แผนการดำเนินการ
ตอบสนองเหตุการณ์ความมั่นคงปลอดภัย
ทางระบบสารสนเทศ
(IT Security Audit Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศสำหรับสำนักงานปลัดกระทรวงสาธารณสุข เพื่อให้สามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร ให้ทราบถึงรูปแบบการดำเนินการที่เป็นรูปธรรม กำหนดเงื่อนไขหรือนโยบายการดำเนินงาน บุคลากรและอุปกรณ์ที่ใช้ภายในหน่วยงาน และแนวทางการปฏิบัติตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศแยกตามบทบาทหน้าที่หรือตามอุปกรณ์ เพื่อให้ทีมงานหรือบุคลากรภายในหน่วยงานสามารถนำไปปฏิบัติได้ กล่าวถึงแนวทางการสำรองข้อมูลและการปรับปรุงข้อมูลให้ทันสมัย รวมถึงการบริหารจัดการบันทึกการเปลี่ยนแปลงของกระบวนการดำเนินงานและเป็นขั้นตอนที่สำคัญที่สุดเพื่อให้แน่ใจว่ากระบวนการดังกล่าวยังสามารถปฏิบัติได้อย่างมีประสิทธิภาพ รวมถึงตัวอย่างระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์ให้ปลอดภัยตามรายละเอียดเนื้อหาออกเป็นส่วน ๆ ดังนี้

ส่วนที่ 1 แผนการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนที่ 2 (ร่าง) ระเบียบว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

ส่วนที่ 3 (ร่าง) แนวทางปฏิบัติการตรวจสอบระบบสารสนเทศ

ส่วนที่ 4 ระเบียบปฏิบัติการการรักษาความปลอดภัยระบบสารสนเทศ สป.(ฉบับร่าง)

ส่วนที่ 5 ข้อกำหนดการปฏิบัติการศูนย์ปฏิบัติการคอมพิวเตอร์

ส่วนที่ 6 การรักษาความปลอดภัยในการเข้าถึงข้อมูล สำหรับผู้บริหารเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

ภาคผนวก แบบบันทึกการปฏิบัติงาน บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย

ส่วนที่ 1

แผนการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

1. แนวทางการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ ตามบทบาทหน้าที่

ทีมงานดูแลเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ สามารถนำแนวทางการดำเนินการแยกตามบทบาทหน้าที่ตามอุปกรณ์ที่ใช้ไปใช้ และทำรายงานสรุปการดำเนินการให้หัวหน้าทีมดูแลเหตุการณ์ความมั่นคงปลอดภัยตรวจสอบ แยกตามอุปกรณ์ได้ดังนี้

1. ระบบป้องกันผู้บุกรุก

แผนดำเนินการรายวัน

1. **ดำเนินการตรวจสอบไฟล์ล็อกของหรือรายงานของระบบป้องกันการบุกรุก** สิ่งที่ควรตรวจสอบมีดังต่อไปนี้

- การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายเป็นผู้โจมตี
- อื่นๆตามที่นโยบายด้านความปลอดภัยขององค์กรกำหนด

2. **ดำเนินการรายงานสรุปผลที่ได้จากระบบป้องกันการบุกรุก**

นำข้อมูลที่ได้จากข้อ 1 ข้างต้นมาเขียนรายงาน และรายงานไปยังหัวหน้าและทีมงานดูแลเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ ทางอีเมล์ เพื่อให้สะดวกในการเก็บข้อมูลและโต้ตอบ

- ศึกษาเพิ่มเติมว่าระบบป้องกันผู้บุกรุกที่ใช้งานอยู่
- สามารถสร้างรายงานได้ตามแนวทางการตรวจสอบหรือไม่ ถ้าได้ให้สร้างรายงานสรุปทุกวัน
- ถ้าระบบป้องกันผู้บุกรุกไม่สนับสนุน ให้ดำเนินการหามาตรการในการสร้างรายงานอย่างรวดเร็วเพื่อลดภาระงานของทีมงาน

3. **ตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ**

- แจ้งข้อมูลให้กับหัวหน้าทีมดูแลเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์เพื่อตัดสินใจดำเนินการแก้ไขปัญหาในขั้นต้น และวางแผนแก้ปัญหาระยะยาวกับผู้อำนวยการสารสนเทศ หลังจากดำเนินการแก้ไขปัญหาระยะสั้นไปแล้ว โดยมีข้อมูลสำคัญที่ต้องแจ้งดังนี้

- การโจมตีหรือการละเมิดสำเร็จหรือไม่
- ข้อมูลของการโจมตีหรือข้อมูลเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ

2. ระบบไฟร์วอลล์

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

1. ดำเนินการตรวจสอบกฎของของระบบป้องกันการบุกรุก ควรทำการตรวจสอบกฎอย่างน้อยเดือนละ 1 ครั้ง และควรมีการทำเอกสารเกี่ยวกับคำอธิบายกฎประกอบไว้ด้วย

2. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อกและรายงานของไฟร์วอลล์ สิ่งที่ควรตรวจสอบมีดังต่อไปนี้

- ไฟร์วอลล์ได้ทำการ block packet มากน้อยเพียงใด
- ลักษณะของ packet ส่วนใหญ่ที่ถูก block เป็น
- Packet ของหมายเลขไอพีของเครือข่ายใดถูกblock เป็นจำนวนมาก
- อื่น ๆตามที่นโยบายด้านความปลอดภัยขององค์กรกำหนด

3. ดำเนินการรายงานสรุปผลที่ได้จากไฟร์วอลล์ นำข้อมูลที่ได้จากข้อ 2 ข้างต้นมาเขียนรายงาน

4. ตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศแจ้งข้อมูลให้กับหัวหน้าทีมดูแลเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์เพื่อตัดสินใจดำเนินการแก้ไขปัญหาในขั้นต้น และวางแผนแก้ปัญหาระยะยาวกับผู้อำนวยการสารสนเทศ หลังจากดำเนินการแก้ไขปัญหาระยะสั้นไปแล้วโดยมีข้อมูลสำคัญที่ต้องแจ้งดังนี้

- การพยายามโจมตีไฟร์วอลล์ทำได้สำเร็จหรือไม่
- ข้อมูลของการโจมตีหรือข้อมูลเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ

---

3. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต

ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) ประกอบไปด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจันรวมถึงสปายแวร์

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

1. ดำเนินการตรวจสอบไฟล์ล็อกและรายงาน ของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ตสิ่งที่ควรตรวจสอบมีดังต่อไปนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในองค์กรออกไปยังภายนอกหรือไม่
- อื่นๆ ตามที่นโยบายด้านความปลอดภัยขององค์กรกำหนด

2. ดำเนินรายงานสรุปผลที่ได้จากอุปกรณ์ที่เกี่ยวข้องกับการตรวจสอบมัลแวร์บนเครื่องไคลเอ็นต์ นำข้อมูลที่ได้จากข้อ 1 ข้างต้นมาเขียนรายงาน

3. ควรศึกษาวิธีการแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายขององค์กร

4. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอกหรือพบมีกระจายของมัลแวร์ในองค์กรเป็นจำนวนมาก ควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์ กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องของผู้ใช้โดยทันที ซึ่งรายละเอียดการแก้ไขนั้นสามารถศึกษาได้จากเว็บไซต์ของเจ้าของผลิตภัณฑ์ ในกรณีที่เครื่องที่ติดมัลแวร์ เป็นเครื่องเซิร์ฟเวอร์ควรติดต่อผู้ดูแลระบบให้ดำเนินการแก้ไขต่อไปและบันทึกการปฏิบัติงานต่อวัน ในกรณีที่ปัญหาพบว่ามีปัญหากระทบต่อการดำเนินการขององค์กรให้ประสานงานกับหัวหน้าทีมเพื่อดำเนินการตัดสินใจแก้ปัญหาต่อไป

4. ระบบตรวจสอบและป้องกันช่องโหว่ความมั่นคงปลอดภัย

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

1. ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของระบบตรวจสอบและป้องกันช่องโหว่ความมั่นคงปลอดภัย สิ่งที่ควรตรวจสอบมีดังต่อไปนี้

