แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน

และภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

(IT Contingency Plan) พ.ศ. 2562

จัดทำโดย

กลุ่มงานเทคโนโลยีสารสนเทศ

เอกสารภายในที่ถูกควบคุม		
รหัสเอกสาร : S-IT-009		☑ ต้นฉบับ
แก้ไขครั้งที่ : 01 จำนวนหน้า 14		☐ สำเนาที่.....
ประกาศใช้ : 11/ม.ค./2562		
จัดทำโดย	ทบทวนโดย	อนุมัติโดย

บทนำ

ข้อมูลสารสนเทศเป็นทรัพยากรที่มีความสำคัญยิ่งต่อการบริหารราชการและการให้บริการประชาชนของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ จำเป็นต้องได้รับการแลรักษา ให้เกิดความมั่งคงปลอดภัยสามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษา และป้องกันแก้ไขปัญหา อันอาจส่งผลกระทบต่อฐานข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งระบบเครือข่าย ของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

กลุ่มงานเทคโนโลยีสารสนเทศ
25 ธันวาคม 2561

สารบัญ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน
และภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ
โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์
(IT Contingency Plan)

1.หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานด้านต่าง ๆ ของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์โดยเฉพาด้านการบริการผู้ป่วยที่หน่วยงาน ครอบคลุมทั้งผู้ป่วยนอกและผู้ป่วยใน การจัดเก็บข้อมูล และการพัฒนาระบบการจัดการข้อมูลต่าง ๆ ที่เกี่ยวข้องกับงานด้านการบริการโดยใช้เทคโนโลยีสารสนเทศ ทำให้การดำเนินงานเพื่อสนองยุทธศาสตร์ของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์มีความสะดวกรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้เทคโนโลยีสารสนเทศ ยังช่วยอำนวยความสะดวกในการติดต่อสื่อสาร การประสานงานด้านต่าง ๆ ทั้งภายในส่วนราชการเองและเครือข่ายที่ดำเนินงานร่วมกับโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ แต่การนำเทคโนโลยีสารสนเทศมาใช้งานก็มีความเสี่ยงอยู่หลายประการที่จะทำให้เกิดปัญหาในการปฏิบัติงาน หากไม่มีการควบคุมและการจัดการความเสี่ยงที่ดีพอ โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่าง ๆ จึงได้มอบหมายให้กลุ่มงานเทคโนโลยีสารสนเทศ โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษา และป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อฐานข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งระบบเครือข่ายของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

2.วัตถุประสงค์

2.1 เพื่อเป็นแนวทางในการลดความเสียหายที่จะเกิดขึ้นแก่ระบบฮาร์ดแวร์ ซอร์ฟแวร์และการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ

2.2 เพื่อลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อให้ระบบข้อมูลสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง

2.4 เพื่อเตรียมความพร้อมของบุคลากรของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์รับสถานการณ์ฉุกเฉินที่จะเกิดขึ้นและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ในระบบข้อมูลสารสนเทศและระบบฮาร์ดแวร์

2.5 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

3. เป้าหมาย

3.1 ระบบสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลบริการผู้ป่วย online ฐานข้อมูลผู้พยายามฆ่าตัวตาย(506S) ฐานข้อมูลบุคลากร ฐานข้อมูลเงินเดือน ฐานข้อมูลวิจัยสุขภาพจิตและจิตเวช ฐานข้อมูลคลังยาโปรแกรมปฏิบัติการเพื่อการบริหารงาน (Back Office) เช่น โปรแกรมจองห้องประชุม โปรแกรมบริการห้องสมุด โปรแกรมขออนุมัติใช้รถยนต์ โปรแกรมเบิกจ่ายพัสดุ โปรแกรมปฏิทินแผนงานโครงการ โปรแกรมแจ้งเวียนหนังสือภายใน โปรแกรมป้องกันและกำจัดไวรัส (Anti-virus) โปรแกรม Web site www.jvkk.go.th, https://dmhc1.dmh.go.th/506s10/index.php/sessions/login โปรแกรม web mail ฐานข้อมูล Username และ Password เพื่อใช้พิสูจน์ตัวบุคคลใช้งานอินเตอร์เน็ต

