ประกาศโรงพยาบาลบ้านด่าน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบ้านด่าน

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลบ้านด่าน เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่างๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลบ้านด่าน และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และกฎหมายอื่นๆ ที่เกี่ยวข้อง โรงพยาบาลบ้านด่านจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลบ้านด่าน ทำให้ดำเนินงานได้อย่างปลอดภัย และต่อเนื่อง

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลบ้านด่านได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริการ เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลบ้านด่าน ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะมีการทบทวนนโยบายปีละ ๑ ครั้ง

อาศัยอำนาจตามในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โรงพยาบาลบ้านด่านจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบ้านด่าน ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลบ้านด่าน” เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลบ้านด่าน กำหนดประเด็นสำคัญดังต่อไปนี้

๒.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๒.๑.๑ ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒.๑.๒ นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาลบ้านด่าน

๒.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๒.๑.๔ กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๕ กำหนดให้ทบทวนและปรับปรุงนโยบายปีละ ๑ ครั้ง

๒.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๖ ส่วน คือ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงผู้ใช้งาน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

แนวปฏิบัติในด้านรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลบ้านด่าน พ.ศ.๒๕๖๒ ซึ่งกำหนดผู้รับผิดชอบตาม ซึ่งสาระสำคัญ มีดังต่อไปนี้

(๑) นโยบายควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลบ้านด่าน

๒) หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติ ดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๒) นโยบายเกี่ยวกับการสำรองและการกู้คืนข้อมูล กำหนดให้มีการจัดทำระบบสำรองข้อมูลสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และกำหนดให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อป้องกันการหยุดชะงักในการให้บริการสารสนเทศของโงพยาบาลบ้านด่าน

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลบ้านด่าน

๒) หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติ ดังต่อไปนี้

๑) แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๒) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๓ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลบ้านด่านเกิดความเสียหาย หรือได้รับอันตรายจากภัยคุกคามทางด้านต่างๆ ผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย ละเว้น หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาลบ้านด่านเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๔ ให้ใช้แนวปฏิบัติในการรักษาความมันคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

ข้อ ๕ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่.....๒.....มกราคม.....พ.ศ. ๒๕๖๗

(นายศาสตรา เข็มบุบผา)
ผู้อำนวยการโรงพยาบาลบ้านด่าน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบ้านด่าน

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดหลักเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ (๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ หรือเจ้าของข้อมูล หรือเจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ (๒) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

ข้อ (๓) ผู้ดูแลระบบ จะต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๑.๒ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายรายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๓ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหารโรงพยาบาลบ้านด่าน
- ระดับชั้นสำหรับผู้ดูแลระบบของโรงพยาบาลบ้านด่าน
- ระดับชั้นสำหรับเจ้าหน้าที่ของโรงพยาบาลบ้านด่าน
- ระดับชั้นสำหรับบุคคลทั่วไปมาใช้บริการของโรงพยาบาลบ้านด่าน

ข้อ (๔) ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ (๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๖) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๗) กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงผู้ใช้งาน (User Access Management)

ข้อ (๘) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูและระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ (๙) ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ (๑๐) ผู้ดูแลระบบ ต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ (๑๑) การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้และรหัสผ่านต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) ในกรณีที่มีความจำเป็นต้องใช้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นกำหนดระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับ ว่าสามารถเข้าถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ (๑๒) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงชั้นตุละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๖) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ (๑๓) ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่าน พิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่เชื่อมโยงเข้าด้วยกัน เช่น ระหว่างโรงพยาบาลบ้านด่านกับหน่วยงานที่ขอมาเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคคลใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ (๑๔) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งประกอบด้วยตัวเลข ตัวอักษร และตัวอักษรพิเศษ

(๓) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๔) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคล ไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๖) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ (๑๕) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

ข้อ (๑๖) การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้ เป็นความรับผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ (๑๗) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของโรงพยาบาลบ้านด่านและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากการใส่รหัสผิดเกิน ๓ ครั้งก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนก่อนการใช้งานทุกครั้ง

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล๊อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๓๐ นาที

ข้อ (๑๘) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลบ้านด่านหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ (๑๙) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของโรงพยาบาลบ้านด่าน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลบ้านด่าน

ข้อ (๒๐) ผู้ใช้งานมีส่วนร่วมในการดุแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลบ้านด่าน และข้อมูลของผู้มารับบริการ หากเกิดการสูญเสีย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ (๒๑) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ (๒๒) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลบ้านด่านจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลบ้านด่าน ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลซึ่งโรงพยาบาลบ้านด่านอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ (๒๓) ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านด่าน ที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลบ้านด่าน