- มีเครื่องคอมพิวเตอร์จำนวนเพียงใดที่ทำการปรับปรุงช่องโหว่และที่ไม่ได้ปรับปรุงช่องโหว่
- การปรับปรุงช่องโหว่ที่เครื่องคอมพิวเตอร์ภายในเครือข่ายยังไม่ได้ลงนั้น มีความสำคัญหรือไม่มากน้อยเพียงใด

2. ตรวจพบว่ามีเครื่องคอมพิวเตอร์ภายในเครือข่ายยังไม่ได้ลงปรับปรุงช่องโหว่ แจ้งให้หัวหน้าทีมรับทราบและดำเนินการตรวจสอบสาเหตุที่ไม่สามารถปรับปรุงช่องโหว่ได้ รวมถึงประเมินผลกระทบจากการปรับปรุงช่องโหว่ว่ามีผลมากน้อยเพียงใด

3. ดำเนินการตรวจสอบค่าการปรับแต่งของระบบตรวจสอบและป้องช่องโหว่ความมั่นคงปลอดภัยควรทำการตรวจสอบอย่างน้อยเดือนละ 1 ครั้ง และควรมีการทำเอกสารเกี่ยวกับค่าการ

ปรับแต่งของระบบรวมถึงการวันเวลาที่มีการปรับปรุงช่องโหว่และปัญหาที่พบในแต่ละครั้งประกอบไว้ด้วย

2. แนวทางการสำรองข้อมูลอุปกรณ์เสริมสร้างความมั่นคงปลอดภัยบนระบบสารสนเทศ

ทีมงานดูแลเหตุการณ์ความมั่นคงปลอดภัยบนระบบสารสนเทศ ต้องดำเนินการสำรองข้อมูลบนระบบและรายงานสรุปการดำเนินการสำรองข้อมูลให้กับหัวหน้าทีมด้วยทุกครั้ง โดยแนวทางการดำเนินการสำหรับอุปกรณ์เสริมสร้างความปลอดภัยภายในองค์กรที่ประกอบด้วย

- ระบบป้องกันผู้บุกรุก
- ระบบไฟร์วอลล์
- ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต
- ระบบตรวจสอบและป้องกันช่องโหว่ความมั่นคงปลอดภัย และดำเนินการตรวจสอบตามนี้

แผนการดำเนินการ

1. ดำเนินการสำรองข้อมูลไฟล์ล็อก ควรทำการสำรองข้อมูล อย่างน้อยวันละ 1 ครั้งโดยข้อมูลที่สำรองนี้ควรเก็บไว้ในที่ปลอดภัย

2. ดำเนินการสำรองค่าปรับแต่งของอุปกรณ์ ควรทำการสำรองข้อมูลของค่าปรับแต่งเก็บไว้ในที่ปลอดภัยหนึ่งชุด และควรสำรองข้อมูลก่อนที่จะดำเนินการเปลี่ยนแปลงต่อไปที่อาจส่งผลกระทบให้ระบบไม่สามารถทำงานได้

3. แนวทางการปรับปรุงข้อมูลอุปกรณ์เสริมสร้างความมั่นคงปลอดภัยบนระบบสารสนเทศ

ทีมงานดูแลเหตุการณ์ความมั่นคงปลอดภัยบนระบบสารสนเทศ ต้องดำเนินการปรับปรุงข้อมูลของอุปกรณ์ เสริมสร้างความมั่นคงปลอดภัยบนระบบสารสนเทศให้ทันสมัย และรองรับภัยคุกคามใหม่เสมอ และรายงานสรุปการดำเนินการสำรองข้อมูลให้กับหัวหน้าทีมด้วยทุกครั้ง โดยแนวทางการดำเนินการสำหรับอุปกรณ์เสริมสร้างความปลอดภัยภายในองค์กรที่ประกอบด้วย

- ระบบป้องกันผู้บุกรุก
- ระบบไฟร์วอลล์
- ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต
- ระบบตรวจสอบและป้องกันช่องโหว่ความมั่นคงปลอดภัยและดำเนินการตรวจสอบตามนี้

แผนการดำเนินการ

1. ดำเนินการปรับปรุงกฎบนอุปกรณ์เพื่อทำให้ระบบนั้นสามารถป้องกันการโจมตีหรือรองรับภัยคุกคามแบบใหม่ได้

ควรทำการปรับปรุงกฎบนอุปกรณ์อย่างน้อยวันละ 1 ครั้งหรือตามที่เจ้าของผลิตภัณฑ์ประกาศว่าให้ทำการปรับปรุงกฎหรือสัญลักษณ์ในการตรวจจับหรือป้องกัน

2. ดำเนินการปรับปรุงช่องโหว่ของอุปกรณ์และติดตามข่าวสารของเจ้าของผลิตภัณฑ์อย่างสม่ำเสมอควรทำการปรับปรุงช่องโหว่อย่างน้อยสัปดาห์ละ 1 ครั้ง

4. แนวทางการบันทึกการเปลี่ยนแปลงของอุปกรณ์เสริมสร้างความมั่นคงบนระบบสารสนเทศ

ความมั่นคงปลอดภัยของระบบสารสนเทศ นอกจากความสำคัญของกระบวนการในการปฏิบัติงานที่ถูกต้องเหมาะสมแล้ว การบันทึกข้อมูลการดำเนินการและการบริหารจัดการการเปลี่ยนแปลงเป็นสิ่งสำคัญและมีผลกระทบต่อการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศทั้งระยะสั้นและระยะยาวอย่างหลีกเลี่ยงไม่ได้ กระบวนการบริหารจัดการการเปลี่ยนแปลงเรียกว่า Change Management Process ซึ่งมีขั้นตอนการดำเนินการ ดังนี้

1. เลือกกระบวนการที่ต้องมีการบันทึกการเปลี่ยนแปลง กระบวนการสำคัญตามแนวทางทั้งสามแนวทาง คือ แนวทางการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ แนวทางการสำรองข้อมูลและแนวทางการปรับปรุงข้อมูลอุปกรณ์เสริมสร้างความมั่นคงปลอดภัย ถือเป็นกระบวนการสำคัญที่ควรมีการดำเนินการบันทึกการเปลี่ยนแปลง

2. การกำหนดสิทธิของผู้มีหน้าที่หรือผู้ที่สามารถเปลี่ยนแปลงการปรับแต่งค่าหรือเปลี่ยนแปลงกฎของอุปกรณ์เสริมสร้างความมั่นคงปลอดภัยทางระบบสารสนเทศ สิทธิและบทบาทหน้าที่เป็นสิ่งสำคัญที่ควรมีการกำหนดให้ชัดเจนในการกำหนดบทบาทหน้าที่ของบุคลากร และสิทธิในการแก้ไขภาระหน้าที่รับผิดชอบรวมถึงภาระหน้าที่ในการบันทึกการเปลี่ยนแปลง

3. ขั้นตอนการบันทึกการเปลี่ยนแปลง คือการบันทึกการเปลี่ยนแปลงที่เกิดขึ้นภายในขั้นตอนดำเนินการสิ่งที่ต้องระบุเมื่อมีการเปลี่ยนแปลงคือ วันเวลา การแก้ไขเปลี่ยนแปลงที่เกิดขึ้นกับอุปกรณ์ทรัพยากรหรือบุคลากรที่เกี่ยวข้อง เหตุผลที่ต้องมีการเปลี่ยนแปลง

4. ขั้นตอนการดำเนินการสรุปการดำเนินการเปลี่ยนแปลงที่เกิดขึ้นกับอุปกรณ์ ทีมงานตอบสนองเหตุการณ์ความมั่นคงปลอดภัยระบบสารสนเทศควรจะสรุปการเปลี่ยนแปลงที่เกิดขึ้นในแต่ละเดือนเป็นอย่างน้อยสรุปให้หัวหน้าทีมเพื่อใช้ในการติดตามตรวจสอบต่อไป

5. ขั้นตอนการตรวจสอบข้อมูลการบันทึกการเปลี่ยนแปลง หัวหน้าทีมตอบสนองเหตุการณ์ความมั่นคงทางระบบสารสนเทศ มีหน้าที่ในการตรวจสอบการบันทึกการเปลี่ยนแปลงและความถูกต้องของทีมงานโดยละเอียดและดำเนินการแก้ไขปัญหาเพิ่มเติม ก่อนจะสรุปปัญหาสำคัญให้กับ