3.2 อุปกรณ์คอมพิวเตอร์ (Hard ware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายและระบบเน็ตเวิร์ค (Network & Server), เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล (Database Server), เครือข่ายอุปกรณ์จัดเก็บข้อมูลภายนอก (Storage Area Network), เครื่องคอมพิวเตอร์แม่ข่ายให้บริการเว็บไซต์ Web server, เครื่องป้องกันการบุกรุกจากภายนอก (Firewall), เครื่องคอมพิวเตอร์แม่ข่ายบริการอินเตอร์เน็ต (Proxy server, DHCP,DNS), เครื่องคอมพิวเตอร์ Note Book ,เครื่องคอมพิวเตอร์สำนักงาน, เครื่อง Scanner, เครื่องพิมพ์ (Laser, Inkjet, Dot Matrix), เครื่องสำรองไฟฟ้า UPS, เครื่องกระจายสัญญาณ (Switching, HUB), เครื่องกระจายสัญญาณไร้สาย (Wireless Access Point) เครื่องแสกนนิ้วบันทึกเวลามาปฏิบัติราช (Finger print) เครื่องพิมพ์บัตรคิว (Thermal Printer) เป็นต้น

4. วิเคราะห์และประเมินระดับความรุนแรงของสถานการณ์และความเสี่ยง

จากการวิเคราะห์และประเมินความเสี่ยงต่าง ๆ ในระบบสารสนเทศของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์พบว่าความเสี่ยงที่เป็นอันตราย ต่อระบบสารสนเทศที่สำคัญได้แก่

4.1 เกิดจากระบบไฟฟ้าขัดข้อง หรือความเสียหายจากเพลิงไหม้ โดยได้มีการติดตั้งอุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply) ขนาด 20 Kva เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับห้อง Data center ระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการแก้ไขสถานการณ์อันเนื่องมาจากเพลิงไหม้ ได้ติดตั้งเครื่องดับเพลิงแบบสารเคมีในกลุ่มงานเทคโนโลยีสารสนเทศ เพื่อการควบคุมเพลิงในเบื้องต้น

4.2 เกิดจากไวรัสคอมพิวเตอร์ (Virus Computer, Worm, Malware, Spyware) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ให้ใช้งานไม่ได้ มีการดำเนินการดังนี้

1). ติดตั้ง firewall ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัส (Trend Micro/Windows defender security) ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

2). อบรมให้ความรู้แก่บุคลากรเรื่องการดูแลบำรุงรักษาเครื่องคอมพิวเตอร์ การแสกนไวรัส แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

3). ติดตั้งโปรแกรม Deep Freeze ให้กับเครื่องลูกข่ายป้องกันไม่ให้มีการติดตั้งโปรแกรมอื่นนอกจากที่กำหนดให้โดยกลุ่มงานเทคโนโลยีสารสนเทศ

4.) ปิดช่อง USB Port เครื่องลูกข่ายทุกเครื่อง ยกเว้นเครื่องที่ใช้ทำธุรกรรมทางการเงินหน่วยงานละ 1 เครื่อง เช่นฝ่ายพัสดุ ฝ่ายการเงิน คลังยาและเวชภัณฑ์ ถ้าผู้ใช้ต้องการใช้ USB ให้มาใช้ได้ที่กลุ่มงานเทคโนโลยีสารสนเทศ

4.3 เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) ขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้าน human error ให้น้อยที่สุด

4.4 เกิดจากการโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่ายได้ ดำเนินการโดยจัดให้เป็นพื้นที่ห้ามเข้าโดยไม่ได้รับอนุญาตและล็อกกุนแจเข้าห้อง Data center

5. การเตรียมความพร้อมรับสถานการณ์ความไม่แน่นอนและภัยพิบัติ

5.1 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจาก ระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้า และป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์ แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ 3.23 ชั่วโมง และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) มีระยะเวลาสำรองไฟฟ้าประมาณ 15 นาที
2. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
3. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ทำงานยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ
4. ให้มีการสำรองฐานข้อมูลทุกวัน

5.2 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจาก ระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้เป็นการป้องกันและแก้ไขปัญหาจาก สถานการณ์ ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1. จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากเหตุเพลิงไหม้
2. ปฏิบัติตามขั้นตอนเมื่อพบเหตุเพลิงไหม้ของคณะกรรมการป้องกันอัคคีภัย
3. ร่วมซ้อมแผนอัคคีภัยอย่าน้อย 1 ครั้ง/ปี
4. ติดตั้งถังดับเพลิงแบบสารสนเคมีที่ห้อง Server จำนวน 2 ถัง

5.3 การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัสโจมตีระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เกิดความเสียหายแก่เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์

