สภาองค์กรของผู้บริโภค
Thailand Consumers Council

แนวนโยบาย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานสภาองค์กรของผู้บริโภค

ศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ
ฝ่ายบริหารสำนักงาน
สำนักงานสภาองค์กรของผู้บริโภค
31 กรกฎาคม 2567

คำนำ

องค์กรของผู้บริโภคเป็นหน่วยงานอิสระและจัดตั้งขึ้นตามเจตนารมณ์ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ มาตรา ๔๖ เพื่อทำหน้าที่เป็นผู้แทนของผู้บริโภคมีสิทธิ หน้าที่ และอำนาจตามบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย ตามมาตรา ๔๖ แห่งพระราชบัญญัติการจัดตั้งสภาองค์กรของผู้บริโภค พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้องนั้น

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสำนักงานสภาองค์กรของผู้บริโภคที่ช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานของสำนักงานสภาองค์กรของผู้บริโภคที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ และเว็บไซต์ที่ทำหน้าที่เป็นช่องทางในการประชาสัมพันธ์ข่าวสาร เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวก แต่ในขณะเดียวกันก็มีความเสี่ยงสูงและอาจทำให้ก่อเกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติงานในสำนักงานสภาองค์กรของผู้บริโภคได้

ด้วยเหตุนี้ สำนักงานสภาองค์กรของผู้บริโภคจึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง จึงหวังเป็นอย่างยิ่งว่าแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการและผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภคทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

สารบัญ

แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หลักการและเหตุผล

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสำนักงานสภาองค์กรของผู้บริโภคที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานของสำนักงานสภาองค์กรของผู้บริโภคที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ เว็บไซต์ที่ทำหน้าที่สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสาร เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวก แต่ในขณะเดียวกันก็มีความเสี่ยงสูงและอาจทำให้ก่อเกิดภัยอันตราย หรือสร้างความเสียหายต่อการปฏิบัติงานในสำนักงานสภาองค์กรของผู้บริโภคได้ เช่นกัน เนื่องจากเพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่าง ๆ ทำให้มีโอกาสถูกภัยคุกคามบุกรุกจากภายนอกได้มากขึ้นซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือข้อมูลที่เป็นระดับการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้รวมถึงการขโมยข้อมูล หรือความลับของสำนักงานสภาองค์กรของผู้บริโภค ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศความเชื่อมั่นต่อองค์กรเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของสำนักงานสภาองค์กรของผู้บริโภค ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงต้องตระหนักถึงการให้การดูแลบำรุงรักษาและควบคุมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ด้วยเหตุนี้ สำนักงานสภาองค์กรของผู้บริโภคจึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว และจึงหวังเป็นอย่างยิ่งว่าแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภคทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

วัตถุประสงค์

๑. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค ให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล

๒. เพื่อให้มีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นกรอบในการกำหนดมาตรฐาน

ขั้นตอนปฏิบัติงาน ผู้รับผิดชอบ และใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค

๓. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศ และการสื่อสารอย่างสม่ำเสมอ

๔. เพื่อเผยแพร่ให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานสภาองค์กรของผู้บริโภคได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

องค์ประกอบของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศถือเป็นส่วนหนึ่ง ในการกำหนดควบคุมให้เป็นไปมาตรฐานทางด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค ทั้งนี้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกจะต้องคำนึงถึงการควบคุมในส่วนต่าง ๆ โดยจัดแบ่งสาระสำคัญออกเป็น ๑๒ หมวด ประกอบด้วย

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

หมวดที่ ๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

หมวดที่ ๓ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับพนักงาน (Human Resource Security)

หมวดที่ ๔ การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

หมวดที่ ๕ การควบคุมการเข้าถึง (Access Control)

หมวดที่ ๖ การเข้ารหัสข้อมูล (Cryptography)

หมวดที่ ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

หมวดที่ ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

หมวดที่ ๑๐ การจัดหา พัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development and Maintenance)

หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

หมวดที่ ๑๒ การปฏิบัติตามข้อกำหนด (Compliance)

นิยามคำศัพท์

นโยบาย หมายถึง แนวนโยบายการรักษาความมั่นคงปลอดภัยด้าสารสนเทศสำนักงานสภาองค์กรของผู้บริโภค

สารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการ บริหาร การวางแผน การตัดสินใจ และอื่น ๆ

ระบบงาน หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จ ตาม

วัตถุประสงค์ที่ตั้งไว้

ระบบปฏิบัติการ หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ เช่น การจัดสรรหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูลและอุปกรณ์แสดงผล

ระบบเครือข่าย หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค

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

ความลับ (Confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและ จะมีเพียงผู้มีสิทธิเท่านั่นที่จะเข้าถึงข้อมูลเหล่านั้นได้

ความถูกต้อง (Integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

สภาพพร้อมใช้งาน (Availability) หมายถึง การรับรองว่าข้อมูล หรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

ความเสี่ยง หมายถึง โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการรักษาความปลอดภัย

การเข้ารหัส (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ ตามปกติ

ช่องโหว่ หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบ ทำให้ประสิทธิภาพของการทำงานลดลง

สินทรัพย์ หมายถึง เครื่องคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค เครือข่าย ข้อมูลและระบบสารสนเทศต่าง ๆ ที่สำนักงานสภาองค์กรของผู้บริโภคพัฒนาหรือจัดหาเพื่อใช้ในกิจการของสำนักงานสภาองค์กรของผู้บริโภค และพนักงานของสำนักงานสภาองค์กรของผู้บริโภค

ผู้บริหารระดับสูง (Chief Executive Officer : CEO) หมายถึง เลขาธิการสำนักงานสภาองค์กรของผู้บริโภค

ผู้บริหาร หมายถึง ผู้บังคับบัญชา และผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของฝ่ายงานภายในสำนักงานสภาองค์กรของผู้บริโภค ซึ่งประกอบด้วย รองเลขาธิการ หัวหน้าฝ่าย

ผู้ใช้งาน หมายถึง พนักงานสำนักงานสภาองค์กรของผู้บริโภคทุกตำแหน่ง รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบ เทคโนโลยีสารสนเทศและสินทรัพย์ต่าง ๆ ของสำนักงานสภาองค์กรของผู้บริโภค และได้รับอนุญาตให้เข้าใช้งานสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ลูกข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และระบบสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

ผู้พัฒนาระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุง ระบบงานสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค รวมถึงบุคคลภายนอกที่ได้รับมอบหมายหรือผู้รับจ้างให้

ดำเนินงานตามเงื่อนไขที่กำหนด

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บริหารระดับสูงให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

เจ้าของระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึง ระบบงาน เช่น การให้สิทธิ การเพิ่มสิทธิ การลดสิทธิ การยกเลิกสิทธิ รวมทั้งการพัฒนา ปรับปรุงดูแล บำรุงรักษาระบบงาน

บัญชีผู้ใช้งาน หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศ ระบบปฏิบัติการ ระบบเครือข่าย รวมถึงโปรแกรมประยุกต์และสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

สิทธิของผู้ใช้งาน หมายความว่า สิทธิในการเข้าถึงระบบสารสนเทศ สิทธิในการเข้าถึง ระบบปฏิบัติการ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับโปรแกรมประยุกต์และสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

ผู้ให้บริการภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสำนักงานสภาองค์กรของผู้บริโภค โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้อง รับผิดชอบในการรักษาความลับของข้อมูล และผลกระทบต่อความเสียหายที่อาจเกิดขึ้นจากการปฏิบัติงาน

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการ ป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ
(Information Security Policy)

วัตถุประสงค์

เพื่อกำหนดกรอบทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภคเพื่อให้เกิดการดำเนินการตามมาตรฐานสากล และสอดคล้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ข้อกำหนดตามกฎหมาย

ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศบางประเด็นอาจเกี่ยวข้องกับกฎหมายที่บัญญัติ เช่น

(๑) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

(๒) กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(๓) กฎหมายลิขสิทธิ์

ผู้ที่ได้รับผลกระทบจากนโยบาย

นโยบาย นี้มีผลบังคับใช้กับพนักงานสำนักงานสภาองค์กรของผู้บริโภค รวมถึงบุคคลภายนอกหรือผู้ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค และได้รับอนุญาตให้เข้าใช้งาน

สารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค

การใช้งาน

การใช้งานสารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องเป็นไปอย่างเหมาะสมโดยอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของผู้อื่น เคารพและปฏิบัติอย่างถูกต้องตามกฎหมายและไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใด ๆ

พื้นที่ที่มีผลบังคับใช้

มีผลบังคับใช้กับพื้นที่ ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภครวมถึงการเรียกใช้งานจากทางบ้าน หรือการเข้าถึงจากระยะไกลและการเชื่อมโยงจากองค์กรภายนอกการอนุญาตและมอบสิทธิในการเข้าถึงทุกระบบฯ ต้องดำเนินการตามนโยบาย และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจเกิดขึ้น

การตรวจสอบและทบทวน

สำนักงานสภาองค์กรของผู้บริโภคต้องกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่กำกับดูแลนโยบาย และรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบาย อย่างสม่ำเสมอและทันเหตุการณ์ โดยให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์เปลี่ยนแปลงที่สำคัญ เพื่อความเหมาะสมและปกป้องผลประโยชน์ของสำนักงานสภาองค์กรของผู้บริโภค

หมวดที่ ๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ
(Organization of Information Security)

วัตถุประสงค์

เพื่อให้การบริหารและการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภคดำเนินการได้อย่างชัดเจน และพนักงานของสำนักงานสภาองค์กรของผู้บริโภคทุกคนได้ตระหนักถึงความสำคัญในเรื่องความมั่นคงปลอดภัยของสารสนเทศ มีความรู้ ความเข้าใจ และมีความรับผิดชอบตามภาระหน้าที่ และร่วมกันในการจำกัดภาวะความเสี่ยงและภัยคุกคามซึ่งมีแนวโน้มของความซับซ้อนและความรุนแรงเพิ่มมากขึ้น

ผู้รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๑. ระดับสำนักงานฯ

ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบการบริหารจัดการและกำกับดูแลภาพรวมของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค โดยมอบหมายให้งานศูนย์ข้อมูลและเทคโนโลยีสารเทศทำหน้าที่รับผิดชอบในส่วนของนโยบายการรักษาความมั่นคงปลอดภัย ทั้งนี้ฝ่ายงานที่เป็นเจ้าของข้อมูลที่อยู่ในระบบส่วนกลาง และในระบบที่สร้างขึ้นเองต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบาย และแนวปฏิบัติของ

สำนักงานสภาองค์กรของผู้บริโภค

๒. ระดับฝ่ายงาน

ผู้บริหารหรือพนักงานในฐานะเจ้าของข้อมูลเป็นผู้รับผิดชอบในการประสานความร่วมมือ และกำกับดูแลให้มีการปฏิบัติตามนโยบาย และแนวปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภค

ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๑. ผู้บริหาร

ผู้บริหารระดับสูง (Chief Executive Officer : CEO) และผู้บริหาร ภายใต้โครงสร้างสำนักงานสภาองค์กรของผู้บริโภคต้องกำกับดูแล ให้พนักงานได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศและปฏิบัติตามนโยบาย และแนวปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภค

๒. ผู้ใช้งาน

พนักงานของสำนักงานสภาองค์กรของผู้บริโภคต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภค และต้องรายงานต่อผู้บริหารหากพบปัญหาหรือช่องโหว่ที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภคใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยความลับของสำนักงานสภาองค์กรของผู้บริโภคโดยมิได้รับอนุญาต

๓. ผู้พัฒนาและผู้ดูแลระบบ

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของสำนักงานสภาองค์กรของผู้บริโภคต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และต้องมีภาระงานในเรื่องความมั่นคงปลอดภัยของสารสนเทศ ทั้งด้านเทคนิค การตรวจสอบ การเฝ้าระวัง การประเมินและรายงานความเสี่ยงต่อสำนักงานสภาองค์กรของผู้บริโภค

อุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล

ต้องมีการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกลโดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภค

หมวดที่ ๓ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับพนักงาน
(Human Resource Security)

วัตถุประสงค์

เพื่อให้พนักงานของสำนักงานสภาองค์กรของผู้บริโภค และพนักงานของผู้รับสัญญาว่าจ้างจากสำนักงานสภาองค์กรของผู้บริโภคได้เข้าใจบทบาทและหน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง รวมทั้งการใช้สารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศอย่างไม่ถูกต้องหรือผิดวัตถุประสงค์

ความมั่นคงปลอดภัยก่อนการจ้างงาน

สำนักงานสภาองค์กรของผู้บริโภคต้องกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของ

สารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการตรวจสอบคุณสมบัติของผู้สมัครตามระเบียบที่เกี่ยวข้องโดยพิจารณาจากจดหมายรับรองประวัติการทำงานและต้องมีการระบุเงื่อนไขการจ้างงานซึ่งรวมถึงความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

ความมั่นคงปลอดภัยระหว่างการจ้างงาน

พนักงานของสำนักงานสภาองค์กรของผู้บริโภค หรือพนักงานของผู้รับสัญญาว่าจ้างจากสำนักงานสภาองค์กรของผู้บริโภคต้องปฏิบัติตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยของสำนักงานสภาองค์กรของผู้บริโภค โดยต้องมีการให้ความรู้และฝึกอบรมด้านความมั่นคงปลอดภัยแก่พนักงาน และพนักงานของผู้รับสัญญาว่าจ้างจากสำนักงานสภาองค์กรของผู้บริโภคในกรณีที่กระทำความผิด ต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบของสำนักงานสภาองค์กรของผู้บริโภค

การสิ้นสุดหรือการเปลี่ยนการจ้าง

เมื่อสิ้นสุดการเป็นพนักงาน หรือมีการโยกย้ายสับเปลี่ยนหน้าที่ความรับผิดชอบ หรือการเปลี่ยนสัญญาการจ้างงานต้องมีการคืนทรัพย์สินของสำนักงานสภาองค์กรของผู้บริโภค และถอดถอน หรือมอบสิทธิที่เหมาะสมในการเข้าถึงระบบสารสนเทศของพนักงาน นั้น

หมวดที่ ๔ การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร
(Asset Management)

วัตถุประสงค์

เพื่อป้องกันสินทรัพย์สารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสมโดยมีการจัดทำบัญชีสินทรัพย์ระบุผู้เป็นเจ้าของสินทรัพย์และกำหนดหลักเกณฑ์ในการใช้งาน และส่งคืนสินทรัพย์รวมถึงการทำลายสื่อบันทึกข้อมูลที่เหมาะสมมีการจัดหมวดหมู่ตามระดับชั้นความลับและจัดทำป้ายชื่อเพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้

ความรับผิดชอบต่อสินทรัพย์สารสนเทศ

สำนักงานสภาองค์กรของผู้บริโภคต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำบัญชีสินทรัพย์สารสนเทศและปรับปรุงให้ถูกต้องอยู่ เสมอและต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์ในการใช้สินทรัพย์อย่างเป็นลายลักษณ์อักษรเพื่อให้เกิดการใช้งานได้อย่างเหมาะสม และเพื่อป้องกันความเสียหายต่อสินทรัพย์เหล่านั้น

การจัดหมวดหมู่

สำนักงานสภาองค์กรของผู้บริโภคต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อสำนักงานสภาองค์กรของผู้บริโภค ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม รวมทั้งจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์สารสนเทศ ตามหมวดหมู่ที่กำหนดไว้

