



สถาบันวิจัยสมุนไพรมหาวิทยาลัยมหิดล
เลขรับที่ 0323
รับวันที่ 11 ก.พ. 2552
เวลา...

ประกาศกรมวิทยาศาสตร์การแพทย์
กระทรวงสาธารณสุข

ผู้รับ	...
วันที่	8 ก.พ. 2552
เวลา	17.30 น.

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ISO/IEC 27001)
กรมวิทยาศาสตร์การแพทย์ เพื่อเตรียมความพร้อมกฎหมายทางด้านเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์การแพทย์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง และให้หน่วยงานต่างๆ ของกรมวิทยาศาสตร์การแพทย์ ได้เตรียมความพร้อมตามกฎหมายต่างๆ ที่กระทรวงเทคโนโลยีสารสนเทศได้ออกมาบังคับใช้ เช่น

- พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551
- พระราชกฤษฎีกากำหนดประเภทธุรกรรมกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

นอกจากนี้ยังรวมถึงการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ด้วย กรมวิทยาศาสตร์การแพทย์จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) ระเบียบวิธีปฏิบัติ (Procedure) แนวปฏิบัติ (Guideline) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล และปฏิบัติได้อย่างถูกต้องตามกฎหมายต่างๆ ที่เกี่ยวข้องได้กำหนดไว้

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

ที่ สธ. 0601.01/ว 0901

...2/

เรียน ผู้อำนวยการสถาบันวิจัยสมุนไพรมหาวิทยาลัยมหิดล

สำนักงานเลขานุการกรมวิทยาศาสตร์การแพทย์

วันที่ 10 ก.พ. 2552

1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและ
เจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายอย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ
และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการ
ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้ง
ต่อปี หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

2. องค์ประกอบของนโยบาย

2.1 คำนิยาม

2.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

2.3 การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

2.4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.6 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

2.7 การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

2.8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและ
การสื่อสารขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน
(Standard) ระเบียบวิธีปฏิบัติ (Procedure) และแนวปฏิบัติ (Guideline) ในการรักษาความมั่นคงปลอดภัยระบบ
เทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบ
เทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน
บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็น
มาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่
ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

เขียน ผู้เชี่ยวชาญ/หัวหน้าห้องปฏิบัติการ/ศูนย์/
โรงงาน/คหวิ/สวน/งานสารบรรณ/งานพัสดุ
และงานการเงิน

ประกาศ ณ วันที่ 10 กุมภาพันธ์ พ.ศ. 2552

- เพื่อทราบ/ลงนาม
- แจ้งผู้เกี่ยวข้องทราบ/ลงนาม
- แจ้งผู้เกี่ยวข้องทราบ/ลงนาม

12 ก.พ. 2552

(นายมานิต ชีระคันธุวานนท์)
อธิบดีกรมวิทยาศาสตร์การแพทย์

16 ก.พ. 52

16 ก.พ. 52

16-2-52