

 โรงพยาบาลอุดรธานี Udon Thani Hospital	นโยบาย เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ดูแลระบบสารสนเทศ	หน้า 2/10 รหัสเอกสาร : QM - IT - 002 แก้ไขครั้งที่ : - วันที่แก้ไข : 01 สค. 2568

1. นโยบาย :

ระเบียบปฏิบัติงานนี้เพื่อเป็นแนวทางการบริหารความมั่นคงปลอดภัย การควบคุม และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโรงพยาบาลอุดรธานี

2. วัตถุประสงค์ :

เพื่อเป็นแนวทางการบริหารความมั่นคงปลอดภัย การควบคุม และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโรงพยาบาลอุดรธานี

3. ขอบเขต :

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับผู้ดูแลระบบสารสนเทศ หรือเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

4. กลุ่มเป้าหมาย :

ผู้ดูแลระบบสารสนเทศของโรงพยาบาล ต้องปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

5. นิยามศัพท์/คำจำกัดความ :

กฎระเบียบการควบคุมดูแลเครื่องคอมพิวเตอร์และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่าย

- 1) "โรงพยาบาล" หมายถึง โรงพยาบาลศูนย์อุดรธานี
- 2) "ศูนย์คอมพิวเตอร์" หมายถึง กลุ่มงานภารกิจสุขภาพดิจิทัล โรงพยาบาลศูนย์อุดรธานี
- 3) "เครื่องคอมพิวเตอร์และเครือข่าย" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของ โรงพยาบาล ทั้งที่อยู่ภายใน และภายนอกส่วนกลาง รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ อุปกรณ์เครือข่ายที่ เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในโรงพยาบาล ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ ที่มีได้จัด ให้เป็นสื่อสาธารณะ
- 4) "หน่วยงาน" หมายถึง หน่วยงานต่างๆ ของโรงพยาบาลศูนย์อุดรธานี
- 5) "ผู้ดูแลระบบ" หมายถึง ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ควบคุมดูแลระบบเครื่องคอมพิวเตอร์และเครือข่ายได้

6. ขั้นตอน/วิธีปฏิบัติ :

6.1 การควบคุมการเข้าถึงสารสนเทศ (Access Control)

6.1.1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

 โรงพยาบาลอุดรธานี Udon Thani Hospital	นโยบาย เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ดูแลระบบสารสนเทศ	หน้า 3/10
		รหัสเอกสาร : QM - IT - 002 แก้ไขครั้งที่ : - วันที่แก้ไข : 01 สค. 2568

6.1.2 กำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอโดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญัตินั้น

ผู้ใช้งานระบบสารสนเทศ	สิทธิการเข้าถึงข้อมูลระบบข้อมูล					
	อ่านอย่างเดียว	สร้างข้อมูล	ป้อนข้อมูล	แก้ไขข้อมูล	ลบข้อมูล	อนุมัติการใช้ข้อมูล
ผู้บริหารโรงพยาบาล	/					/
เจ้าหน้าที่ผู้ใช้ระบบสารสนเทศ	/	/	/	/	/	
กลุ่มผู้ดูแลระบบ	/	/	/	/	/	

6.1.3 กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

6.1.4 ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามที่หัวหน้าหน่วยงานมอบหมาย ดังนี้

- 1) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้อีกเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- 2) กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างสม่ำเสมอ
- 3) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

6.1.5 จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ. 2561 ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

1) จัดแบ่งระดับชั้นการเข้าถึง

- 1.1) ระดับชั้นสำหรับผู้บริหาร
- 1.2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- 1.3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

2) จัดแบ่งลำดับชั้นความลับของข้อมูล

- 2.1) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- 2.2) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงมาก
- 2.3) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
4. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

3) จัดแบ่งประเภทของข้อมูล

3.1) ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชีข้อมูลการจราจรทางคอมพิวเตอร์

3.2) ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

4) จัดแบ่งระดับชั้นการเข้าถึง

4.1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น

4.2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป

4.3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้ โดยสิทธิที่ได้รับมอบหมายตามอำนาจหน้าที่

6.1.6 รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553

6.1.7 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

1) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

2) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

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

6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษาตรวจสอบให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

7) กำหนดเวลาการเข้าถึงระบบสารสนเทศหากมีการบันทึกแก้ไขข้อมูลสารบบคืออิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเช้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั้น เนื่องจากระบบจะทำการประมวลผลตอนเที่ยงคืน

8) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนดส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา 15 นาที

6.1.8 มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

- 1) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิเกี่ยวข้องกับระบบสารสนเทศ
- 2) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

