นโยบายการรักษาความมั่นคงปลอดภัยของ

ระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลทุ่งใหญ่

พ.ศ. 2558

โดย

ทีมสารสนเทศ (IM)

โรงพยาบาลทุ่งใหญ่

ฉบับปรับปรุง 16 กุมภาพันธ์ 2558

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลทุ่งใหญ่

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

1.2. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001

1.3. นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลทุ่งใหญ่ได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ

1.6. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

2. องค์ประกอบของนโยบาย

2.1. คำนิยาม

2.2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับโรงพยาบาล

2.3. การบริหารจัดการทรัพย์สินของโรงพยาบาล

2.4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

2.5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

2.6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล

2.7. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อที่จะทำให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอยู่ในระดับที่ปลอดภัย

นโยบายการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบสารสนเทศซึ่งเจ้าหน้าที่ของโรงพยาบาลทุ่งใหญ่จะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **โรงพยาบาล** หมายถึง โรงพยาบาลทุ่งใหญ่
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่
- **มาตรการ** หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น
- **วิธีปฏิบัติ** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลทุ่งใหญ่
- **ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว
- **สารสนเทศ** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่รูปของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet)
    - **ระบบแลน (LAN)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
    - **ระบบอินเตอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถ

นำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูล และสารสนเทศ เป็นต้น

- **การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ** หมายถึง การตรวจสอบการอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้
- **เครื่องเซิร์ฟเวอร์ (Server)** หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย
- **อุปกรณ์ UPS** หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้าเกิดมีปัญหาขึ้นมา เช่นไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่ UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า
- **ซอฟต์แวร์ (software)** หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้

  โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงานของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้
- **ไวรัสคอมพิวเตอร์** หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบ คอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน

  การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

- **เวชระเบียน** หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่เป็นเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลทุ่งใหญ่
- **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- **สถานการณ์ความไม่แน่นอนและภัยพิบัติ** หมายถึง บุคลากรของหน่วยงาน สถานการณ์หรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆที่เป็นภัยต่อระบบข้อมูลสารสนเทศ
- **แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ** หมายถึง ข้อปฏิบัติในการแก้ไขปัญหาเมื่อเกิดสถานการณ์ความไม่แน่นอน หรือภัยพิบัติ ได้แก่ การนำระบบกลับคืนสู่สภาพปกติ แนวทางปฏิบัติ ผังกระบวนการกรณีเกิดเหตุอัคคีภัย/อุทกภัย ผังกระบวนการกรณีไฟฟ้าดับและผังกระบวนการกรณีโดนเจาะระบบคอมพิวเตอร์

ส่วนที่ 1
โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับโรงพยาบาล
(Organization of information security)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ

โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร

1. ผู้บริหารต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2. คณะกรรมการบริหารโรงพยาบาล ต้องกำหนดให้มีตัวแทนเจ้าหน้าที่จากหน่วยงานต่างๆ ภายในโรงพยาบาลเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร

3. คณะกรรมการสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลไว้อย่างชัดเจน

4. คณะกรรมการสารสนเทศต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อโรงพยาบาล

ส่วนที่ 2
การบริหารจัดการทรัพย์สินของโรงพยาบาล
(Asset management)

1. วัตถุประสงค์

เพื่อเป็นมาตรการในการป้องกันทรัพย์สินของโรงพยาบาลจากความเสียหายที่อาจเกิดขึ้นได้จากมนุษย์หรือภัยพิบัติต่างๆ

2. มาตรการและแนวทางปฏิบัติ

หน้าที่ความรับผิดชอบต่อทรัพย์สินของโรงพยาบาล

1. หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อโรงพยาบาลให้ถูกต้องอยู่เสมอ

2. หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดให้มีการระบุผู้เป็นเจ้าของทรัพย์สินสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน

3. หัวหน้างานพัสดุและผู้ดูแลระบบ จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานอุปกรณ์สารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น

ส่วนที่ 3
ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
(Human resources security)

