<table>
<tr><td rowspan="2">BANCHANG hospital
โรงพยาบาลบ้านฉาง</td><td>ระเบียบปฏิบัติ (Work procedure)
เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ดูแลระบบสารสนเทศ</td><td>หน้า : ๑ / ๑๐</td></tr>
<tr><td colspan="2">รหัสเอกสาร : WP-DH-๐๐๐๑-๐๐๒
ทบทวนครั้งที่ : ๑ วันที่ทบทวน : ๒๕ ก.พ. ๒๕๖๘</td></tr>
<tr><td colspan="2">ชื่อหน่วยงาน : กลุ่มงานสุขภาพดิจิทัล</td><td>วันที่อนุมัติ : ๐๗ มี.ค. ๒๕๖๘</td></tr>
<tr><td colspan="2">ผู้ตรวจสอบ :
(นางอรปรียา แก้วคำสอน)
เจ้าพนักงานเวชสถิติชำนาญงาน
หัวหน้ากลุ่มงานสุขภาพดิจิทัล</td><td>ผู้อนุมัติ :
(นายสุรชัย คำภักดี)
ผู้อำนวยการโรงพยาบาลบ้านฉาง</td></tr>
</table>

๑. วัตถุประสงค์

ระเบียบปฏิบัติงานนี้เพื่อเป็นแนวทางการบริหารความมั่นคงปลอดภัย การควบคุม และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโรงพยาบาลบ้านฉาง

๒. ขอบข่าย

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับผู้ดูแลระบบสารสนเทศ หรือเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

๓. ความรับผิดชอบ

ผู้ดูแลระบบสารสนเทศของโรงพยาบาลบ้านฉาง ต้องปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

๓.๑ ศึกษา ทำความเข้าใจ และปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓.๒ เมื่อมีข้อสงสัยเกี่ยวกับการปฏิบัติ ให้ปรึกษาผู้บังคับบัญชา หรือกลุ่มภารกิจสุขภาพดิจิทัล

๓.๓ เมื่อพบปัญหา การปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้รายงานข้อมูลได้ทุกช่องทาง ได้แก่ รายงานผู้บังคับบัญชาโดยตรง การเขียนรายงานอุบัติการณ์ เป็นต้น

๔. คำจำกัดความที่เกี่ยวข้อง

๔.๑. ผู้ดูแลระบบเทคโนโลยีสารสนเทศ หมายถึง เจ้าหน้าที่กลุ่มภารกิจสุขภาพดิจิทัล ที่ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

๔.๒. ระบบสารสนเทศโรงพยาบาล หมายถึง ระบบคอมพิวเตอร์ที่ใช้สำหรับบริหารงานโรงพยาบาล ซึ่งประกอบไปด้วย ข้อมูลผู้ป่วย ข้อมูลการรักษา และข้อมูลอื่นๆ ที่เกี่ยวข้องกัน

๕. รายละเอียด

๕.๑. การควบคุมการเข้าถึงสารสนเทศ (Access Control)

๕.๑.๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับ อนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล ให้ทำหนังสือ ขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณีเพื่อให้ ความเห็นชอบและอนุญาตก่อน

๕.๑.๒. กำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอโดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญาตนั้น

ผู้ใช้งานระบบสารสนเทศ	สิทธิการเข้าถึงข้อมูล/ระบบข้อมูล					
	อ่านอย่างเดียว	สร้างข้อมูล	ป้อนข้อมูล	แก้ไขข้อมูล	ลบข้อมูล	อนุมัติการใช้ข้อมูล
ผู้บริหารโรงพยาบาล	✓					✓
เจ้าหน้าที่ผู้ใช้ระบบสารสนเทศ	✓	✓	✓	✓	✓	
กลุ่มผู้ดูแลระบบ	✓	✓	✓	✓	✓	

๕.๑.๓. กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๕.๑.๔. ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามที่หัวหน้าหน่วยงานมอบหมาย ดังนี้

๑. อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒. กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างสม่ำเสมอ

๓. ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

๕.๑.๕. จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการ รักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสาร อิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๑) จัดแบ่งระดับชั้นการเข้าถึง

๑. ระดับชั้นสำหรับผู้บริหาร
๒. ระดับชั้นสำหรับผู้ใช้งานทั่วไป
๓. ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๒) จัดแบ่งลำดับชั้นความลับของข้อมูล

๑. ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๒. ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงมาก

๓. ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๔. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๓) จัดแบ่งประเภทของข้อมูล

๑. ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบายข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชีข้อมูลการจราจรทางคอมพิวเตอร์

๒. ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการ รักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

๔) จัดแบ่งระดับชั้นการเข้าถึง

๑. ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น

๒. ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป

๓. ระดับขั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิที่ได้รับมอบหมายตามอำนาจหน้าที่

๕.๑.๖. รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๕.๑.๗. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

๕) การรับ-ส่งข้อมูลด้วย SSL, VPN หรือ XML Encryption ผ่านระบบเครือข่ายต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๗) กำหนดเวลาการเข้าถึงระบบสารสนเทศหากมีการบันทึกแก้ไขข้อมูลสาระบบคดีอิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเข้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั้น เนื่องจากระบบจะทำการประมวลผลตอนเที่ยงคืน