ข้อ (๒๔) ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านด่าน เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้การโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาลบ้านด่าน

ข้อ (๒๕) ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านด่าน เพื่อประโยชน์ทางการค้า ที่มิใช้ภารกิจโรงพยาบาลบ้านด่าน

ข้อ (๒๖) ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลบ้านด่าน โดยเด็ดขาด ไม่ว่าจะด้วยวิธีใดๆก็ตาม

ข้อ (๒๗) ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลบ้านด่าน ต้องหยุดชะงัก

ข้อ (๒๘) ห้ามใช้ระบบสารสนเทศของโรงพยาบาลบ้านด่าน เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนทศภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ (๒๙) ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ (๓๐) ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลบ้านด่าน โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ (๓๑) มาตรการควบคุมการเข้า-ออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องมาติดต่อผู้ดูแลระบบเพื่อขออนุญาตเข้าไปยังห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง ผู้ดูแลระบบจะกำกับดูแลตลอดเวลาเมื่อหน่วยงานภายนอกอยู่ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ต้องมาติดต่อผู้ดูแลระบบเพื่อขออนุญาตเข้าไปยังห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง ผู้ดูแลระบบจะกำกับดูแลตลอดเวลาเมื่อหน่วยงานภายนอกอยู่ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

ข้อ (๓๒) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของโรงพยาบาลบ้านด่าน ต้องได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์และปฏิบัติตามแนวปฏิบัตินี้โดยเคร่งครัด

ข้อ (๓๓) การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลต่อผลกระทบต่อการทำงานของระบบและผู้ใช้งานอื่น

ข้อ (๓๔) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณ (Switch) อุปกรณ์เชื่อมต่อระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ (๓๕) ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การเข้าใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของโรงพยาบาลบ้านด่าน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายทั้งหมดต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลบ้านด่านในลักษณะที่ผิดปกติ

(๖) การเข้าระบบเครือข่ายภายในโรงพยาบาลบ้านด่าน โดยผ่านระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในโรงพยาบาลบ้านด่าน

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ข้อ (๓๖) ผู้ดูแลระบบ ต้องบริหาร ควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ (๓๗) การติดตั้งหรือปรับปรุงซอฟต์แวร์ระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบก่อนดำเนินการ

ข้อ (๓๘) กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ (๓๙) การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ.คอมพิวเตอร์ ๒๕๖๐

ข้อ (๔๐) กำหนดมาตรฐานควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกโรงพยาบาลบ้านด่าน เพื่อดูและรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคลากรจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาลบ้านด่าน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศโรงพยาบาลบ้านด่าน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าระบบอย่างรัดกุม

(๓) วิธีการใดๆ ที่สามารถเข้าถึงข้อมูลและระบบข้อมูลได้จากระยะไกลต้องได้รับอนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศโรงพยาบาลบ้านด่าน

ข้อ (๔๑) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามความจำเป็นในการใช้งาน เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Internet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ (๔๒) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งให้บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ (๔๓) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกโรงพยาบาลบ้านด่านต้องเชื่อมต่อผ่านอุปกรณ์ปกกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่นการใช้ไฟร์วอลล์ (Firewall) หรือ ฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับ (Malware) ด้วย

ข้อ (๔๔) การใช้งานเครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและการจัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ (๔๕) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลบ้านด่าน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งภายในโรงพยาบาลบ้านด่าน เป็นต้น

ข้อ (๔๖) กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๔) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านด่าน ร่วมกัน

(๕) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่ได้อยู่ที่หน้าจอเป็นเวลานาน

(๖) ซอฟต์แวร์ที่โรงพยาบาลบ้านด่าน จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อไปใช้งานที่อื่น

(๗) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลบ้านด่าน เพื่อประโยชน์ทางการค้า

(๘) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปแบบไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๙) ห้ามผู้ใช้งานของโรงพยาบาลบ้านด่าน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

ข้อ (๔๗) การระบุยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้ และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ (๔๘) การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out) ให้ดำเนินการ ดังนี้

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกโรงพยาบาลบ้านด่าน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ (๔๙) ผู้ดูแลระบบ ต้องกำหนดระยะเวลาการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งภายในโรงพยาบาลบ้านด่าน เป็นต้น

ข้อ (๕๐) ผู้ดูและระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๓๐ นาที ระบบจะยุติการใช้งานของผู้ใช้งาน ต้องทำการลงบันทึกเข้าใช้งานก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ (๕๑) ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ (๕๒) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกโรงพยาบาล บ้านด่าน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ (๕๓) การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำมาส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากการประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