การจัดสื่อที่ใช้บันทึกข้อมูล

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต มีการป้องกันในการนำส่งหรือการขนย้าย หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัยเมื่อหมดความต้องการในการใช้งาน

หมวดที่ ๕ การควบคุมการเข้าถึง
(Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตป้องกันการการเปิดเผยหรือขโมยสารสนเทศและสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภค จำเป็นต้องมีการกำหนดนโยบายการเข้าถึงระบบการบริหารจัดการการเข้าถึงของผู้ใช้และการควบคุมการเข้าถึงเครือข่าย

การควบคุมการเข้าถึงระบบตามความต้องการทางธุรกิจ

สำนักงานสภาองค์กรของผู้บริโภคต้องมีนโยบายควบคุมการเข้าถึงเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรและทบทวนตามระยะเวลาที่กำหนดไว้โดยพิจารณาให้สอดคล้องกับภารกิจของสำนักงานสภาองค์กรของผู้บริโภคและความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

การบริหารจัดการการเข้าถึงของผู้ใช้งาน

สำนักงานสภาองค์กรของผู้บริโภคต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่านรวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

หน้าที่ความรับผิดชอบของผู้ใช้งาน

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด

การควบคุมการเข้าถึงระบบ

การเข้าถึงระบบภายในสำนักงานสภาองค์กรของผู้บริโภคหรือการเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งาน ที่ได้รับอนุญาตผ่านเข้าสู่เครือข่ายและใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

หมวดที่ ๖ การเข้ารหัสข้อมูล
(Cryptography)

วัตถุประสงค์

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลป้องกันความลับ การปลอมแปลงหรือความถูกต้องของสารสนเทศ

นโยบายการควบคุมการเข้ารหัสเพื่อป้องกันข้อมูลสารสนเทศ

นโยบายการควบคุมการเข้ารหัสมีการพิจารณาถึงการควบคุมการเข้ารหัส ผลของการประเมินความเสี่ยงเพื่อระบุระดับการป้องกัน

การบริหารจัดการกุญแจ

การบริหารจัดการการเข้ารหัส (Key Management) และมาตรฐานอื่น ๆ ที่มีประสิทธิภาพการใช้งานการป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

หมวดที่ ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์ ป้องกันการถูกเปิดเผยโดยมิได้รับอนุญาต และป้องกันมิให้กิจกรรมการดำเนินงานด้านเทคโนโลยีสารสนเทศของสำนักงานสภาองค์กรของผู้บริโภคเกิดการติดขัดหรือหยุดชะงัก อาทิ การมีระบบไฟฟ้าสำรอง ระบบสื่อสารสำรอง

การรักษาความปลอดภัยทางกายภาค

สำนักงานสภาองค์กรของผู้บริโภคต้องกำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมีระบบป้องกันการเสียหายและการควบคุมการเข้าออกในการรักษาความมั่นคงปลอดภัย อาทิ ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค ต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด

การควบคุมการเข้าถึงอุปกรณ์

อุปกรณ์ทุกชนิดต้องกำหนดให้มีผู้รับผิดชอบโดยตรง และผู้รับผิดชอบเท่านั้นที่ได้รับสิทธิในการเข้าถึงโดยต้องจัดให้มีระบบสำหรับจัดเก็บข้อมูลการเข้าถึงเพื่อใช้เป็นหลักฐานในการตรวจสอบ

การรักษาความปลอดภัยของอุปกรณ์

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ ต้องมีการจัดวางอย่างถูกต้อง มีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่ออุปกรณ์และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจน และต่อเนื่อง

การนำอุปกรณ์ออกนอกหน่วยงาน

การนำอุปกรณ์ทุกชิ้นออกนอกหน่วยงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของสำนักงานสภาองค์กรของผู้บริโภคและต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน
(Operations Security)

