โรงพยาบาลอุดรธานี

ระดับเอกสาร : ระเบียบปฏิบัติ (System Procedure) เลขที่	ฉบับที่ : ๑
เรื่อง : การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ	วันที่

กลุ่มงาน : สารสนเทศทางการแพทย์(ศูนย์คอมพิวเตอร์)

ผู้จัดทำ : .....
(นายธนพล ธนอำพนสกุล)
ตำแหน่ง หัวหน้าหน่วยงานสารสนเทศทางการแพทย์

ผู้ทบทวน : .....
(นายสุรพงศ์ แสนโภชน์)
ตำแหน่ง รองผู้อำนวยการฝ่ายแพทย์ ลำดับที่ ๒

ผู้อนุมัติ : .....
(นายทรงเกียรติ เล็กตระกูล)
ตำแหน่ง ผู้อำนวยการโรงพยาบาลอุดรธานี

๑. วัตถุประสงค์ :

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

๒. ขอบข่าย :

ระบบเทคโนโลยีสารสนเทศและการสื่อสารโรงพยาบาลอุดรธานี

๓. อุปกรณ์/เครื่องมือ : -

๔.ความรับผิดชอบ :

กลุ่มงานสารสนเทศทางการแพทย์(ศูนย์คอมพิวเตอร์)

๕.คำจำกัดความ : -

๖. เอกสารอ้างอิง :

กลุ่มบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการ. (๒๕๖๕). *ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕*, สำนักงานปลัดกระทรวงสาธารณสุข ถนนติวานนท์ จังหวัดนนทบุรี, สธ ๐๒๑๒/ว๙๐๔๓.

๗. รายละเอียด :

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

๑. ระบบป้องกันผู้บุกรุก

๑.ก. ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

๒. ระบบไฟร์วอลล์ (Fire Wall)

๒.ก. ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒.ข. ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทาการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒.ค. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดาเนินการแก้ไขปัญหา

๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือ มัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์(Spyware)

๓.ก. ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในกระทรวงสาธารณสุขไปยังภายนอกหรือไม่

๓.ข. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกระทรวงสาธารณสุข

๓.ค. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที