เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศ โรงพยาบาลศรีนคร พ.ศ. 2566

คำนำ

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่องและจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่าย นอกจากนั้นยังต้องมีการตรวจสอบอย่างสม่ำเสมอ เพื่อปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อให้ระบบสารสนเทศของโรงพยาบาลศรีนครเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้มีการถูกคุกคามจากภัยต่าง ๆ โรงพยาบาลศรีนครจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเผยแพร่ให้ข้าราชการ เจ้าหน้าที่บุคลากรทุกระดับได้รับทราบ และขอความร่วมมือให้ปฏิบัติตามอย่างเคร่งครัดต่อไป

สารบัญ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์และขอบเขต

เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลศรีนครเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถด าเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และภัยคุกคามต่างๆ โรงพยาบาลศรีนครจึงเห็นสมควรกำหนด นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกากำหนด หลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ในมาตรา 5 “หน่วยงานของรัฐ ต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและ เชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลศรีนครประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอน วิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งข้าราชการ เจ้าหน้าที่ บุคลากร ของโรงพยาบาลศรีนคร และบุคคลภายนอกที่ปฏิบัติงานร่วมกับโรงพยาบาลศรีนคร จะต้องปฏิบัติตามอย่างเคร่งครัด

กำหนดวัตถุประสงค์ในการจัดทำนโยบายและแนวปฏิบัติฯ ไว้ดังนี้

1) เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีนครให้เป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

2) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนครอ้างอิงตามมาตรฐาน ISO/IEC27001 และมีการปรับปรุงอย่างต่อเนื่อง

3) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร ข้าราชการ เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานร่วมกับโรงพยาบาลศรีนครตระหนักถึงความสำคัญของการรักษา ความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนครในการดำเนินงานและถือปฏิบัติตามอย่างเคร่งครัด

4) เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

5) เพื่อเผยแพร่และส่งเสริมให้กับข้าราชการ เจ้าหน้าที่ บุคลากรทุกระดับ ในโรงพยาบาลศรีนคร มีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และถือปฏิบัติอย่างเคร่งครัด

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 1 นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

1) การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)
2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
3) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
4) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
5) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
6) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
7) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control
8) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
9) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
10) การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)
11) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา
12) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
13) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)
14) การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)
15) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
16) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ส่วนที่ 2 นโยบายระบบสารสนเทศและระบบส ารองของสารสนเทศ
1) การสำรองข้อมูลและระบบคอมพิวเตอร์
2) การกู้คืนระบบ
3) การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายโรงพยาบาลศรีนคร
4) การบริหารจัดการการเข้าถึงระบบเครือข่าย
5) การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย
6) การบริหารจัดการการบันทึกและตรวจสอบ
7) การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศ
8) การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก
9) การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)
10) ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 3 แผนเตรียมความพร้อมกรณีฉุกเฉิน
ส่วนที่ 4 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
ส่วนที่ 5 นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

3. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลศรีนครว่าด้วยคำนิยาม

1. โรงพยาบาล	โรงพยาบาลศรีนคร
2. หน่วยงาน	ประกันสุขภาพยุทธศาสตร์และเทคโนโลยีสารสนเทศทางการแพทย์
3. งานเทคโนโลยีสารสนเทศ	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษาพัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบโรงพยาบาล และเครือข่ายภายในโรงพยาบาลศรีนคร

4. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Secueity)	การรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
5. ผู้ใช้งาน	บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลศรีนครโดยมีสิทธิ์ และหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของโรงพยาบาลศรีนครได้ ได้แก่ ผู้บริหาร หมายถึง ผู้อำนวยการโรงพยาบาลศรีนคร หัวหน้างาน ผู้ดูแลระบบ (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจาก ผู้บริหารให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และ ระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการ ฐานข้อมูลของเครือข่ายคอมพิวเตอร์ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง ชั่วคราว ลูกจ้างประจำ/จ้างเหมา บุคคลภายนอก หมายถึง เจ้าหน้าที่จากหน่วยงานภายนอกที่ปฏิบัติการร่วมกับโรงพยาบาลศรีนคร
6. ผู้มีสิทธิใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลศรีนคร
7. สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับโรงพยาบาล ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ได้แก่ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์
8. การเข้าถึงหรือการอนุญาตควบคุมการใช้งานสารสนเทศ	การกำหนดสิทธิหรือมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศโดยที่เจ้าของข้อมูลอนุญาตให้ใช้งานระบบสารสนเทศนั้นได้
9. เจ้าของข้อมูล	ผู้ได้รับมอบหมายจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. หน่วยงานภายนอก	องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของโรงพยาบาล โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
11. ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูล อิเล็กทรอนิกส์

	ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
12. สารสนเทศ	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การตัดสินใจ
13. ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่เป็นแนวทางให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
14. ระบบเทคโนโลยีสารสนเทศ	ระบบงานของโรงพยาบาลที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่โงพยาบาลสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนาและการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ
15. ระบบเครือข่าย	ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของโรงพยาบาลได้ ได้แก่ ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)
16. ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet)	เครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
17. ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงาน เข้ากับเครือข่ายอินเทอร์เน็ตสากล
18. จดหมาอิเล็กทรอนิกส์ (e-Mail)	ระบบที่บุคคลใช้ในการรับส่งข้อมูลระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ ผ่านโพรโตคอล SMTP POP3 IMAP Exchange
19. สื่อบันทึกพกพา (Portable Media)	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD, DVD, FlashDrive, External Hard Disk
20. ชื่อผู้ใช้ (Username)	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
21. รหัสผ่าน (Password)	ชุดของตัวอักษร หรืออักขระ หรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
22. การเข้ารหัสลับ (Encryption)	การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้ จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้ งานได้ตามปกติ
23. อุปกรณ์จัดเส้นทาง (Router)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
24. การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
25. SSID (Service SetIdentifier)	ชื่อระบุเครือข่ายไร้สาย
26. WPA (Wi-Fi Protected Access)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย

27. MAC Address (Media Access Control Address)	หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่าน ข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
28. VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
29. แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของโรงพยาบาล
30. มาตรฐาน (Standard)	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย
31. วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
32. แนวทางปฏิบัติ (Guideline)	แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
33. ชุดคำสั่งไม่พึงประสงค์	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือ ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
34. สถานการณ์ความเสี่ยง	ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล สามารถแยกเป็นภัยต่าง ๆ ได้ 4 ประเภท ได้แก่ -ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) -ภัยที่เกิด Software -ภัยจากไฟไหม้หรือระบบไฟฟ้า -ภัยจากน้ำท่วม (อุทกภัย)
35. สถานการณ์ด้านความมั่นคง พึงประสงค์หรือไม่อาจคาดคิด	สถานการณ์หรือเหตุการณ์ ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศเปิดเผย เปลี่ยนแปลง ทำลาย ปฏิเสธ การทำงานหรือการกระทำอื่น ๆ
36. เหตุการณ์ด้านความปลอดภัย	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
37. สื่อสังคมออนไลน์ (Social Network)	สื่อหรือช่องทางในการติดต่อในลักษณะของการสื่อสารแบบสองทางผ่านระบบเครือข่ายอินเทอร์เน็ต เป็นสื่อรูปแบบใหม่ (New Media) ที่บุคคลทั่วไปสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่างๆ

ส่วนที่ 1
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

มาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการควบคุมบุคคลที่ ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล และป้องกันการบุกรุกผ่าน ระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนครได้อย่างถูกต้อง

วัตถุประสงค์

1) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของโรงพยาบาลศรีนคร

2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับโรงพยาบาลศรีนคร ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1) ศูนย์เทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) เจ้าหน้าที่ที่ได้รับมอบหมาย

4) ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวทางปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

1.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ

การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ให้ผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง มีดังนี้

1) สิทธิ์อ่านอย่างเดียว

2) สิทธิ์การเพิ่มข้อมูล

3) สิทธิ์การแก้ไขข้อมูล

4) สิทธิ์การลบข้อมูล

5) สิทธิ์การอนุมัติ/อนุญาต

6)ไม่มีสิทธิ

1.2 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

1) การจัดแบ่งประเภทของข้อมูลออกเป็น

(1) ข้อมูลที่เปิดเผยได้ทั่วไป

(2) ข้อมูลที่เปิดเผยเฉพาะที่มีการจำกัดการเข้าถึง ได้แก่ ข้อมูลเชิงบริหาร ข้อมูลส่วนบุคคล

2) การจัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 4 ระดับ คือ

(1) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(2) ข้อมูลที่มีระดับความสำคัญมาก

(3) ข้อมูลที่มีระดับความสำคัญปานกลาง

(4) ข้อมูลที่มีระดับความสำคัญน้อย

การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูล ด้วยวิธีการประเมินผลกระทบ ของปัญหา คุณภาพข้อมูลที่มีต่อองค์กร ซึ่งฐานข้อมูลแต่ละระบบจะมีความสำคัญต่อกระบวนการทำงานไม่เท่ากัน หากข้อมูลใดมีปัญหาไม่สมบูรณ์จะมีผลกระทบต่อกระบวนการทำงานหลักมาก ทำให้หน่วยงานไม่สามารถดำเนินงานที่สำคัญได้ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูล มีดังนี้

(1) พิจารณาจากวิธีการเชื่อมโยงข้อมูล โดยเปรียบเทียบประโยชน์และความเป็นไปได้

(2) พิจารณาจากความพยายามที่จะเชื่อมโยงข้อมูล

(3) พิจารณาว่าข้อมูลรายการนั้นมีผลกระทบต่อกระบวนการทำงานโดยรวมเนื่องจากเป็นข้อมูล ที่ใช้ร่วมกันในกระบวนการทำงานหลายๆ อย่าง หากผลกระทบโดยรวมดังกล่าว ทำให้การทำงานใดงานหนึ่ง ถึงขั้นล้มเหลวย่อมถือว่าสำคัญมาก

(4) พิจารณาจากความยากง่ายของการได้มาของข้อมูลแต่ละรายการ ซึ่งอาจขึ้นอยู่กับปัจจัยหลายประการ เช่น ความพร้อมของหน่วยงานเจ้าของข้อมูล การทำสัญญาข้อตกลงระหว่างหน่วยงานในการขอใช้ข้อมูล งบประมาณสนับสนุนค่าใช้จ่ายที่จะเกิดขึ้นในการเชื่อมโยงระบบข้อมูล

(5) สรุปผลการพิจารณา จากขั้นตอนที่ 1-4 เพื่อหาลำดับความสำคัญของข้อมูลแต่ละรายการ

ตัวอย่างการจัดลำดับความสำคัญของฐานข้อมูล

ข้อมูล	แนวทางในการเชื่อมโยงข้อมูล (ก)	ความพยายามที่ต้องใช้ในการเชื่อมโยงข้อมูล (ข)	ผลกระทบของข้อมูลที่มีปัญหาต่อกระบวนการทำงาน การบริหารจัดการ (ค)	ความยาก/ง่ายในการได้ข้อมูล (ง)	สรุปผลการพิจารณา (ก+ข+ค+ง)
ฐานข้อมูล	3	3	3	2	11 (A)
ฐานข้อมูล	2	2	4	2	10 (B)

ผลกระทบของข้อมูลที่มีปัญหาต่อกระบวนการทำงานของหน่วยงาน

4 = ขั้นตอน/กระบวนการท างานล้มเหลวโดยสิ้นเชิง หรือมีแนวโน้มเกิดความเสี่ยงทางการเงิน หรือการปฏิบัติตามกฎระเบียบต่างๆ

3 = ขั้นตอนการทำงานติดขัด และมีผลต่อสถานภาพองค์กร เช่น ด้านเศรษฐกิจ สังคม

2 = มีผลต่อสถานภาพองค์กรเล็กน้อย

1 = ไม่สำคัญ มีผลต่อสถานภาพองค์กรน้อยที่สุด

ระดับความยากง่ายในการได้มาของข้อมูล

1 = ง่าย 2 = ปานกลาง 3 = ยาก

ระดับความพยายามในการเชื่อมโยงข้อมูล

1 = ต่ า 2 = ปานกลาง 3 = สูง

แนวทางในการเชื่อมโยงข้อมูล

1 = ไม่มีการเชื่อมโยง/มีน้อยมาก 2 = การขอโอนไฟล์ข้อมูลเป็นครั้งคราว 3 = การเชื่อมโยงออนไลน์

สรุปผลการจัดลำดับคะแนน

4 คะแนน = ความสำคัญน้อย D

5-7 คะแนน = ความสำคัญปานกลาง C

8-10 คะแนน = ความสำคัญมาก B

11-13 คะแนน = ความสำคัญมากที่สุด A

3) การจัดแบ่งลำดับชั้นความลับของข้อมูล

(1) ข้อมูลลับที่สุดหากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียงหายอย่างร้ายแรงที่สุด

(2) ข้อมูลลับมากหากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(3) ข้อมูลลับหากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียหาย

(4) ข้อมูลทั่วไปข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

การกำหนดชั้นความลับ ให้พิจารณาจากความสำคัญของเนื้อหา แหล่งที่มาของข้อมูล วิธีการนำไปใช้ ประโยชน์ จำนวนบุคคลที่ควรรับทราบผลกระทบหากมีการเปิดเผย และหน่วยงานที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ ทั้งนี้ให้มีการจัดทำข้อตกลงการรักษาความลับที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่จะเปิดเผยได้เฉพาะบุคคล เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลแล้วเท่านั้น

4) การจัดแบ่งระดับชั้นการเข้าถึง โดยแบ่งสิทธิการเข้าถึงตามประเภทของข้อมูล

(1) ประเภทของข้อมูลทั่วไป ก าหนดสิทธิให้สามารถเข้าถึงข้อมูลได้ทุกคน

(2) ประเภทของข้อมูลที่ต้องก าหนดสิทธิการเข้าถึง มีระดับการเข้าถึงดังนี้

[1] ระดับผู้ปฏิบัติงาน

[2] ระดับผู้ตรวจสอบข้อมูล

[3] ระดับผู้ลงนามรับรองผล/อนุมัติ

[4] ระดับการเข้าถึงรายงานสรุปผล

[5] ระดับผู้ดูแลระบบระดับหน่วยงาน

[6] ระดับผู้ดูแลระบบย่อย ตามคำสั่งหน่วยงานผู้รับผิดชอบข้อมูล

[7] ระดับผู้ดูแลระบบสูงสุด

กรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ ดังนี้

[1] Server เก็บ LOG ระยะเวลาตามกฎหมาย

[2] ระบบที่มีความสำคัญ มีการเก็บประวัติการเข้าใช้งาน

5) การกำหนดเวลาที่ได้เข้าถึงระบบสารสนเทศ ดังนี้

(1) ระบบงานบริการ (Front Office) ส าหรับผู้ใช้งานทั่วไป เข้าถึงได้ตลอดเวลา

(2) ระบบงานภายใน (Back Office) ส าหรับผู้ใช้งานภายใน ผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลาดังนี้

[1] การเข้าถึงในเวลาราชการ (08.30-16.30 น)

[2] การเข้าถึงนอกเวลาราชการ (นอกช่วงเวลา 08.30-16.30 น.)

