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