(สำเนาคู่ฉบับ)

ที่ สธ 0202.05/ว **473**

กระทรวงสาธารณสุข

ถนนติวานนท์ จังหวัดนนทบุรี 11000

28 กรกฎาคม 2553

เรื่อง ประกาศนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เรียน อธิบดี เลขาธิการ ผู้อำนวยการองค์การเภสัชกรรม ผู้อำนวยการหน่วยงานในสังกัดสำนักงานปลัดกระทรวง นายแพทย์สาธารณสุขจังหวัด และผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง

สิ่งที่ส่งมาด้วย ประกาศนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข จำนวน 1 ฉบับ

ตามที่ สำนักงาน ก.พ.ร. ได้กำหนดให้ทุกส่วนราชการนำเรื่องการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) มาใช้เป็นเครื่องมือในการพัฒนาระบบราชการให้มีประสิทธิภาพ โดยกำหนดให้ทุกส่วนราชการจัดทำแผนปรับปรุงระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องกับแผนปฏิบัติราชการ 4 ปี และแผนปฏิบัติราชการประจำปีของส่วนราชการ เพื่อให้มีขีดสมรรถนะที่เหมาะสม สามารถปฏิบัติงานให้บรรลุตามเป้าหมายที่กำหนดไว้ นั้น

ในการนี้ สำนักงานปลัดกระทรวง ได้ดำเนินการจัดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข ขึ้น โดยมีวัตถุประสงค์เพื่อให้ระบบเทคโนโลยีสารสนเทศของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องได้

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้ผู้เกี่ยวข้องทราบและถือปฏิบัติต่อไปด้วย

ขอแสดงความนับถือ

(นายศิริวัฒน์ ทิพย์ธราดล)
รองปลัดกระทรวงสาธารณสุข ปฏิบัติราชการแทน
ปลัดกระทรวงสาธารณสุข
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร 0-2590-1208 โทรสาร 0-2590-1215

ร่าง
พิมพ์
ตรวจ

(สำเนาคู่ฉบับ)

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 รวมทั้งล็อคหน้าจอด้วยโปรแกรม 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 ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ขององค์กรหรือที่องค์กรกลางจัดให้เท่านั้น 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

(นายศิริวัฒน์ ทิพย์ธราดล)

รองปลัดกระทรวงสาธารณสุข ปฏิบัติราชการแทน

ปลัดกระทรวงสาธารณสุข

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กระทรวงสาธารณสุข

ร่าง

พิมพ์

ตรวจ

ประกาศสำนักงานปลัดกระทรวงสาธารณสุข

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

****

ตามที่มีการประกาศพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และมีผลบังคับใช้แล้ว นั้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร(ศทส.) สำนักงานปลัดกระทรวงสาธารณสุข จึงได้จัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ คู่มือและข้อปฏิบัติสำหรับ user สป.สธ. และ นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใช้ในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับระบบฐานข้อมูลและสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงสาธารณสุข โดยให้ถือปฏิบัติในทิศทางเดียวกัน

วัตถุประสงค์

เพื่อให้เกิดความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบฐานข้อมูลและสารสนเทศ สอดคล้องกับมาตรฐาน ISO/IEC27001 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

องค์ประกอบของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงสาธารณสุข คือให้ทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับวันที่ 4 กันยายน 2552 อย่างเคร่งครัด อันประกอบด้วยประเด็นสำคัญดังนี้

1. การบริหารจัดการระบบเครือข่ายและสารสนเทศ
2. การบริหารจัดการระบบฐานข้อมูลและสารสนเทศให้มีความพร้อมใช้งาน
3. การปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
4. การเตรียมพร้อมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)
5. ข้อปฏิบัติสำหรับ USER สำนักงานปลัดกระทรวงสาธารณสุข

นโยบายภายใต้ระบบบริหารความเสี่ยง

สำนักงานปลัดกระทรวงสาธารณสุข มีการดำเนินงานตามแนวทางการดำเนินการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) มาอย่างต่อเนื่อง และภายใต้หมวด 4 IT6 ว่าด้วยระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ กำหนดให้ส่วนราชการต้องแสดงนโยบายความมั่นคงปลอดภัยให้ชัดเจน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงขอแสดงนโยบายตามประเด็นการพิจารณาดังนี้

