

แผนบริหารความต่อเนื่องในการให้บริการ  
BUSINESS CONTINUITY PLAN

**BCP**

กลุ่มงานสุขภาพดิจิทัล โรงพยาบาลเวียงป่าเป้า

## บทนำ

ด้วยโรงพยาบาลเวียงป่าเป้า ได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริการจัดการภายในองค์กร และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กรการบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรจึงจำเป็นต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าว จึงได้จัดทำแผนบริหารความต่อเนื่อง Business Continuity Plan : BCP ในการไปใช้งานได้อย่างต่อไป คาดหวังว่าแผนบริหารความต่อเนื่องเล่มนี้ จะเป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงานในสภาวะวิกฤต และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

## แผนการดำเนินการกรณีระบบสารสนเทศล่มโรงพยาบาลเวียงป่าเป้า (Business Continuity Plan : BCP)

แผนบริหารงานความต่อเนื่อง Business Continuity Plan : BCP จัดทำขึ้น เพื่อให้หน่วยงานภายในโรงพยาบาลเวียงป่าเป้าสามารถนำไปใช้ในการตอบสนอง และปฏิบัติงานในสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินต่างๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร โดยไม่ให้การดำเนินงานต้องหยุดลง หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง การที่หน่วยงานไม่มีกระบวนการรองรับให้การดำเนินงานเป็นไปอย่างต่อเนื่อง อาจส่งผลกระทบต่อหน่วยงานในด้านต่างๆ เช่น ด้านการให้บริการทางระบบงานคอมพิวเตอร์และระบบเครือข่าย ด้านการพัฒนาาระบบสารสนเทศ ด้านการเข้าช่วยเหลือเพื่อซ่อมบำรุงอุปกรณ์ระบบคอมพิวเตอร์ ด้านการให้บริการระบบอินเทอร์เน็ตกับ ดังนั้นการจัดทำแผนบริหารความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้หน่วยงานสามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิดและทำให้กระบวนการสำคัญ สามารถกลับมาดำเนินการได้อย่างปกติ ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นได้

กรอบแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤติ 4 ขั้นตอน คือ

1. การสร้างความรู้ความเข้าใจให้กับบุคลากรภายในโรงพยาบาลเวียงป่าเป้า
2. การเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศ ในการจัดทำแผนรองรับการดำเนินการกิจการ ให้บริการด้านเทคโนโลยีสารสนเทศ ตามบทบาทหน้าที่ได้อย่างต่อเนื่อง (Business Continuity Plan: BCP)
3. การซักซ้อมแผนและนำไปปฏิบัติได้จริง
4. การจัดการหลังเกิดภัย

โดยแนวคิดการบริหารความต่อเนื่องของหน่วยเทคโนโลยีสารสนเทศ คือ การควบคุมดูแลและป้องกันทรัพยากรที่สำคัญต่อการดำเนินงานหรือการให้บริการ เพื่อสร้างประโยชน์สูงสุดสำหรับผู้รับบริการ

### 1.วัตถุประสงค์

- 1.1 เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง
- 1.2 เพื่อให้หน่วยเทคโนโลยีสารสนเทศมีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤติตามแผนที่ได้

กำหนดไว้

- 1.3 เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ
- 1.4 เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

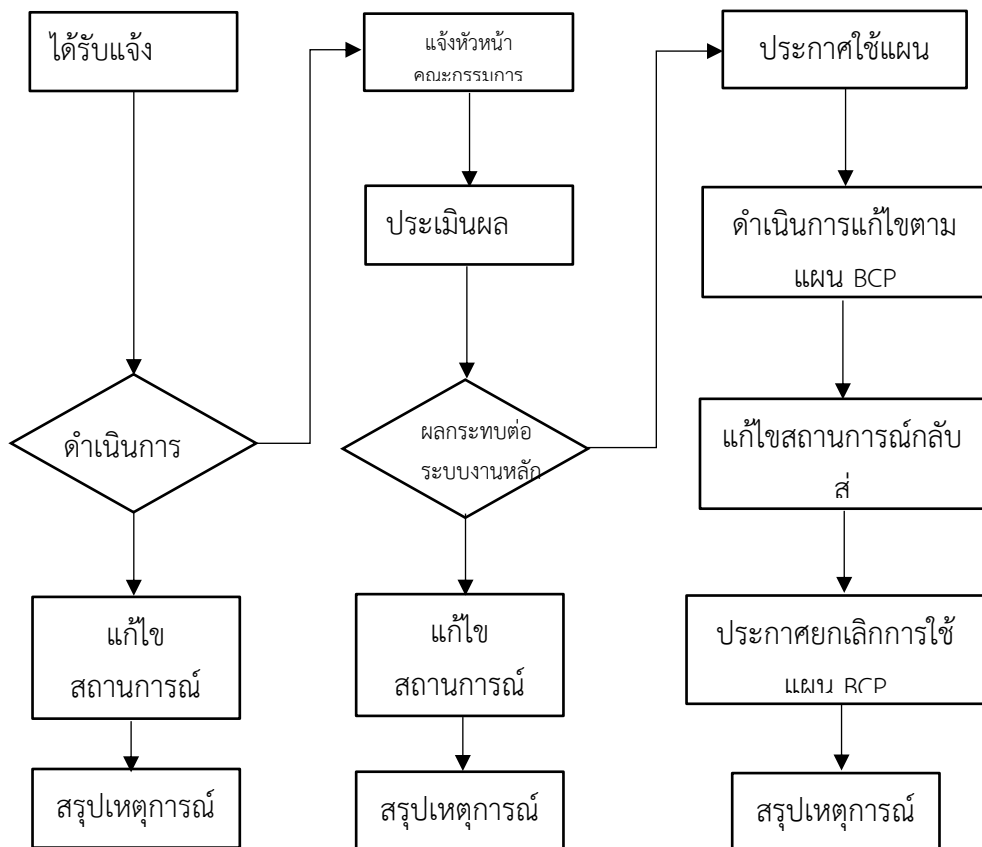
### 2.การประเมินผลกระทบที่เกิดขึ้นกับองค์กรในกรณีที่เกิดการหยุดชะงัก (Business Impact Analysis)

ระบบงาน	ระยะเวลาระบบหยุดทำงาน		
	ระยะเวลา น้อยกว่า 30 นาที	ระยะเวลา 30 - 60 นาที	ระยะเวลา มากกว่า 60 นาที
ระบบ HOSxP	ปานกลาง	ปานกลาง	รุนแรง
ระบบเครือข่ายโรงพยาบาลทั้งระบบ	ปานกลาง	ปานกลาง	รุนแรง
Internet	ไม่รุนแรง	ปานกลาง	รุนแรง

รายละเอียดของระดับเหตุการณ์ต่าง ๆ

ระดับของเหตุการณ์	รายละเอียด
ไม่รุนแรง	ระดับเหตุการณ์ ที่ไม่รุนแรง เป็นระดับที่สามารถยอมรับได้ หน่วยงานต่างๆ ยัง สามารถรอ ได้
ปานกลาง	ระดับปานกลางเป็น ระดับเหตุการณ์ที่ คณะกรรมการ BCP จะต้องมีการประชุม เพื่อประเมินระดับ ความรุนแรงของสถานการณ์เพื่อทำการพิจารณา จะประกาศใช้ แผน หรือไม่
รุนแรง	ระดับเหตุการณ์ถึงระดับที่รุนแรงเป็นระดับที่วิกฤตจะดำเนินการประกาศใช้แผน BCP ในการดำเนินงานทันที

ลำดับขั้นตอน ในการประกาศใช้แผนสร้างความต่อเนื่องเมื่อเกิดเหตุการณ์ฉุกเฉิน





4. หัวหน้ากลุ่มงานสุขภาพดิจิทัลแจ้ง/สื่อสารและประชาสัมพันธ์ ประกาศแจ้งให้ผู้มาใช้บริการและเจ้าหน้าที่รับทราบความปัญหาและการดำเนินการแก้ไขของระบบสารสนเทศล่ม อาจได้รับความล่าช้าหรือได้รับความสะดวกน้อยลงขออภัยมา ณ ที่นี้ รวมทั้งประชาสัมพันธ์ให้เจ้าหน้าที่ดำเนินการตามแผนปฏิบัติการของหน่วยงาน

5. ภายหลังจากสิ้นสุดแผนปฏิบัติการฉุกเฉินกรณีระบบสารสนเทศล่ม ให้แต่ละจุดบริการดำเนินการลงบันทึกข้อมูลย้อนลงเข้าสู่ระบบตามแผน งานสารสนเทศกลุ่มงานสุขภาพดิจิทัลร่วมประเมินความเสียหาย และสรุปเพื่อรายงานต่อผู้บริหาร