1. ทำการติดตั้ง Firewall ทำหน้าที่ป้องกันการเข้าถึงและกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก
2. มีการติดตั้งซอร์ฟแวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)
3. Update โปรแกรม Anti-virus ทุก 2 ชั่วโมง
4. ปิด USB Port ของเครื่องลูกข่ายที่ไม่เกี่ยวข้องกับธุรกรรมทางการเงิน
5. เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศสอนการตรวจสอบ Scan virus แก่บุคลากรอย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น
6. ตรวจสอบการทำงานของ Firewall และ User เพื่อวิเคราะห์การใช้งาน Internet ของ User

5.4 การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

1. กำหนดมาตรการควบคุมการเข้าออกห้อง Data Center และการป้องกันความเสียหาย
2. บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ห้ามเข้าไปในห้อง Data Center หากจำเป็นต้องได้รับอนุญาตและ มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้นำพาเข้าไป
3. ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตเข้าถึงระบบเครือข่าย และมีการติดตั้งระบบ ตรวจจับผู้บุกรุก IDS (Intrusion Detection System) มีระบบ ป้องกันผู้บุกรุก IPS (Intrusion Prevention System) และระบบบันทึกใช้งานเครือข่าย (Log File)
4. มีการกรอง Web Filtering & Mail Filtering เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website และเข้า website ไม่เหมาะสม ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
5. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่าย อินเตอร์เน็ตขององค์กร เพื่อสังเกตุปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป
6. การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ภายในองค์กร ได้ใช้ระบบพิสูจน์สิทธิ์ (Authorization) ก่อนเข้าใช้งานจะต้องมีชื่อในบัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ ตามอำนาจหน้าที่และความรับผิดชอบ
7. มีการปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ใช้งานระบบคอมพิวเตอร์และเครือข่าย ระเบียบดังกล่าวจะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัย คุกคามคอมพิวเตอร์ได้เป็นอย่างดีโดยบันทึกข้องมูลการจราจรทางคอมพิวเตอร์ที่ให้บริการ (Log File) ไว้อย่างน้อย 90 วัน

5.5 การเตรียมความพร้อมรับสถานการณ์จากผู้ใช้งานงานขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจ ในด้าน Hardware และ ด้าน Software เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เหลือน้อยที่สุด

1. วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบ เครือข่ายคอมพิวเตอร์
2.จัดทำคู่มือการใช้งานระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ
3.แนะนำการใช้งานเบื้องต้นกรณีขอมี Username & Password ใหม่
4.อบรมให้ความรู้แก่บุคลากรการใช้งาน Software ระบบ online, scan virus, ลบ Temp file, ลบขยะ, การใช้ Flash drive, การดูแลบำรุงรักษาเครื่องสำรองไฟฟ้า, การเปิด-ปิดเครื่อง, การทำความสะอาดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

5.6 การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการ

จัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

1) แผ่น Boot disk

2) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ/File config ระบบ Server

3) แผ่น/File สำรองข้อมูลและระบบงานที่สำคัญ

4) แผ่น/File โปรแกรม antivirus/spyware

5) แผ่น/File Driver อุปกรณ์ต่างๆ

6) ระบบสำรองไฟฉุกเฉิน

7) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

6. <u>การสำรองฐานข้อมูลระบบสารสนเทศไปไว้ที่อาคารอื่น</u> (Backup Site)

จะดำเนินการเมื่อเวลาสิบหกนาฬิกาของทุกวันทำการ เป็นแบบ Manual เพื่อเพิ่มความมั่นคงปลอดภัย และเมื่อมีเหตุภัยพิบัติ ผลการประเมินและวิเคราะห์สถานการณ์ความเสี่ยง เช่น อัคคีภัยเป็นต้น และหากปล่อยให้ข้อมูลและระบบสารสนเทศดังกล่าว ได้รับผลกระทบจากเหตุภัยพิบัติ จะส่งผลเสียหายต่อการดำเนินงานหลักของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์เป็นอย่างมาก

ดังนั้นโดยกลุ่มงานเทคโนโลยีสารสนเทศ ได้ติดตั้งระบบสำรองข้อมูลฉุกเฉินแบบ Manual ไว้ที่ตึกอังสนาชั้นสอง ซึ่งอยู่ต่างอาคารกัน เพื่อเตรียมการ เมื่อถึงเวลาฉุกเฉินดังกล่าว สามารถให้บริการได้ภายใน 2 ชั่วโมง ได้แก่

6.1 ระบบ HIS (Hospital Information System) บริการผู้ป่วย Online เครื่องแม่ข่ายให้บริการหลัก Ip Address 192.168.44.14 จัดเก็บข้อมูลไว้ที่เครื่อง

