นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
กรมกิจการผู้สูงอายุ

โดย
กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน
กรมกิจการผู้สูงอายุ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
กรมกิจการผู้สูงอายุ

๑. แนวทางการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กรมกิจการผู้สูงอายุ กำหนดให้มีการจัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มีวัตถุประสงค์เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งาน อ้างอิงมาตรฐานตาม ISO/IEC ๒๗๐๐๑ มีการกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรรับทราบและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ตลอดจนดำเนินการตรวจสอบและประเมินนโยบายตามความเหมาะสมในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร

สำหรับมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ มีดังนี้

๑.๑ กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๑.๒ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๑.๓ กำหนดแนวทางปฏิบัติ แนวทางแก้ไขหรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๑.๔ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๑.๕ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๒. นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ ประกอบด้วย ๗ ส่วน ได้แก่ คำนิยาม การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม การควบคุมการเข้าออกห้องศูนย์เทคโนโลยีสารสนเทศ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์และอินเทอร์เน็ต และการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยมีรายละเอียดดังนี้

๒.๑ คำนิยาม

คำนิยามสำคัญที่ใช้ประกอบในนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศนี้ประกอบด้วย

๑) **องค์กร** หมายถึง กรมกิจการผู้สูงอายุ

๒) **ผู้บังคับบัญชา** หมายถึง หัวหน้าหน่วยงานราชการตามโครงสร้างการบริหารขององค์กร

๓) **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งกำหนดไว้ ดังนี้

๓.๑) ผู้บังคับบัญชา

๓.๒) ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๓.๓) เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กรที่เป็นผู้ใช้งานคอมพิวเตอร์ และโปรแกรมเครือข่ายคอมพิวเตอร์

๔) **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

๕) **ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารและการสนับสนุนการให้บริการ ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๖) **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น พื้นที่ทำงานทั่วไป พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ และพื้นที่ใช้งานระบบเครือข่ายไร้สาย

๗) **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒.๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ผู้ดูแลระบบ และเจ้าหน้าที่องค์กร	ผู้ติดต่อจากหน่วยงานภายนอกองค์กร
๑. กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศ อย่างเหมาะสม และจัดทำเป็นเอกสาร ๒. ผู้บริหาร กำหนดพื้นที่กำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้เข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน	หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการอนุญาตฯ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๒.๓ การควบคุมการเข้าออกห้องศูนย์เทคโนโลยีสารสนเทศ

ผู้ดูแลระบบ และเจ้าหน้าที่องค์กร	ผู้ติดต่อจากหน่วยงานภายนอกองค์กร
๑. ผู้ดูแลระบบ จัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน ๒. มีการลงบันทึกตามแบบฟอร์ม“บันทึกการเข้าออกศูนย์เทคโนโลยีสารสนเทศ และห้องคอมพิวเตอร์	๑. แลกบัตรที่ใช้ระบุตัวตน กับผู้ดูแลระบบ แล้วทำการลงบันทึกข้อมูลลงใน “บันทึกการเข้าออกพื้นที่” ๒. กรณีนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ใน

	แบบฟอร์มการขออนุญาตเข้าออก ๓. ผู้ดูแลระบบ ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๒ ครั้ง

๒.๔ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

กระบวนการหลักในการควบคุมการเข้าถึงระบบ	กระบวนการอื่นๆ ในการควบคุมการเข้าถึงระบบ
๑. สถานที่ตั้งมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น ๒. ผู้ดูแลระบบ กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน ๓. ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้ ๔. ผู้ดูแลระบบ ติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร	๑. ควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ๒. บริหารจัดการการเข้าถึงของผู้ใช้ ๓. การบริหารจัดการการเข้าถึงระบบเครือข่าย ๔. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย ๕. การบริหารจัดการการบันทึกและตรวจสอบ ๖.การควบคุมการเข้าใช้งานระบบจากภายนอก ๗. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๒.๕ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร

๒) หน่วยงานภายนอก ที่ทำงานให้กับองค์กร จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓) เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๔) ควรมอบหมายให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้ง มีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๒.๖ การใช้งานเครื่องคอมพิวเตอร์และอินเทอร์เน็ต

๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๒) ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคาม

๓) กรมกิจการผู้สูงอายุ ใช้เทคโนโลยีเพื่อปกป้องคอมพิวเตอร์และอินเตอร์เน็ต ดังนี้

๓.๑) Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ์ หรือผู้ที่ได้รับการอนุมัติเท่านั้นจึงจะผ่าน Fire Wall เพื่อเข้าถึงข้อมูลได้

๓.๒) Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มี ประสิทธิภาพสูง และ Update อย่างสม่ำเสมอ และติดตั้ง Scan Virus Software บนเครื่อง Server

๒.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑) ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบ

๒) ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๓) ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

๔) ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๕) ผู้ดูแลระบบควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๖) ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย