ไปรษณีย์ไทย
THAILAND POST

ประกาศ บริษัท ไปรษณีย์ไทย จำกัด
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยของหน่วยงานเป็นลายลักษณ์อักษร นั้น

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีมติในการประชุม ครั้งที่ ๑/๒๕๖๒ วันที่ ๑๒ กุมภาพันธ์ ๒๕๖๒ เห็นชอบแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัท ไปรษณีย์ไทย จำกัด ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท ไปรษณีย์ไทย จำกัด มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง รวมทั้งป้องกันการถูกคุกคามจากภัยต่างๆ บริษัท ไปรษณีย์ไทย จำกัด จึงออกประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

ข้อ ๑ วัตถุประสงค์และขอบเขตของนโยบาย

๑.๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ การสื่อสาร และเครือข่ายคอมพิวเตอร์ของ บริษัท ไปรษณีย์ไทย จำกัด ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001 และให้มีการปรับปรุงอย่างต่อเนื่อง

๑.๓ นโยบายนี้ ต้องเผยแพร่ให้พนักงานของบริษัททุกระดับได้รับทราบ และต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้ บริษัท ไปรษณีย์ไทย จำกัด ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท ไปรษณีย์ไทย จำกัด ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ นโยบายนี้ต้องมีการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ องค์ประกอบของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ บริษัท ไปรษณีย์ไทย จำกัด ประกอบด้วย ๑๔ หมวด ดังต่อไปนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ
หมวด ๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร
หมวด ๓ ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล
หมวด ๔ การบริหารจัดการสินทรัพย์
หมวด ๕ การควบคุมการเข้าถึงสารสนเทศ
หมวด ๖ การเข้ารหัสข้อมูล
หมวด ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
หมวด ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน
หมวด ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
หมวด ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
หมวด ๑๑ การบริหารจัดการความสัมพันธ์กับผู้ให้บริการภายนอก
หมวด ๑๒ การบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศ
หมวด ๑๓ การบริหารความต่อเนื่องในการดำเนินงาน
หมวด ๑๔ การปฏิบัติตามข้อกำหนด

นโยบายในแต่ละหมวด ประกอบด้วยวัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหมวดนั้นๆ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ บริษัท ไปรษณีย์ไทย จำกัด เพื่อให้ บริษัท ไปรษณีย์ไทย จำกัด มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากร ทำให้ บริษัท ไปรษณีย์ไทย จำกัด เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่างๆ ในการดำเนินงานได้อย่างมั่นคงและมีความปลอดภัยตามมาตรฐานสากล

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ บริษัท ไปรษณีย์ไทย จำกัด ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ บริษัท ไปรษณีย์ไทย จำกัด ซึ่งพนักงานของบริษัททุกระดับ รวมทั้งลูกจ้าง และหน่วยงานภายนอก จะต้องปฏิบัติตามอย่างเคร่งครัด

ข้อ ๕ หน่วยงานเจ้าของระบบต้องจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ข้อ ๖ หน่วยงานเจ้าของระบบต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศทั้งทางด้านความต่อเนื่องของระบบสารสนเทศ ด้านภัยคุกคามต่อระบบสารสนเทศเป็นประจำอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ นโยบาย มาตรฐาน และแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief of Information Officer: CIO) เป็นผู้รับผิดชอบในการกำกับ ติดตาม ทบทวน

ข้อ ๘ แผนสำรอง หรือแผนรองรับเหตุฉุกเฉินอื่นๆ ที่ได้ประกาศใช้แล้ว ให้ผู้บังคับบัญชาที่มีอำนาจสูงสุดของหน่วยงานเจ้าของระบบ เป็นผู้รับผิดชอบในการกำกับ ติดตาม ทบทวน

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๒ เดือน มีนาคม พ.ศ. ๒๕๖๒

(นางสมร เทิดธรรมพิบูล)
กรรมการผู้จัดการใหญ่
บริษัท ไปรษณีย์ไทย จำกัด

๖๑๗