ประกาศกระทรวงสาธารณสุข

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

กระทรวงสาธารณสุข

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงสาธารณสุข หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องได้ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 เพื่อให้การกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความสอดคล้องกับมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

1.3 เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการดำเนินการทบทวนตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร "การตรวจสอบประเมินนโยบาย"

...../2. องค์ประกอบของนโยบาย

2. องค์ประกอบของนโยบาย

2.1 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

กำหนดพื้นที่ควบคุม กระบวนการควบคุมการเข้าออกเฉพาะบุคคลที่ได้รับการอนุญาตเพื่อปฏิบัติงานในพื้นที่ควบคุม การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม การบริหารจัดการระบบสารสนเทศและอุปกรณ์สนับสนุนการปฏิบัติงาน และการบำรุงรักษาอุปกรณ์

2.2 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.2.1 ผู้ดูแลระบบต้องตรวจสอบการอนุมัติและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User Authentication) เท่านั้นที่สามารถเข้าถึงระบบได้ การเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์

2.2.2 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน การทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัย

2.2.3 การบริหารจัดการการเข้าถึงระดับเครือข่าย ผู้ดูแลต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อใช้งานอินเตอร์เน็ต ต้องผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Firewall, IPS/IDS, Proxy, การตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบ

2.2.4 การควบคุมการเข้าใช้งานจากภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบจะต้องกำหนดให้มีการควบคุมการใช้งานจากภายนอก (Remote Access) โดยการกำหนดสิทธิ์ ควบคุมพอร์ต (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม และมีการแสดงตัวตนของผู้ใช้งาน (Identification) และการพิสูจน์ยืนยันตัวตน (Authentication) เช่น การใช้รหัสผ่าน Smart card เป็นต้น

2.3 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

2.3.1 กำหนดให้ใช้เครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินขององค์กร รวมทั้งโปรแกรมใช้งานต่าง ๆ ควรมีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามการติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับงานที่ปฏิบัติ

2.3.2 กำหนดให้ใช้ Username และ Password ก่อนใช้งานเครื่อง รวมทั้งล๊อคหน้าจอด้วยโปรแกรม Screen Saver ในเวลาพักงานหรือพักการใช้เครื่องชั่วคราว

2.3.3 ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลและกู้คืนข้อมูลบนสื่อเก็บข้อมูลที่มีความเหมาะสม และต้องเก็บรักษาไว้ในที่ปลอดภัย

..../2.4 นโยบายการใช้งานอินเตอร์เน็ต

2.4 นโยบายการใช้งานอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

2.4.1 ผู้ดูแลระบบจะต้องกำหนดให้เฉพาะผู้ที่มีสิทธิ์ (User Authentication) จึงจะสามารถเชื่อมต่อระบบเพื่อใช้งานอินเตอร์เน็ตหรือจดหมายอิเล็กทรอนิกส์ได้

2.4.2 มีระบบรักษาความปลอดภัยขององค์กรเพื่อตรวจสอบการใช้งานและภัยคุกคาม

2.4.3 กำหนดแนวทางปฏิบัติการใช้งานอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ที่ถูกต้อง โดยไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่สร้างปัญหาให้แก่ระบบหรือผู้ใช้อื่น

2.4.4 ในการติดต่อเรื่องที่เป็นงานราชการ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ขององค์กร หรือที่องค์กรกลางจัดให้เท่านั้น ห้ามใช้ Free e-mail ของบริษัทเอกชนที่เปิดให้บริการในการติดต่อเรื่องดังกล่าว

2.4.5 ต้องมีการเก็บข้อมูลการเข้าถึงระบบและข้อมูลจราจรทางคอมพิวเตอร์

2.5 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ดูแลระบบจะต้องกำหนดรหัสผ่านและสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) และลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง กำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสม เพื่อป้องกันไม่ให้บุคคลภายนอกที่ไม่เกี่ยวข้อง หรือไม่ได้รับอนุญาตเข้าใช้งานได้

2.6 นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี

ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่จะนำมาต่อกับระบบเครือข่ายคอมพิวเตอร์ขององค์กรต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และผู้ใช้จะต้องตรวจสอบไวรัสคอมพิวเตอร์จากสื่อเก็บข้อมูลทุกชนิดก่อนนำมาใช้งานร่วมกับคอมพิวเตอร์

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ ได้กำหนดขึ้นเพื่อที่จะทำให้องค์กรมีมาตรการและแนวทางในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ 28 กรกฎาคม พ.ศ. 2553

ศิริวัฒน์ ทิพย์ธราดล

(นายศิริวัฒน์ ทิพย์ธราดล)

รองปลัดกระทรวงสาธารณสุข ปฏิบัติราชการแทน

ปลัดกระทรวงสาธารณสุข

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กระทรวงสาธารณสุข