[3] การเข้าถึงในช่วงเวลาวันหยุดราชการและวันหยุดนักขัตฤกษ์

[4] การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุเป็นช่วงเวลา ระยะเวลาการเข้าถึง

6) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

(1) ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

(2) ระบบโทรศัพท์ (เข้าถึงได้ในเวลาราชการ)

(3) หนังสือหรือบันทึกข้อความ (เข้าถึงได้ทุกช่วงเวลา)

(4) ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

(5) ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

(6) ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

(7) ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

(8) เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนดเวลา)

(9) การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และช่วงเวลาพิเศษเป็นรายครั้ง)

1.3 ข้อกำหนดการใช้งานตามภารกิจ

1) การใช้งานตามภารกิจโรงพยาบาลจัดให้บริการสารสนเทศ เพื่อใช้ประโยชน์ตามภารกิจของโรงพยาบาล ได้แก่ การบริหาร การวิเคราะห์ การทำวิจัย ทั้งนี้การใช้งานตามภารกิจต้องอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่นเคารพและปฏิบัติให้ถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจ การค้าใดๆ โดยกำหนดสิทธิ์การเข้าถึงจะแบ่งตามลำดับชั้นการบริหารจัดการของผู้บริหาร ไว้ดังนี้

(1) ผู้บริหารระดับสูง ได้แก่ ผู้อำนวยการ สามารถเข้าถึงข้อมูลได้ตามภารกิจที่กำกับดูแล

(2) ผู้บริหารระดับหน่วยงาน ได้แก่ หัวหน้าฝ่าย ผู้รับผิดชอบงานเฉพาะด้าน สามารถเข้าถึงข้อมูลภายใต้ความรับผิดชอบดูแล

(3) ผู้ปฏิบัติงาน สามารถเข้าถึงได้เฉพาะส่วนที่ตนเองได้รับมอบหมาย

2) การกำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

(1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

(2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

(3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

3) ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิ์สำหรับผู้ใช้งานมีดังนี้ ตำแหน่งงาน หน่วยงานต้นสังกัด คำสั่งมอบหมายงานและหน้าที่รับผิดชอบ ระยะเวลาการจ้างงาน/ระยะเวลาการปฏิบัติงาน

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่ เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาตรวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศได้ โดยกำหนดแนวปฏิบัติ ดังนี้

2.1 การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

1) มีการเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศให้ผู้ใช้งานได้รับทราบ

2) มีการฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึง

ภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

2.2 การกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration)

1) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

2) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

3) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

4) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

5) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

6) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการอนุญาตจากผู้อำนวยการ

7) มีหลักเกณฑ์ในการยกเลิก เพิกถอน การอนุญาต ให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการ ลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง

8) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบ ต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

9) มีการแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน อย่างน้อยทุก 6 เดือนส าหรับผู้ใช้งานทั่วไป และอย่างน้อยทุก 3 เดือน สำหรับผู้บริหารและผู้ดูแลระบบ หรือตามระยะเวลาที่เหมาะสม

2.3 การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

1) ผู้ดูแลระบ ต้องกำหนดรหัสผู้ใช้ รหัสผ่าน และสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ ตามหน้าที่ความรับผิดชอบของแต่ละกลุ่มผู้ใช้งาน เพื่อใช้ในการตรวจสอบยืนยันตัวตนของผู้ใช้งาน

2) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ทั้งนี้ต้องได้รับหนังสือจากต้นสังกัดโดยให้มีการพิจารณาควบคุมการใช้งาน ดังนี้

(1) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบนั้น ๆ

(2) ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้มีการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) มีการเปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะนานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน

2.4 มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

1) กระบวนการจัดสรรหรือแจกจ่ายรหัสผ่านให้กับผู้ใช้งาน

(1) กำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

(2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

3) ส่งมอบรหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน

(4) ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน

(5) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

2) ข้อกำหนดการเปลี่ยนรหัสผ่าน

(1) อนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง

(2) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(3) ผู้ใช้งาน ควรทำการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

2.5 การทบทวนสิทธิการเข้าถึงผู้ใช้งาน (Review of User Access Rights)

1) ผู้ดูแลระบบ ทบทวนสิทธิการเข้าถึงของผู้ใช้งานปีละ 1 ครั้งเป็นอย่างน้อย มีแนวทางปฏิบัติ ดังนี้

(1) จัดทำหนังสือถึงฝ่ายบนิหาร เพื่อขอข้อมูลบุคลากรพ้นสภาพบุคลากร ยกเว้นกรณีเกษียณอายุราชการ

(2) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งจากหน่วยงาน

2) ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

3) ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลง การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

4) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

2.6 การเพิกถอนสิทธิการเข้าถึงของผู้ใช้งาน

1) ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพบุคลากร ของโรงพยาบาลศรีนครยกเว้นกรณีเกษียณอายุราชการ โดยดำเนินการแจ้งเจ้าของข้อมูล เพื่อขอรายชื่อ บุคลากร ที่พ้นสภาพอย่างน้อยปีละ 1 ครั้ง

2) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศทันที เมื่อผู้ใช้งานนั้นพ้นจากสภาพบุคลากร ยกเว้นกรณีเกษียณอายุราชการ โดยอ้างอิงจากบันทึกจากฝ่ายบริหาร

3) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานเปลี่ยนตำแหน่งงาน

3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งาน มีข้อปฏิบัติดังนี้

3.1 วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password Use)

1) แนวปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(1) ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที

(2) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(3) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(4) ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

(5) ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด และผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป โดยกำหนดอย่างน้อยทุก 6 เดือน สำหรับผู้ใช้งานทั่วไป และอย่างน้อยทุก 3 เดือน สำหรับผู้บริหารและผู้ดูแลระบบ หรือตามระยะเวลาที่เหมาะสม

(6) ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

2) คุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

(1) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลข และสัญลักษณ์เข้าด้วยกัน

(2) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

(3) หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน หรือกลุ่มของตัวอักขระที่เหมือนกัน

3) ข้อระวังการใช้งานรหัสผ่านที่ปลอดภัย

(1) ผู้ใช้งานไม่ควรใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(2) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(3) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล

(4) ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

3.2 การป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ให้กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของโรงพยาบาลในขณะที่ไม่มีผู้ดูแล ดังนี้

1) กำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ อุปกรณ์คอมพิวเตอร์ทันที เมื่อใช้งานเสร็จ

2) ผู้ใช้งานควรล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

3) กำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

4) กำหนดให้มีการตั้งล็อกหน้าจอเครื่องคอมพิวเตอร์หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

3.3 การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Deskand Clear Screen Policy) โดยควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่ได้รับสิทธิ์ และกำหนดให้ผู้ใช้งานออกจากระบบ เมื่อว่างเว้นจากการใช้งาน ดังนี้

1) มีการกำหนดมาตรการป้องกันทรัพย์สินของโรงพยาบาล และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานการณ์ที่ไม่ปลอดภัยครอบคลุมเรื่องต่างๆ ดังนี้

(1) การจัดการบริเวณล้อมรอบ

(2) การควบคุมการเข้า-ออก

(3) การจัดบริการการเข้าถึงการส่งผลิตภัณฑ์โดยบุคลภายนอก

(4) การวางอุปกรณ์

(5) ระบบและอุปกรณ์สนับสนุนการทำงาน

2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ได้แก่ แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ และวัฒนธรรมองค์กร

3) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

(1) ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของโรงพบาบาล

(2) ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

(3) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

(4) ล็อคเครื่องคอมพิวเตอร์เมื่อไม่ใช้งาน

(5) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสาร กล้องดิจิตอล โดยไม่ได้รับอนุญาต

(6) ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

(7) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

3.4 การเข้ารหัสใช้กับข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษา

ความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

4.1 การใช้บริการเครือข่าย

1) มีการกำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้ใช้งานได้

2) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น

3) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ฯลฯ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ 1 ครั้ง

4.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก (User Authentication for External Connection) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคล ดังนี้

1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

2) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง ด้วยการใช้รหัสผ่าน

4.3 การระบุอุปกรณ์บนเครือข่าย (Equipment Identifiction in Network) มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

1) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

2) มีการควบคุมการใช้งานอย่างเหมาะสม

3) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึง ทั้งทางกายภาพและเครือข่าย ดังนี้

1) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

2) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

3) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

4.5 การแบ่งแยกเครือข่าย (Segregation in Network)

แนวทางปฏิบัติ

1) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรออกเป็นเครือข่ายภายใน และภายนอก

2) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรออกเป็นเครือข่ายย่อยๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

3) กำหนดให้มีการควบคุมการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเหล่านั้น ทั้งนี้เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเหล่านั้นและทำการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่ายหรืออื่นๆ โดยไม่ได้รับอนุญาต

4) กำหนดมาตรการความมั่นคงปลอดภัยที่เหมาะสมกับเครือข่ายย่อย เหล่านั้น เช่นใช้ไฟร์วอลล์กั้นและป้องกันเครือข่ายย่อยเหล่านั้นจากการถูกบุกรุก หรือเข้าถึงโดยไม่ได้รับอนุญาต

5) กำหนดให้มีการใช้เกตเวย์เช่น ไฟร์วอลล์เพื่อกั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ กรองหรือจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น และควบคุมการเข้าถึงเครือข่ายย่อยภายในโดยไม่ได้รับอนุญาต

