



นโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลศิริราชเมืองใหม่

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของเป็นไปอย่างเหมาะสม มีความมั่นคง ปลอดภัย และสามารถสนับสนุนการดำเนินงานของโรงพยาบาลศิริราชเมืองใหม่ได้อย่างต่อเนื่อง มีการใช้งานระบบใน ลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมาย อื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่โรงพยาบาลศิริราชเมืองใหม่ โรงพยาบาล ศิริราชเมืองใหม่ฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความ สำหรับ ศัพท์ที่ใช้ในงานนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

1. “โรงพยาบาล” หมายความว่า โรงพยาบาลศิริราชเมืองใหม่ ที่ใช้ระบบสารสนเทศ และระบบเครือข่ายและ คอมพิวเตอร์ร่วมกัน
2. “งานการเจ้าหน้าที่” หมายความว่า งานการเจ้าหน้าที่ โรงพยาบาลศิริราชเมืองใหม่
3. “งานสารสนเทศทางการแพทย์” หมายความว่า งานสารสนเทศทางการแพทย์ โรงพยาบาลศิริราชเมืองใหม่
4. “ผู้ใช้งาน” หมายความว่า ผู้บริหาร ผู้ปฏิบัติงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก ที่ได้รับอนุญาต ให้สามารถเข้าใช้งานระบบเครือข่ายของโรงพยาบาล
5. “ผู้ปฏิบัติงาน” หมายความว่า ผู้ปฏิบัติงาน ลูกจ้างทดลองงาน และลูกจ้างชั่วคราวของโรงพยาบาลศิริราชเมือง ใหม่
6. “ผู้ใช้งานที่เกี่ยวข้อง” หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของโรงพยาบาล ที่เข้ามาดำเนิน กิจกรรมภายในโรงพยาบาลศิริราชเมืองใหม่
7. “ผู้ใช้งานภายนอก” หมายความว่า บุคคล หรือนิติบุคคลนอกเหนือจากข้อ (6) และข้อ (7)

8. “ผู้ดูแลระบบ” หมายความว่า หัวหน้างานสารสนเทศทางการแพทย์ เจ้าหน้าที่งานสารสนเทศทางการแพทย์หรือผู้ปฏิบัติงานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแล รักษาระบบสารสนเทศและระบบเครือข่าย ที่ใช้งานอยู่ในโรงพยาบาลศรีเมืองใหม่หรือหน่วยงานที่มีหน้าที่ และรับผิดชอบในการดูแลระบบสารสนเทศและระบบเครือข่าย โดยตรง
9. “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผ่นผัง แผนที่ ภาพถ่าย फिल्म การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
10. “ระบบสารสนเทศ” หมายความว่า ระบบงานของโรงพยาบาลศรีเมืองใหม่ ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการ ทำงานของโรงพยาบาลศรีเมืองใหม่
11. “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของโรงพยาบาลศรีเมืองใหม่ ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบInternet และระบบการสื่อสารอื่นๆ
12. “สินทรัพย์” หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่า สำหรับโรงพยาบาลศรีเมืองใหม่ ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อโรงพยาบาลศรีเมืองใหม่
13. “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่ โดยอ้างไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน(Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง(Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (non-Repudiation) และความน่าเชื่อถือ (Reliability)

14. “สิทธิ์ของผู้ใช้งาน” หมายความว่า ระดับขั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ปฏิบัติงาน และผู้ใช้งานที่เกี่ยวข้อง ได้แก่สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่
15. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
16. “บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงานผู้ใช้งานที่เกี่ยวข้องและผู้ใช้งานภายนอก
17. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือ มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
18. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ซึ่งอาจทำให้ระบบของโรงพยาบาลศรีเมืองใหม่ ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
19. “การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
20. “การยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
21. “SSL (Secure Socket Layer)” หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน
22. “VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

หมวดที่ 1

การกำกับดูแลและบริหารจัดการ IT ระดับองค์กรที่ดี (Governance of Enterprise IT)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อให้แน่ใจว่า โรงพยาบาลศรีเมืองใหม่สามารถบรรลุเป้าหมายที่กำหนดไว้โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากร และข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมาย ขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่โรงพยาบาลศรีเมืองใหม่นำมาใช้งานสามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับโรงพยาบาลศรีเมืองใหม่ โดยโรงพยาบาลศรีเมืองใหม่ต้องพิจารณาดำเนินการอย่างน้อยดังต่อไปนี้

1. นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

1.1 โรงพยาบาลศรีเมืองใหม่ต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และโรงพยาบาลศรีเมืองใหม่ต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจ และสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในโรงพยาบาลศรีเมืองใหม่ เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

1.2 โรงพยาบาลศรีเมืองใหม่ต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลศรีเมืองใหม่

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

2.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศผู้จัดการส่วนเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

- ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย(Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการ เข้า-ออก และการใช้งาน การตรวจสอบระบบต่างๆ เช่น ระบบเตือนอุณหภูมิกายในห้อง ระบบเตือน อัคคีภัย เป็นต้น

- ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีมัลแวร์ หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ ต้องมีตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่ง อีเมล เป็นต้น

- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล

2.3 การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

- ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี
- ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
- ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
- ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

2.4 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่โรงพยาบาลศรีเมืองใหม่ยอมรับได้ จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภท ความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และ ระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

2.5 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

หมวดที่ 2

การรักษาความมั่นคงปลอดภัยของระบบ IT (IT Security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของ IT (Information Security Policy)

o วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

o แนวทางปฏิบัติ

- ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งผิดกฎหมาย หรือขัดต่อศีลธรรมอันดีเป็นต้น
- ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
- ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ
- ห้ามก่อวินาศกรรม ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- ห้ามลักลอบดักจับข้อมูลในเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

o วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในโรงพยาบาลศรีเมืองใหม่

o แนวทางปฏิบัติ

- ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่
- หัวหน้างานสารสนเทศทางการแพทย์ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในงานสารสนเทศทางการแพทย์รับผิดชอบการดูแลระบบสารสนเทศที่โรงพยาบาลศรีเมืองใหม่ใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่
- หัวหน้างานสารสนเทศทางการแพทย์ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลศรีเมืองใหม่
- ผู้ปฏิบัติงานงานสารสนเทศทางการแพทย์ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
- ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของโรงพยาบาลศรีเมืองใหม่ ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

o วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่

o แนวทางปฏิบัติ

1. ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่เข้าปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่

2. ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงานว่าจะไม่เปิดเผยความลับของโรงพยาบาลศรีเมืองใหม่ (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปีภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
3. เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด งานการเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้หัวหน้างานสารสนเทศทางการแพทย์ทราบทันที เมื่อมีเหตุดังนี้
 - การว่าจ้างงาน
 - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
 - การลาออกจากงาน หรือการสิ้นสุดการปฏิบัติหน้าที่และผู้ปฏิบัติงานของโรงพยาบาลศรีเมืองใหม่
 - การโยกย้ายหน่วยงาน
4. ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
5. ผู้ปฏิบัติงานใหม่ของโรงพยาบาลศรีเมืองใหม่ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ
6. หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที

4. การบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management)

1. การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral AccessControl)

▪ วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของโรงพยาบาลศรีเมืองใหม่ให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

▪ แนวทางปฏิบัติ

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้
- งาน

- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่เพื่อประกอบธุรกิจการค้าหรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็กไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
- ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็คทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็คไปในทางเดียวกัน ห้ามเช็คแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของโรงพยาบาลศรีเมืองใหม่ออกนอกโรงพยาบาลศรีเมืองใหม่
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

2. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

▪ วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจ การใช้งานโปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

▪ แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

- มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในโรงพยาบาลศรีเมืองใหม่ตามสิทธิ์การใช้งานที่กำหนด
- มีหน้าที่รับผิดชอบในการติดตั้ง และอัปเดตโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
- ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อโรงพยาบาลศรีเมืองใหม่และ/หรือหน่วยงานแจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ข้อกำหนดสำหรับผู้ใช้งาน
- ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับโรงพยาบาลศรีเมืองใหม่
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่อย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่โรงพยาบาลศรีเมืองใหม่มีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

3. การควบคุมสินทรัพย์ด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์

▪ แนวทางปฏิบัติ

ต้องควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศ อยู่ในสถานะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

1. ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
2. มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
3. ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้

- ในฐานะข้อมูลของระบบ Application นั้นๆ ที่จัดเก็บภายใน Data Center ของโรงพยาบาลศรีเมืองใหม่ การ Export ข้อมูลออกมาจากระบบ Application ไม่สามารถทำได้

- สามารถจัดเก็บใน Shared File (Drive กลาง) ใน ตามสิทธิ์ที่ได้รับ

4. ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

5. การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อก (Lock) หน้าจอโดยอัตโนมัติ หลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที

6. ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกโรงพยาบาลศรีเมืองใหม่ทุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของโรงพยาบาลศรีเมืองใหม่ออกนอกโรงพยาบาลศรีเมืองใหม่

7. ระมัดระวังและดูแลทรัพย์สินของโรงพยาบาลศรีเมืองใหม่ ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเล็กน้อย ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

4. การใช้งานจดหมายอิเล็กทรอนิกส์

▪ วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และ

มาตรการรักษาความปลอดภัยข้อมูลข่าวสารของโรงพยาบาลศรีเมืองใหม่ ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญ และตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งานต้อง เข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

■ แนวทางปฏิบัติ

1. ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการ กระทำความผิด เกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กฎหมายที่เกี่ยวข้อง และนโยบายและ ข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่โรงพยาบาลศรีเมืองใหม่กำหนด
2. หน่วยงานหรือผู้ปฏิบัติงานผู้ให้บริการจดหมายอิเล็กทรอนิกส์ของ โรงพยาบาลศรีเมืองใหม่ จะต้องใช้จดหมาย อิเล็กทรอนิกส์ เพื่อผลประโยชน์ของโรงพยาบาลศรีเมืองใหม่
3. ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียน ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากการเจ้าหน้าที่
4. ไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ เว้นแต่จะได้รับการ ยินยอมจากเจ้าของผู้ให้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมาย อิเล็กทรอนิกส์ของตน
5. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
6. การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของโรงพยาบาลศรีเมืองใหม่ ผู้ใช้งานจะต้องใช้ระบบ จดหมายอิเล็กทรอนิกส์ของโรงพยาบาลศรีเมืองใหม่เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ใน กรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลศรีเมืองใหม่ขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้ว เท่านั้น
7. การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อ ไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของ โรงพยาบาลศรีเมืองใหม่ หรือก่อให้เกิดความเสียหายต่อโรงพยาบาลศรีเมืองใหม่
8. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลศรีเมืองใหม่ เพื่อเผยแพร่ ข้อมูล ข้อความรูปภาพ หรือสิ่งอื่น ใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมายหมิ่นต่อสถาบันพระมหากษัตริย์ หรือ กระทบต่อการดำเนินงานของโรงพยาบาลศรีเมืองใหม่ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของ โรงพยาบาลศรีเมืองใหม่

9. ห้ามผู้ให้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีกรกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ให้บริการ เป็นผู้รับผิดชอบการกระทำดังกล่าว
10. ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่(Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น
11. ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของโรงพยาบาลศรีเมืองใหม่ให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของโรงพยาบาลศรีเมืองใหม่
12. การส่งข้อมูลข่าวสารที่เป็นความลับโรงพยาบาลศรีเมืองใหม่ ควรมีการเข้ารหัสข้อมูลข่าวสารนั้นและไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
13. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง
14. กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ
15. หากผู้ให้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำผิด เกิดขึ้นในโรงพยาบาลศรีเมืองใหม่ ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของโรงพยาบาลศรีเมืองใหม่
16. การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ให้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการเท่านั้น ผู้ดูแลระบบและโรงพยาบาลศรีเมืองใหม่ไม่มีส่วนเกี่ยวข้องใดๆ

5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

การใช้งานระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่

▪ วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่ เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่างๆ ผ่านระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่

■ แนวทางปฏิบัติ

1. งานสารสนเทศทางการแพทย์ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
2. เครื่องคอมพิวเตอร์ของโรงพยาบาลศรีเมืองใหม่ ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน
3. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
4. ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของโรงพยาบาลศรีเมืองใหม่
5. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของโรงพยาบาลศรีเมืองใหม่ ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของโรงพยาบาลศรีเมืองใหม่
6. ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
7. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
8. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของโรงพยาบาลศรีเมืองใหม่ เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
9. ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อโรงพยาบาลศรีเมืองใหม่ รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของโรงพยาบาลศรีเมืองใหม่ในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่โรงพยาบาลศรีเมืองใหม่กำหนดไว้อย่างเคร่งครัด
10. ข้อปฏิบัติสำหรับผู้ที่ได้รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้น
 1. ผู้ที่ได้รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยได้ (ช่วงเวลาปัจจุบัน หมายถึงขณะทำการรักษาเท่านั้น)
 2. กรณีที่ผู้ป่วยช่วยเหลือตัวเองไม่ได้ หรือหมดสติ ต้องได้รับความยินยอมจากญาติในการรักษาและเข้าถึงข้อมูลผู้ป่วย