แนวปฏิบัติในการการกำหนดหน้าที่ความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ 1 ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้อำนวยการ (CEO)
- ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)
- ผู้อำนวยการฝ่ายเทคนิคและวิศวกรรม หรือเทียบเท่าระดับผู้อำนวยการฝ่าย

(1) รับผิดชอบต่อความเสี่ยง ความเสี่ยงหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 2 ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้าส่วนงาน

(1) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(2) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบข้อมูล

ข้อ 3 ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้อำนวยการ เช่น นักวิชาการคอมพิวเตอร์ เจ้าพนักงานเครื่องคอมพิวเตอร์ พนักงานเทคโนโลยีสารสนเทศ

(1) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(2) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(3) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(4) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(5) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(6) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(7) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความปลอดภัยด้านสารสนเทศ

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
โรงพยาบาลบ้านด่าน
อำเภอบ้านด่าน จังหวัดบุรีรัมย์

บทที่ ๑ บทนำ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดกาสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กรทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ โรงพยาบาลบ้านด่าน

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

โรงพยาบาลบ้านด่านมีระบบบริหารจัดการข้อมูลสารสนเทศ และได้นำระบบบริการผู้ป่วยโดยใช้ฐานข้อมูลตั้งแต่ปี ๒๕๕๗ โดย เริ่มต้นด้วยโปรแกรม HOSxP ซึ่งเป็นโปรแกรมที่พัฒนาโดยบริษัทบางกอกเมดิคอลซอฟแวร์

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กรและการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำ จัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. **หน้าที่การปฏิบัติงาน** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆโดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup andRecovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑. การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒. การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้User/Password ที่ทางศูนย์คอมฯ ออกให้แล้ว อาจจะบอกให้ผู้ใต้บังคับบัญชาของตนทราบ User/Passwordดังกล่าว และเมื่อผู้ใต้บังคับบัญชาทราบUser/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่งทางศูนย์คอมฯต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น และกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๓. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้นการควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

๔.การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายเป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการแพทย์ ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การขำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้าย หรืออื่นๆ

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก(Hacker)โดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลาย เสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็น ประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุก กรณีตามที่ระบุ

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์โรงพยาบาลบ้านด่าน มีการกำหนดนโยบายและมาตรการในการรักษา ความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์ เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้ โปรแกรมป้องกันไวรัสและFirewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของโรงพยาบาล เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบัน เครือข่ายของ โรงพยาบาลบ้านด่าน มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๑.	**ความเสี่ยงด้าน Hardware**		
	๑.๑ อุปกรณ์คอมพิวเตอร์เสียหาย	- หมดอายุการใช้งาน - มีการใช้งานหนัก - สภาวะแวดล้อม (ไฟฟ้า ,อากาศ)	ไม่สามารถทำงานต่อไปได้
	๑.๒ ระบบเครือข่ายมีปัญหา	- อุปกรณ์เครือข่ายเสียหาย - ผู้ให้บริการเครือข่าขัดข้อง	ไม่สามารถใช้บริการผ่านเครือข่ายได้
๒.	**ความเสี่ยงด้าน Software**		
	๒.๑ Software ไม่สามารถทำงานได้	- ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด - Virus /Hacker /Spyware	ไม่สามารถให้บริการได้
๓.	**ความเสี่ยงด้านบุคลากร**		
	๓.๑ ขาดทักษะในการทำงาน	- ไม่เข้าใจระบบงานนั้นๆ อย่างถี่ถ้วน - ปรับเปลี่ยนตำแหน่ง	งานที่ได้ไม่มี ประสิทธิภาพเท่าที่ควร
	๓.๒ ไม่ใช่หน้าที่หลักที่รับผิดชอบ	- ทำงานที่ไม่ใช่หน้าที่ของตน	งานอาจผิดพลาด

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน(ต่อ)