6) กำหนดให้มีการใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย (ทั้งจากภายใน และภายนอกองค์กร) ให้สอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานระบบเครือข่ายของโรงพยาบาล

7) กำหนดให้มีการใช้ขีดความสามารถของอุปกรณ์เครือข่าย เช่น การทำ IP Switching เพื่อแบ่งแยกเครือข่ายออกเป็นส่วนๆ รวมทั้งควบคุมการไหลของข้อมูล ระหว่างเครือข่ายย่อยเหล่านั้น

8) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ความต้องการในการเข้าถึงเครือข่ายหรือระบบงาน เช่น ความต้องการของผู้ใช้งานกลุ่มต่างๆ หรือของผู้บริหาร เป็นต้น

9) กำหนดให้มีการแยกวงของเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของโรงพยาบาล

10) กำหนดให้มีการประเมินความเสี่ยงและกำหนดมาตรการป้องกันที่ เหมาะสมก่อนแบ่งแยกวงเครือข่ายไร้สาย

4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) แนวปฏิบัติการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน มีดังนี้

1) มีการตรวจสอบการเชื่อมต่อเครือข่าย

2) จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

3) ระบุอุปกรณ์ เครื่องมือ ที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

4) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

5) ควบคุมไม่ให้มีการเปิดให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

4.7 การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control) มีการควบคุมดังนี้

1) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address Plan)

2) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

3) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

5.1 ผู้ดูแลระบบ (System Adminstrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ให้บริการสารสนเทศของโรงพยาบาล และกำหนดชื่อผู้ใช้งานให้กับเครื่องคอมพิวเตอร์

5.2 กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบเสร็จสมบูรณ์

5.3 ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identififation and Atuhentication) กำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

3) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่นสมาร์การ์ด RFID เครื่องอ่านลายนิ้วมือ ฯลฯ

5.4 การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

5.5 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ดำเนินการดังนี้

1) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้งานโปรแกรม

2) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

4) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

5.6 การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out) กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเกิน 30 นาที ตามความเหมาะสม ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้มีการพิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญ

5.7 การจำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Network Usage Idle Time) กำหนดหลักเกณฑ์การยุติการใช้งานระบบเครื่อข่ายเมื่อว่างเว้นจากการใช้งานเป็นเวลาเกิน 1 ชั่วโมงหากต้องการเชื่อมต่อ ต้องเข้ารหัสผ่านเพื่อยืนยันตัวตนอีกครั้ง

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access control)

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

6.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อโรงพยาบาลดำเนินการดังนี้

1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญ

2) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

3) มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกโรงพยาบาล ที่เกี่ยวข้องกับระบบดังกล่าว

6.3 การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

2) การยืมใช้อุปกรณ์ ต้องมีการบันทึกรายละเอียดการยืมใช้งานอย่างเป็นลายลักษณ์อักษร

3) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

4) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

5) เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

6) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาณอย่างร้ายแรงของผู้นำไปใช้ ผู้นาไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

7. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาล จะต้องทำการลงทะเบียนกับ

ผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

2) ผู้ดูแลระบบ ต้องดำเนินการดังนี้

(1) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่าเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(2) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(3) ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

(4) ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

(5) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(6) ควรเปลี่ยนค่า ชื่อล๊อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อล๊อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(7) ต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

(8) ควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

(9) ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

(10) ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

(11) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่าเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อหัวหน้างานทราบโดยทันที

8. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

8.1 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1) กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยภายในโรงพยาบาล มีการจำแนกและกำหนดพื้นที่ของเครื่องแม่ข่าย อุปกรณ์เครื่องแม่ข่าย ระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม และให้กำหนดพื้นที่รักษาความมั่นคงปลอดภัย ของระบบสารสนเทศและเครือข่าย มีจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น โดยการกำหนดพื้นที่ดังกล่าวออกเป็น

(1) พื้นที่ทำงาน

(2) พื้นที่ติดตั้ง จัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย

2) กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

(1) จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

(2) กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออกพื้นที่

(3) บุคคลภายนอกเข้ามาติดต่อต้องมีหนังสือขอความอนุเคราะห์ดูงาน ถึงผู้อำนวยการศูนย์ฯ และต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

(4) บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

(5) ประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน

(6) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในโรงพยาบาล จะต้องได้รับอนุญาตจากหัวหน้ากลุ่มงาน

(7) มีระบบสนับสนุนการทำงานของระบบสารสนเทศที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ดับเพลิง ระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่าเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(8) ติดตั้งระบบแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

8.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ

1) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงไ

2) ให้มีการป้องกันสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

3) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

4) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

5) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

6) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงบุคคลภายนอก

7) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

8.3 การบำรุงรักษาอุปกรณ์

1) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

2) ปฏิบัติตามคำแนะนาในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายใน

6) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

8.4 การนาทรัพย์สินของมหาวิทยาลัยออกนอกโรงพยาบาล

1) ให้มีการขออนุญาตก่อนนาอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกโรงพยาบาล

2) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกโรงพยาบาล

3) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกโรงพยาบาล

4) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

5) บันทึกข้อมูลการนำอุปกรณ์ขอโรงพยาบาลออกไปใช้งานนอกโรงพยาบาล เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

8.5 การจัดการอุปกรณ์ที่ใช้งานอยู่นอกโรงพยาบาล

1) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของโรงพยาบาลไว้โดยลำพังในที่สาธารณะ

2) เจ้าหน้าที่มีความรับผิดชอบอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

8.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

2) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ

ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ

8.7 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

1) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

2) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

3) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น ฯลฯ

9. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

9.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

1) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของโรงพยาบาลเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

2) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของโรงพยาบาล

3) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนการดำเนินงาน

4) ไม่ควรติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

5) กำหนดให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

6) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ฯลฯ

7) ให้ผู้ที่เกี่ยวข้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

8) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม และขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

9) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

9.2 การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

1) แจ้งให้ผู้ที่เกี่ยวข้องระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลง

ระบบปฏิบัติการ

2) พิจารณาวางแผนดำเนินเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

9.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

1) ควรจัดให้มีการควบคุมการพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคลหรือหน่วยงานภายนอก

2) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

3) ให้กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

5) ให้มีการจัดทำข้อตกลงการรักษาความลับที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ที่จะสามารถเปิดเผยได้เฉพาะบุคคลเท่านั้น เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลแล้วเท่านั้น

9.4 มาตรการควบคุมช่องโหว่ทางเทคนิค

1) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศ โดยให้มีการบันทึกดังต่อไปนี้

(1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

(2) สถานที่ติดตั้ง

(3) เครื่องที่ติดตั้ง

(4) ผู้ผลิตซอฟต์แวร์

(5) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

2) กำหนดให้มีการจัดการช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

3) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบดำเนินการดังนี้

(1) มีการเฝ้าระวังติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(2) ให้กำหนดแหน่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของโรงพยาบาล

(3) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับการแจ้งหรือทราบเกี่ยวกับช่องโหว่

4) ปิดการใช้งานหรือควบคุมการเข้าพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

9.5 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

1) ข้อมูลบัญชีผู้ใช้งาน

2) ข้อมูลวันเวลาที่เข้าถึงระบบ

3) ข้อมูลวันเวลาที่ออกจากระบบ

4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

5) ข้อมูลการล๊อกอิน ทั้งที่สำเร็จและไม่สาเร็จ

6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

7) ข้อมูลการเปลี่ยนคอนฟิกกูเรชัน (Configuration) ของระบบ

8) ข้อมูลแสดงการใช้งานแอพพลิเคชัน

9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่นเปิด ปิด เขียน หรืออ่านไฟล์ ฯลฯ

10) ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง

11) ข้อมูลโพรโทคอลเครือข่ายที่ใช้

12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

13) ข้อมูลแสดงการสำรองข้อมูลไม่สาเร็จ

10. การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room) เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูล โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย

10.1 ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

1) หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต

(1) อนุมัติสิทธิเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

(2) อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

2) ผู้ดูแลห้องควบคุมระบบเครือข่ายตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ปฏิบัติการให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