๘) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนดส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

๕.๑.๘. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิเกี่ยวข้องกับระบบสารสนเทศ

๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๕.๑.๙. การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความขึ้น

๒) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

๓) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

๔) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

๕) ตรวจสอบสอดส่องดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ภายในห้องศูนย์ข้อมูล (Data Center)

๖) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกัน หนู นก กระรอก แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับสัญญาณ การตัดสายสัญญาณอันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

๗) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่างๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อป้องกัน การเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

๕.๒. เจ้าหน้าที่กลุ่มงานสุขภาพดิจิทัล

๕.๒.๑. การบริการจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบ เทคโนโลยีสารสนเทศ

๕.๒.๒. กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศ

๑) กำหนดสิทธิเฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร โดยมีระบบที่เกี่ยวข้องได้แก่

-ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application)

-จดหมายอิเล็กทรอนิกส์ (E-Mail)

-ระบบเครือข่ายไร้สาย (Wireless LAN)

-ระบบอินเทอร์เน็ต (Internet)

๕.๒.๓. ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างโดยปฏิบัติตามแนวทาง ดังนี้

๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

๓) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๔) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิในระดับสูง ด้วยความถี่มากกว่าผู้ใช้งาน

๕) เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ถอดถอนสิทธิภายใน ๑ - ๒ วันทำการ

๕.๒.๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๔) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๕) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕.๒.๕. บริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ

ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

๑) ผู้ดูแลระบบต้องกำหนดขั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่าน ระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ

๒) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๓) ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงข้อมูลโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้น ความลับข้อมูล

๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่ เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การใช้งานรหัสผ่านผู้ใช้งาน”

๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๗) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อยปีละ ๑ ครั้งเพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๘) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

๕.๒.๖. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)

ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกระทรวงสาธารณสุขหรือหน่วยงานที่มาขอเชื่อมโยง

๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมในกรณีที่ระบบไม่มี มาตรการป้องกันเพียงพอ

๕.๒.๗. การตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy)

๑) IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัย ของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๒) IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๓) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๔) ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการ ก่อนการติดตั้งและเปิดให้บริการ

๕) โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๖) ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

๗) ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๘) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่าย ของระบบสารสนเทศตามปกติ

๙) เครื่องแม่ข่ายที่มีการติดตั้ง Host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๑๐) จะต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและ ไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทราบทันที ที่ตรวจพบ

๑๑) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๑๒) ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๑๓) หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๑๔) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล

บ้านฉางการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงาน ของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๕.๒.๘. การสำรองข้อมูล

๑) ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

๒) ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๓) ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน

๔) ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๑. กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๒. กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๓. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน เวลา ชื่อ ข้อมูล ที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔. ตรวจสอบค่า Config ต่าง ๆ ของระบบการสำรองข้อมูล

๕. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๖. จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงทอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๘. ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๙. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๑๐. ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

๑๑. กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๕) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

๑. มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒. มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๓. มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๔. มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล มีการกำหนดขั้น และทดสอบกู้คืนข้อมูลที่สำรองไว้

๕. มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๖. การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๖) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๗) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๘) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่ จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๙) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๕.๒.๙. ผู้ใช้งานระบบ

ให้ผู้ดูแลระบบสารสนเทศ ปฏิบัติตามระเบียบปฏิบัติ (Work Procedure) เรื่อง : ความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศสำหรับผู้ใช้งานระบบสารสนเทศ หัวข้อผู้ใช้งานระบบ

๖. ภาคผนวก

๖.๑. ผู้รับผิดชอบ

๖.๑.๑. คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีหน้าที่กำหนดระเบียบปฏิบัติที่เหมาะสม และเป็นไปตามประกาศและระเบียบที่เกี่ยวข้อง

๖.๑.๒. คณะกรรมการบริหารโรงพยาบาล มีหน้าที่ สื่อสารนโยบายและแนวปฏิบัติตามที่คณะทำงานพัฒนาคุณภาพ ระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้กำหนด รวมถึง กำกับ ติดตาม การปฏิบัติของบุคลากร ในหน่วยงานให้เป็นไปในแนวทางเดียวกัน

๗. เอกสารอ้างอิง

๗.๑ ประกาศโรงพยาบาลบ้านฉางเรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลบ้านฉางลงวันที่ ๓ มกราคม ๒๕๖๘

๗.๒ ประกาศโรงพยาบาลบ้านฉางเรื่อง แนวปฏิบัติในการรักษามั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลบ้านฉางลงวันที่ ๑๐ มีนาคม ๒๕๖๘

๗.๓ ประกาศโรงพยาบาลบ้านฉางเรื่อง ระเบียบปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖ (สำหรับเจ้าหน้าที่ทั่วไปของโรงพยาบาลบ้านฉาง) ลงวันที่ ๑๐ มีนาคม ๒๕๖๘

๗.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และระเบียบว่าด้วยการรักษาความลับ ของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑

๗.๕ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลง เอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๗.๖ ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