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๔.	**ความเสี่ยงด้านข้อมูล**		
	๔.๑ ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน
	๔.๒ ข้อมูลผิดพลาด	- เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	๔.๓ ความปลอดภัยของข้อมูล	- ขาดอุปกรณ์ป้องกันข้อมูลที่ดี - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้อย่างแท้จริง	อาจทำให้ข้อมูลเสียหาย ข้อมูลรั่วไหล
๕.	**ความเสี่ยงด้านหน้าที่การปฏิบัติ**		
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	- ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรืองานมีความผิดพลาด
	๕.๒ ละเลยการปฏิบัติ	- ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ															
๑.๑ ระบบฐานข้อมูล/ โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													
๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
๒.๑ ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	- ทุก ๓ เดือน			√			√			√			√	
๒.๓ ฝนฟ้าคะนอง อุปกรณ์ต่อพ่วงเสียหาย	- ตรวจสอบความพร้อมของระบบป้องกันไฟกรรโชก กราวป้องกันฟ้าผ่า ทำแผนซื้ออุปกรณ์ป้องกันเพิ่ม	- ช่วงฤดูฝน								←	—	—	—	→	
๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล															
๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	
๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๓.๔ ขาดเครื่องมือป้องกันหรือตรวจจับไวรัส	- มีโปรแกรมป้องกันไวรัสและ Update ฐานข้อมูลไวรัส	- สัปดาห์ละ ๑ ครั้ง	←											→	
๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
๔.๑ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์การโดยไม่ได้รับอนุญาต	- กำหนดสิทธิในการเข้าถึงข้อมูล	- เมื่อแต่งตั้ง/โยกย้าย /ลาออก / เกษียณอายุราชการ	←											→	
๕. อุปกรณ์คอมพิวเตอร์เสียหาย	- บำรุงรักษาคอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	- สัปดาห์ละ ๑ ครั้ง													
๕.๑ คอมพิวเตอร์ไม่สามารถใช้งานได้			←											→	

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
- ป้อมข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(2.2) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจักการการเข้าถึงของผู้ใช้ (User Access Management) ที่ได้กำหนดไว้

(2.3) ผู้ใช้งานต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

(3) ขั้นตอนการปฏิบัติเพื่อการจัดการเก็บข้อมูล

(3.1) จัดแบ่งประเภทข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เช้า ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(3.2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระบบสำคัญน้อยที่สุด

(3.3) จัดแบ่งลำดับชั้นความลับของข้อมูล

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

(3.4) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(3.5) การกำหนดเวลาที่ได้เข้าถึง

(3.6) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ 2 ข้อมูลข่าวสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ 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 หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างโรงพยาบาลบ้านด่าน กับหน่วยงานภายนอก ดังต่อไปนี้

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

(8) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟแวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ 2 การสำรองข้อมูล

ข้อ 6 พิจารณาคัดเลือกระบบสารเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ 7 กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ 8 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของโรงพยาบาลบ้านด่าน พร้อมกำหนดระบบสารสนเทศที่จัดทำระบบสารอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

ข้อ 9 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(1) กำหนดประเภทของข้อมูลที่ต้องการทำการสำรองเก็บไว้ และความถี่ในการสำรอง
(2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
(3) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
(4) จัดการข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล 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

แนวปฏิบัติในการรักษาความปลอดภัยด้วนกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่าน

แนวปฏิบัติ

ข้อ 1 อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายความว่า ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ 2 ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(1) กำหนดเป็นเขตห้วงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(2) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า – ออก ของบุคคลเป็นจำนวนมาก

(3) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(4) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(5) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

(6) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(7) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ 3 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(1) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

ข้อ 4 การควบคุมการเข้าออก อาคารสถานที่

(1) กำหนดสิทธิ์ผู้เข้าใช้งาน มีสิทธิ์ผ่านเข้า – ออก พื้นที่ใช้งานระบบ อย่างชัดเจน

(2) การเข้าถึงอาคารของศูนย์คอมพิวเตอร์โรงพยาบาลบ้านด่าน ของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น

(3) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(4) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(5) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(6) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(7) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(8) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(9) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยที่ละ 1 ครั้ง

ข้อ 5 ระบบและอุปกรณ์สนับสนุน (Supporting Utilities)

(1) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่าน ที่เพียงพอต่อความต้องการใช้งานโดยมีระบบ ดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ

(2) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้น อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

ข้อ 6 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

(1) หลีกเลี้ยงการเดินสายสัญญาณเครือข่ายของโรงพยาบาลบ้านด่าน ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(2) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(3) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

ข้อ 7 การบำรุงรักษาอุปกรณ์ Equipment Maintenance)

(1) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณีสำหรับการให้บริการสำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในโรงพยาบาลบ้านด่าน

ข้อ 8 การนำทรัพย์สินของโรงพยาบาลบ้านด่าน ออกนอกโรงพยาบาลบ้านด่าน (Removal of Property)

(1) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกโรงพยาบาลบ้านด่าน

(2) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากโรงพยาบาลบ้านด่าน

(3) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกโรงพยาบาลบ้านด่าน

(4) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(5) บันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาลบ้านด่านออกไปใช้งานนอกโรงพยาบาลบ้านด่านเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ 9 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกโรงพยาบาลบ้านด่าน(Security of Equipment off-premises)

(1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของโรงพยาบาลบ้านด่าน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(2) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของโรงพยาบาลบ้านด่านไว้โดยลำพังในที่สาธารณะ