10.2 กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย มีแนวทางปฏิบัติดังนี้

1) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้อง และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูและระบบ (System

Administrator) เป็นต้น

2) สิทธิในการเข้าออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

3) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

4) การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มหรืออุปกรณ์บันทึกข้อมูลการเข้าออกพื้นที่

10.3 แนวปฏิบัติการจัดทำเอกสารระบุสิทธิในการเข้าถึงพื้นที่ มีดังนี้

1) กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและช่วงเวลาที่มีสิทธิในการผ่านเข้าออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

2) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ ที่ออกโดยหน่วยงานราชการ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

3) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน

4) เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

5) บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่ออุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

6) ผู้ใช้จะได้รับสิทธิให้เข้าออกพื้นที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

7) หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้ขอเข้าพื้นที่ โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่หน่วยงานราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

11. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

11.1 การใช้งานทั่วไป

1) ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

2) เครื่องคอมพิวเตอร์และเครือข่ายของโรงพยาบาลศรีนครเป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น

3) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาล ต้องเป็นโปรแกรมที่โรงพยาบาลได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

4) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับโรงพยาบาลเท่านั้น

5) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบหาไวรัสโดยโปรแกรมป้องกันไวรัส

6) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

7) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น ตกหรือหลุดมือ

8) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

9) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

10) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

11) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ และเครื่องดื่มต่าง ๆ ฯลฯ

12) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

13) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

14) ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

15) ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น (อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ) ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

16) ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คาแนะนำที่โรงพยาบาลศรีนครกำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

17) หากผู้ใช้งานกระทำการล่วงละเมิด หรือ พยามยามจะล่วงละเมิด ศูนย์เทคโนโลยีสารสนเทศในฐานะผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของโรงพยาบาล ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือ การใช้งานใดๆ ตามความเหมาะสม

18) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

19) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

20) ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง

21) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

22) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

23) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือศูนย์เทคโนโลยีสารสนเทศ

24) ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

25) ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟท์แวร์ที่จัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

26) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาล เพื่อประโยชน์ทางการค้า

27) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

28) ห้ามผู้ใช้งานใช้ระบบสารสนเทศของโรงพยาบาล เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

11.2 การสำรองข้อมูลและการกู้คืน แนวปฏิบัติ มีดังนี้

1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD และ External Hard Disk ฯลฯ

2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่าเสมอ

3) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Hard Disk ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

12. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

วิธีการปฏิบัติ มีดังนี้

1) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีการปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

2) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

3) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

4) การรับส่งข้อมูลข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสลับ (encryption) ที่เป็นมาตรฐานสากล

5) ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

6) ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโงพยาบาล ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อก่อน

7) การใช้ข้อมูลภายในร่วมกันต้องอยู่ในกรอบหน้าที่และความรับผิดชอบที่ได้รับมอบหมายเท่านั้น การแสดงชั้นความลับของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ให้แสดงชั้นความลับไว้ ณ ที่ที่แสดงข้อมูลข่าวสารลับนั้น เช่น เมื่อเรียกแฟ้มข้อมูลมาแสดงภาพที่หน้าจอภาพ ให้แสดงชั้นความลับทั้งหมดทุกหน้าของข้อมูลข่าวสารลับ ที่แสดงภาพบนจอนั้น และสื่ออิเล็กทรอนิกส์ที่จัดเก็บ เช่น แผ่นซีดีรอม แผ่นดิสก์Flash drive เป็นต้น ให้แสดงชั้นความลับบนภาชนะที่บรรจุ หรือใช้กระบวนการทางคอมพิวเตอร์ให้ปรากฏชั้นความลับ เมื่อเรียกแฟ้มข้อมูลมาแสดงภาพ เช่น การจัดทำลายน้ำบนข้อมูลทางระบบอิเล็กทรอนิกส์การป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัสด้วยเครื่องเข้ารหัสหรือโปรแกรมเข้ารหัส ซึ่งการใช้กุญแจ

รหัสประเภทใดและจานวนครั้งของการเข้ารหัสขึ้นอยู่กับความสำคัญของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ให้อยู่ในดุลพินิจของเจ้าของข้อมูลการป้องกันสื่อบันทึกข้อมูลลับ ต้องมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัยเพื่อให้ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ดำเนินการได้อย่างต่อเนื่อง และความคงอยู่ของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์การทำลายสื่อบันทึกข้อมูลลับ และแฟ้มข้อมูลลับ เพื่อป้องกันการกู้คืน เช่น แผ่นดิสก์ ฮาร์ดดิสก์Flash Drive ที่สามารถใช้บันทึกซ้าได้ ให้ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทาหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้ กรณีที่จัดเก็บอยู่ในสื่อที่ไม่สามารถใช้บันทึกซ้าได้ ให้ใช้การทำลายด้วยวิธีทุบ ทำาลายให้สิ้นสภาพการใช้งาน

13. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail) กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของโรงพยาบาล ดังนี้

1) แนวทางการควบคุมการใช้งาน สำหรับผู้ดูแลระบบ

(1) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาล ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่าเสมอ เช่น การลาออกเป็นต้น

(2) กำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาล

(3) รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น (*) ในการพิมพ์แต่ละตัวอักษร

(4) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ได้ไม่เกิน 5 ครั้ง

(5) ผู้ดูแลระบบ ควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ล็อกเอ้าท์ออกจากหน้าจอ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

2) การใช้งานสำหรับผู้ใช้

(1) ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจารหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

(2) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

(3) ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อโรงพยาบาล หรือละเมิดสิทธิสร้างความราคาญต่อผู้อื่น หรือผิดกฎหมาย ละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมาอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของโรงพยาบาล

(4) ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(5) ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของโรงพยาบาลศรีนคร เพื่อการทำงานของโรงพยาบาลศรีนครเท่านั้น

(6) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(7) ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

(8) ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(9) ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทาให้เสียชื่อเสียงของโรงพยาบาลศรีนคร ผ่านทางจดหมายอิเล็กทรอนิกส์

(10) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(11) ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจานวนน้อยที่สุด

(12) ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(13) ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

14. การใช้งานระบบอินเทอร์เน็ต (Use of the Internet) เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทาผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้

1) ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลศรีนคร จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

2) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรม ป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

3) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัส (Virus Canning) ป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

4) ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของโรงพยาบาลศรีนคร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

5) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของโรงพยาบาลศรีนคร

6) ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับโรงพยาบาลศรีนคร

7) ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงพยาบาลศรีนคร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

8) ผู้ใช้งาน ต้องไม่นาเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

9) ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

10) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของก่อนนำข้อมูลไปใช้งาน

11) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรม ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

12) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาลศรีนคร รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

13) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้จากบุคคลอื่น

15. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ปัจจุบันมีแหล่งให้บริการเครือข่ายทางสังคมเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจานวนมาก ตัวอย่างเช่น Facebook, Twitter, Linkedln, Google Plus, MySpace, YouTube, Blog, Wiki รวมทั้งเว็บไซต์ต่างๆ ทั้งในประเทศและต่างประเทศ ที่เป็นให้บริการ File Sharing, Photo Sharing, Video Sharing และกระดานข่าว (Webboard) เป็นต้น และเนื่องจากสื่อสังคมออนไลน์ เป็นเครื่องมือที่มีทั้งประโยชน์และโทษที่ควรระวัง โดยเฉพาะข้อมูลข่าวสารบางอย่างที่เผยแพร่ออกสู่สาธารณะไปแล้วอาจไม่สามารถเรียกกลับคืนได้ และอาจก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อองค์กร ดังนั้น เพื่อให้ผู้ปฏิบัติงานในโรงพยาบาลศรีนคร สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพและ

เกิดประโยชน์สูงสุด ทางโรงพยาบาลศรีนครจึงมีนโยบายและแนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อสังคมออนไลน์ (Social Network) และแสดงตนในฐานะบุคลากรหรือนักศึกษาในสังกัดโรงพยาบาลศรีนครแม่โจ้ ดังนี้

1) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่โรงพยาบาลศรีนครได้กำหนดไว้เท่านั้น

2) ควรแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ หากพบว่ามีข้อความบน Social Network ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงของหน่วยงาน ส่วนงานของโรงพยาบาลศรีนครได้

3) พึงระลึกว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และข้อบังคับว่าด้วยจรรยาบรรณของบุคลากรโรงพยาบาลศรีนคร และข้อบังคับว่าด้วยวินัยราชการ มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบน Social Network ด้วย ทั้งนี้การละเมิดจรรยาบรรณอย่างร้ายแรงดังที่กำหนดไว้ในข้อบังคับดังกล่าว เช่น การเปิดเผยความลับของผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่ผู้รับบริการ หรือการทำให้เกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของโรงพยาบาลศรีนคร ถือเป็นความผิดทางวินัยอย่างร้ายแรงและผู้ที่ละเมิดสามารถถูกดำเนินการทางวินัยได้ด้วย

4) ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว พึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

5) พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บน Social Network เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้

6) การนำเสนอข้อมูลข่าวสาร การแสดงความคิดเห็น ผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามจริยธรรมวิชาชีพและแนวปฏิบัติจริยธรรม

7) การใช้สื่อสังคมออนไลน์ (Social Media) พึงระมัดระวังการใช้ถ้อยคาและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

8) ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

9) ผู้ใช้งาน พึงระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้าน และควรอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง

10) ผู้ใช้งาน สามารถใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือในการรายงานข่าวในนามของ

บุคคลธรรมดาได้ แต่ควรแสดงให้ชัดเจนว่า ข้อความใดเป็น “ข่าว” ข้อความใดเป็น “ความคิดเห็นส่วนตัว” ทั้งนี้พึงตระหนักว่าการใช้ Social Network นั้นการแบ่งแยกระหว่างเรื่องส่วนตัว และเรื่องหน้าที่การงาน เป็นสิ่งที่ทำได้ยาก หากประสงค์จะใช้ Social Network เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน ยกตัวอย่างเช่น การใช้ Facebook ของผู้ที่ทาหน้าที่ประชาสัมพันธ์ของส่วนงาน ควรมีการแยก Facebook Profile ที่ใช้สำหรับติดต่อเครือข่ายของตนในเรื่องส่วนตัว เรื่องครอบครัว ออกจาก Facebook Profile ที่ใช้ประชาสัมพันธ์ส่วนงาน หรืออาจตั้งเป็น Facebook Page ประจำส่วนงานขึ้นแทนที่จะใช้ Profile ส่วนตัว

11) หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือโรงพยาบาลศรีนครต้องแจ้งให้หัวหน้าส่วนงานเทคโนโลยีสารสนเทศทราบ และต้องแจ้งรายชื่อของผู้ดูแล Page (Admin) หรือเจ้าของ Account นั้นให้หัวหน้าส่วนงานเทคโนโลยีสารสนเทศทราบ และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้นคืนแก่ส่วนงานหรือโรงพยาบาลศรีนคร เมื่อพ้นจากหน้าที่ที่ต้องดูแล หรือพ้นสภาพจากการเป็นบุคลากรของโรงพยาบาลศรีนคร

12) ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือสื่อสารข้อมูลในกิจการของโรงพยาบาลศรีนคร หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ควรแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูลโปรไฟต์ (Profile) และพึงใช้ด้วยความสุภาพ และมีวิจารณญาณ

13) การเผยแพร่ข้อมูล หรือแสดงความเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นของโรงพยาบาลศรีนคร ส่วนงานหรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของโรงพยาบาลศรีนคร ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของโรงพยาบาลศรีนคร ส่วนงานหรือหน่วยงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง

14) ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ใต้บังคับบัญชาได้ ทั้งนี้ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนเช่นเดียวกับข้อ 12

15) ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของโรงพยาบาลศรีนคร หรือข้อมูลที่ใช้ภายในโรงพยาบาลศรีนครก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ

16) ในการสื่อสารข้อมูลในกิจการขององค์กรทางสื่อสังคมออนไลน์ (Social Media) ห้ามแสดงสัญลักษณ์พรรคการเมือง กลุ่มกดดันรณรงค์ทางสังคม กลุ่มลัทธิทางศาสนา และพึงระมัดระวังในการใช้สัญลักษณ์ที่ก่อให้เกิดความเข้าใจผิดและไม่ควานารูปบุคคลอื่น มาแสดงว่าเป็นรูปของตนเอง

17) การส่งต่อข้อมูลในสื่อสังคมออนไลน์ (Social Media)

(1) พึงละเว้นการส่งต่อข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคลหรือสังคม

(2) พึงระมัดระวังการส่งต่อข้อมูลในสถานการณ์ภัยพิบัติธรรมชาติ การก่อการร้าย การจลาจล วินาศกรรมหรือภาวะสงคราม

(3) พึงระมัดระวังการส่งต่อข้อมูลเรื่อง บุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ

(4) พึงระมัดระวังการส่งต่อข้อมูลที่กระทบต่อสิทธิ ความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์

18) ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสมนอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อหน่วยงาน ส่วนงาน และโรงพยาบาลศรีนครได้

19) หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ เกิดความผิดพลาดจนก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรอื่น ทางองค์กรหรือผู้ใช้งานที่รับผิดชอบข้อความนั้น ไม่ว่าจะเป็นการส่งข้อความเองหรือรับส่งข้อมูลต่อ ต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคาขอโทษต่อบุคคลหรือองค์กรที่ได้รับความเสียหาย ทั้งนี้ต้องให้ผู้ที่ได้รับความเสียหายมีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

16. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติ ดังต่อไปนี้

1) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

2) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาลศรีนคร (IT Auditor) หรือบุคคลที่โรงพยาบาลศรีนครมอบหมาย

3) กำหนดให้มีการบันทึกให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง

4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ 2

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

4. เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

ผู้รับผิดชอบ

1) งานเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5)

แนวทางปฏิบัติ

1.การสำรองข้อมูล

1.) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในฮาร์ดดิสก์ 1 ชุดในเวลาเที่ยงคืนของทุกวัน

2.) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรอง (Backup) ข้อมูลตามระยะเวลาที่กำหนด รวมทั้งให้จัดเก็บข้อมูลสำรองไว้ทั้งออนไลน์และออฟไลน์เพื่อป้องกันข้อมูลสูญหาย

2.การกู้ข้อมูล

1.) ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้ทำการสำรอง ไว้ใน External Hard disk ทุกวันศุกร์ของสัปดาห์

2.) ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการ ของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

3. ข้อมูลที่ต้องทำการ Recovery ทันที ได้แก่ เช่น ระบบ Hosxp ระบบ Datacenter, ระบบบริหารงานภายใน Back Office ได้แก่ Smart Office, โปรแรมแจ้งซ่อม, โปรแกรมครุภัณฑ์

3. การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย (Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนคร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนคร ได้อย่างถูกต้อง

3.1 กระบวนการหลักในการควบคุมการเข้าถึงระบบ

1) สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่าเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งานหรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

3) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

4) ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนคร และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

5) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3.2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

1) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

2) เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตาม ความจำเป็นขั้นต่ำเท่านั้น

3) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงาน ตามความจำเป็นต่อการ

ใช้งานระบบเทคโนโลยีสารสนเทศ

3.3 การบริหารจัดการการเข้าถึงของผู้ใช้

1.) การลงทะเบียนเจ้าหน้าที่ใหม่ของโรงพยาบาลศรีนคร ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป ต้องทาภายใน 24 ชั่วโมง หรือเมื่อเปลี่ยนตาแหน่งงานภายในต้องทำภายใน 7 วัน

2.) กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ตเป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่าเสมอ

3.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

1) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

2) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

3) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึงผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(1) ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

(2) ควรควบคุมการใช้งานอย่างเข้มงวด เช่นการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(4) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือนเป็นต้น

4. การบริหารจัดการการเข้าถึงระบบเครือข่าย

1) ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

2) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

3) ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

4) ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่าย

ไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

5) ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ กำรกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

6) ระบบเครือข่ายทั้งหมดของโรงพยาบาลศรีนคร ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทา Packet Filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

7) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

8) การเข้าสู่ระบบงานเครือข่ายภายในโรงพยาบาลศรีนคร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล็อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