1. วัตถุประสงค์

เพื่อเป็นมาตรการให้เจ้าหน้าที่ได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทเมื่อมีการลาออกหรือย้ายหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ

2.1. กลุ่มงานการจัดการต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่ลาออกหรือย้ายหน่วยงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

2.2. ผู้ดูแลระบบต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่ลาออกหรือย้ายหน่วยงาน

3. วิธีปฏิบัติ

วิธีปฏิบัติเรื่อง การจัดการการลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่

ส่วนที่ 4
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environmental security)

1. วัตถุประสงค์

เพื่อเป็นมาตรการในการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินของโรงพยาบาล

2. มาตรการและแนวทางปฏิบัติ

2.1. **บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย**

2.1.1. คณะกรรมการสารสนเทศต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

2.1.2. คณะกรรมการสารสนเทศต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม ปลวก หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

2.2. ความมั่นคงปลอดภัยของอุปกรณ์รวมถึงแฟ้มเวชระเบียน

2.2.1. เจ้าหน้าที่ต้องจัดวางและป้องกันอุปกรณ์ภายในหน่วยงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2.2.2. ต้องกำหนดให้มีการเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

3. วิธีปฏิบัติ

1. วิธีปฏิบัติเรื่อง การใช้งานห้องเครื่อง Server

ส่วนที่ 5
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศและซอฟต์แวร์ให้เป็นไปอย่างถูกต้องสมบูรณ์ ปลอดภัยจากการถูกทำลาย และมีความพร้อมใช้ของสารสนเทศ

2. มาตรการและแนวทางปฏิบัติ

2.1. การป้องกันโปรแกรมที่ไม่ประสงค์ดี

2.1.1. ผู้ดูแลระบบต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืน เพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี

2.1.2. ผู้ดูแลระบบต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

2.2. **การสำรองข้อมูล**

คณะกรรมการสารสนเทศต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ

2.3. **การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายของโรงพยาบาล**

คณะกรรมการสารสนเทศต้องกำหนดการบริหารจัดการสำหรับบริการเครือข่ายและสารสนเทศของโรงพยาบาล

3. วิธีปฏิบัติ

1. วิธีปฏิบัติเรื่อง การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
2. วิธีปฏิบัติเรื่อง การจัดการไวรัสคอมพิวเตอร์
3. วิธีปฏิบัติเรื่อง การสำรองข้อมูล
4. วิธีปฏิบัติเรื่อง การสำรองข้อมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic Files
5. วิธีปฏิบัติเรื่อง การใช้งานคอมพิวเตอร์และเครือข่าย

ส่วนที่ 6
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกที่จะสร้างความเสียหายแก่ข้อมูล

2. มาตรการและแนวทางปฏิบัติ

2.1. การบริหารจัดการการเข้าถึงของผู้ใช้

2.1.1. ผู้ดูแลระบบต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

2.1.2. ผู้ดูแลระบบต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

2.2. **หน้าที่ความรับผิดชอบของผู้ใช้**

เจ้าหน้าที่ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สารสนเทศที่ไม่มีเจ้าหน้าที่ดูแล

2.3. **การควบคุมการเข้าถึงระบบปฏิบัติการ**

2.3.1. ผู้ดูแลระบบต้องจัดให้ผู้ใช้มีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และจะต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

2.3.2. ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

2.3.3. ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

2.3.4. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

2.4. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ

ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

3. วิธีปฏิบัติ

3.1.1. วิธีปฏิบัติเรื่อง การจัดเก็บข้อมูลตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐

3.1.2. วิธีปฏิบัติเรื่อง การตั้งรหัสผ่าน กำหนดและป้องกันรหัสผ่าน

3.1.3. วิธีปฏิบัติเรื่อง การรักษาความปลอดภัย/ ป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบ Electronic File และป้องกันการโจรกรรมข้อมูล

3.1.4. วิธีปฏิบัติเรื่อง การปฏิบัติเพื่อป้องกันและแก้ปัญหา Hacker เข้าเจาะระบบเว็บไซต์โรงพยาบาล

(ลงชื่อ)

(นายแพทย์จรัส จันทร์ตระกูล)

ผู้อำนวยการโรงพยาบาลทุ่งสง รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

วันที่ .....

