บันทึกข้อความ

ส่วนราชการ กองแผนงาน กลุ่มเทคโนโลยีสารสนเทศ โทร. 0 2590 4293

ที่ สธ 0905.03/484 **วันที่** 31 มีนาคม 2553

เรื่อง ขออนุมัตินโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย

เรียน อธิบดีกรมอนามัย

ตามที่กรมอนามัยได้ดำเนินการตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด 4 การวัด วิเคราะห์ และการจัดการความรู้ ซึ่งตามเกณฑ์การประเมิน IT 6 (ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ) กำหนดให้มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นลายลักษณ์อักษร นั้น

ในการนี้ กองแผนงานร่วมกับคณะกรรมการหมวด 4.1 การวัด การวิเคราะห์ ได้จัดทำประกาศกรมอนามัย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย โดยสอดคล้องกับแนวทางการดำการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข และมาตรฐาน ISO/IEC 27001 ดังรายละเอียดที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามอนุมัติประกาศกรมอนามัยดังกล่าว จะเป็นพระคุณ

สร้อยทอง เตชะเสน
(นางสาวสร้อยทอง เตชะเสน)
ผู้อำนวยการกองแผนงาน กรมอนามัย

- เห็นชอบ
- อนุมัติ

(นายประดิษฐ์ วินิจจะกูล)
รองอธิบดีกรมอนามัย ปฏิบัติราชการแทน
อธิบดีกรมอนามัย

31 มี.ค. 2553

ประกาศกรมอนามัย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
กรมอนามัย

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอนามัย มีความมั่นคงปลอดภัย ลดความเสี่ยง และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง หรือการคุกคามจากภัยคอมพิวเตอร์ ซึ่งอาจสร้างความเสียหายแก่กรมอนามัย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องได้ กรมอนามัยจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์ดังต่อไปนี้

1.1 เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย

1.2 เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีความสอดคล้องกับมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

1.3 เพื่อให้มีนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย ซึ่งสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ให้แก่เจ้าหน้าที่ทุกระดับในกรมอนามัย และบุคคลที่เกี่ยวข้อง ตระหนักและถือปฏิบัติอย่างเคร่งครัด

1.4 เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสม่ำเสมอ

2. องค์ประกอบของนโยบาย

ส่วนที่ 1 คำนิยาม
ส่วนที่ 2 นโยบายการรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
ส่วนที่ 3 นโยบายการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ส่วนที่ 4 นโยบายการใช้งานของผู้ใช้บริการ

ส่วนที่ 1 คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **ส่วนราชการ** หมายถึง ส่วนราชการภายในของกรมอนามัยที่มีฐานะเป็น สำนัก กอง ศูนย์ หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากอง
- **เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง เทคโนโลยีที่เกี่ยวข้องกับข่าวสาร ข้อมูล และการสื่อสาร นับตั้งแต่การสร้าง การนำมาวิเคราะห์หรือประมวลผลการรับและส่งข้อมูล การจัดเก็บและการนำไปใช้งานใหม่ เทคโนโลยีเหล่านี้ หมายถึงคอมพิวเตอร์ ซึ่งประกอบด้วยส่วนอุปกรณ์ (hardware) ส่วนคำสั่ง (software) และส่วนข้อมูล (data) และระบบการสื่อสารต่างๆ ไม่ว่าจะเป็นโทรศัพท์ ระบบสื่อสารข้อมูล ดาวเทียม หรือเครื่องมือสื่อสารใดๆ ทั้งมีสายและไร้สาย
- **ผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนราชการ
- **ผู้ใช้บริการ** หมายถึง ข้าราชการ พนักงานของรัฐ พนักงานราชการ ลูกจ้าง หรือผู้ที่ส่วนราชการอนุญาตให้ใช้ระบบคอมพิวเตอร์ได้
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมได้
- **ระบบสารสนเทศ** หมายถึง กระบวนการจัดเก็บรวบรวมข้อมูลซึ่งทำให้เป็นสารสนเทศ การจัดเก็บและการนำเสนอสารสนเทศให้เป็นปัจจุบันทันเหตุการณ์

ส่วนที่ 2 นโยบายการรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. วัตถุประสงค์

เพื่อควบคุมการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยป้องกันระบบคอมพิวเตอร์ ระบบสารสนเทศ ระบบเครือข่าย ที่ติดตั้งในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร จากภาวะเสี่ยงต่อการสูญหาย หรือได้รับความเสียหายจากการเข้าถึงโดยผู้ไม่มีสิทธิ์

2. ข้อปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2.1. การมอบหมายเจ้าหน้าที่รับผิดชอบเป็นผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.1.1. ส่วนราชการระดับกรม ให้กองแผนงานมอบหมายเจ้าหน้าที่ในกลุ่มเทคโนโลยีสารสนเทศ กองแผนงาน เป็นผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย โดยจัดทำเป็นลายลักษณ์อักษร และให้เจ้าหน้าที่ลงนามรับทราบ