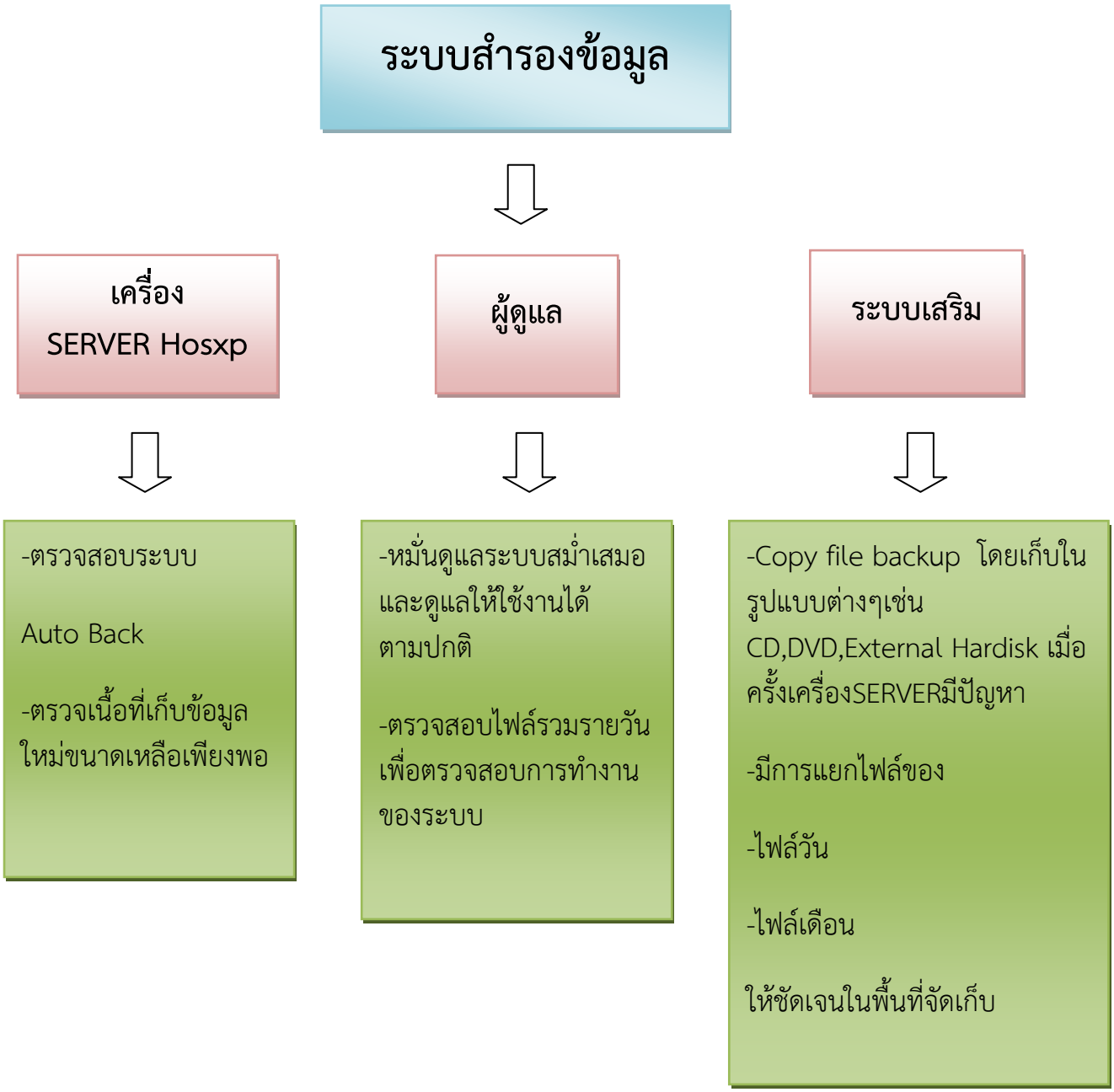
(3) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ 10 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or-use of Equipment)

(1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(2) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

แผนผังการจัดระบบการสำรองข้อมูล



แผนผังระบบป้องกันความเสียหายจากระบบไฟฟ้าขัดข้อง

ระบบไฟฟ้า

ภาวะปกติ

-ติดตั้งเครื่องสำรองไฟ (UPS)ทั้งเครื่องหลักและเครื่องรอง

-ตรวจสอบ UPS ให้ใช้ได้เสมอ

-ติดตั้งระบบไฟฟ้าระบบป้องกันการลัดวงจร

-ติดตั้งเครื่องปั่นไฟ (ถ้ามี)ตรวจสอบสภาพให้ใช้งาน

ภาวะฉุกเฉิน
เช่น ไฟดับ ไฟตก ไฟรั่ว

-เครื่องสำรองไฟ UPS ต้องใช้งานต่อเนื่องได้ไม่เกินกว่า ๒๐ นาที

-ควรรีบบันทึกงานที่ค้างอยู่แล้วรีบปิดคอมพิวเตอร์ตามลำดับความสำคัญ

-ถ้าเกิดไฟฟ้าลัดวงจรหรือเกิดเหตุฉุกเฉินให้ตัดระบบจ่ายไฟและย้ายเครื่องSERVERไปยังในที่ที่ปลอดภัย