3. เก็บรวบรวมข้อมูลผู้ป่วยเท่าที่จำเป็น
4. การเข้าถึงข้อมูลผู้ป่วย ของนักศึกษาแพทย์ หรือนักศึกษาฝึกประสบการณ์ ต้องอยู่ในการกำกับดูแลของพี่เลี้ยง ที่โรงพยาบาลมอบหมายอย่างเคร่งครัด
5. ห้ามนำข้อมูลของผู้ป่วย ไปเผยแพร่ให้บุคคลที่ 3 ทราบ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล
6. หากผู้ที่รับผิดชอบดูแลรักษาผู้ป่วย ต้องการเข้าถึงข้อมูลผู้ป่วยนอกช่วงเวลาปัจจุบัน ที่ทำการรักษาต้องทำหนังสือเป็นลักษณะอักษร ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลศรีเมืองใหม่ และเข้าถึงข้อมูล หรือใช้ข้อมูล ตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น ห้ามใช้นอกเหนือวัตถุประสงค์
7. กรณีนักศึกษาแพทย์ หรือนักศึกษาฝึกประสบการณ์ ที่ต้องการข้อมูลผู้ป่วยไปปรึกษาอาจารย์หรือทำรายงาน การขอข้อมูลผู้ป่วย ต้องใช้ตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น ห้ามใช้นอกเหนือวัตถุประสงค์ ไม่ระบุข้อมูลส่วนบุคคล เช่น ชื่อ-สกุล, รูปถ่าย และต้องทำหนังสือเป็นลักษณะอักษรขออนุญาตจากผู้อำนวยการโรงพยาบาลศรีเมืองใหม่
8. กรณีนักศึกษาแพทย์ หรือนักศึกษาฝึกประสบการณ์ ต้องการเข้าถึงข้อมูลผู้ป่วย ต้องได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลเมืองจันทร์ก่อน และอยู่ในการกำกับดูแลของพี่เลี้ยง ที่โรงพยาบาลมอบหมายอย่างเคร่งครัด
9. ผู้ที่รับผิดชอบดูแลรักษาผู้ป่วย มีหน้าที่ต้องป้องกันดูแลรักษาไว้ซึ่งความลับบุคคล เช่น ชื่อ-สกุล, รูปถ่ายผู้ป่วย, รูปถ่ายเวชระเบียน และความถูกต้อง ความพร้อมใช้ของข้อมูลตลอดจน เอกสารเวชระเบียนของผู้ป่วย
10. ห้ามผู้รับผิดชอบดูแลรักษาผู้ป่วย เผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณีนอกจากได้รับมอบหมายให้ ดำเนินการจากผู้อำนวยการโรงพยาบาลศรีเมืองใหม่
11. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกันให้ดำเนินการโดยเคร่งครัด เช่น ไม่ใช้ให้ผู้ป่วยเป็นผู้ถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุดอื่นๆ
12. ห้ามส่งข้อมูลผู้ป่วยโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ส่งทาง LINE หรือ social media อื่นๆ
13. ไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
14. ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูล เช่น CD-ROM, USB Drive, External Hard Disk อุปกรณ์เครือข่าย เช่น Hub, Switch, Wi-Fi Router ฯลฯ มาเชื่อมต่อกับ เครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่ยกเว้นได้รับอนุญาตจากผู้อำนวยการ

6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

▪ วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล้วงรู้ หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มีได้มีอำนาจหน้าที่เกี่ยวข้อง

▪ แนวทางปฏิบัติ

1. การบริหารจัดการข้อมูล

1. ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภทรวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่

2. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส(Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น

3. ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input)ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กันต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

4. ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโรงพยาบาลศรีเมืองใหม่ เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

2. การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

1. ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2. ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3. ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น โรงพยาบาลศรีเมืองใหม่จะใช้ปัจจัยประกอบการพิจารณาในภาพรวม ดังต่อไปนี้

- ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
- ควรควบคุมการใช้งานของผู้ใช้ที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 1 เดือน เป็นต้น

4. ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มีได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มีได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

5. ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิ์ดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6. ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

1. ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น โรงพยาบาลศรีเมืองใหม่จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

- ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)

- ควรใช้อักขระพิเศษประกอบ เช่น : ; < > \$ @ # เป็นต้น
 - สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 1 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 2 เดือน
 - ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด
 - ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd” เป็นต้น
 - ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
 - ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
 - ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt -Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน
 - ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
 - ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
 - ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
 - สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ SAP เป็นต้น ทางผู้ดูแลจะมีการแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด
2. ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง
 3. ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้นพร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น