2.1.2. ส่วนราชการระดับสำนัก/กอง/ศูนย์ หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากอง ให้หัวหน้าส่วนราชการมอบหมายเจ้าหน้าที่ในส่วนราชการ เป็นผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนราชการ โดยจัดทำเป็นลายลักษณ์อักษรและให้เจ้าหน้าที่ลงนามรับทราบ

2.2. ให้ส่วนราชการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน เพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วง ระบบปฏิบัติการ โปรแกรมอรรถประโยชน์ ระบบสารสนเทศ และข้อมูล ที่อยู่ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3. ให้ผู้ดูแลระบบรับผิดชอบการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และกำหนดวิธีปฏิบัติการควบคุมการเข้า-ออกพื้นที่ใช้งานเป็นลายลักษณ์อักษร

ส่วนที่ 3 นโยบายการบริหารจัดการระบบเทคโนโลยีสารสนเทศ และการสื่อสาร

1. วัตถุประสงค์

เพื่อบริหารจัดการการใช้งานและควบคุมการเข้าถึงระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย กรมอนามัย ให้อยู่ในสภาพพร้อมใช้งาน และสามารถพิสูจน์ตัวบุคคลที่เข้าใช้งานได้

2. ข้อปฏิบัติการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.1. ให้ผู้ดูแลระบบรับผิดชอบบริหารจัดการระบบเครือข่ายกรมอนามัย และกำหนดวิธีปฏิบัติเป็นลายลักษณ์อักษร เพื่อดำเนินการจัดทำแผนผังระบบเครือข่าย การแบ่งแยกเครือข่าย การกำหนดเส้นทางบนเครือข่าย การควบคุมการเข้าถึงระบบคอมพิวเตอร์และเครือข่าย ระบบรักษาความปลอดภัย การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.2. ให้ผู้ดูแลระบบรับผิดชอบบริหารจัดการระบบคอมพิวเตอร์ ระบบสารสนเทศ โดยดำเนินการควบคุมการเข้าถึงระบบปฏิบัติการ การเข้าถึงโปรแกรมประยุกต์ หรือระบบสารสนเทศ และข้อมูล การสำรองข้อมูลและกู้คืนข้อมูล การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.3. ให้ผู้ดูแลระบบรับผิดชอบการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยดำเนินการบริหารจัดการสิทธิ์และรหัสผ่านสำหรับผู้ใช้บริการตามความจำเป็นขั้นต่ำ การลงทะเบียนผู้ใช้บริการ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้บริการ

2.4. ให้ผู้ดูแลระบบรับผิดชอบตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้มีการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่อง

2.5. ผู้ดูแลระบบต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

ส่วนที่ 4 นโยบายการใช้งานของผู้ใช้บริการ

1. วัตถุประสงค์

เพื่อให้ผู้ใช้บริการได้รับทราบถึงหน้าที่ความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย และถือปฏิบัติ

2. ข้อปฏิบัติการใช้งานของผู้ใช้บริการทั่วไป

2.1. ผู้ใช้บริการทุกคนต้องผ่านการพิสูจน์ตัวตนจากระบบ กรมอนามัย เมื่อจะเข้าใช้งานระบบเครือข่าย กรมอนามัย ทั้งระบบเครือข่ายระยะใกล้ และเครือข่ายอินเตอร์เน็ต

2.2. ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่กรมอนามัยจัดสรรไว้เท่านั้น และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัยเป็นลายลักษณ์อักษรแล้ว

2.3. ผู้ใช้บริการต้องใช้จดหมายอิเล็กทรอนิกส์กลางของภาครัฐในการติดต่อเรื่องที่เป็นงานราชการเท่านั้น

2.4. การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้บริการต้องปฏิบัติตามระเบียบกรมอนามัยว่าด้วยการใช้ระบบคอมพิวเตอร์ พ.ศ. 2551

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารกรมอนามัยนี้ ได้กำหนดขึ้นเพื่อทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรมีความมั่นคงปลอดภัย ลดความเสี่ยง และปัญหาที่อาจจะเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง หรือการคุกคามจากภัยคอมพิวเตอร์ ซึ่งเจ้าหน้าที่กรมอนามัย และบุคคลที่เกี่ยวข้องจะต้องถือปฏิบัติอย่างเคร่งครัด

ประกาศ ณ วันที่ เดือนมีนาคม พ.ศ.2553

(นายประดิษฐ์ วินิจจะกูล)
รองอธิบดีกรมอนามัย ปฏิบัติราชการแทน
อธิบดีกรมอนามัย