วัตถุประสงค์

เพื่อให้การดำเนินการที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย ในแต่ละขั้นตอนของการปฏิบัติงานต้องมีการบันทึกและจัดเก็บเป็นลายลักษณ์อักษรเพื่อประโยชน์สำหรับการกู้คืนข้อมูลในกรณีที่เกิดการเสียหายรวมถึงการป้องกันและเฝ้าระวัง การ บริหารจัดการช่องโหว่

ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ

โครงสร้างพื้นฐานและสารสนเทศทุกระบบต้องมีผู้รับผิดชอบมีเอกสารขั้นตอนการปฏิบัติงานที่ได้ บันทึกไว้เป็นลายลักษณ์อักษร ในกรณีที่มีการเปลี่ยนแปลงข้อมูล หรือการปรับเปลี่ยนเวอร์ชั่นของระบบ หรือโปรแกรมภายใน ต้องมีการบันทึกการจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จมีการบริหารขีดความสามารถของโครงสร้างพื้นฐานและระบบสารสนเทศ

การป้องกันโปรแกรมที่ไม่พึงประสงค์

สำนักงานสภาองค์กรของผู้บริโภค ต้องจัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงานหรืออุปกรณ์หลักของสำนักงานสภาองค์กรของผู้บริโภคและกำหนดให้มีระเบียบ และขั้นตอนวิธีปฏิบัติที่เหมาะสม และสนับสนุนให้หน่วยงานภายในที่มีการใช้งานผ่านระบบเครือข่ายของสำนักงานสภาองค์กรของผู้บริโภค ได้ยึดถือและปฏิบัติตาม

การสำรองข้อมูล

สำนักงานสภาองค์กรของผู้บริโภค ต้องจัดให้มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติรวมทั้งแผนการ สำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในสำนักงานสภาองค์กรของผู้บริโภค เพื่อป้องกันการสูญหายอันจะ เกิดขึ้นจากภาวะคุกคามหรือจากการเกิดภัยพิบัติโดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้

การบันทึกข้อมูลล็อกและการเฝ้าระวัง

สำนักงานสภาองค์กรของผู้บริโภค ต้องจัดให้มีการเฝ้าระวังระบบที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การ ปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้อง ให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทาง คอมพิวเตอร์และต้องกำหนดขั้นตอนวิธีปฏิบัติในการตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกัน

โดยอ้างอิง จากแหล่งเวลาที่ถูกต้องที่ช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัย ของระบบคอมพิวเตอร์ของสำนักงานสภาองค์กรของผู้บริโภค

การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

ต้องมีมาตรการในการรักษาความสมบูรณ์ของระบบปฏิบัติงานโดยมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานตามมาตรฐานที่สภาองค์กรของผู้บริโภคกำหนดโดยก่อนการติดตั้งในระบบต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีไม่ก่อให้เกิดปัญหากับระบบ

การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้สามารถทำงานได้เป็นปกติ ต้องปรับปรุงช่องโหว่ในระบบต่าง ๆ มีการประเมินความเสี่ยงของช่องโหว่เหล่านั้นตามระยะเวลาที่กำหนด กำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

สิ่งที่ต้องพิจารณาการตรวจประเมินระบบ

ต้องลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการโดยการกำหนดวิธีการปฏิบัติงานที่ชัดเจนในการใช้งานซอฟต์แวร์ที่ใช้ในการตรวจประเมินเพื่อป้องกันมิให้นำซอฟต์แวร์ไปใช้ในทางที่ผิด

หมวดที่ ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล
(Communications Security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลบนเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศโดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของเครือข่ายและการถ่ายโอนข้อมูลสารสนเทศรวมถึงข้อกำหนดในการรักษาความลับหรือการไม่เปิดเผยความลับ

การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย

ต้องจัดให้มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจจับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่สำนักงานสภาองค์กรของผู้บริโภคประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งาน ได้ตามข้อกำหนด และมีการบำรุงรักษาระบบให้ใช้งานได้ดีอยู่เสมอ