9) IP Address ภายในของระบบงานเครือข่ายภายในของโรงพยาบาลศรีนคร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

10) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

11) การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

12) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศเท่านั้น

13) ผู้ใช้งาน ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐาน และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาลศรีนคร

14) การขออนุญาตนาเครื่องคอมพิวเตอร์เชื่อมต่อระบบเครือข่ายและขอหมายเลขไอพี (IP Address) และชื่อโดเมน (Domain Name) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาตส่งผ่านหน่วยงานต้นสังกัดมายังศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาดำเนินการ

15) ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของโรงพยาบาลศรีนครได้

16) ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของโรงพยาบาลศรีนคร ศูนย์เทคโนโลยีสารสนเทศ อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

17) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network)

5. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

1) กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรม ระบบ (System Software) อย่างชัดเจน

2) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

3) เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet FTP หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

4) ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่าเสมอ เช่น webserver เป็นต้น

5) มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

6) การติดตั้งและเชื่อต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

6. การบริหารจัดการการบันทึกและตรวจสอบ

1) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย 3 เดือน

2) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่าเสมอ

3) มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7. การควบคุมการเข้าใช้งานระบบจากภายนอก ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

1) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของโรงพยาบาล

ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

2) วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนามาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของโรงพยาบาลศรีนคร ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด โดยต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน วิธีการเข้ารหัส ฯลฯ

3) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับโรงพยาบาลอย่างเพียงพอ และต้องได้รับอนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศอย่างเป็นทางการ

4) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสม

5) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

6) ไม่อนุญาตให้ครอบครัวหรือเพื่อนเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลสำหรับการปฏิบัติงานจากภายนอกสำนักงาน

8. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของโรงพยาบาล ดังนี้

1) แสดงชื่อผู้ใช้งาน (Username)

2) ใส่รหัสผ่าน (Password)

9. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control) การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตเป็นต้นเพื่อให้การควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล เป็นไปอย่างมั่นคงปลอดภัย มีแนวทางปฏิบัติดังนี้

9.1 แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

1) หัวหน้างานกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2) การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

(1) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลจะต้องทาเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศ

(2) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้ เหตุผลในการขอใช้ระยะเวลาในการใช้ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย และการตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

3) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(1) หน่วยงานภายนอกที่ ทำงานให้กับโรงพยาบาลทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในโรงพยาบาลหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของโรงพยาบาล โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(2) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(3) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของโรงพยาบาลศรีนคร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(4) โรงพยาบาลศรีนคร มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่าโรงพยาบาลศรีนคร สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(5) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

10. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ภายใต้บังคับของมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดประเภทของผู้ให้บริการ ไว้ดังนี้

1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ 4 ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and

Broadcast Carrier)

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ได้แก่ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด และผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการหรือบริษัท

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider) ได้แก่ ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) การให้บริการเช่า Web Server ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) และผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)

ง. ผู้ให้บริการร้านอินเทอร์เน็ต

2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่น (Application Service Provider) ได้แก่

(1) ผู้ให้บริการเว็บบอร์ด (Web Board) หรือผู้ให้บริการบล๊อค (Blog)

(2) ผู้ให้บริการการทาธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชาระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider)

(3) ผู้ให้บริการเว็บเซอร์วิส (Web Services)

(4) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์

(e-Transactions) หน้าที่ “ผู้ให้บริการ” ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยให้ผู้ให้บริการเก็บเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น ด้วยวิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

1) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

2) มีระบบการเก็บรักษาความลับของขอมูลที่จัดเก็บ และกำหนดชั้นความลับในการเขาถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ Centralized Log Server การทำ Data Archiving หรือทำ Data Hashing เป็นตน เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กรกำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่นผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมายเป็นต้น

3) จัดให้มีผูมีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตาม พระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. 2550 เพื่อใหการส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

4) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) ,Proxy Cache , Cache Engine ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

5) ในกรณีที่ผูให้บริการประเภทหนึ่งประเภทใด ในข้อ 1 ถึงข้อ 4 ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกลาวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ 1 ถึงข้อ 4 ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการนั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ส่วนที่ 3

แผนเตรียมความพร้อมกรณีฉุกเฉิน

1. หลักการและเหตุผล

ปัจจุบัน โรงพยาบาลศรีนคร มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการระบบด้านสุขภาพและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ การวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ มีจำนวนเพิ่มมากขึ้น ดังนั้นจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่นำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพ

งานประกันสุขภาพยุทธศาสตร์และเทคโนโลยีสารสนเทศทางการแพทย์ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานขององค์กร และให้บริการผู้มารับบริการตลอดจนบุคลากรได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอก ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

1.) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.) เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

3.) เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

4.) เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

5.) เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

3. การวิเคราะห์ความเสี่ยง

โรงพยาบาลศรีนครมีการใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่จะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

แนวปฏิบัติ

1. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)

1) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทาให้ไม่สามารถเข้าใช้ระบบงานได้ ฯลฯ

3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ ฯลฯ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

7) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ 1 ครั้ง

2. ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้องกรณีเครื่องลูกข่าย

1) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุนั้นให้เจ้าหน้าที่ทราบ หรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ งานเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงานในโรงพยาบาลศรีนครทราบ

2) เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สายLAN) ออกจากเครื่องนั้นโดยเร็ว

3) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงานภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสายLANออกจากจุดชุมสายในชั้นนั้นออกให้หมด

4) ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด

5) ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

6) ให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศแจ้งเหตุขัดข้องนั้นให้หัวหน้างานทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (Server) และอุปกรณ์เครือข่าย

1) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2) ถ้าไฟฟ้าดับ/ไฟฟ้าตกให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ,ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟฟ้า

3) ตัดระบบจ่ายไฟในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

4) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

5) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองมาเปลี่ยนโดยเร็วที่สุด

6) ผู้ดูแลระบบต้องรีบแจ้งให้หัวหน้างานทราบโดยเร็ว

3. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อให้ระบบงานของโรงพยาบาลสามารถดำเนินการได้อย่างต่อเนื่องในช่วงการเกิดภัยคุกคามครอบคลุมสถานการณ์ฉุกเฉิน โดยการจัดหาระบบเทคโนโลยีสารสนเทศในการสนับสนุนการบริหารจัดการ การปฏิบัติงานและการให้บริการ ให้สามารถดำเนินการได้อย่างต่อเนื่อง ตลอดจนบริหารจัดการความเสี่ยงด้านระบบสารสนเทศที่อาจส่งผลต่อการปฏิบัติงาน และการให้บริการของโรงพยาบาลให้อยู่ในวิสัยที่ยอมรับหรือควบคุมได้

4. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

เพื่อให้ระบบอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็วเพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด โดยแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

1) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

5) นำ BACKUP TAPE/CD-ROM/HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore ใช้

6) ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

7) ทำการตรวจสอบระบบปฏิบัติการระบบฐานข้อมูลตรวจสอบความถูกต้องของข้อมูลและระบบ

8) อื่น ๆ ที่เกี่ยวข้อง

5. การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

กำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขสถานการณ์ฉุกเฉินได้อย่างรวดเร็ว ต่อเนื่อง และมีประสิทธิภาพ ดังนี้

5.1 การจัดหน่วยปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน หรือสายการบังคับบัญชา (Lines of Authority)

1) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

(1) กำหนดนโยบายให้งานเทคโนโลยีสารสนเทศ

(2) ให้คำปรึกษาแก่ผู้หัวหน้างานเทคโนโลยีสารสนเทศในฐานะผู้มีอำนาจหน้าที่ในการควบคุมการดำเนินงานด้านสารสนเทศและดูแลงานเทคโนโลยีสารสนเทศ

2) หัวหน้างานประกันสุขภาพ ยุทธศาสตร์และเทคโนโลยีสารสนเทศทางการแพทย์

(1) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

(2) มีอำนาจสั่งการให้ทุกหน่วย ปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

(3) มีอำนาจสั่งทาลายกุญแจอาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

(4) ประชุมหารือกับคณะกรรมการนโยบายและพัฒนาระบบสารสนเทศและคณะกรรมการอื่นที่เกี่ยวข้อง

(5) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

(6) รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหาร

3) ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย (หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต)