ผู้อำนวยการระบบสารสนเทศ เพื่อใช้ในการวางแผนระยะยาวขององค์กร นำไปสู่การเปลี่ยนแปลงอย่างต่อเนื่อง การบริหารจัดการการเปลี่ยนแปลงเป็นสิ่งสำคัญที่หน่วยงานตอบสนองความมั่นคงปลอดภัยทางคอมพิวเตอร์ควรปรับและนำไปใช้ภายในองค์กรให้เหมาะสมกับทีมงานภายในหน่วยงานสามารถปฏิบัติและตรวจสอบการบันทึกการเปลี่ยนแปลงได้

ส่วนที่ 2

(ร่าง) ระเบียบว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

ด้วยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ได้จัดให้มีเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกของบุคลากรในการปฏิบัติงาน ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง เห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

"องค์กร" หมายถึง สำนักงานปลัดกระทรวงสาธารณสุข

"เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุข "ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของสำนักงานปลัดกระทรวงสาธารณสุข "บุคลากร" หมายถึง ข้าราชการและลูกจ้างของสำนักงานปลัดกระทรวงสาธารณสุข รวมถึงบุคคลอื่นที่สำนักงานปลัดกระทรวงสาธารณสุข มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ผู้ดูแลเครือข่ายคอมพิวเตอร์" หมายความถึง ข้าราชการและลูกจ้างที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ให้มี "คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ " ที่ผู้บังคับบัญชาแต่งตั้งจากโดยมีอำนาจหน้าที่ดังต่อไปนี้

* กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้

* ให้คำปรึกษาแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์เกี่ยวกับการปฏิบัติตามระเบียบนี้

* ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล

* จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม

* ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้

* ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3 ข้อปฏิบัติของบุคลากรในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ 1 บุคลากรมีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่บุคลากรที่ฝ่าฝืนตามความเหมาะสมต่อไป

ข้อ 2 บุคลากรพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ 3 บุคลากรพึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย อาทิ เช่น ไม่ใช้การส่ง mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ 4 บุคลากรมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ 5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล บุคลากรจะต้อง

* ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่บุคลากรครอบครองใช้งานอยู่ ทั้งในระดับ BIOS และระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลขและสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

* ใช้รหัสผ่านสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

* ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่บุคลากรครอบครองอยู่

* ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ 6 บุคลากรจะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

* เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

* เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

* เพื่อการพาณิชย์

* เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือบุคคลภายนอกก็ตาม

* เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น

* เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

* เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังบุคลากรหรือบุคคลอื่น เป็นต้น

* เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของบุคลากรอื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ

* เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ(web site) ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

* เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

ข้อ 7 เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม บุคลากรจะต้อง

* ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

* ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน

* ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กร ได้

* ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (server) ที่ต้องใช้งานตลอด 24 ชั่วโมง

* ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กร ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กร จัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

* ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

* ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งองค์กร จัดให้สำหรับใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร

* ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคลากรและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการดังกล่าวด้วย

* ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์แล้วแต่กรณี

* ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต

* คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่องค์กร รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากองค์กร ภายในกำหนด 7 วันนับแต่วันพ้นสภาพการเป็นบุคลากร

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

ข้อ 1 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของบุคลากรเพื่อให้เป็นไป ตามระเบียบนี้

หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าบุคลากรผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุดและในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของบุคลากรดังกล่าวได้ทันที

ข้อ 2 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ 3 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

ข้อ 4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ 5 เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่องค์กร ในทันทีที่พ้นหน้าที่ และให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ 6 ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กร จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป

ส่วนที่ 3

(ร่าง) แนวทางปฏิบัติการตรวจสอบระบบสารสนเทศ

การตรวจสอบระบบประจำวัน

๑. เครื่องให้บริการ (Server) สำหรับระบบที่มีช่วงเวลาให้บริการ ให้สำรวจ Drive ที่ใช้ Boot ระบบได้ ไม่ให้มีแผ่นดิสก์ หรือ CD ใด ๆ ค้างอยู่ ก่อนเปิดระบบ และให้เปิดอุปกรณ์ที่ต้องใช้กระแสไฟฟ้าเป็นปริมาณมากก่อน เช่น เครื่องปรับอุณหภูมิ รวมทั้งอุปกรณ์รายล้อมอื่น ๆ

๑.๑ ในการเริ่มต้นทำงานแต่ละวัน (เมื่อระบบเริ่มทำงานแล้ว) ให้ตรวจสอบโปรแกรมรักษาความปลอดภัยที่ติดตั้ง ดังนี้

- Audit Log File / รายงานจากโปรแกรม Firewall / รายงานจากโปรแกรม Anti Virus / รายงานจากโปรแกรมตรวจสอบการบุกรุกเครือข่าย (Intrusion Detection Network System) ตรวจดูการใช้งานระบบที่ผ่านมา เพื่อหาการลับลอบเข้าระบบนอกเวลา หรือ พฤติกรรมน่าสงสัย เช่น ใส่รหัสผ่าน ผิดมากเกินไป มีการใช้งานระบบโดยใช้สิทธิของผู้ใช้ที่ไม่ได้มาทำงาน มีการส่งข้อมูลออกไปนอกระบบที่ไม่ได้อนุญาต
- Security Assessment Tools ตรวจหาช่องโหว่ของระบบ เพื่อแก้ไขจุดอ่อนของระบบ และ Update ข้อมูลของโปรแกรมตรวจสอบ ถ้าพบว่าไม่ทันสมัย แล้วตรวจระบบอีกครั้ง
- ตรวจสอบข่าวสาร รปภ.ระบบ แจ้งเตือนภัย การประกาศข้อบกพร่องของระบบปฏิบัติการ หรือซอฟต์แวร์ใช้งานประเภทต่าง ๆ รวมทั้งเว็บที่เกี่ยวข้องกับกลุ่ม แฮกเกอร์ เพื่อให้สามารถปรับการป้องกันได้ทันที จากแหล่งข้อมูลต่อไปนี้
  - ThaiCERT
  - ผู้ผลิตโปรแกรมป้องกันไวรัส

๑.๒ ระหว่างช่วงเวลาทำงาน ให้หมั่นตรวจสอบความปลอดภัยของระบบ ดังนี้

- จุดอ่อนของระบบ ตรวจสอบจาก Security Assessment Tools เมื่อพบให้แก้ไขทันที หรือไม่ควรเกิน ๑ วัน
- การ Scan port โดยเฉพาะ Server ที่มีการเชื่อมต่อกับอินเตอร์เน็ต
- การพยายามเข้าระบบโดยไม่ถูกต้อง ตรวจสอบจาก Audit Log File

๑.๓ ก่อนปิดระบบ หรือก่อนเลิกปฏิบัติงาน ให้ตรวจสอบระบบ ดังนี้

- ตรวจสอบการสำรองข้อมูลสำคัญภายใน Server (ถ้ามี)
- ตรวจสอบผู้ใช้งานว่าได้ออกจากระบบอย่างถูกต้องหมดแล้ว
- ตรวจสอบผู้ใช้งานให้มีการสำรองข้อมูลที่ต้องการก่อนปิดระบบ ๑๐ นาที

๑.๔ การดำเนินการเมื่อตรวจพบการละเมิด และข้อบกพร่องที่ต้องแก้ไข

- หากพบว่ามีการบุกรุกจากภายในระบบ ให้ตรวจสอบแหล่งกระทำผิด และตัดออกจากเครือข่าย หาผู้ละเมิด แจ้งเตือนให้ผู้รับผิดชอบระบบอื่น ๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด ปรับแก้ไข รายงานผู้บังคับบัญชา ลงโทษทางวินัย (ถ้าหาผู้ละเมิดได้) ในความผิดไม่ร้ายแรง ลงโทษทางกฎหมาย กรณีเกิดความเสียหายร้ายแรงแก่ทางราชการ
- หากพบว่ามีการบุกรุกจากภายนอกระบบ ประสานหน่วยเกี่ยวข้องหาแหล่งกระทำผิด แจ้งเตือนให้ผู้รับผิดชอบระบบอื่น ๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด แก้ไขจุดอ่อนที่เป็นสาเหตุ รายงานผู้บังคับบัญชา ลงโทษทางกฎหมายผู้ละเมิด (ถ้ามี)
- หากพบการแพร่กระจายไวรัสคอมพิวเตอร์กำลังดำเนินอยู่ ตรวจสอบและแยกแหล่งแพร่ไวรัสออกจากเครือข่าย โดยถอดสาย LAN ออก ตรวจสอบระบบที่ถูกทำลาย แก้ไขข้อบกพร่องที่เป็นสาเหตุ เช่น ปรับข้อมูลการตรวจสอบไวรัสให้ทันสมัย แก้ไขจุดอ่อนของระบบปฏิบัติการ
- กรณีหน่วยไม่สามารถแก้ไขสถานการณ์ได้เอง ให้ขอรับการสนับสนุนที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข โทร ๐๒ – ๕๙๐๑๒๐๘ หรือ ๐๒ – ๕๙๐๑๒๑๒ หรือ E-mail : boonchai_c@health.moph.go.th ,suwanna@health.moph.go.th