เอกสารอ้างอิง

คณะอนุกรรมการด้านความมั่นคง ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2550. **มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550**. หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ.

ภาคผนวก

ระบบรักษาความปลอดภัย (Security)

ทีมสารสนเทศโรงพยาบาลทุ่งใหญ่ ได้มีการวางมาตรการระบบรักษาความปลอดภัย โดยกำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบความปลอดภัย (Security) และระบบบริหารความเสี่ยงของข้อมูลและสารสนเทศ เพื่อเตรียมความพร้อมในการแก้ไขปัญหาที่เกิดจากภัยพิบัติได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ ทีมสารสนเทศโรงพยาบาลทุ่งใหญ่ ได้ดำเนินการจัดแบ่ง เจ้าหน้าที่และบุคคลากรผู้รับผิดชอบดำเนินงาน ดังนี้

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา เมื่อเกิดเหตุฉุกเฉิน (กรณีอัคคีภัย/อุทกภัย)

1. ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

1.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินของระบบสารสนเทศ

1.2 มีอำนาจสั่งการให้ทุกฝ่ายหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

1.3 ประชุมหารือกับคณะกรรมการบริหารโรงพยาบาล และคณะกรรมการอื่นที่เกี่ยวข้อง

1.4 ประเมินสถานการณ์ และสั่งให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

2. ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย

2.1 ประธานทีมสารสนเทศ

2.1.1 วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการโรงพยาบาล

2.1.2 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการโรงพยาบาลจะมาถึงที่เกิดเหตุ

2.1.3 การให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (แผนฉุกเฉิน)

2.1.4 ทำหน้าที่แทนผู้อำนวยการโรงพยาบาลเพื่อระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ผู้อำนวยการโรงพยาบาลไม่อยู่

2.2 เลขานุการทีมสารสนเทศ

2.2.1 ประสานกับหัวหน้างานที่เกี่ยวข้อง เช่น หัวหน้ากลุ่มการจัดการ ช่างไฟฟ้า เป็นต้น

2.2.2 ทำหน้าที่แทนประธานทีมสารสนเทศในกรณีที่ประธานทีมสารสนเทศไม่สามารถทำหน้าที่ได้

2.3 กรรมการทีมสารสนเทศ

ทำหน้าที่ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

3. ผู้ดูแลระบบเครือข่ายและผู้ช่วยผู้ดูแลระบบเครือข่าย (LAN Administrator)

3.1 กรณีเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ถังดับเพลิงเข้าทำการดับเพลิง

3.2 พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ มาช่วยเหลือ

3.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

3.4 ป้องกัน ชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

3.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ประธานทีมสารสนเทศและผู้อำนวยการโรงพยาบาลทราบ อุปกรณ์ที่ต้องตรวจสอบได้แก่

- ทำการตรวจสอบ Firewall
- ทำการตรวจสอบ Virus, worm, spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยงแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบ Configuration ของระบบ

3.6 เตรียมเครื่องมืออุปกรณ์ทั้งด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

3.7 ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกในการกู้ระบบ ได้แก่ ทีมผู้ดูแลระบบจากโรงพยาบาลใกล้เคียง

3.8 ทำการสำรองข้อมูลจากฐานข้อมูล HOSxP ของโรงพยาบาลแบบ Real-time ทุกวัน และทำการสำรองข้อมูลแบบตั้งเวลาสำรองอัตโนมัติทุกวัน ในเวลา 01.00น. และ 12.00น.