-ดำเนินการให้ระบบกลับสู่ภาวะปกติโดยเร็วที่สุด

โรงพยาบาลบ้านด่าน		จำนวนหน้า : ๒
นโยบายและวิธีปฏิบัติ BD-IMIT-๐๑๓		ฉบับที่ ๑
เรื่อง : การปฏิบัติกรณีเครื่อง Server/Database มีปัญหา		วันที่ ๑๘ กุมภาพันธ์ ๒๕๖๔
แผนก : งานสารสนเทศ	แผนกที่เกี่ยวข้อง : จนท.รพ.ที่เกี่ยวข้อง	วันที่ปรับปรุง : ๑๘ กุมภาพันธ์ ๒๕๖๔
ผู้จัดทำ :: งานสารสนเทศ	ผู้อนุมัติ (นายศาสตรา เข็มบุบผา) ผู้อำนวยการโรงพยาบาลบ้านด่าน	

แนวทางปฏิบัติกรณีเครื่อง Server/Database มีปัญหา

๑. กรณีเครื่อง Server /Database มีปัญหา สามารถแก้ไขได้ภายใน ๓๐ นาที

<u>เจ้าหน้าที่ศูนย์คอมพิวเตอร์</u>

- นักวิชาการคอมพิวเตอร์ หรือ เจ้าหน้าที่เครื่องคอมพิวเตอร์ งานสารสนเทศตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน ๓๐ นาที แจ้งประกาศให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP ชั่วคราว
- ดำเนินการแก้ไข ตรวจสอบความพร้อมให้เรียบร้อย
- ประกาศให้ทุกหน่วยงานสามารถใช้งาน HOSxP ได้ตามปกติ
- สรุปสาเหตุของปัญหา และลงบันทึกในโปรแกรมความเสี่ยง

<u>เจ้าหน้าที่หน่วยงานต่างๆ</u>

- เมื่อได้รับแจ้งจากงานสารสนเทศ ให้หยุดการใช้งานคอมพิวเตอร์ชั่วคราว
- ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ และจัดบริการที่สามารถทำได้โดยบันทึกลงในแบบฟอร์ม OPD card พร้อมใบ Slip OPD และเก็บเอกสารเพื่อรอลงบันทึกย้อนหลัง
- เมื่อได้รับแจ้งให้ใช้งานคอมพิวเตอร์ได้ตามปกติ ให้เริ่มนำข้อมูลบริการลงบันทึกในโปรแกรม HOSxP

๒. กรณีเครื่อง Server /Database มีปัญหา ไม่สามารถแก้ไขได้ภายใน ๓๐ นาที

<u>เจ้าหน้าที่งานสารสนเทศ</u>

- นักวิชาการคอมพิวเตอร์ ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขได้ภายใน ๓๐นาที ให้แจ้งหัวหน้างานสารสนเทศ / ผู้อำนวยการโรงพยาบาลหนองกี่ทราบ
- ผู้อำนวยการโรงพยาบาลหนองกี่ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้ โดยใช้มาตรการเดียวกับข้อ **กรณีไฟฟ้าดับ** มากกว่า ๓๐ นาที ให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP
- งานสารสนเทศดำเนินการแก้ไขปัญหา Server ให้สามารถใช้งานได้ตามปกติภายใน ๒๔ ชั่วโมง
- ประสานผู้เกี่ยวข้องเพื่อตรวจสอบการลงบันทึกข้อมูลในโปรแกรม HOSxP ย้อนหลัง
- เมื่อเครื่อง Server สามารถทำงานได้ตามปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย

- ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งาน HOSxP และเริ่มบันทึกข้อมูลย้อนหลัง
- ติดตามตรวจสอบความเรียบร้อยของการลงบันทึกข้อมูลของหน่วยงานต่างๆ จนกระทั่งระบบข้อมูลเป็นปัจจุบัน และสามารถให้บริการได้ตามปกติ
- ผู้อำนวยการโรงพยาบาลหนองกี่ ประกาศยกเลิกใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้
- ลงบันทึกในโปรแกรมความเสี่ยงสรุปรายงานนำเสนอผู้อำนวยการและคณะกรรมการบริหารทราบ

หมายเหตุ กรณีเครื่อง Server/Database กำหนดให้ผู้มีรายชื่อดังต่อไปนี้เป็นผู้ตรวจสอบและแก้ไขปัญหา