๒. เครื่องลูกข่าย ให้ตรวจสอบดังนี้

- โปรแกรมป้องกันไวรัสที่ติดตั้ง ได้รับการปรับข้อมูลให้ทันสมัยแล้ว ทุกเครื่อง
- รหัสผ่านของผู้ใช้ทุกคนมีความแข็งแกร่ง
- ระบบปฏิบัติการได้รับการปรับข้อแก้ไขทั้งหมดแล้ว ทุกเครื่อง
- การตั้งค่าของโปรแกรมรักษาความปลอดภัยเช่น Firewall Anti Virus มีความเหมาะสม
- มีการสำรองข้อมูลที่ใช้งานแล้วอย่างครบถ้วน หลังปฏิบัติงานเรียบร้อยแล้ว

ส่วนที่ 4

ระเบียบปฏิบัติการ การรักษาความปลอดภัยระบบสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข (ฉบับร่าง)

นิยาม คำศัพท์ในระเบียบปฏิบัตินี้

๑. " จนท.ดูแลรักษาความปลอดภัยระบบสารสนเทศ สป." หมายถึง ผู้รับผิดชอบการดูแลรักษาความปลอดภัยระบบสารสนเทศ ของ สป.

๒. " จนท.ดูแลรักษาความปลอดภัยระบบสารสนเทศ ของหน่วยงาน และ ผู้ดูแลดูแลรักษาความปลอดภัยระบบสารสนเทศ ของหน่วยงาน "

หมายถึงผู้รับผิดชอบการ รปภ.ระบบสารสนเทศ ของหน่วยงาน(ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)

๓. " ทรัพยากร " หมายถึง อุปกรณ์ในระบบคอมพิวเตอร์ ระบบสื่อสาร สารสนเทศ รวมทั้งสิ่งอำนวยความสะดวกต่าง ๆ

ข้อบังคับ

๑. ใช้ห้องศูนย์ปฏิบัติการคอมพิวเตอร์และเครือข่าย ตามเวลาราชการ กำหนดเวลาทำการ ๐๖.๐๐ – ๑๘.๐๐ นอกเหนือจากนั้น ให้ถือเป็นการปฏิบัตินอกภารกิจ ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ได้รับมอบหมายจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน

๒. การเปิด ปิดห้องตามปกติให้กระทำโดยเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓. การเปิด ปิดระบบการตรวจสอบตามปกติให้กระทำโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. การใช้ระบบตรวจสอบความปลอดภัย ฯ และทรัพยากรอื่น ๆ ให้กระทำโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๕. ห้ามผู้ไม่เกี่ยวข้อง ทำการเคลื่อนย้าย เปลี่ยนแปลง แก้ไข ทรัพยากรในระบบ

๖. กรณีฉุกเฉินต้องใช้ระบบตรวจสอบ ไม่สามารถปฏิบัติตามที่กำหนดในข้อบังคับ ๑ – ๕ ผู้ดำเนินการ บันทึกสาเหตุ ความจำเป็น และผลกระทบที่ได้ รายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบทันที

๗. ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศ ของหน่วยงาน สามารถนำข้อบังคับในระเบียบปฏิบัตินี้ไปปรับใช้กับระบบสารสนเทศของหน่วยงานได้

ตารางการใช้ห้องปฏิบัติงานและการตรวจสอบความปลอดภัยระบบสารสนเทศประจำวัน

	Server	Client
เช้า **๐๖.๐๐ – ๐๙.๐๐**	เริ่มตรวจสอบก่อนการปฏิบัติงาน - โปรแกรมตรวจสอบการบุกรุกเครือข่าย - โปรแกรมตรวจสอบไวรัสคอมพิวเตอร์ - โปรแกรมตรวจสอบจุดอ่อนของระบบ	เริ่มตรวจสอบก่อนการปฏิบัติงาน - โปรแกรมตรวจสอบไวรัสคอมพิวเตอร์
ระหว่างปฏิบัติงาน **๐๙.๐๐ - ๑๕.๐๐**	ตรวจสอบระหว่างปฏิบัติงาน - การเข้าระบบที่ไม่ถูกต้อง - การใช้ระบบที่ไม่ถูกต้อง - พฤติกรรมที่น่าสงสัย - ข้อมูลข่าวสารด้านรักษาความปลอดภัยระบบการแจ้งเตือนภัย - จุดอ่อนของระบบ	ตรวจสอบระหว่างปฏิบัติงาน - ข้อมูลข่าวสารด้านรักษาความปลอดภัยระบบ - การแจ้งเตือนภัย
ก่อนเลิกงาน **๑๕.๐๐ – ๑๘.๐๐**	ตรวจสอบก่อนเลิกงาน - สำรองข้อมูล - การออกจากระบบอย่างถูกต้อง	ตรวจสอบก่อนเลิกงาน - สำรองข้อมูล

ส่วนที่ 5
ข้อกำหนดการปฏิบัติการศูนย์ปฏิบัติการคอมพิวเตอร์

รายการเครื่องแม่ข่าย

1. Web Sever : IP 203.157.19.1 (www.moph.go.th)
   ระบบปฏิบัติการ Window 2003 Server
2. FTP Sever : IP 203.157.240.58 (ftp.moph.go.th)
   ระบบปฏิบัติการ Linux
3. Mail Sever : IP 203.157.0.1 (webmail.moph.go.th)
   ระบบปฏิบัติการ Linux
4. Pmoc Sever : IP 10.177.2.131 ระบบปฏิบัติการ Window 2003
5. ระบบงานสารบรรณ : IP 203.157.2.5 ระบบปฏิบัติการ Window 2003 Server
6. ICT Server : IP 203.157.19.21 (ict.moph.go.th) ระบบปฏิบัติการ Window 2003

ระดับการปฏิบัติการ

- **การดูแลระบบเครื่องแม่ข่ายและความปลอดภัย**
  1. การติดตั้งและกำหนดค่าระบบ(System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)
  2. การจัดการบริหารบัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ(User Account Management)
  3. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)
- **การดูแลและปฏิบัติการระบบฐานข้อมูล**
  4. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)
  5. ติดตั้งฐานข้อมูล โปรแกรมบริการ / โปรแกรมระบบงานต่างๆ / กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล
- **การปฏิบัติการบริหารความเสี่ยงของระบบสารสนเทศ**
  6. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และการกู้คืนฐานข้อมูล (Database Restore)
  7. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ
  8. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

วิธีดำเนินการ

1. การปฏิบัติการประจำ / การตรวจสอบระบบ หรือการรับทราบ รับแจ้งปัญหาระบบปฏิบัติการ
2. การดำเนินการตามขั้นตอน ระยะเวลา ตามข้อกำหนด
3. การศึกษา / ค้นหาวิธีการปรับปรุงระบบ / ค้นหาปัญหา และวิธีการจัดการ/แก้ไข
4. ดำเนินการแก้ไข / การแจ้งผู้ใช้งาน / การสำรองระบบ
5. บันทึกการปฏิบัติการ (ปรับปรุงแก้ไขระบบ / สำรองข้อมูล) / การแก้ไขปัญหา / การกู้คืน , ระดับปฏิบัติการ และผลสรุปการปฏิบัติการ