3.9 ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ

3.10 นำระบบสำรองข้อมูลออกมาใช้เพื่อให้สามารถดำเนินการต่อไปได้

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingercy Plan) โรงพยาบาลทุ่งใหญ่

1. หลักการและเหตุผล

ระบบข้อมูลและสารสนเทศถือเป็นทรัพย์สินที่มีความสำคัญต่อโรงพยาบาล จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบฐานข้อมูลและสารสนเทศสำคัญๆของโรงพยาบาลทุ่งใหญ่จะไม่สูญหายสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

โรงพยาบาลทุ่งใหญ่ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศ ซึ่งอาจมีปัจจัยภายนอกและปัจจัยภายในที่ส่งผลกระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลและสารสนเทศที่ใช้ในการให้บริการแก่ผู้มารับบริการ การบริหารจัดการและใช้สนับสนุนการดำเนินงานโรงพยาบาลให้บรรลุตามวิสัยทัศน์ ตลอดจนข้อมูลสารสนเทศที่เป็นความต้องการของหน่วยงานภายนอก

ดังนั้นทีมสารสนเทศ (IM) โรงพยาบาลทุ่งใหญ่ จึงจัดทำแผนแก้ไขปัญหาสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการแก้ปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนสู่ความเป็นปกติ ตลอดจนการดูแลรักษาฐานข้อมูลและสารสนเทศให้มีเสถียรภาพพร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

2. วัตถุประสงค์

2.1 เพื่อเป็นแนวทางในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับฐานข้อมูลและสารสนเทศ

2.2 เพื่อป้องกันและลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อสนับสนุนให้การบริการระบบเทคโนโลยีสารสนเทศดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2.4 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

3. เป้าหมาย

3.1 ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) ที่สำคัญได้แก่ ฐานข้อมูลโปรแกรม HOSxP, ฐานข้อมูลจัดเก็บการใช้งานอินเทอร์เน็ต (Log File)

3.2 อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server), เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server/ Slave Server), เครื่องแม่ข่ายสำหรับจัดเก็บการใช้งานอินเทอร์เน็ต (Proxy Server), เครื่องคอมพิวเตอร์แม่ข่ายตรวจสอบและอัพเดต Virus (Antivirus Server), เครื่องพิมพ์ (Printer), เครื่องคอมพิวเตอร์ลูกข่าย (Client Server), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB), อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point)

4. การนำระบบกลับคืนสู่สภาพปกติ

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

1) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4) นำอุปกรณ์ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบตามความเหมาะสมดังนี้

