

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล
โรงพยาบาลบ้านด่าน
อำเภอบ้านด่าน จังหวัดบุรีรัมย์

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของโรงพยาบาลบ้านด่าน สามารถให้บริการได้อย่างต่อเนื่อง
2. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
3. เพื่อให้ผู้ใช้งานได้รับการรับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ 1 การรักษาความปลอดภัยฐานข้อมูล

ข้อ 1 กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

- (1) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน
- (2) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้
 - (2.1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง
 - อ่านอย่างเดียว
 - สร้างข้อมูล
 - ป้อนข้อมูล
 - แก้ไข
 - อนุมัติ
 - ไม่มีสิทธิ์
 - (2.2) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management) ที่ได้กำหนดไว้
 - (2.3) ผู้ใช้งานต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ
- (3) ขั้นตอนการปฏิบัติเพื่อการจัดการเก็บข้อมูล
 - (3.1) จัดแบ่งประเภทข้อมูล
 - ข้อมูลสารสนเทศด้านการบริหาร เข้า ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
 - (3.2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ
 - ข้อมูลที่มีระดับความสำคัญมากที่สุด
 - ข้อมูลที่มีระดับความสำคัญปานกลาง
 - ข้อมูลที่มีระดับความสำคัญน้อยที่สุด

(3.3) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(3.4) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(3.5) การกำหนดเวลาที่ได้เข้าถึง

(3.6) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ 2 ข้อมูลข่าวสารสนเทศทุกประเภทในฐานะข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ 3 การปฏิบัติที่เกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.2544 และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ เรื่อง แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ข้อ 12

ข้อ 4 ผู้ดูแลระบบของศูนย์คอมพิวเตอร์เป็นผู้มีสิทธิ์และอำนาจในการพิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log fire) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ 5 ในกรณีฐานข้อมูลที่มีการใช้งานร่วมกันระหว่างหน่วยงาน หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากหน่วยงานภายนอกให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างโรงพยาบาล บ้านด่าน กับหน่วยงานภายนอก ดังต่อไปนี้

- (1) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง
- (2) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น
- (3) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล
- (4) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ
- (5) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น
- (6) กำหนดสิทธิ์การเข้าถึงข้อมูล
- (7) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

- (8) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กฎเกณฑ์ที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ 2 การสำรองข้อมูล

ข้อ 6 พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ 7 กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ 8 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของโรงพยาบาลบ้านด่าน พร้อมกำหนดระบบสารสนเทศที่จัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

ข้อ 9 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- (1) กำหนดประเภทของข้อมูลที่ต้องการทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- (2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
- (3) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- (4) จัดการข้อมูลสำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

ข้อ 10 ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

- (1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- (2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรฐานเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบได้
- (3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- (4) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- (5) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ 11 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