ข้อกำหนด เกณฑ์การปฏิบัติการระบบ

การติดตั้งและกำหนดค่าระบบ(System Installation and Configuration) /

1. **การปรับปรุงระบบปฏิบัติการ(Operating System Update)**

- ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ประกอบ
- ติดตั้งระบบปฏิบัติการตรงตามความต้องการใช้งาน
- กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ(System Administrator) และชื่อผู้ใช้(User)
- กำหนดค่าติดตั้ง ชื่อเครื่อง(Computer Name)/ IP Address
- ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)
- ติดตั้งโปรแกรม Antivirus / ปรับปรุง virus definition และการกำหนดค่าการตรวจสอบระบบการสแกน และการปรับปรุงโปรแกรม

2. **การบริหารบัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ(User Account Management)**

- กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ(System Administrator)
- กำหนดชื่อผู้ใช้(User) รหัสผ่าน(Password) และสิทธิการเข้าใช้ระบบ
- บันทึกบัญชีผู้ใช้ และสิทธิการเข้าใช้ระบบ

3. **การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)**

- ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ เช่น Log File หรือตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง
- ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา
- ปรับปรุงโปรแกรม Antivirus และ definition ให้ทันสมัยเป็นประจำทุกสัปดาห์ และทุก Update เฉพาะ
- scan ตรวจหาไวรัสคอมพิวเตอร์

4. **ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)**

- ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้หรือรองรับงานบริการ

- กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นๆ กำหนด
- สร้าง และกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล(Database Admin) ชื่อผู้ใช้อื่นและสิทธิการใช้
- ปรับปรุง / กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

5. ติดตั้งฐานข้อมูล โปรแกรมบริการ / โปรแกรมระบบงานต่าง ๆ / กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

- ติดตั้งโปรแกรมการให้บริการ หรือโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา
- กำหนดค่าระบบ หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมบริการหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ
- ติดตั้งฐานข้อมูลและเชื่อมต่อกับระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด
- แจ้งผู้ใช้ หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อรหัสผ่านและสิทธิการเข้าใช้งานระบบ และฐานข้อมูลตามระบบกำหนด
- ระบุเกณฑ์การสำรอง / สำเนา / ทดสอบกู้คืน(Restore Test)
- บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้แต่ละระดับของระบบทุกครั้งที่มีการสร้าง/ปรับปรุง

6. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และการกู้คืนฐานข้อมูล (Database Restore)

- ตรวจสอบการทำงานโปรแกรมการให้บริการ / โปรแกรมระบบงาน ที่ใช้ฐานข้อมูล
- ตรวจสอบการทำงานของฐานข้อมูลในระบบ Database System และขนาดความจุ ตามระยะเวลาที่กำหนดแต่ละระบบ (ทุกวัน หรือ จันทร์/พุธ/ศุกร์ หรือ รายสัปดาห์)
- ตรวจสอบการทำงานและขนาดของ Device ที่จัดเก็บฐานข้อมูลด้านการทำงานและรองรับบริการได้ปกติหรือไม่
- ทำการสำรองข้อมูล Back up ฐานข้อมูลบันทึกลง สื่อที่กำหนดไว้
- ระบุชื่อ Backup โดยระบุ ชื่อฐานข้อมูล + วันที่ Backup
- ทำการสำเนา Backup ฐานข้อมูลตามระบบกำหนด และส่งให้หน่วยงานจัดเก็บสำเนาที่ระบุ
- ทดสอบการกู้คืนฐานข้อมูลจาก Back up ตามกำหนด
- ปฏิบัติการกู้คืนจาก Backup ล่าสุด ในกรณีมีความเสียหายของระบบฐานข้อมูล

- บันทึกการปฏิบัติการทุกครั้ง ตามชื่อฐานข้อมูล (ชื่อ Backup / Restore Test หรือ การกู้คืน) / ระดับปฏิบัติการ / วันที่ปฏิบัติการ / ปัญหาหรือผลสำเร็จ / ชื่อผู้ปฏิบัติการ / การสำเนาระบบ / Destination Area
- แจ้งผู้ควบคุมกำกับ ผู้รับผิดชอบระบบ และผู้ใช้ระบบฐานข้อมูลถึงความเสียหาย การแก้ไข การกู้คืนและการใช้งาน

7. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

- ตรวจสอบการทำงานส่วนประกอบของเครื่องแม่ข่าย ได้แก่ สถานภาพการทำงานของเครื่อง โดยรวม Harddisk / System Fan / System Led / จอภาพ และอุปกรณ์อื่นๆ
- ทำความสะอาดเครื่อง อุปกรณ์ เป็นระยะ ตามกำหนด
- ตรวจสอบการทำงานของอุปกรณ์สำรองไฟฟ้า หากมีการติดตั้ง
- ตรวจสอบสถานะการทำงาน ประสิทธิภาพของระบบ จาก Device Monitor และ Performance Monitor ของ Operating System ได้แก่ สถานะการทำงานของ CPU / Memory / หน่วย Hard Drive ขนาดความจุที่เหลือ
- แจ้งผลการตรวจสอบ / ปัญหา ให้ผู้บริหารระบบ System Administrator ทราบ
- บันทึกการตรวจสอบ / แก้ไข และการดูแลบำรุงรักษาทุกครั้ง

แบบบันทึกการปฏิบัติการระบบ

เครื่องแม่ข่าย : Server : IP 203.157.19.1 (www.moph.go.th)

: FTP Sever: IP 203.157.240.58 (ftp.moph.go.th)

: Mail Sever : IP 203.157.0.1 (webmail.moph.go.th)

: Pmoc Sever : IP 10.177.2.131 ระบบปฏิบัติการ Window 2003

: IP 203.157.2.5 ระบบปฏิบัติการ Window 2003 Server

: IP 203.157.19.21 (ict.moph.go.th) ระบบปฏิบัติการ Window 2003

( ) : backup รายวัน

( ) : backup รายสัปดาห์

( ) : backup รายเดือน

หน่วยจัดเก็บสำเนา : **ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** (CD Storage)

(Contingency Plan)

มอบหมายผู้ดูแล : ชื่อ นายรังสรรค์ จันทนสมิต System Administrator and Operator

: ชื่อ นายชวลิต ลิ้มปิยินทรากูล System Administrator and Operator

: ชื่อ นางกนกวรรณ มาป้อง System Administrator and Operator

: ชื่อ นายศิวัช ชาวบางงาม System Administrator and Operator

ระดับปฏิบัติการ

1. การติดตั้งและกำหนดค่าระบบ(System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)
2. การบริหารบัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ(User Account Management)
3. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)
4. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)
5. ติดตั้งโปรแกรมให้บริการ / โปรแกรมระบบงานต่างๆ และกำหนดค่าการทำงานของโปรแกรมบริการ
6. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และการกู้คืนฐานข้อมูล (Database Restore)
7. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ

8. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ
9. ปฏิบัติการอื่นๆ

ขั้นตอนการปฏิบัติการระบบฐานข้อมูล

1. ทดสอบการใช้ฐานข้อมูลงานโปรแกรมต่างๆ ที่เรียกใช้ฐานข้อมูล
2. ตรวจสอบสถานะการทำงานของ Database Server และฐานข้อมูล
3. ทำ Back Up ฐานข้อมูลที่อยู่ในเครื่องแม่ข่าย ทุกฐานข้อมูลที่กำหนด จัดเก็บตาม Device ที่เตรียมไว้
4. copy ไฟล์ backup ไปเก็บยังเครื่อง back up server ของตัวเอง
5. ทดสอบ Restore ฐานข้อมูลบนเครื่องแม่ข่ายสำรอง ตามระยะเวลากำหนด
6. ตรวจสอบการทำงานของระบบความปลอดภัย และ การป้องกันไวรัส
7. ตรวจสอบการทำงานของเครื่องแม่ข่ายและอุปกรณ์
8. ดูแล บำรุงรักษา และทำความสะอาดอุปกรณ์

<u>ส่วนที่ 6</u>

การรักษาความปลอดภัยในการเข้าถึงข้อมูล
สำหรับผู้บริหารเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

ผู้บริหารเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข จะได้รับบัญชีผู้ใช้ (User Account) และรหัสผ่าน (Password) สำหรับการเข้าถึงข้อมูลเฉพาะในการบริหาร ตัดสินใจเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศฯ เช่น สถานภาพและประสิทธิภาพของการรักษาความปลอดภัยระบบ ฯ ของศูนย์เทคโนโลยีสารสนเทศฯ การมอบหมายภาระหน้าที่รักษาความปลอดภัยระบบ ฯ ให้แก่บุคลากรที่มีความสามารถ รวมทั้งข้อมูล อื่น ๆ ทั้งหมด ภายในเว็บไซต์กระทรวงสาธารณสุข หรือ http://www.moph.go.th

เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ และผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของศูนย์เทคโนโลยีสารสนเทศฯ จะได้รับบัญชีผู้ใช้ (User Account) และรหัสผ่าน (Password) สำหรับการเข้าถึงข้อมูลเฉพาะในด้านเทคโนโลยีของการรักษาความปลอดภัยระบบ ฯ การแจ้งเตือนภัย การแนะนำแนวทางปฏิบัติ ฯ ซึ่งจะไม่เปิดเผยแก่ผู้ไม่เกี่ยวข้องอื่น ๆ ภายในเว็บไซต์กระทรวงสาธารณสุข หรือ http://www.moph.go.th เพื่อให้การติดต่อประสานด้านการรักษาความปลอดภัยระบบ ฯ ระหว่างศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กับผู้เกี่ยวข้องของหน่วยงานให้เป็นไปอย่างมีประสิทธิภาพและรวดเร็ว

<u>การสร้างรหัสผ่าน (password) ที่แข็งแกร่ง (Strong Password)</u>

๑. มีการผสมกันระหว่าง ตัวอักษร ตัวเลข ตัวอักษรพิเศษ

๒. หลีกเลี่ยงการตั้งรหัสผ่านตามชื่อคน ชื่อเล่น นามแฝง หรือ คำอื่น ๆ เกี่ยวกับตัวท่านที่เป็นที่ทราบกันโดยทั่วไป เช่น ชื่อสมาชิกใน ครอบครัว ชื่อคนรัก ชื่อสัตว์เลี้ยงที่โปรดปราน สถานที่ทำงาน ฯลฯ หรือการใช้คำศัพท์ตามพจนานุกรม สมุดโทรศัพท์ วันเดือนปีเกิด

๓. ตั้งคำหรือวลีเป็นรหัสผ่านที่จดจำได้ง่ายสำหรับท่านแต่คาดเดาได้ยากสำหรับผู้อื่น

๔. มีขนาด ๖ ถึง ๘ ตัวอักษร หรือมากกว่า

<u>การใช้งานรหัสผ่าน (password) อย่างปลอดภัย</u>

๑. รหัสผ่านมีเพียงผู้เป็นเจ้าของเท่านั้นที่จะทราบได้ เมื่อได้รับรหัสผ่านชั่วคราวจากผู้ดูแลระบบ ฯ (กรณีนี้คือ ผู้ดูแลเว็บไซต์ http://www.moph.go.th) ทั้งนี้รวมถึงรหัสชั่วคราวจากบริษัทผู้ผลิตฮาร์ดแวร์หรือซอฟต์แวร์เพื่อเข้าใช้ระบบเป็นครั้งแรก ให้รีบเปลี่ยนรหัสผ่านใหม่ด้วยตนเองภายใน ๓ วัน

๒. จดจำรหัสผ่านแทนการเขียนบันทึก หากเจ้าของรหัสผ่านลืมรหัสผ่าน หรือต้องการแก้ไขให้เจ้าของรหัสผ่านแจ้งผู้ดูแลระบบ ฯ ให้ดำเนินการ

๓. เปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด หรือตามความเหมาะสม สำหรับระบบที่มีความสำคัญมาก และไม่ควรนำรหัสผ่านที่เคยใช้กลับมาใช้ใหม่ภายใน ๑ ปี

๔. ขณะใช้รหัสผ่านต้องระมัดระวังมิให้ผู้อื่นล่วงรู้ได้

<u>สิ่งที่ไม่ควรปฏิบัติ</u>

๑. ไม่โอนสิทธิ์หรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน เจ้าของรหัสผ่านต้องไม่เปิดเผยรหัสผ่านให้แก่ผู้ใดทั้งสิ้น (รวมถึงผู้ดูแลระบบ ฯ) ยกเว้นกรณีจำเป็น เช่น ได้รับการขอร้องจากผู้ดูแลระบบ ฯ และต้องกระทำอย่างปลอดภัย เช่น ไม่ส่งรหัสผ่านทางโทรศัพท์ หรือ การจดบันทึก หรือผ่านบุคคลที่สาม เมื่อเสร็จสิ้นความจำเป็นนั้นแล้วให้ยกเลิกรหัสผ่านนั้นโดยการเปลี่ยนรหัสผ่านใหม่ด้วยตัวเองทันที

๒. ไม่สร้างรหัสผ่านเดียวกันสำหรับเข้าถึงระบบสารสนเทศมากกว่า ๑ ระบบ

๓. ไม่ใช้รหัสผ่านร่วมกับผู้อื่นโดยเด็ดขาด แม้ว่าจะเป็นผู้ร่วมงานที่ต้องใช้แฟ้มข้อมูลเดียวกัน ทุกคนที่ได้รับอนุญาตจะต้องมีรหัสผ่านเป็นของตนเองในการเข้าใช้ข้อมูลดังกล่าว

ภาคผนวก

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Server : IP 203.157.19.1 (www.moph.go.th)

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นายชวลิต ลิ้มปิยินทรางกูล
2.		Reserve Admin	นางสาวสุวันต์นา เสมอเนตร
3.		Reserve Admin	นายรังสรรค์ จันทนสมิต
4.		System Operator	นางสาวนภาพร
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Pmoc Sever : IP 10.177.2.131 ระบบปฏิบัติการ Window 2003

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นายชวลิต ลิ้มปิยินทรางกูล
2.		Reserve Admin	นายบุญชัย ฉัตรวิรุฬพันธ์
3.		Reserve Admin	นางสาวสุวันต์นา เสมอเนตร
4.		System Operator	นายรังสรรค์ จันทนสมิต
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Mail Sever : IP 203.157.0.1 (webmail.moph.go.th)

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นายชวลิต ลิ้มปิยินทรางกูล
2.		Reserve Admin	นายบุญชัย ฉัตรวิรุฬพันธ์
3.		Reserve Admin	นายรังสรรค์ จันทนสมิต
4.		System Operator	นายสุเทพ แก่นจันทร์ นางสุรีย์ กฤษณายุทธ
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Server : IP 203.157.0.58 (FTP)

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นายชวลิต ลิ้มปิยินทรางกูล
2.		Reserve Admin	นายรังสรรค์ จันทนสมิต
3.		Reserve Admin	นายบุญชัย ฉัตรวิรุฬพันธ์
4.		System Operator	นางสาวสุวันต์นา เสมอเนตร
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Server : IP 203.157.2.5 (ระบบงานสารบรรณ)

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นางกนกวรรณ มาป้อง
2.		Reserve Admin	นายดุลยวัฒน์ มาป้อง
3.		Reserve Admin	นางทิพวรรณ ยงศิริวิทย์
4.		System Operator	นางกนกวรรณ มาป้อง
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

แบบบันทึกการปฏิบัติงาน

บัญชีรายชื่อผู้ดูแล / ผู้ใช้ระบบ เครื่องแม่ข่าย (User Account)

: Server : IP 203.157.19.21 (ict.moph.go.th)

ลำดับที่	User Name	สิทธิการเข้าถึง	ชื่อผู้ใช้สิทธิ
1.	Administrator	System Admin All Access	นายศิวัช ชาวบางงาม
2.		Reserve Admin	นายศิวัช ชาวบางงาม
3.		Reserve Admin	นายศิวัช ชาวบางงาม
4.		System Operator	นายศิวัช ชาวบางงาม
5.		user (Read Only)	ผู้ใช้ทั่วไป
6.		user	ผู้ใช้ระบบทั่วไป