ข้อ 1 นโยบายการควบคุมการเข้าถึงสารสนเทศ (Access Control Policy)

ให้ถือปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับวันที่ 4 กันยายน 2552 หัวข้อดังนี้

- ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง (หน้า 7, 24)
- ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ (หน้า 11)
- ระเบียบปฏิบัติสำหรับการลงทะเบียนเข้าใช้ระบบงาน (หน้า 24)
- ระเบียบปฏิบัติสำหรับการกำหนดและป้องกันรหัสผ่าน (หน้า 22)
- ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน (หน้า 23)

ข้อ 2 นโยบายการใช้งานเครือข่ายไร้สายภายในอาคาร (Wireless Policy)

(1) การตั้งชื่อ Access Point จะสอดคล้องกับตำแหน่งที่ตั้ง แสดงความหมายว่าอุปกรณ์ตัวนั้นติดตั้งอยู่ที่ อาคารใด ชั้นใดและเป็นตัวที่เท่าไหร่ : MOPH(ตึก)-(ชั้น)(ตัวที่)

(2) ให้เลือกเครือข่ายที่แสดงคุณภาพสัญญาณดีที่สุด

(3) อนุญาตให้ใช้งาน DHCP, DNS, HTTP, HTTPS, LDAP, NTP, UDP, mswindows, TrendMicro, Stream-1935, webmin, mms-port Pubnet, Gits-Mail-IMAP, H323, NetMeeting, PING, SIP-MSNmessenger, SSH, mms-port และ policy ที่เปิดให้ใช้ได้ตามความเหมาะสมของสถานการณ์ในปัจจุบันเท่านั้น

ข้อ 3 นโยบายการใช้งานอุปกรณ์ป้องกันภัยคุกคามระบบเครือข่าย (Firewall Policy)

(1) กำหนดให้อุปกรณ์ Firewall ทำหน้าที่ควบคุมการรับ-ส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก (Internet) ดังนี้

1. Firewall สป. (ใช้สองตัว ทำงานแบบ HA)
2. Firewall หน่วยงานระดับกรม
3. Firewall เครือข่ายไร้สาย (wireless) และห้องอบรม
4. Firewall ศูนย์เทคโนฯ
5. Firewall เครือข่าย GiN
6. Firewall เครือข่าย สบทร.

(2) กำหนดเปิดพอร์ต(port) ตามมาตรฐานการใช้งานพื้นฐานทั่วไป กรณีหน่วยงานใดต้องการใช้งานพอร์ตพิเศษ ให้ประสานงานกับเจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ. เพื่อดำเนินการให้ต่อไป

(3) กำหนดให้ทำการตรวจสอบและตอบโต้การบุกรุกจากผู้ไม่ประสงค์ดี และภัยคุกคามทางอินเทอร์เน็ตตลอด 24 ชั่วโมง

(4) กำหนดให้เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ. มีสิทธิ์ในการเข้าถึงอุปกรณ์ Firewall เท่านั้น โดยต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิ์ทุกครั้ง

ข้อ 4 นโยบายการใช้งานบริการอินเทอร์เน็ตองค์กร (Internet Security Policy)

ให้ถือปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับวันที่ 4 กันยายน 2552 หัวข้อดังนี้

- ระเบียบปฏิบัติสำหรับการใช้งานอินเทอร์เน็ต (หน้า 18)

ข้อ 5 นโยบายการใช้บริการระบบ Webmail **กระทรวงสาธารณสุข** (E-Mail Policy)

ให้ถือปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับวันที่ 4 กันยายน 2552 หัวข้อดังนี้

- ระเบียบปฏิบัติสำหรับการใช้งานอีเมลล์ (หน้า 19)

ข้อ 6 นโยบายการตรวจจับและป้องกันการบุกรุกระบบเครือข่าย (IDS/IPS Policy)

(1) กำหนดให้ระบบ IPS : Intrusion Prevention System ทำหน้าที่ตรวจดูแพ็คเก็ต (Packets) ที่วิ่งอยู่ในเครือข่ายและทำการบล็อก (Block) แพ็คเก็ตที่สอพฤติกรรมเสี่ยงเป็นการบุกรุก/โจมตีเครือข่าย ตลอด 24 ชั่วโมง และจัดเก็บสถิติ