- เครื่องแม่ข่ายสำรองหมายเลข IP Address 192.168.44.15, 192.168.44.16, และ 192.168.44.17

6.2 ฐานข้อมูลระบบ Web Server ได้แก่ เว็บไซต์โรงพยาบาล ระบบฐานข้อมูลวิจัยด้านสุขภาพจิตและจิตเวช เว็บไซต์และฐานข้อมูลโครงการช่วยเหลือผู้ที่เสี่ยงต่อการฆ่าตัวตายจัดเก็บไว้ที่

- เครื่องแม่ข่ายหมายเลข IP Address 192.168.0.57 (Backup_Server)

6.3 ฐานข้อ Username & Password เพื่อใช้งาน Internet & Authentication จัดเก็บไว้ที่

- เครื่องแม่ข่ายหมายเลข IP Address 192.168.0.57 (Backup_Server)

6.4 ฐานระบบงานสำคัญตามภารกิจ เช่น ระบบข้อมูลครุภัณฑ์และเบิกจ่ายพัสดุ ระบบข้อมูลขออนุมัติไปราชการ ระบบฐานข้อมูลห้องสมุด ระบบข้อมูลเงินเดือน พกส. ระบบข้อมูลบุคลากร ระบบจองห้องประชุม ระบบขออนุมัติใช้รถยนต์จัดเก็บไว้ที่

- เครื่องแม่ข่ายหมายเลข IP Address 192.168.0.57 (Backup_Server)

7. <u>การนำระบบกลับคืนสู่สภาพปกติ (Restore)</u>

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำ

ได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1) จัดหาอุปกรณ์ชิ้นส่วนใหม่มีไว้สำรองเพื่อทดแทน

2.) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

5) นำฐานข้อมูลจาก Backup File/ CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบและโปรแกรมเมอร์) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

6) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูล และระบบอื่นๆที่เกี่ยวข้อง

8. แนวทางการปฏิบัติ

1) จัดทำ / ทบทวน และปรับปรุง คู่มือการสำรองข้อมูลและการกู้คืนข้อมูล

2) ประสานงานกับคณะกรรมการสิ่งแวดล้อมและความปลอดภัย เพื่อเข้าร่วมการซักซ้อมกรณีเกิดเหตุไฟไหม้

3) เมื่อมีอุปสรรคขัดข้องในการปฏิบัติตามแผนฯ ให้เจ้าหน้าที่ผู้รับผิดชอบหรือผู้เกี่ยวข้องหาทางแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่ หากไม่สามารถแก้ไขได้ให้รายงานและขอความช่วยเหลือจากผู้บริหารสูงสุด

9. การจัดองค์กรปฏิบัติการฉุกเฉินและกำหนดผู้รับผิดชอบในระบบสารสนเทศโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ เมื่อเกิดเหตุฉุกเฉิน ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

9.1 ระดับนโยบาย/ระดับอำนวยการ ได้แก่

1. ผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์/ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office: CIO)

รับผิดชอบ ในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม

ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

1) เป็นผู้บังคับบัญชาสูงสุดในการควบคุมและปฏิบัติการฉุกเฉินระบบสารสนเทศ

2) มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

3) กำหนดจุดปลอดภัยสำหรับบุคคลและวัสดุอุปกรณ์ต่างๆ ในสถานที่เหมาะสม ในการร่วมซ้อมแผนอัคคีภัย

4) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

9.2. ระดับประสานงานเหตุฉุกเฉิน ได้แก่

1. หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

2. ประธานคณะกรรมการสารสนเทศ

รับผิดชอบ

1) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ เพื่อระงับเหตุฉุกเฉิน

2) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์จะมาถึงที่เกิดเหตุ

3) มีอำนาจสั่งการแทนผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ ในกรณีที่ผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ ไม่สามารถสั่งการได้

4) สั่งการให้เจ้าหน้าที่ผู้เกี่ยวข้องมาปฏิบัติการตามแผนฯ

5) พิจารณาขั้นตอนและวิธีการป้องกันชีวิต ทรัพย์สิน ให้เสียหายน้อยที่สุด

6) กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือจำเป็นต้องขอเพิ่มเติมในอนาคต

9.3 ระดับหัวหน้าสั่งการ ณ ที่เกิดเหตุ ได้แก่

1. หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

2. รองหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

1) รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวนวางแผน

ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

2) แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่น และทรัพย์สินออกจากที่เกิดเหตุไปเก็บรักษา ณ จุดปลอดภัยโดยเร็ว

3) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์และเจ้าหน้าที่ประสานงานรักษาความปลอดภัย ทราบ

4) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และทำรายงานเสนอผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์เมื่อเหตุการณ์เข้าสู่สภาวะปกติ

9.4 ระดับทีมงานที่เกี่ยวข้องกับแผนและระดับทีมปฏิบัติงานตามแผน

ทีม	หน้าที่	ผู้รับผิดชอบ	ปฏิบัติตามแผน

1.ทีมรับผิดชอบดูแล บำรุงรักษาข้อมูล	มีหน้าที่เฝ้าระวังและ ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของข้อมูลพื้นฐาน รวมทั้งการทำสำเนาและกู้คืน ข้อมูลพื้นฐาน	1.หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ 2. นักวิชาการคอมพิวเตอร์ 3.นักเทคโนโลยีสารสนเทศ	เหตุเพลิงไหม้ (อัคคีภัย)
2.ทีมรับผิดชอบดูแลระบบโปรแกรมสารสนเทศ	มีหน้าที่เฝ้าระวังและ ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบโปรแกรมสารสนเทศ รวมทั้งการทำสำเนาและกู้คืน	1.หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ 2. นักวิชาการคอมพิวเตอร์	เหตุปัญหาไฟฟ้าดับ/ไฟกระชาก
3.ทีมรับผิดชอบดูแลระบบเทคโนโลยีคอมพิวเตอร์	มีหน้าที่เฝ้าระวังและ ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบเทคโนโลยีคอมพิวเตอร์ รวมทั้งดำเนินตามแผนรองรับสถานการณ์ฉุกเฉิน	1.หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ 2.นักเทคโนโลยีสารสนเทศ 3.เจ้าหน้าระบบงานคอมพิวเตอร์	เหตุปัญหาไฟฟ้าดับ/ไฟกระชาก
4.ทีมรับผิดชอบดูแลระบบเครือข่าย	มีหน้าที่เฝ้าระวังและ ตรวจสอบ แก้ไข บำรุงรักษา ข้อบกพร่องต่างๆของระบบเครือข่าย รวมทั้งการทำสำเนาและกู้คืนฐานข้อมูลบนระบบแม่ข่าย	1.หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ 2. นักวิชาการคอมพิวเตอร์ 3.เจ้าหน้าระบบงานคอมพิวเตอร์	เหตุบุกรุกและภัยคุกคามทางคอมพิวเตอร์

10. มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

10.1 กรณีเครื่องลูกข่าย

1.) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุนั้นให้เจ้าหน้าที่ของกลุ่มงานเทคโนโลยีสารสนเทศหรือผู้จัดการระบบฐานข้อมูลสารสนเทศ ทราบ หรือในกรณีเกิดจากระบบเทคโนโลยีสารสนเทศไม่สามารถให้บริการได้ตามปกติได้กลุ่มงานเทคโนโลยีสารสนเทศ จะต้องประกาศให้หน่วยงานที่เกี่ยวข้องทราบ

2.) กรณีเกิดการขัดข้องเนื่องจากไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็วในกรณีเหตุที่เกิดนั้นจะ

เป็นอันตราย ต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบไวรัส ให้ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ในชั้นนั้นออกให้หมด

3.) ให้เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้ให้แจ้งเหตุขัดข้องแก่หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศสารเทศฯ เพื่อแก้ไขปัญหาต่อไป

10.2 กรณีเครื่องแม่ข่ายบริการ (Server)

1.) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2.) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ Shut down เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และตรวจสอบประสิทธิภาพของเครื่องสำรองไฟฟ้า

3.) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ และให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

4.) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัย ให้รีบขนย้ายไปไว้ที่ปลอดภัย

5.) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

6.) รีบขนย้ายเครื่องคอมพิวเตอร์นั้นไปไว้ในที่ปลอดภัย

7.) ประสานขอความช่วยเหลือกับหน่วยรักษาความปลอดภัยหรือฝ่ายอาคารสถานที่ หรือหน่วยงานอื่นที่เกี่ยวข้องโดยเร็วที่สุด