เอกสารมอบหมายงาน

ผู้รับผิดชอบหน้าที่ดูแลระบบปฏิบัติการคอมพิวเตอร์แม่ข่าย

ชื่อผู้รับมอบหมายงาน นายชวลิต ลิ้มปิยินทรางกูล

ตำแหน่ง เจ้าหน้าที่เครื่องคอมพิวเตอร์ 6

สังกัด สำนักงานปลัดกระทรวงสาธารณสุข

ได้รับมอบหมายให้ปฏิบัติหน้าที่ ปฏิบัติการระบบคอมพิวเตอร์แม่ข่าย อินเตอร์เน็ต

ตั้งแต่ วันที่ 1 ตุลาคม 2549 ถึง 30 กันยายน 2550

มอบหมายให้ปฏิบัติงาน ดังนี้

ภารกิจ/ ปฏิบัติการ /กิจกรรม	เป้าหมายที่ต้องการ
1. การติดตั้งและกำหนดค่าระบบ (System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)	ระบบปฏิบัติการ(Operating System) ให้บริการได้มีประสิทธิภาพและทันสมัย
2. จัดการและบริหาร บัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ (User Account Management)	มีการกำหนดสิทธิผู้เข้าใช้งานระบบงานตามที่กำหนด
3. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)	เครื่องแม่ข่ายมีระบบความปลอดภัยที่ทันสมัย
4. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)	ระบบจัดการฐานข้อมูลสามารถให้บริการอย่างถูกต้อง
5. ติดตั้งฐานข้อมูล กำหนดสิทธิผู้ใช้ เชื่อมต่อโปรแกรมให้บริการและกำหนดค่าการทำงานของโปรแกรมบริการ	โปรแกรมระบบงานที่ต้องการสามารถให้ทำงานได้ถูกต้อง
6. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และ การกู้คืนฐานข้อมูล (Database Restore)	ฐานข้อมูล มีการสำรอง / สำเนา และ การกู้คืนอย่างถูกต้อง
7. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ	มีการสำรองหรือสำเนาระบบตามกำหนด
8. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ	เครื่องแม่ข่ายทำงานได้ถูกต้อง
9. การ Backup ข้ามเครือข่ายกับกรมอนามัย	มีฐานข้อมูลที่ได้รับการสำรองอย่างถูกต้อง เก็บไว้เพื่อป้องกันปัญหาจากภัยพิบัติและอัคคีภัย

ผู้รับมอบหมาย....บุญชัย ฉัตรพิรุฬห์พันธุ์

(นายบุญชัย ฉัตรพิรุฬห์พันธุ์)

ประธานคณะกรรมการรักษาความมั่นคงปลอดภัย

ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ผู้รับมอบหมาย....ชวลิต ลิ้มปิยินทรางกูล

(นายชวลิต ลิ้มปิยินทรางกูล)

เจ้าหน้าที่เครื่องคอมพิวเตอร์ 6

เอกสารมอบหมายงาน

ผู้รับผิดชอบหน้าที่ดูแลระบบปฏิบัติการคอมพิวเตอร์แม่ข่าย

ชื่อผู้รับมอบหมายงาน นายรังสรรค์ จันทนสมิต

ตำแหน่ง นักวิชาการคอมพิวเตอร์7

สังกัด สำนักงานปลัดกระทรวงสาธารณสุข

ได้รับมอบหมายให้ปฏิบัติหน้าที่ ปฏิบัติการระบบคอมพิวเตอร์แม่ข่าย

ตั้งแต่ วันที่ 1 ตุลาคม 2549 ถึง 30 กันยายน 2550

มอบหมายให้ปฏิบัติงาน ดังนี้

ภารกิจ/ ปฏิบัติการ /กิจกรรม	เป้าหมายที่ต้องการ
10. การติดตั้งและกำหนดค่าระบบ (System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)	ระบบปฏิบัติการ(Operating System) ให้บริการได้มีประสิทธิภาพและทันสมัย
11. จัดการและบริหาร บัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ (User Account Management)	มีการกำหนดสิทธิผู้เข้าใช้งานระบบงานตามที่กำหนด
12. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)	เครื่องแม่ข่ายมีระบบความปลอดภัยที่ทันสมัย
13. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)	ระบบจัดการฐานข้อมูลสามารถให้บริการอย่างถูกต้อง
14. ติดตั้งฐานข้อมูล กำหนดสิทธิผู้ใช้ เชื่อมต่อโปรแกรมให้บริการและกำหนดค่าการทำงานของโปรแกรมบริการ	โปรแกรมระบบงานที่ต้องการสามารถให้ทำงานได้ถูกต้อง
15. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และ การกู้คืนฐานข้อมูล (Database Restore)	ฐานข้อมูล มีการสำรอง / สำเนา และ การกู้คืนอย่างถูกต้อง
16. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ	มีการสำรองหรือสำเนาระบบตามกำหนด
17. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ	เครื่องแม่ข่ายทำงานได้ถูกต้อง
18. การ Backup ข้ามเครือข่ายกับกรมอนามัย	มีฐานข้อมูลที่ได้รับการสำรองอย่างถูกต้อง เก็บไว้เพื่อป้องกันปัญหาจากภัยพิบัติและอัคคีภัย

ผู้รับมอบหมาย....บุญชัย ฉัตรพิรุฬห์พันธุ์

(นายบุญชัย ฉัตรพิรุฬห์พันธุ์)

ประธานคณะกรรมการรักษาความมั่นคงปลอดภัย

ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ผู้รับมอบหมาย....รังสรรค์ จันทนสมิต

(นายรังสรรค์ จันทนสมิต)

นักวิชาการคอมพิวเตอร์7

เอกสารมอบหมายงาน

ผู้รับผิดชอบหน้าที่ดูแลระบบปฏิบัติการคอมพิวเตอร์แม่ข่าย

ชื่อผู้รับมอบหมายงาน นางกนกวรรณ มาป้อง

ตำแหน่ง เนักวิชาการคอมพิวเตอร์7

สังกัด สำนักงานปลัดกระทรวงสาธารณสุข

ได้รับมอบหมายให้ปฏิบัติหน้าที่ ปฏิบัติการระบบคอมพิวเตอร์แม่ข่าย อินเตอร์เน็ต

ตั้งแต่ วันที่ 1 ตุลาคม 2549 ถึง 30 กันยายน 2550

มอบหมายให้ปฏิบัติงาน ดังนี้

ภารกิจ/ ปฏิบัติการ /กิจกรรม	เป้าหมายที่ต้องการ
19. การติดตั้งและกำหนดค่าระบบ (System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)	ระบบปฏิบัติการ(Operating System) ให้บริการได้มีประสิทธิภาพและทันสมัย
20. จัดการและบริหาร บัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ (User Account Management)	มีการกำหนดสิทธิผู้เข้าใช้งานระบบงานตามที่กำหนด
21. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)	เครื่องแม่ข่ายมีระบบความปลอดภัยที่ทันสมัย
22. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)	ระบบจัดการฐานข้อมูลสามารถให้บริการอย่างถูกต้อง
23. ติดตั้งฐานข้อมูล กำหนดสิทธิผู้ใช้ เชื่อมต่อโปรแกรมให้บริการและกำหนดค่าการทำงานของโปรแกรมบริการ	โปรแกรมระบบงานที่ต้องการสามารถให้ทำงานได้ถูกต้อง
24. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และ การกู้คืนฐานข้อมูล (Database Restore)	ฐานข้อมูล มีการสำรอง / สำเนา และ การกู้คืนอย่างถูกต้อง
25. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ	มีการสำรองหรือสำเนาระบบตามกำหนด
26. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ	เครื่องแม่ข่ายทำงานได้ถูกต้อง
27. การ Backup ข้ามเครือข่ายกับกรมอนามัย	มีฐานข้อมูลที่ได้รับการสำรองอย่างถูกต้อง เก็บไว้เพื่อป้องกันปัญหาจากภัยพิบัติและอัคคีภัย

ผู้รับมอบหมาย....บุญชัย ฉัตรพิรุฬห์พันธุ์

(นายบุญชัย ฉัตรพิรุฬห์พันธุ์)

ประธานคณะกรรมการรักษาความมั่นคงปลอดภัย

ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ผู้รับมอบหมาย....กนกวรรณ มาป้อง

(นางกนกวรรณ มาป้อง)