(2) ติดตั้งระบบเพื่อกั้นระหว่างเครือข่ายภายในกับเครือข่ายภายนอกอาคารสำนักงานปลัดกระทรวงสาธารณสุข

(3) จัดทำรายงานสถิติในกรณีเกิดปัญหาเครือข่ายที่ส่งผลกระทบต่อเครือข่ายสำนักงานปลัดกระทรวงสาธารณสุข

(4) กำหนดให้เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ. มีสิทธิ์ในการเข้าถึงระบบIPS เท่านั้น โดยต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิ์ทุกครั้ง

ประกาศ ณ วันที่ 27 มกราคม 2553

(นายศิริวัฒน์ ทิพย์ธราดล)
รองปลัดกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงสาธารณสุข

(ภาคผนวก)

การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในสำนักงานปลัดกระทรวงสาธารณสุข ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้บริหาร

เพื่อสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข ผู้บริหารจะให้การสนับสนุนในการกำหนดมาตรการป้องกัน นโยบาย ระเบียบปฏิบัติ ข้อปฏิบัติและอื่นๆ รวมทั้งกระบวนการในการทบทวน เพื่อให้สามารถปรับปรุงหรือแก้ไขข้อบกพร่องหรือปัญหาทางด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

<u>หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง</u> ดังนี้

1. **เจ้าหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุข** (End User)
   - ปฏิบัติตามนโยบายฉบับนี้โดยเคร่งครัด
2. CIO **กระทรวงสาธารณสุข** (IT Manager)
   - กำหนดให้มีการจัดทำ/ปรับปรุง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)
   - กำหนดมาตรการควบคุม กำกับ ดูแลให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุขปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯอย่างเคร่งครัด
   - กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข
   - จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย
3. **นักวิชาการคอมพิวเตอร์และเจ้าพนักงานเครื่องคอมพิวเตอร์** (Help Desk)
   - ช่วยเหลือและประสานงานกับเจ้าหน้าที่ผู้ใช้งานของสำนักงานปลัดกระทรวงสาธารณสุข (End User) ในการแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์
   - ทำหน้าที่รับมือเหตุการณ์ความมั่นคงปลอดภัยตามที่ได้รับรายงานโดยปฏิบัติตามขั้นตอน/คู่มือปฏิบัติอย่างเคร่งครัด
   - บันทึกข้อมูลปัญหาการใช้งานเครื่องคอมพิวเตอร์และข้อมูลเหตุการณ์ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำรายงานสรุปปัญหาเสนอผู้บังคับบัญชา

4. **นักวิชาการคอมพิวเตอร์และผู้รับมอบหมาย** (System Administrator)

- ดูแลบัญชีผู้ใช้ กำหนดสิทธิและทบทวนสิทธิการใช้งานของระบบงานต่างๆ เช่น ระบบการใช้งาน Internet

- บริหารจัดการเครื่อง Server และอุปกรณ์เครือข่ายให้มีความมั่นคงปลอดภัย และสามารถใช้งานได้ตลอดเวลา

- ตรวจสอบข้อมูล Log ของ Server และอุปกรณ์เครือข่าย รวมทั้งจัดทำรายงานสรุปเสนอผู้บังคับบัญชา

- ทำการสำรองข้อมูลสำคัญและตรวจสอบข้อมูลที่สำรองไว้

5. **นักวิชาการคอมพิวเตอร์** (System Developer)

- ร่วมกับเจ้าของระบบงานหรือ Application ต่างๆ เพื่อกำหนด User Requirement และ Security Requirement สำหรับระบบงานหรือ Application

- พัฒนาระบบโดยคำนึงถึงความถูกต้องของข้อมูลนำเข้า ข้อมูลที่อยู่ในระหว่างการประมวลผลและรายงานสารสนเทศ

- ทำการทดสอบระบบงานหรือ Application ก่อนเริ่มต้นใช้งานจริง

- จัดทำคู่มือการใช้งาน คู่มือสำหรับการตรวจสอบระบบและวิธีการดำเนินงาน

- จัดอบรมการใช้งานระบบงานหรือ Application ให้กับผู้ใช้งานที่เกี่ยวข้อง