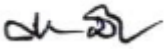
๑. นางสาวดวงจันทร์ ชะงักรัมย์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ เบอร์ ๐๘๐-๔๘๔๕๙๓๔

๒. นางสาวบุษรา หงษ์เรืองรัมย์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ เบอร์ ๐๖๑-๖๙๑๖๙๖๕

หากไม่สามารถติดต่อได้ ให้ใช้ระเบียบปฏิบัติเช่นเดียวกับ **กรณีไฟฟ้าดับ**

- บันทึกรายงานความเสี่ยงและสรุปปัญหาเสนอ ผู้อำนวยการและคณะกรรมการบริหาร

ผู้รับผิดชอบ : เจ้าหน้าที่งานสารสนเทศโรงพยาบาลบ้านด่าน

โรงพยาบาลบ้านด่าน		จำนวนหน้า : ๓
นโยบายและวิธีปฏิบัติ BD-IMIT-๐๑๔		ฉบับที่ ๑
เรื่อง : การปฏิบัติกรณีไฟฟ้าดับ		วันที่ ๑๘ กุมภาพันธ์ ๒๕๖๔
แผนก : งานสารสนเทศ	แผนกที่เกี่ยวข้อง : จนท.รพ.ที่เกี่ยวข้อง	วันที่ปรับปรุง : ๑๘ กุมภาพันธ์ ๒๕๖๔
ผู้จัดทำ :: งานสารสนเทศ	ผู้อนุมัติ  (นายศาสตรา เข็มบุบผา) ผู้อำนวยการโรงพยาบาลบ้านด่าน	

แนวทางปฏิบัติกรณีไฟฟ้าดับ

วิธีปฏิบัติ

๑. กรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไม่ทำงาน ระยะเวลาไม่เกิน 30 นาที

<u>เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ</u>

- หัวหน้า/รองหัวหน้า หรือผู้รับแจ้งปัญหาของศูนย์คอมพิวเตอร์ประสานงานกับงานซ่อมบำรุง เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน 30 นาที ให้ตรวจสอบการทำงานของ UPS ที่ห้อง server
- ประกาศแจ้งทางเสียงตามสาย/โทรศัพท์/แจ้งด้วยวาจา ให้หน่วยงานต่างๆ ทราบเพื่อปิดคอมพิวเตอร์และเครื่องสำรองไฟชั่วคราว
- สำรวจ/รับแจ้งปัญหา การทำงานของเครื่องสำรองไฟฟ้า(UPS) เครื่องคอมพิวเตอร์ของหน่วยงานต่างๆ ขณะไฟฟ้าดับว่าสามารถไฟได้หรือไม่
- เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย Switch HUB, Access Point
- ตรวจสอบการเข้าใช้งานโปรแกรม HOSxP
- ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งาน HOSxP ได้ตามปกติ

<u>เจ้าหน้าที่งานเวชระเบียน</u>

- เมื่อได้รับแจ้งจากงานสารสนเทศ ให้นำแบบฟอร์ม OPD card พร้อมใบ Slip OPD เพื่อใช้บันทึกข้อมูลชั่วคราว
- เมื่อระบบมีการใช้งานได้ตามปกติให้นำข้อมูลที่บันทึกไว้ใน OPD card บันทึกในโปรแกรม HOSxP

<u>เจ้าหน้าที่หน่วยงานต่างๆ</u>

- เมื่อได้รับแจ้งจากงานเทคโนโลยีสารสนเทศ ให้ปิดแอร์ /ปิดคอมพิวเตอร์ชั่วคราว

- ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ ให้บริการตามปกติ และเขียนข้อมูลลงในแบบฟอร์ม OPD card พร้อมใบ Slip OPD และเก็บเอกสารไว้ที่ห้องจ่ายยาเพื่อลงบันทึกบริการย้อนหลัง
- กรณีเครื่องสำรองไฟฟ้า (UPS) มีปัญหาไม่สำรองไฟ ให้แจ้งงานสารสนเทศ
- เมื่อได้รับแจ้งว่าระบบคอมพิวเตอร์สามารถใช้งานได้ตามปกติ ให้นำข้อมูลบริการลงบันทึกใน HOSxP ย้อนหลัง

2. กรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไม่ทำงาน ระยะเวลาเกิน 30 นาที

