหลาย ๆ Port ทำหน้าที่เป็นศูนย์กลางในการส่ง-รับ ข้อมูลให้อุปกรณ์อื่นๆ เช่น คอมพิวเตอร์, Printer, IP Phone หรือ Server เพื่อส่งผ่านข้อมูลไปยังระบบเครือข่าย หรือตัวกระจายสายแลนไปยังพื้นที่ต่าง ๆ ของอาคารเพื่อให้อุปกรณ์อื่น ๆ เสียบเพื่อเชื่อมต่อเข้าสู่ระบบเครือข่าย หรืออินเตอร์เน็ตนั่นเอง

“เกตเวย์ (Gateway)” หมายถึง อุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายต่าง ๆ เข้าด้วยกัน ไม่ว่าระบบเครือข่ายนั้นจะใช้โปรโตคอลใดก็ตาม โดย Gateway สามารถแปลงรูปแบบ packet ของโปรโตคอลหนึ่งไปเป็นรูปแบบของอีกโปรโตคอลหนึ่ง เช่น แปลงรูปแบบ Packet ของ TCP/IP ไปเป็น Apple Talk เป็นต้น รวมถึงสามารถเชื่อมต่อระบบเครือข่ายภายในกับเครือข่ายภายนอก ได้อย่างไม่มีข้อจำกัด

“หมดอายุเซสชัน (Session-Timeout)” หมายถึง จำนวนชั่วโมงที่แต่ละอุปกรณ์สามารถใช้งานได้อย่างต่อเนื่อง หากเกินจากเวลาที่กำหนดนี้จะต้อง Login ใหม่ เช่น กำหนดไว้ 10 ชั่วโมง จะสามารถใช้งานระบบเครือข่ายแบบร้ายบนอุปกรณ์ใด ๆ ได้ 10 ชั่วโมงติดต่อกัน หลังจากนั้นจะต้อง Login ใหม่

“พารามิเตอร์ (Parameter)” หมายถึง การกำหนดค่าตัวเลขของฟังก์ชันต่างๆ ซึ่งผลลัพธ์ที่ได้ก็จะแปรเปลี่ยนไปตามค่าของพารามิเตอร์ที่ส่งเข้ามานั่นเอง ดังนั้นพารามิเตอร์จึงช่วยให้ฟังก์ชันต่างๆทำงานได้อย่างหลากหลาย เช่น การกำหนด Default Gateway หรือ Subnet Mask ให้กับ NIC เป็นต้น

“นามแฝง (Pseudonymization)” หมายถึง การเปลี่ยนแปลงข้อมูลส่วนบุคคล โดยทำให้ไม่สามารถระบุตัวเจ้าของข้อมูลได้ หากไม่มีข้อมูลประกอบเพิ่มเติม เช่น การไม่ระบุชื่อบุคคลแต่แทนค่าชื่อบุคคลจาก นายใจดี เป็น นาย A หรือนาย B ซึ่งผู้ประมวลผลข้อมูลจะไม่ทราบตัวตนที่แท้จริงของบุคคลนั้น ๆ

“มาตรฐานการลบข้อมูล (DoD 5250.22-M)” หมายถึง วิธีการลบข้อมูลด้วยการเขียนทับข้อมูลที่มีอยู่บนฮาร์ดไดรฟ์หรืออุปกรณ์จัดเก็บข้อมูลอื่น ๆ โดยการเขียนทับซ้ำจำนวนสามครั้ง ซึ่งวิธีการล้างข้อมูล แบบนี้ จะป้องกันไม่ให้กู้คืนไฟล์ได้ วิธีการลบข้อมูล DoD 5220.22-M มักใช้ในวิธีต่อไปนี้