6.1.9 การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

- 1) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น
- 2) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน
- 3) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน
- 4) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอกและให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ
- 5) ตรวจสอบสื่อดูดข้อมูลและสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในห้องศูนย์ข้อมูล (Data Center)
- 6) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกัน หนู นก กระรอก แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับสัญญาณการตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้
- 7) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกันแล้วให้จัดเก็บสายสัญญาณต่างๆ ไว้ในตู้ Rack และปิดใส่สักรักรกญแจให้สนิทเพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

6.2 เจ้าหน้าที่กลุ่มภารกิจสุขภาพดิจิทัล

6.2.1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

- 1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
- 2) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน
- 3) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ 3)
- 4) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

 โรงพยาบาลอุดรธานี Udon Thani Hospital	นโยบาย เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ดูแลระบบสารสนเทศ	หน้า 6/10
		รหัสเอกสาร : QM - IT - 002 แก้ไขครั้งที่ : - วันที่แก้ไข : 01 ส.ค. 2568

6.2.2 กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศ

1) กำหนดสิทธิเฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร โดยมีระบบที่เกี่ยวข้องได้แก่ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet)

6.2.3 ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างโดยปฏิบัติตามแนวทาง ดังนี้

- 1) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน
- 2) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่
- 3) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน
- 4) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน
- 5) เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ถอดถอนสิทธิภายใน 1 - 2 วันทำการ

6.2.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- 1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- 2) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- 3) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการให้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
- 4) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)
- 5) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง
- 6) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

6.2.5 บริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

- 1) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ
- 2) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- 3) ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงข้อมูลโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

5) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การใช้งานรหัสผ่านผู้ใช้งาน”

6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

7) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

8) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมายระเบียบข้อบังคับที่เกี่ยวข้อง

6.2.6 ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)

ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกระทรวงสาธารณสุขหรือหน่วยงานที่มาขอเชื่อมโยง

- 1) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน
- 2) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- 3) พิจารณามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน
- 4) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- 5) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มี

มาตรการป้องกันเพียงพอ

6.2.7 การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention

System Policy: IDS/IPS Policy)

1) IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงานให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

2) IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมดรวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

3) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

4) ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

5) โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

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

7) ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

8) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

9) เครื่องแม่ข่ายที่มีการติดตั้ง Host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

10) จะต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทราบทันทีที่ตรวจพบ

11) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

12) ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

13) หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

14) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล อุดรธานีการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

6.2.8 การสำรองข้อมูล

1) ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

2) ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

3) ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

4) ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(1) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(3) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน เวลาชื่อข้อมูลที่สำรอง สำเร็จไม่สำเร็จ เป็นต้น

(4) ตรวจสอบค่าคอนฟิกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล

(5) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(6) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

- (7) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- (8) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- (9) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้
- (10) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่เกิดขึ้น
- (11) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้
- 5) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย
- (1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- (2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้แผ่นดินไหวการชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
- (3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- (4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- (5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการ เครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- (6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น
- 6) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง
- 7) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- 8) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่เกิดขึ้นเพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ
- 9) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

6.2.9 ผู้ใช้งานระบบ

ให้ผู้ดูแลระบบสารสนเทศปฏิบัติตามระเบียบปฏิบัติ (Work Procedure) เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ใช้งานระบบสารสนเทศ หัวข้อผู้ใช้งานระบบ

	นโยบาย เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ดูแลระบบสารสนเทศ	หน้า 10/10
		รหัสเอกสาร : QM - IT - 002 แก้ไขครั้งที่ : - วันที่แก้ไข : 01 ส.ค. 2568

7. เอกสารอ้างอิง :

- 7.1 ประกาศโรงพยาบาลอุดรธานี เรื่อง ระเบียบปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ. 2566 (สำหรับเจ้าหน้าที่ทั่วไปของโรงพยาบาลอุดรธานี) ลงวันที่ 14 กรกฎาคม 2566
- 7.2 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ. 2561
- 7.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553
- 7.4 ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

8. ตัวชี้วัด :

ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ดูแลควบคุมเครื่องคอมพิวเตอร์และเครือข่ายได้ ปฏิบัติตามระเบียบ 100 %

9. ภาคผนวก :

9.1 ผู้รับผิดชอบ

9.1.1 คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีหน้าที่กำหนดระเบียบปฏิบัติที่เหมาะสมและเป็นไปตามประกาศและระเบียบที่เกี่ยวข้อง

9.1.2 คณะกรรมการบริหารโรงพยาบาล มีหน้าที่ สื่อสารนโยบายและแนวปฏิบัติตามที่ คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้กำหนด รวมถึงกำกับ ติดตาม การปฏิบัติของบุคลากรในหน่วยงานให้เป็นไปในแนวทางเดียวกัน