4.1) ผู้ดูแลระบบของโรงพยาบาลทุ่งใหญ่

4.2) ขอสนับสนุนทีมผู้ดูแลระบบจากโรงพยาบาลใกล้เคียง

4.3) ทีมงานจากบริษัทที่จัดจ้างบำรุงรักษาระบบสารสนเทศ

ให้กู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

5) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้องก่อนเปิดให้บริการ

5. แนวทางปฏิบัติ

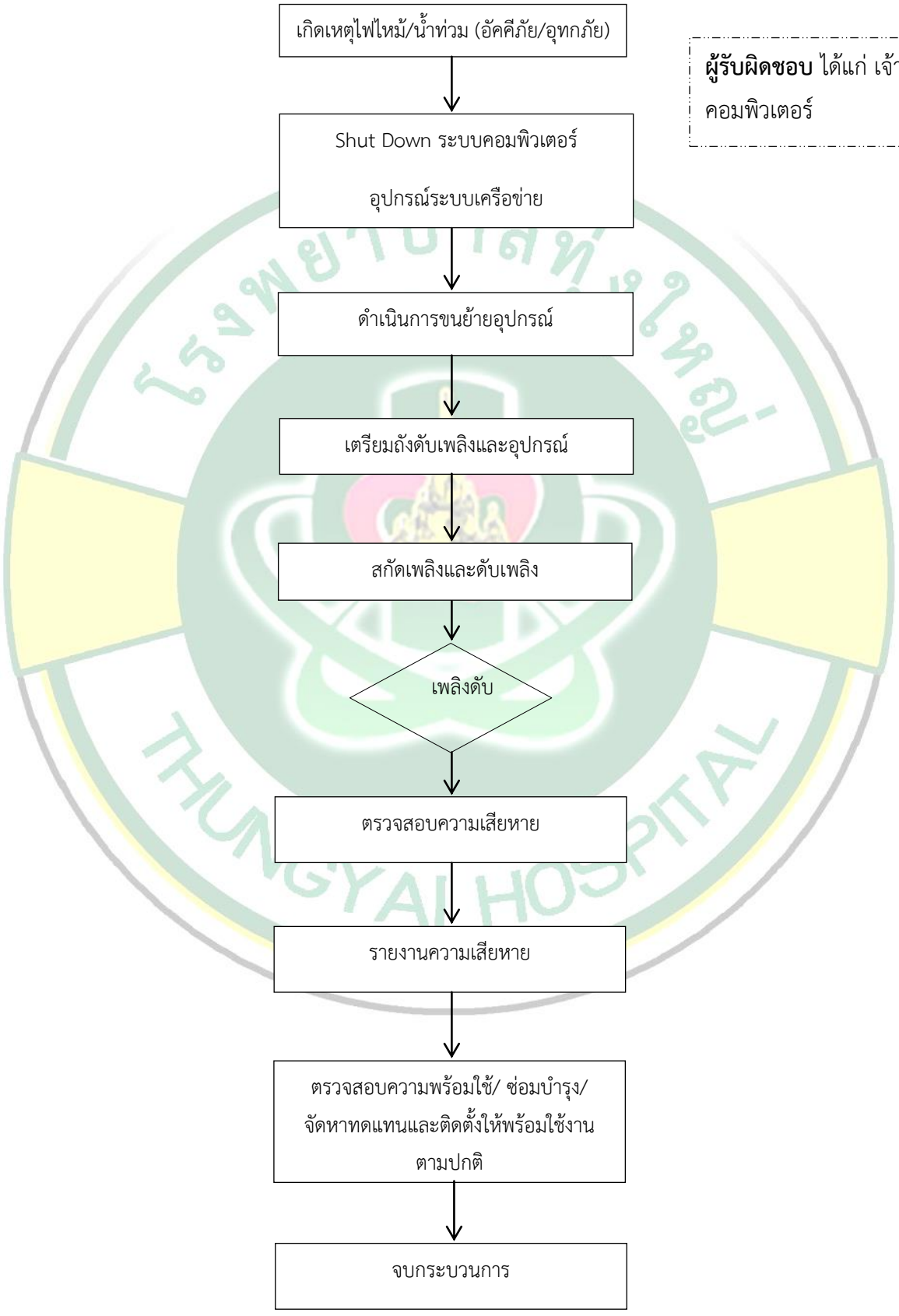
1) แจ้งเวียนกลุ่มงานต่างๆ ภายในโรงพยาบาลทุ่งใหญ่ ให้ถือปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ฉบับนี้

2) เมื่อมีอุปสรรคขัดข้องในการปฏิบัติตามแผนฯให้หน่วยงาน หาทางแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่