ครั้งที่ 1: เขียนศูนย์และตรวจสอบการเขียน

ครั้งที่ 2: เขียนหนึ่งและตรวจสอบการเขียน

ครั้งที่ 3: เขียนอักขระสุ่มและตรวจสอบการเขียน

“คอมมานไลน์ (Command Line)” หมายถึง โปรแกรมรับคำสั่งภาษาสคริปต์เป็นข้อความเพื่อโต้ตอบกับระบบปฏิบัติการโดยตรง แทนการใช้กราฟิกโหมด (GUI) ของระบบปฏิบัติการ เช่น การสั่งปิดคอมพิวเตอร์เวลาหกโมงเย็นของทุกวัน หรือการแก้ไขค่า parameter บางค่าของระบบปฏิบัติ เป็นต้น โดยใช้คำสั่ง (Script) ของโปรแกรม หรือรันชุดคำสั่งที่ผู้ใช้เขียนไว้ใน Batch File (.bat)

“ฐานข้อมูลไวรัส (Virus Definition)” หมายถึง ฐานข้อมูลที่เก็บรวบรวมข้อมูลของไวรัสไว้เพื่อใช้ในการเปรียบเทียบไฟล์ต้องสงสัยว่าเข้าข่ายที่จะเป็นไฟล์ไวรัสหรือไม่ โดยฐานข้อมูลไวรัสผู้ผลิตซอฟท์แวร์หรือฮาร์ดแวร์ Anti-Virus จะเป็นผู้เก็บรวบรวมไว้ และผู้ใช้บริการสามารถอัพเดทฐานข้อมูลไวรัสนี้ได้

“แพคเก็จ (Packet)” หมายถึง ข้อมูลที่แบ่งออกเป็นส่วนย่อย ๆ การแบ่งข้อมูลเป็นส่วนย่อยนี้ แต่ละส่วนย่อยจะถูกส่งไปยังจุดหมายพร้อม ๆ กัน เพื่อช่วยให้การแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายเร็วขึ้น ซึ่งแต่ละอันจะจ่าหน้าถึงผู้รับเดียวกัน แทนการส่งแบบที่ส่งข้อมูลไปครั้งเดียวทั้งหมด ซึ่งทำให้ส่งได้ช้า เช่น การส่ง E-Mail ซึ่ง E-mail จะถูกตัดออกเป็น packet ขนาดเล็กๆ หลายๆ อัน ซึ่งแต่ละอันจะจ่าหน้าถึงผู้รับเดียวกัน packets พวกนี้ก็จะวิ่งไปรวมกับ packets ของคนอื่นๆ ในระบบเครือข่าย ทำให้ packets ของเราอาจจะไม่ได้เรียงติดกัน packets เครื่องปลายทางก็จะเอา packets เหล่านั้นมาเก็บสะสมจนกว่าจะครบ จึงจะต่อกลับคืนให้เป็น E-mail

ภาคผนวก ข.

<u>องค์ประกอบของนโยบายและผู้รับผิดชอบ</u>

องค์ประกอบของนโยบาย	
1	ส่วนที่ 1 นโยบายการใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัย
2	ส่วนที่ 2 นโยบายการควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย
3	ส่วนที่ 3 นโยบายการบริหารจัดการและการรักษาความมั่นคงปลอดภัยข้อมูลและข้อมูลส่วนบุคคล
4	ส่วนที่ 4 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
5	ส่วนที่ 5 นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ
6	ส่วนที่ 6 นโยบายการจัดทำระบบสำรองสารสนเทศและแผนเตรียมพร้อมกรณีฉุกเฉิน
7	ส่วนที่ 7 นโยบายการตรวจสอบ และประเมินความเสี่ยงสารสนเทศ
8	ส่วนที่ 8 นโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ								
ผู้ใช้งาน	1	2	3	4	5	6	7	8
ผู้รับผิดชอบ	1	2	3	4	5	6	7	8
ผู้ดูแลระบบที่ได้รับมอบหมาย	1	2	3	4	5	6	7	8
หน่วยงาน	1	2	3	4	5	6	7	8