นักวิชาการคอมพิวเตอร์7

เอกสารมอบหมายงาน

ผู้รับผิดชอบหน้าที่ดูแลระบบปฏิบัติการคอมพิวเตอร์แม่ข่าย

ชื่อผู้รับมอบหมายงาน นายศิวัช ชาวบางงาม

ตำแหน่ง นักวิชาการคอมพิวเตอร์7

สังกัด สำนักงานปลัดกระทรวงสาธารณสุข

ได้รับมอบหมายให้ปฏิบัติหน้าที่ ปฏิบัติการระบบคอมพิวเตอร์แม่ข่าย

ตั้งแต่ วันที่ 1 ตุลาคม 2549 ถึง 30 กันยายน 2550

มอบหมายให้ปฏิบัติงาน ดังนี้

ภารกิจ/ ปฏิบัติการ /กิจกรรม	เป้าหมายที่ต้องการ
28. การติดตั้งและกำหนดค่าระบบ (System Installation and Configuration) / การปรับปรุงระบบปฏิบัติการ(Operating System Update)	ระบบปฏิบัติการ(Operating System) ให้บริการได้มีประสิทธิภาพและทันสมัย
29. จัดการและบริหาร บัญชีผู้ใช้ / สิทธิการเข้าถึงและใช้งานระบบ (User Account Management)	มีการกำหนดสิทธิผู้เข้าใช้งานระบบงานตามที่กำหนด
30. การปรับปรุงการรักษาความปลอดภัย / Antivirus (System Security & Antivirus Update)	เครื่องแม่ข่ายมีระบบความปลอดภัยที่ทันสมัย
31. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)	ระบบจัดการฐานข้อมูลสามารถให้บริการอย่างถูกต้อง
32. ติดตั้งฐานข้อมูล กำหนดสิทธิผู้ใช้ เชื่อมต่อโปรแกรมให้บริการและกำหนดค่าการทำงานของโปรแกรมบริการ	โปรแกรมระบบงานที่ต้องการสามารถให้ทำงานได้ถูกต้อง
33. ปฏิบัติการระบบฐานข้อมูล การสำรอง / สำเนาฐานข้อมูล (Database Backup) และ การกู้คืนฐานข้อมูล (Database Restore)	ฐานข้อมูล มีการสำรอง / สำเนา และ การกู้คืนอย่างถูกต้อง
34. ปฏิบัติการสำรองหรือสำเนาระบบปฏิบัติการ และโปรแกรมระบบบริการ	มีการสำรองหรือสำเนาระบบตามกำหนด
35. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ	เครื่องแม่ข่ายทำงานได้ถูกต้อง
36. การ Backup ข้ามเครือข่ายกับกรมอนามัย	มีฐานข้อมูลที่ได้รับการสำรองอย่างถูกต้อง เก็บไว้เพื่อป้องกันปัญหาจากภัยพิบัติและอัคคีภัย

ผู้รับมอบหมาย....บุญชัย ฉัตรพิรุฬห์พันธุ์

(นายบุญชัย ฉัตรพิรุฬห์พันธุ์)

ประธานคณะกรรมการรักษาความมั่นคงปลอดภัย

ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

ผู้รับมอบหมาย....ศิวัช ชาวบางงาม

(นายศิวัช ชาวบางงาม)

นักวิชาการคอมพิวเตอร์7

ชื่ออุปกรณ์	หมายเลขประจำอุปกรณ์หรือ IP Address	วิธีการตรวจสอบ	บุคคล/หน่วยงานที่รับผิดชอบในการตรวจสอบ
- **อุปกรณ์เครือข่าย** - Switch Router (Core) - Firewall/Packet shaper - DNS/Proxy	Server : IP 203.157.19.1 Sever: IP 203.157.240.58 : Mail Sever: IP 203.157.0.1 : Pmoc Sever : Sever ระบบสารบรรณ : ict server	**1.การปรับปรุงระบบปฏิบัติการ(Operating System Update)** ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ประกอบ	นายชวลิต ลิ้มปิยินทรางกูล นายรังสรรค์ จันทนสมิต นางกนกวรรณ มาป้อง นายศิวัช ชาวบางงาม
		2. การติดตั้งและกำหนดค่าระบบ(System Installation and Configuration) /	
		3. กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ(System Administrator) และชื่อผู้ใช้(User)	
		4. กำหนดค่าติดตั้ง ชื่อเครื่อง(Computer Name)/ IP Address	
		5. ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)	
		6. ติดตั้งโปรแกรม Antivirus / ปรับปรุง virus definition และการกำหนดค่าการตรวจสอบระบบ การสแกน และการปรับปรุงโปรแกรม	
		7. ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา	
		8. ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ เช่น Log File หรือ ตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง	

ชื่ออุปกรณ์	หมายเลขประจำอุปกรณ์หรือ IP Address	วิธีการตรวจสอบ	บุคคล/หน่วยงานที่รับผิดชอบในการตรวจสอบ
		9. ปรับปรุงโปรแกรม Antivirus และ definition ให้ทันสมัยเป็นประจำทุกสัปดาห์ และทุกเดือน Update และscanตรวจหาไวรัสคอมพิวเตอร์	
Server **ได้แก่** Web Server **จำนวน** 5 **เครื่อง**	http://203.157.19.1	**1.การปรับปรุงระบบปฏิบัติการ**(Operating System Update) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ประกอบ	นายรังสรรค์ จันทนสมิต นายชวลิต ลิ้มปิยทรากูล
		2. **การติดตั้งและกำหนดค่าระบบ**(System Installation and Configuration)	
		3. กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ(System Administrator) และชื่อผู้ใช้(User)	
		4. กำหนดค่าติดตั้ง ชื่อเครื่อง(Computer Name)/ IP Address	
		5. ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)	

ชื่ออุปกรณ์	หมายเลขประจำอุปกรณ์หรือ IP Address	วิธีการตรวจสอบ	บุคคล/หน่วยงานที่รับผิดชอบในการตรวจสอบ
		6. ติดตั้งโปรแกรม Antivirus / ปรับปรุง virus definition และการกำหนดค่าการตรวจสอบระบบ การสแกน และการปรับปรุงโปรแกรม	
		7. ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา	
		8. ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ เช่น Log File หรือ ตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง	
		9. ปรับปรุงโปรแกรม Antivirus และ definition ให้ทันสมัยเป็นประจำทุกสัปดาห์ และทุกเดือน Update และscan ตรวจหาไวรัสคอมพิวเตอร์	

ชื่ออุปกรณ์	หมายเลขประจำอุปกรณ์หรือ IP Address	ช่องโหว่ที่ตรวจพบ
-Firewall ยี่ห้อ Fortigate-3000		โดยตรวจสอบที่ http://www.zone-h.org/en/defacements/filter/filter_domain =.moph.go.th/ ***ตัวอย่าง Server ที่ถูกโจมตี ได้แก่*** pr.anamai.moph.go.th Win 2000 medi.moph.go.th Linux amno.moph.go.th Win 2000 ssko.moph.go.th Linux dpc7.ddc.moph.go.th Linux mail.phayao.moph.go.th Linux
Web server	http://203.157.19.1	ไม่พบช่องโหว่

แนวทางในการจัดการกับช่องโหว่ที่ตรวจพบ	ผู้รับผิดชอบ
1. ติดตั้งโปรแกรมอุดช่องโหว่ในเว็บบราวเซอร์ของกระทรวงสาธารณสุข เพื่อให้บราวเซอร์มีความปลอดภัย	เจ้าหน้าที่บริษัท
2. ใช้ไฟร์วอลล์ทำงานโดยทำการตรวจสอบข้อมูลทั้งหมด (ไวรัส โทรจัน สปายแวร์) ที่เข้าหรือออกจากระบบเครือข่ายกระทรวงสาธารณสุข	เจ้าหน้าที่บริษัท
3. การเฝ้าดูการใช้งานอินเทอร์เน็ตโดยใช้ Web caching เพื่อดูความเคลื่อนไหวของการจราจรในระบบเครือข่าย	เจ้าหน้าที่บริษัท
4. ปรับปรุงซอฟต์แวร์ในการบริหารจัดการความปลอดภัยของระบบเครือข่าย	เจ้าหน้าที่บริษัท
5. ป้องกันไม่ให้ไวรัสเข้ามาในระบบคอมพิวเตอร์	เจ้าหน้าที่บริษัท
6. ไม่เปิดเผยรหัสผ่านในการเข้าเว็บไซต์ให้กับบุคคลหนึ่งบุคคลใดทราบ	เจ้าหน้าที่บริษัท
7. ใช้โปรแกรมเพื่อควบคุมหรือกำจัดคุกกี้ที่ไม่พึงประสงค์(ดาวน์โหลดได้จากเว็บ www.cookiecentral.com และ www.lavasoft.de)	นายรังสรรค์ จันทนสมิต,เจ้าหน้าที่บริษัท