7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

▪ วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล้วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่างๆ ที่โรงพยาบาลศรีเมืองใหม่ควรจัดให้มีภายใน Data Center Room

▪ แนวทางปฏิบัติ

1. การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

1. ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน Data Center Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น

2. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือ ผู้ปฏิบัติงานที่เกี่ยวข้อง ควบคุมดูแลการทำงานตลอดเวลา เป็นต้น

3. ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

4. ควรจัด Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย(Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone) ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้นเพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

2. การป้องกันความเสียหาย

1. ระบบป้องกันไฟไหม้

▪ ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

- Data Center Room หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

2. ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า
- ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง

3. ระบบควบคุมอุณหภูมิและความชื้น

- ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ(Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

4. ระบบเตือนภัยน้ำรั่ว

- ในกรณีที่มีการยกระดับพื้นของ Data Center Room เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและ/หรือสายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลาหาก Data Center Room ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

▪ วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่เป็นไปอย่างถูกต้องและมั่นคงปลอดภัยป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี

▪ แนวทางปฏิบัติ

1. จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของโรงพยาบาลศรีเมืองใหม่เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ
2. กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ เป็นต้น
3. ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
4. ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

5. ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

6. ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล

7. ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกโรงพยาบาล ศรีเมืองใหม่

8. ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

9. ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น

- เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของโรงพยาบาลศรีเมืองใหม่ ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

- ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

- ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

- ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางโรงพยาบาลศรีเมืองใหม่ได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่น นอกเหนือจากที่โรงพยาบาลศรีเมืองใหม่เตรียมไว้ให้ ต้องแจ้งงานสารสนเทศทางการแพทย์เพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

(Communications Security)

▪ วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ

▪ แนวทางปฏิบัติ

1. การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

1.1 กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย

1.2 ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับโรงพยาบาลศรีเมืองใหม่

2. การถ่ายโอนข้อมูล (Information Transfer)

1. ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
2. ต้องมีการลงนามในสัญญาระหว่างโรงพยาบาลศรีเมืองใหม่และหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของโรงพยาบาลศรีเมืองใหม่ (Non-Disclosure Agreement: NDA)

10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

▪ วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงาน คอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

▪ แนวทางปฏิบัติ

1. ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษรโดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน
2. ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
3. ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

▪ การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

3.1 การร้องขอ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น

- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
- ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อ การปฏิบัติตามกฎเกณฑ์ของทางราชการ

3.2 การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (DevelopEnvironment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน(Availability) ของระบบงาน ตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

3. การทดสอบ

- ผู้ที่ร้องขอและงานสารสนเทศทางการแพทย์รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

4. การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

5. การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของ

ระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน ขั้นตอนการทำงาน

ของโปรแกรมและ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

6. การทดสอบหลังการใช้งาน (Post-Implementation Test)

- ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

7. การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง

11. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)

▪ วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของโรงพยาบาลศรีเมืองใหม่ที่มีการเข้าถึงโดย IT Outsourcing และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

▪ แนวทางปฏิบัติ

1. ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของโรงพยาบาลศรีเมืองใหม่ เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของโรงพยาบาลศรีเมืองใหม่ โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของโรงพยาบาลศรีเมืองใหม่
2. ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของโรงพยาบาลศรีเมืองใหม่ เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของโรงพยาบาลศรีเมืองใหม่ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
3. ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการ ภายนอกอย่างสม่ำเสมอ
4. หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

▪ วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

▪ แนวทางปฏิบัติ

1. ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง ปลอดภัยของโรงพยาบาลศรีเมืองใหม่
2. ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
3. หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
4. กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว
5. ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภท ของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน
6. ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมายหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

13. การบริหารความต่อเนื่องในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

▪ วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของโรงพยาบาลศรีเมืองใหม่ อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของโรงพยาบาลศรีเมืองใหม่

▪ แนวทางปฏิบัติ

1. งานสารสนเทศทางการแพทย์ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของโรงพยาบาลศรีเมืองใหม่

2. ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อยปีละ 1 ครั้ง
 3. ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
 4. ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง
- จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 1 ตุลาคม 2568



(นายวศรัณย์ วัฒนธีรางกูร)

ผู้อำนวยการโรงพยาบาลศรีเมืองใหม่