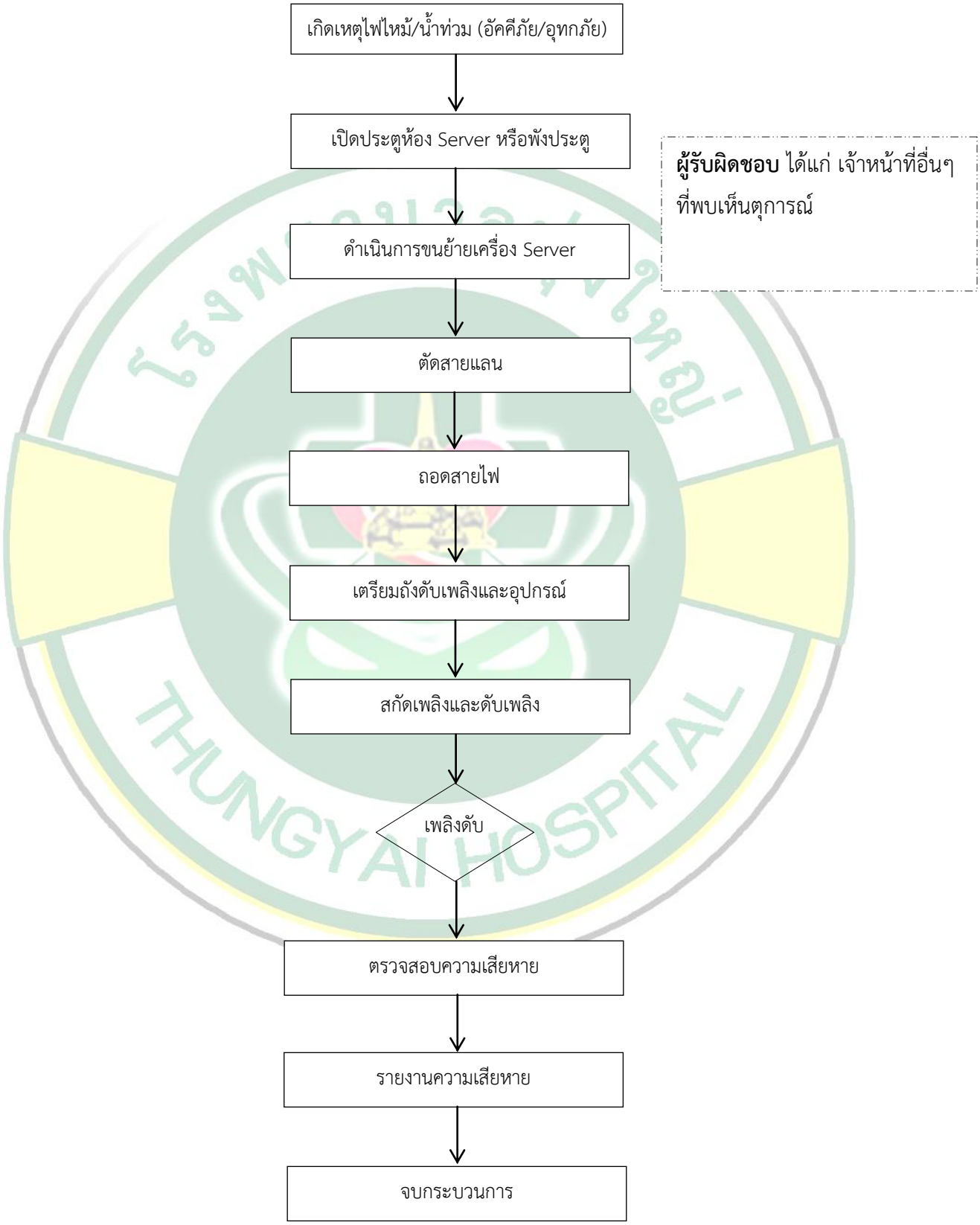
6. ผังกระบวนการ

ผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ 4 กรณีดังต่อไปนี้ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติขั้นตอนในแต่ละกรณี