- หน่วยรักษาความปลอดภัย โทร. 63322, 63323

- ฝ่ายอาคารสถานที่ โทร. 63310, 63311, 63312

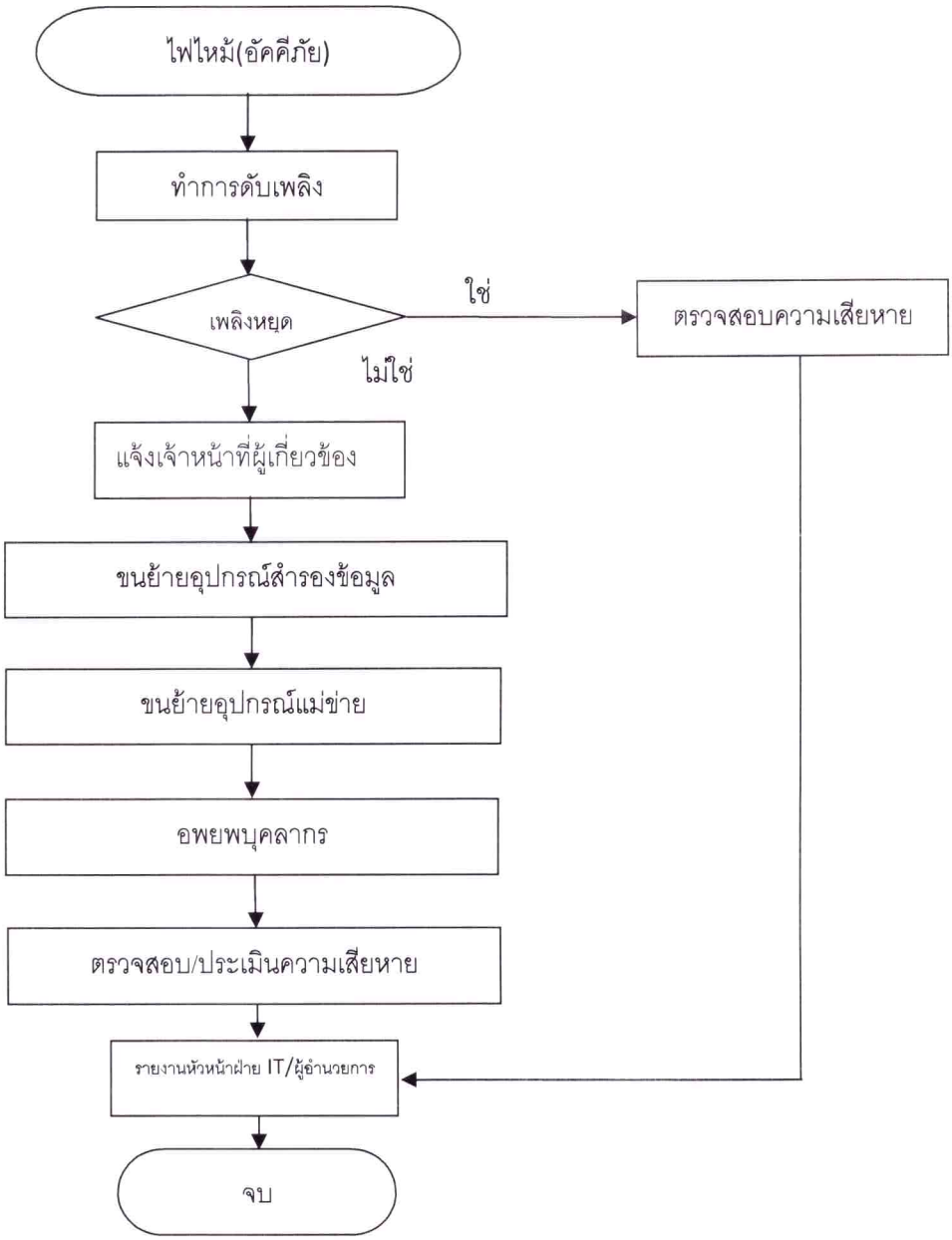
8.) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบจัดหาอุปกรณ์สำรอง หรือถ้าอยู่ในระยะเวลาประกันให้แจ้งบริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

9.) ผู้ดูแลระบบต้องรีบรายงานให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศและผู้อำนวยการทราบโดยเร็ว