การถ่ายโอนสารสนเทศ

ในการถ่ายโอนหรือแลกเปลี่ยนสารสนเทศจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงานมีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอรวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อสำนักงานสภาองค์กรของผู้บริโภค

หมวดที่ ๑๐ การจัดหา พัฒนา และการบำรุงรักษาระบบ
(Systems Acquisition, Development, and Maintenance)

วัตถุประสงค์

เพื่อให้การจัดหาพัฒนาระบบสารสนเทศและการบำรุงรักษาระบบสารสนเทศ ได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญในทุกขั้นตอนตลอดวงจรชีวิตการพัฒนาระบบซึ่งครอบคลุมถึงกระบวนในการพัฒนาการทดสอบ และข้อมูลสำหรับใช้ทดสอบ

ความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศ

การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศบนเครือข่ายสาธารณะรวมถึงธุรกรรมของบริการสารสนเทศ

ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน

การพัฒนาระบบสารสนเทศต้องมีความมั่นคงปลอดภัยมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการ เพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานหลังการเปลี่ยนแปลงนั้น ๆ

ข้อมูลสำหรับการทดสอบระบบ

ต้องมีมาตรการควบคุมการใช้ข้อมูลสำหรับการทดสอบระบบและการป้องกันข้อมูลรั่วไหล เมื่อใช้งานเสร็จต้องลบข้อมูลจริงออกจากระบบทดสอบทันที

หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier Relationships)

วัตถุประสงค์

เพื่อป้องกันสินทรัพย์องค์กรที่สามารถเข้าถึงโดยผู้ให้บริการภายนอก มีข้อตกลงเป็นลายลักษณ์อักษรในส่วนของการเข้าถึงระบบ การประมวลผล การจัดเก็บ และการสื่อสารสารสนเทศ ที่ผู้ให้บริการภายนอกพึงปฏิบัติ และการบริหารจัดการด้านการเปลี่ยนแปลงในการให้บริการของผู้ให้บริการภายนอก

ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์ต่อผู้ให้บริการภายนอก

การรับบริการจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงานมีการเฝ้าระวัง และจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอรวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อสำนักงานสภาองค์กรของผู้บริโภค

การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

ติดตามทบทวนบริการของผู้ให้บริการภายนอกมีการติดตามสภาพการใช้งานและวิเคราะห์ขีด

ความสามารถตรวจรับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่สำนักงานสภาองค์กรของผู้บริโภคประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

หมวดที่ ๑๒ การปฏิบัติตามข้อกำหนด
(Compliance)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมายระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัย ๆ และให้มั่นใจว่าความมั่นคงปลอดภัยสารสนเทศถูกนำไปปฏิบัติ และใช้งานตามนโยบายและระเบียบปฏิบัติของสำนักงานสภาองค์กรของผู้บริโภค

การปฏิบัติตามข้อกำหนดของสัญญาและกฎหมาย

สำนักงานสภาองค์กรของผู้บริโภคต้องมีการศึกษา กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสภาองค์กรของผู้บริโภค เพื่อให้พนักงานได้รับทราบทำความเข้าใจและปฏิบัติตามได้อย่างเคร่งครัด

การทบทวนความมั่นคงปลอดภัยสารสนเทศ

สำนักงานสภาองค์กรของผู้บริโภค ต้องจัดให้มีการทบทวน มาตรการ นโยบาย กระบวนการ ขั้นตอนปฏิบัติเพื่อความมั่นคง ปลอดภัยสารสนเทศ อย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ โดยเทียบกับนโยบายมาตรฐาน ด้านความ มั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง

(นายจักรี รุ่งเรือง)
เจ้าหน้าที่ศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ

(นายณัฐวุฒิ ศรีคงจันทร์)
หัวหน้าฝ่ายบริหารสำนักงาน

(สารี อ่องสมหวัง)
เลขาธิการสำนักงานสภาองค์กรของผู้บริโภค