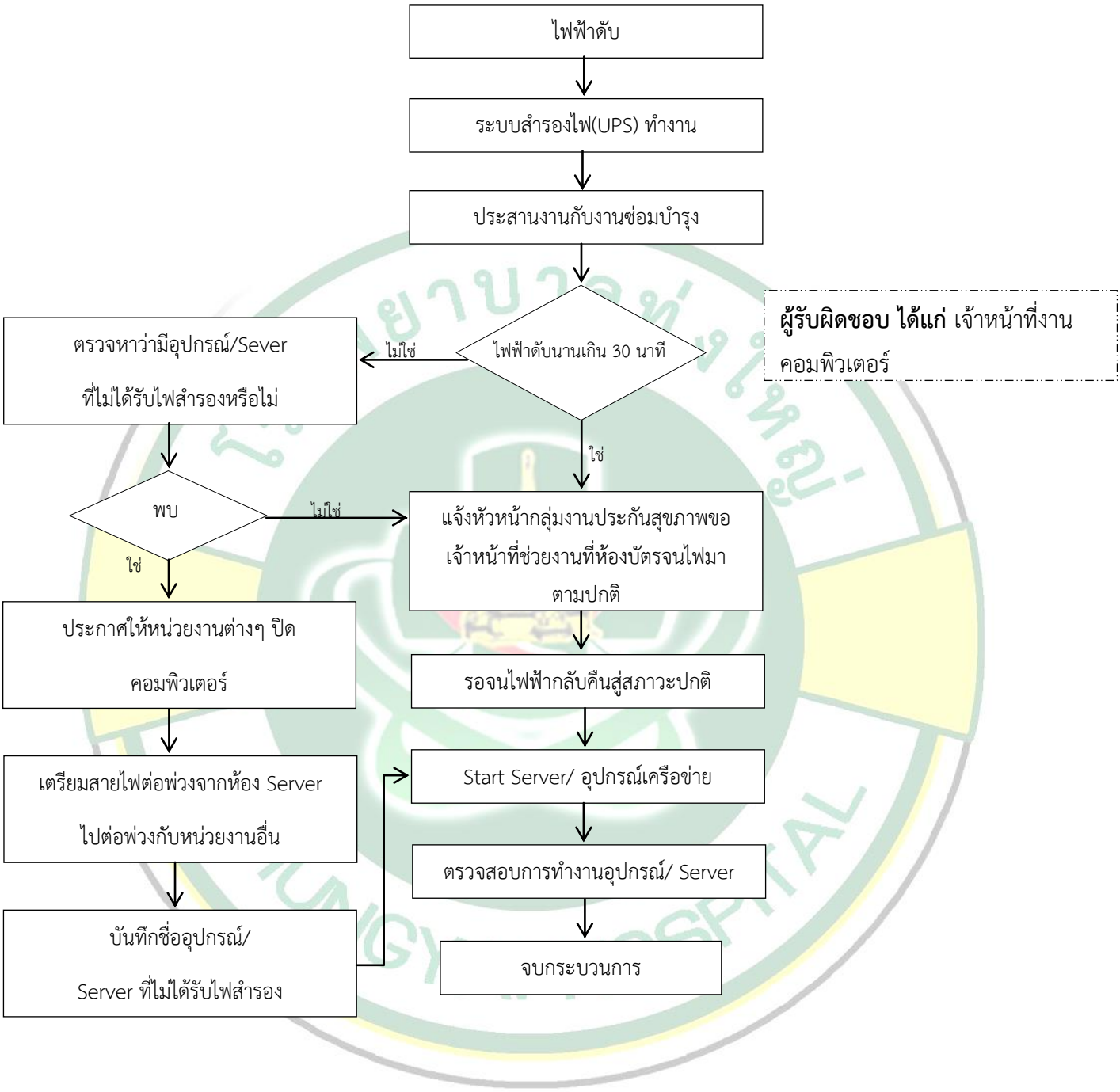
6.1 กรณีเกิดเหตุไฟไหม้/น้ำท่วม (อัคคีภัย/อุทกภัย) และมีเจ้าหน้าที่อยู่ภายในห้อง Server มีกระบวนการปฏิบัติดังนี้