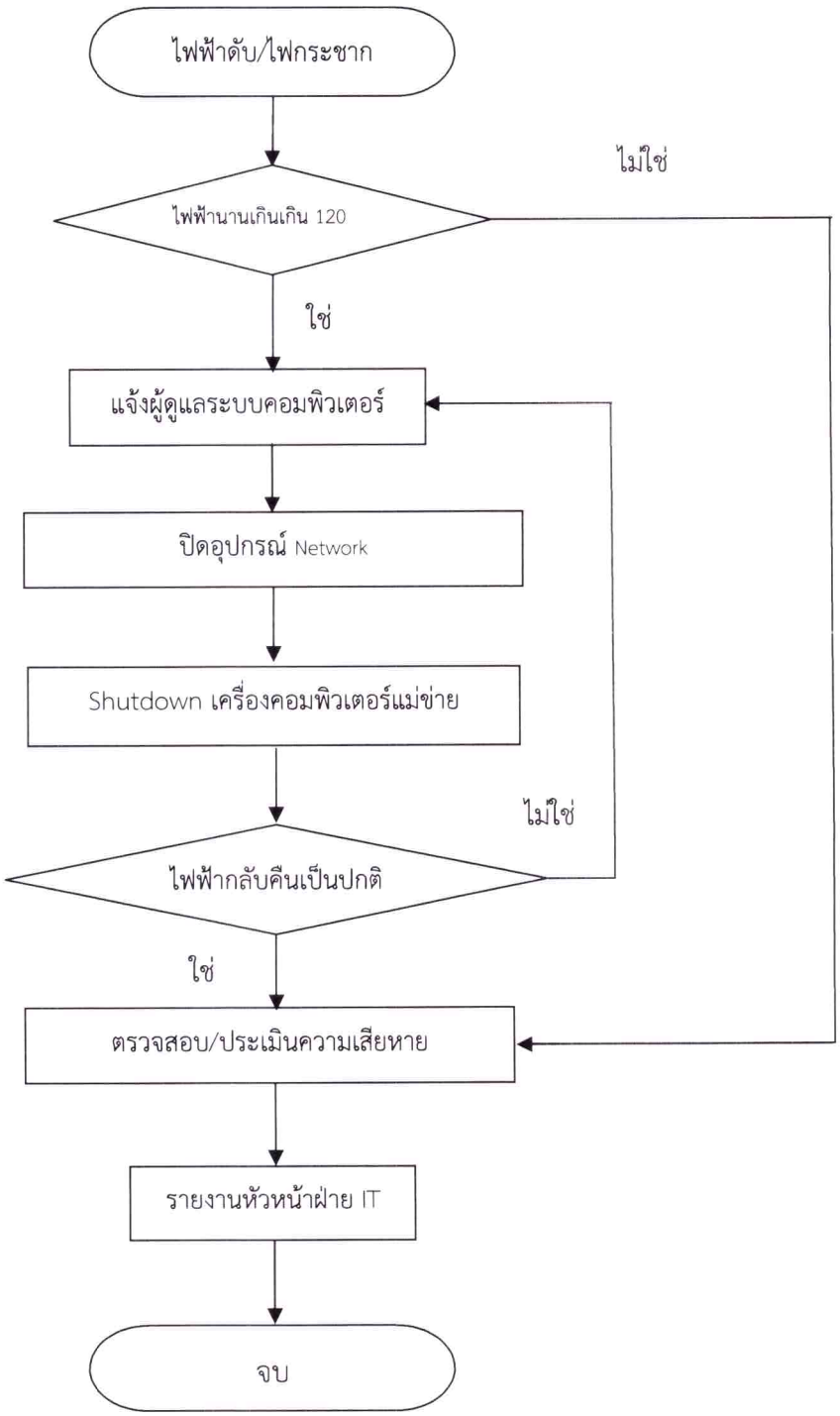
11. ผังกระบวนการ (Flow Chart)

ผัง Flowchart เพื่อรองรับการปฏิบัติการกรณีเกิดเหตุได้อย่างถูกต้องตามขั้นตอนที่จำเป็นต้องปฏิบัติอย่างเคร่งครัด โดยผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ 3 กรณี ดังต่อไปนี้ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติขั้นตอนในแต่ละกรณี โดยกรณีที่วิเคราะห์และกำหนดผังกระบวนการ ได้ประเมินจากปัจจัยด้านอาคารสถานที่ สภาพแวดล้อม บุคลากร และงบประมาณ ของโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