<u>เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ</u>

- หัวหน้างานสารสนเทศ หรือผู้รับแจ้งปัญหาของงานสารสนเทศ ประสานงานกับงานซ่อมบำรุง เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขได้ภายใน 30นาที และไม่มีระบบไฟฟ้าสำรอง ให้แจ้งประธานคณะกรรมการสารสนเทศ /ผู้อำนวยการทราบ
- ผู้อำนวยการโรงพยาบาลหนองกี่/หัวหน้างานสารสนเทศ ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ ให้หน่วยงานต่างๆทราบ
- สำรวจ/รับแจ้งปัญหา การทำงานของเครื่องสำรองไฟฟ้า (UPS) เครื่องคอมพิวเตอร์ของหน่วยงานต่างๆ
- เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Serverและอุปกรณ์เครือข่าย และข้อมูลในโปรแกรม HOSxP
- ผู้อำนวยการโรงพยาบาลหนองกี่/หัวหน้างานสารสนเทศ ประกาศแจ้งยกเลิกแผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ให้หน่วยงานต่างๆทราบ เมื่อระบบสามารถใช้งาน HOSxP ได้ตามปกติ
- ติดตามตรวจสอบการลงบันทึกข้อมูลของหน่วยงานต่างๆ
- สรุปรายงานนำเสนอผู้อำนวยการ และคณะกรรมการบริหารทราบ

<u>เจ้าหน้าที่หน่วยงานเวชระเบียน</u>

- จัดเตรียมอุปกรณ์สำหรับบันทึกข้อมูลดังนี้
    - แบบฟอร์ม OPD card พร้อมใบ Slip OPD
    - ปากกา,ตราปั้มวันที่
    - คอมพิวเตอร์โน้ตบุ๊กของงานเวชระเบียนที่ติดตั้งฐานข้อมูล HOSxP สำหรับค้นข้อมูล HN ของผู้ป่วย
    - เมื่อระบบสามารถกลับมาใช้งานได้ตามปกติ ให้นำข้อมูลจากใบสั่งมาลงบันทึกส่งตรวจย้อนหลังจนเป็นปัจจุบัน

<u>เจ้าหน้าที่จุดคัดกรอง/ห้องตรวจ/ห้องชันสูตร/ห้อง X-ray/ฝ่ายเวชปฏิบัติครอบครัว/ฝ่ายทันตสาธารณสุข/งานเวชกรรมฟื้นฟู/อื่นๆ</u>

- เมื่อได้รับแจ้งประกาศใช้แผนฉุกเฉินกรณีระบบล่ม ให้ปิดเครื่องสำรองไฟฟ้าและหยุดการลงบันทึกข้อมูลในคอมพิวเตอร์
- แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบ
- บันทึกบริการ/กิจกรรม/เวชภัณฑ์ ใน OPD card พร้อมใบ Slip OPD
- เมื่อระบบสามารถใช้งานได้ตามปกติ ให้นำข้อมูลการให้บริการลงบันทึกข้อมูลในคอมพิวเตอร์ย้อนหลังในโปรแกรม HOSxP

<u>เจ้าหน้าที่ห้องจ่ายยา</u>

- เมื่อได้รับแจ้งประกาศใช้แผนฉุกเฉินกรณีระบบล่ม ให้ปิดเครื่องสำรองไฟฟ้าและหยุดการลงบันทึกข้อมูลในคอมพิวเตอร์
- แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบ
- ลงบันทึกการจ่ายเวชภัณฑ์ กิจกรรมลงในใบสั่งยาและเขียนซองยา
- เก็บใบสั่งยากไว้ที่ห้องจ่ายยา เพื่อลงบันทึกข้อมูลย้อนหลังเมื่อระบบสามารถใช้งานได้ตามปกติ

<u>เจ้าหน้าที่ห้องการเงิน</u>

- กรณีมีค่าใช้จ่ายที่สามารถสรุปค่าใช้จ่ายได้ เช่น ใบรับรองแพทย์ให้เก็บเงินโดยใช้ใบเสร็จเล่มเขียว
- กรณีไม่สามารถสรุปค่าใช้จ่ายได้ ให้แยกใบสั่งยาไว้และแจ้งผู้ป่วย/ญาติทราบว่าจะลงบันทึกเป็นผู้ป่วยค้างชำระไว้ก่อนชั่วคราว
- เมื่อระบบคอมพิวเตอร์สามารถใช้งานได้ตามปกติ และหน่วยงานต่างๆ ลงบันทึกข้อมูลบริการในโปรแกรม HOSxP เรียบร้อย การเงินสรุปค่าใช้จ่าย

เมื่อระบบไฟฟ้าสามารถใช้งานได้ตามปกติ ให้งานเวชระเบียนและหน่วยงานที่เกี่ยวข้องในการให้บริการตรวจสอบความสมบูรณ์ของข้อมูลให้เรียบร้อย และเป็นปัจจุบัน จึงประกาศยกเลิกแผนฉุกเฉิน

ผู้รับผิดชอบ : คณะกรรมการสารสนเทศ,งานสารสนเทศ,งานซ่อมบำรุง,เจ้าหน้าที่หน่วยงานต่างๆ