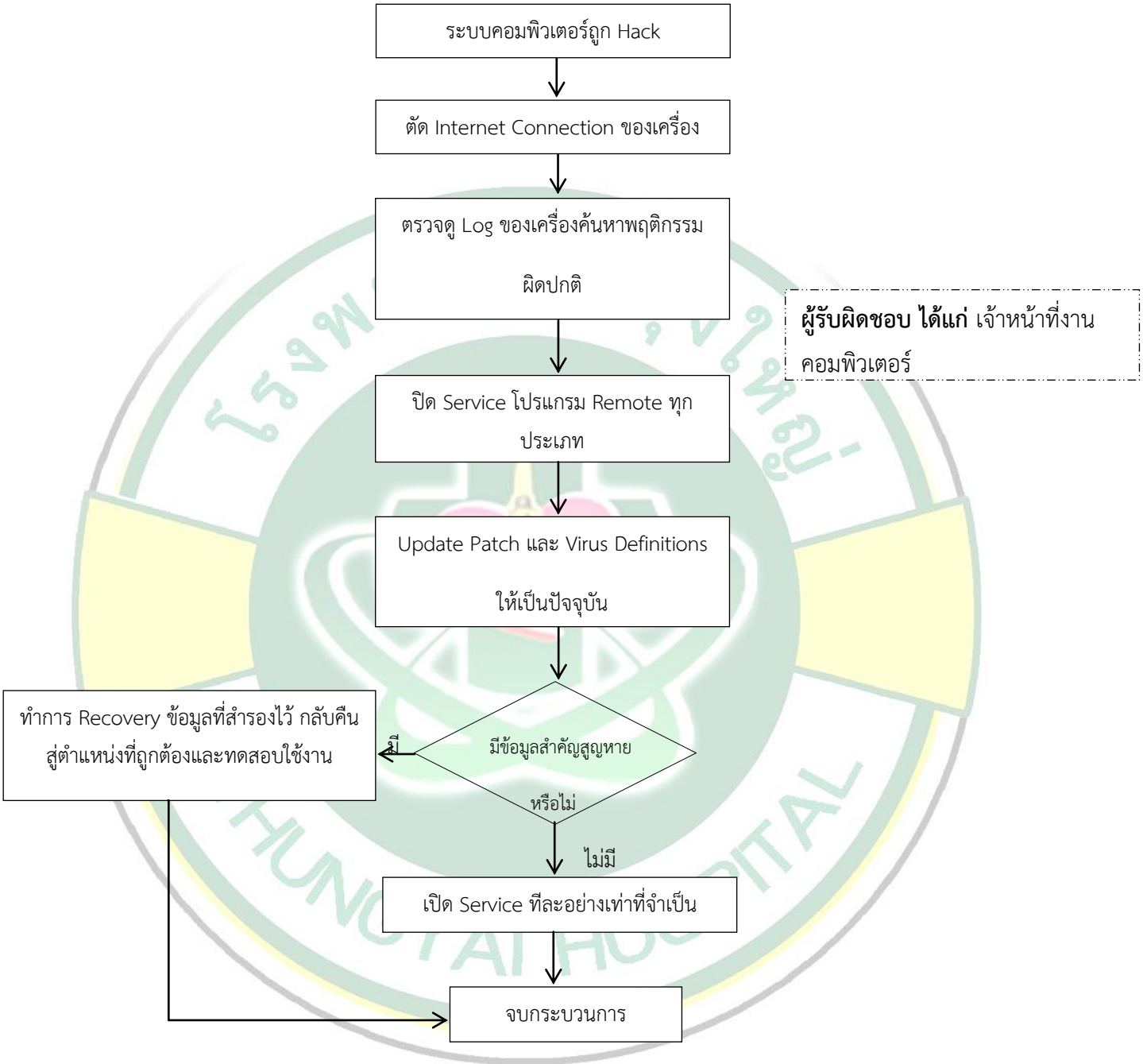
6.2 กรณีเกิดเหตุไฟไหม้/น้ำท่วม (อัคคีภัย/อุทกภัย) และไม่มีเจ้าหน้าที่อยู่ภายในห้อง Server มีกระบวนการปฏิบัติดังนี้



6.3 กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติดังนี้



6.4 กรณีโดนเจาะระบบคอมพิวเตอร์ มีกระบวนการปฏิบัติดังนี้



7. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

7.1 ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ การปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติการ ได้แก่

7.1.1 *ผู้อำนวยการโรงพยาบาลทุ่งใหญ่*

7.1.2 *ประธานทีมสารสนเทศ*

7.2 ระดับปฏิบัติ

7.2.1 คณะกรรมการทีมสารสนเทศ

7.2.2 เจ้าหน้าที่งานคอมพิวเตอร์และสารสนเทศทางการแพทย์

โดยมีหน้าที่

1. ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆของระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

2. รักษาความปลอดภัยของระบบฐานข้อมูล

3. ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ(IT Contingency Plan) ฉบับนี้ตามแต่ละกรณีเหตุการณ์ที่เกิดขึ้น