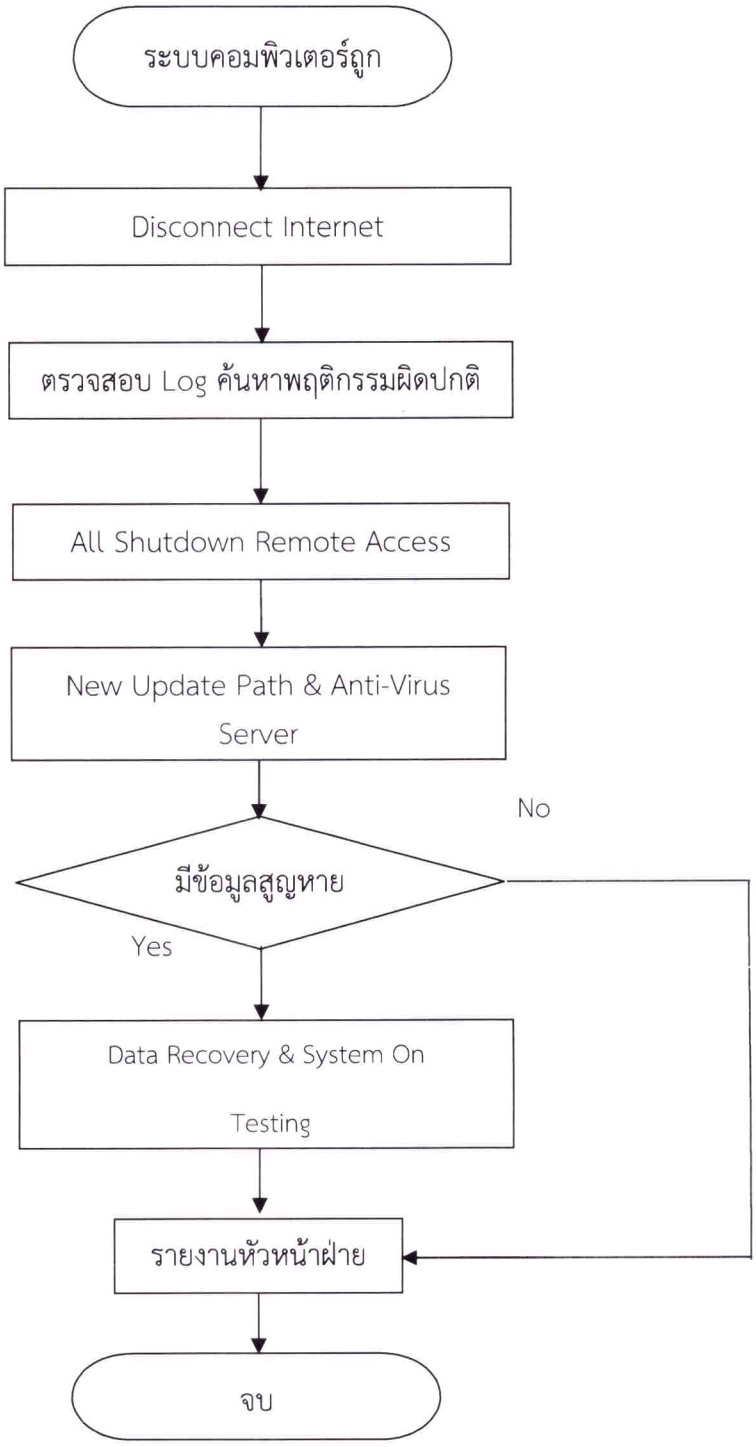
11.1 กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีขบวนการปฏิบัติดังนี้



11.2 กรณีเกิด ไฟฟ้าดับ/ไฟกระชาก..... มีขบวนการปฏิบัติดังนี้



11.3 กรณีเกิด เหตุบุกรุกและภัยคุกคามทางคอมพิวเตอร์ (HACK) มีขบวนการปฏิบัติดังนี้



12. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

12.1 ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตามกำกับดูแล ควบคุมตรวจสอบ การปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

12.1.1 ผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

12.1.2 หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

12.1.3 ประธานคณะกรรมการทีมนำด้านสารสนเทศ

12.2 ระดับปฏิบัติ

12.2.1 คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามคำสั่งโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

12.2.2 บุคลากรกลุ่มงานเทคโนโลยีสารสนเทศ โรงพยาบาลจิตเวชขอนแก่นราชนครินทร์ โดยมีหน้าที่

1.) ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบเครือข่ายคอมพิวเตอร์ และระบบรักษาความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

2.) รักษาความปลอดภัยของระบบฐานข้อมูล รวมทั้งการทำสำเนาฐานข้อมูลที่สำคัญ

3.) ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ฉบับนี้ตามแต่ละกรณีเหตุการณ์ที่เกิดขึ้น

ผู้เสนอแผน .....

(นายสมภาวรรณ์ ภาคภูมิ)

หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

25 ธันวาคม 2561

ผู้อนุมัติ .....

(นายณัฐกร จำปาทอง)

ผู้อำนวยการโรงพยาบาลจิตเวชขอนแก่นราชนครินทร์

25 ธันวาคม 2561