(1) วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อหัวหน้างานเทคโนโลยีสารสนเทศ

(2) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าหัวหน้างานเทคโนโลยีสารสนเทศระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

(3) สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

(4) ทำหน้าที่แทนหัวหน้างานเทคโนโลยีสารสนเทศระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ท่านหัวหน้างานเทคโนโลยีสารสนเทศการระงับเหตุฉุกเฉินไม่อยู่

(5) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

(6) รายงานให้หัวหน้างานเทคโนโลยีสารสนเทศการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

(7) กำหนดอัตรากำลังพลวัสดุอุปกรณ์และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

(8) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

4) ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administor and Staffs)

(1) กรณีเกิดเพลิงไหม้ให้ดำเนินการนาอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

(2) พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย

(3) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

(4) ป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

(5) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้หัวหน้างานเทคโนโลยีสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

[1] ทำการตรวจสอบระบบ Firewall

[2] ทำการตรวจสอบ Virus, Worm, Spyware

[3] ทำการตรวจสอบ UPS

[4] ทำการตรวจสอบ Transaction log files

[5] ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

[6] ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ

[7] ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

[8] ทำการตรวจสอบค่า Configuration ของระบบ

5) ผู้ประสานงานและดูแลสภาพความพร้อมของระบบเครือข่าย

(1) ดำเนินการให้ผู้ที่เกี่ยวข้อง ปฏิบัติตามแผนฯ

(2) ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

(3) ตรวจสอบความเสียหายของทรัพย์สิน ทั้งระบบคอมพิวเตอร์และระบบเครือข่าย

(4) เตรียมเครื่องมืออุปกรณ์ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

(5) ทำการสำรองข้อมูลในส่วนของข้อมูล และสำรองข้อมูลทั้งระบบ สัปดาห์ละ 1 วัน

(6) ทำการเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และแฟ้มข้อมูล Tape Backup รายชื่อโปรแกรม เอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์ สำเนาคู่มือต่างๆ

(7) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

6) หัวหน้าหน่วยงานที่เกิดเหตุ (On-Site Manager)

(1) แจ้งเหตุฉุกเฉินและเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

(2) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่หัวหน้างานเทคโนโลยีสารสนเทศ เพื่อประสานงานในการรักษาความปลอดภัยระบบสารสนเทศ

(3) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพและสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมาและทารายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

การประเมินสถานการณ์ความเสี่ยง

การวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศของโรงพยาบาลศรีนคร พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

1) ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ได้แก่ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทาให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้เกิดการชะงักหรือหยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

(1) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ

Software เบื้องต้นเพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้นทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(2) นำเสนอนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณาในการประชุมคณะกรรมการนโยบายและพัฒนาระบบสารสนเทศ

(3) จัดทำนโยบายว่าด้วยการใช้งานคอมพิวเตอร์ทั่วไปและการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต เผยแพร่ผ่านเว็บไซด์ศูนย์เทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

2) ภัยที่เกิดจาก Software

เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาล ใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

(1) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่ายทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(2) มีการติดตั้งซอฟต์แวร์ Trend Micro Server ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่เป็นซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

(3) แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์โปรแกรมแจ้งซ่อมอย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากSoftware ดังกล่าวให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

3) ภัยจากไฟไหม้หรือระบบไฟฟ้า

จัดเป็นภัยร้ายแรงที่ทาความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งศูนย์เทคโนโลยีสารสนเทศได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง โดยมีการสำรวจตรวจสอบระยะเวลาการสำรองไฟกรณีที่เกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(2) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่ายอุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่าเสมอ

(3) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

4) ภัยจากน้ำท่วม (อุทกภัย)

เนื่องจากห้องควบคุมระบบเครือข่ายอยู่บริเวณชั้น 1 ของอาคาร ซึ่งมีความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทาความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งโรงพยาบาล ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้ภัยในลักษณะดังกล่าวเกิดขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากน้ำท่วม (อุทกภัย)

(1) เฝ้าระวังภัยอันเกิดจากน้าท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(2) เมื่อเกิดน้ำขังหรือมีการรั่วซึมจากน้ำ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อย ๆ มาถึงบริเวณหน้าอาคาร ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครื่องแม่ข่ายทั้งหมด

(3) นำ Back up ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย

(4) ดำเนินการตัดระบบน้าและไฟฟ้าในห้องควบคุม ปิดเบลคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(5) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในชั้นที่สูง

(6) กรณีน้ำลดลงแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(7) เมื่อระบบไฟฟ้าใช้งานได้ตามปกติผู้ดูแลระบบและเจ้าหน้าที่ผู้เกี่ยวข้องช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์ทำหน้าที่แม่ข่าย มาติดตั้งณห้องควบคุมระบบเครือข่าย

(8) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(9) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้บริการได้ตามปกติ

การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลศรีนคร ให้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ ดังนี้

1) แผ่น Boot Disk

2) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

3) แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

4) แผ่นโปรแกรม Antivirus/Spyware

5) แผ่น Driver อุปกรณ์ต่าง ๆ

6) ระบบสำรองไฟฉุกเฉิน

7) Hard Disk สำรอง

8) สำเนารายละเอียดการบันทึกค่าต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

ส่วนที่ 4

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

2) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

1) งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

2) งานตรวจสอบภายใน หรือผู้ตรวจสอบจากภายนอก

3) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

1. การประเมินผลกระทบ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ให้หน่วยงานหรือองค์กรยึดถือหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้เป็นแนวทางในการประเมินระดับผลกระทบ โดยกำหนดการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์จะต้องประเมินผลกระทบในด้านต่อไปนี้

1.1 การประเมินผลกระทบด้านมูลค่าความเสียหายทางการเงินให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

1) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาท ให้จัดเป็นผลกระทบระดับต่ำ

2) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

3) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไป ให้จัดเป็นผลกระทบระดับสูงในการประเมินมูลค่าความเสียหายทางการเงิน ให้คานวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

1.2 การประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัยให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

1) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ให้จัดเป็นผลกระทบระดับต่ำ

2) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ตั้งแต่หนึ่งคนแต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

3) ในกรณีจานวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน ให้จัดเป็นผลกระทบระดับสูง ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัยตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน

1.3 การประเมินผลกระทบต่อจานวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นนอกจากข้อ 2 ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

1) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคน ให้จัดเป็นผลกระทบระดับต่ำ

2) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

3) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูงในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายตามวรรคหนึ่งให้คานวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบ ในหนึ่งวันและคานวณความเสียหายโดยตรงเท่านั้น

1.4 การประเมินผลกระทบด้านความมั่นคงของรัฐให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

1) ในกรณีไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

2) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง

หากปรากฏว่ามีผลประเมินที่เป็นผลกระทบในระดับสูงด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด และหากมีผลกระทบในระดับกลางอย่างน้อยสองด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไป ในกรณีที่ไม่เป็นไปตามวรรคหนึ่ง ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับพื้นฐาน

2. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

(1) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ปีละ 1 ครั้ง

(2) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยสำนักงานตรวจสอบภายในเพื่อให้โรงพยาบาลได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

2) มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

(1) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ 1 ครั้ง

(2) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีละ 1 ครั้ง

(3) มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

(4) มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้

- ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทาลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
- ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
- ในกรณีที่มีเครื่องมือสำหรับการตรวจสอบประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

(5) มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ ปีละ 1 ครั้ง ต่อคณะกรรมการนโยบายและพัฒนาสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงของโรงพยาบาลเพื่อดำเนินการต่อไป

(6) มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

(7) ให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ ตามข้อเสนอแนะและผลการประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้การดำเนินการเป็นไปอย่างมีประสิทธิภาพ

ส่วนที่ 5
นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

1) เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของโรงพยาบาล

2) เพื่อเป็นการป้องกันการกระทาผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

3) เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1) งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5)

แนวปฏิบัติ

1) จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของโรงพยาบาลศรีนคร ปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

2) จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของโรงพยาบาล

3) จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหา แนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของโรงพยาบาล

4) จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

5) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายโดยมีการปรับปรุงความรู้อยู่เสมอ

6) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการผู้ใช้งาน