### วิธีการดำเนินงานเมื่อประกาศใช้แผน Business Continuity Plan (BCP)

#### แนวทางปฏิบัติสำหรับหน่วยงาน กรณีระบบสารสนเทศล่ม

1. เมื่อระบบสารสนเทศเกิดขัดข้อง ทางเจ้าหน้าที่ IT ตรวจสอบเอง หรือได้รับแจ้งจากหน่วยงานต่างๆ (User) ที่ใช้งานให้เจ้าหน้าที่ IT เร่งตรวจสอบสาเหตุอย่างเร่งด่วน

2. เมื่อพบสาเหตุแล้ว ให้วิเคราะห์ว่าเกิดจากสาเหตุอะไร และประเมินระยะเวลาที่จะต้องดำเนินการแก้ไขระบบ จากนั้นให้แจ้งหัวหน้ากลุ่มงานสุขภาพดิจิทัล เพื่อประกาศแผนปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ล่ม

3. หลังจากที่ใช้ประกาศใช้แผน BCP ทีมแก้ไขระบบเข้าแก้ไขปัญหาหากระบบสามารถใช้งานได้ตามปกติแล้วให้ประกาศ(เข้าสู่ภาวะปกติ) โดยหัวหน้ากลุ่มงานสุขภาพดิจิทัลแจ้งงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทางเสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า “ขณะนี้ ระบบสารสนเทศโรงพยาบาล ใช้งานได้ปกติแล้ว เข้าสู่ภาวะการทำงานปกติ”

4. ให้ทุกหน่วยงานหลังจากประกาศ (เข้าสู่ภาวะปกติ) ปฏิบัติตามแนวทางของแต่ละหน่วยงาน พร้อมบันทึกข้อมูลการให้บริการผู้ป่วยในส่วนที่เกี่ยวข้องย้อนหลังในระหว่างระบบสารสนเทศล่มไม่สามารถใช้งานได้ให้ครบถ้วนในของการให้บริการภายใน 24 ชั่วโมง

#### แนวทางปฏิบัติสำหรับหน่วยงาน กรณีระบบสารสนเทศล่ม

##### งานเวชระเบียนผู้ป่วยนอก

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. กรณีบัตรใหม่ : ให้เจ้าหน้าที่ห้องบัตรทำการชั่งประวัติผู้ป่วยใหม่ตามแบบฟอร์มกรอกประวัติผู้ป่วยใหม่ของโรงพยาบาลให้ครบถ้วน
3. กรณีบัตรเก่า : ค้นประวัติผู้ป่วยเก่าตามหมายเลข HN ของบัตรประจำตัวโรงพยาบาลผู้ป่วย
4. ออกใบสั่งยาชั่วคราวพร้อมกรอกรายละเอียดของผู้ป่วยที่สำคัญ คือ ชื่อ-สกุล, เลข HN, เลขบัตรประชาชน 13 หลัก, ลงสิทธิการรักษาผู้ป่วย (ในกรณีที่ทราบข้อมูล)
5. ส่งประวัติผู้ป่วยพร้อมใบสั่งยาชั่วคราวส่งห้องตรวจต่างๆ
6. ห้องบัตรลงทะเบียน HN ผู้ป่วยที่ส่งห้องตรวจต่างๆ ในสมุดทะเบียน

7. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้เจ้าหน้าที่ห้องบัตรลงทะเบียนผู้ป่วยส่งตรวจรักษาในโปรแกรม HOSxP จากสมุดทะเบียนที่ลงบันทึกไว้

#### ห้องตรวจโรคผู้ป่วยนอก (OPD)

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. พยาบาลหน้าห้องตรวจซักประวัติผู้ป่วย และเขียนบันทึกลงในแฟ้มเวชระเบียนผู้ป่วยนอก โดยให้มีรายละเอียดครบถ้วนตามมาตรฐานการดูแลรักษาผู้ป่วย และสืบค้นประวัติข้อมูลสุขภาพผ่านระบบ MOPH PHR viewer ผ่าน URL <https://phr1.moph.go.th/phr/> (หมอปพร้อม)
3. แพทย์ดำเนินการตรวจรักษา และตรวจสอบประวัติผู้ป่วยสืบค้นประวัติข้อมูลสุขภาพผ่านระบบ MOPH PHR viewer ผ่าน URL <https://phr1.moph.go.th/phr/> (หมอปพร้อม) แพทย์บันทึกการรักษาในแฟ้มเวชระเบียน โดยให้มีรายละเอียดครบถ้วนตามมาตรฐานการดูแลรักษาผู้ป่วย
4. ในกรณีมีการส่ง Lab , X-ray ให้แพทย์เขียนรายละเอียดการส่งในแฟ้มเวชระเบียน และใบส่งตรวจ
5. แพทย์บันทึกคำวินิจฉัยโรค และรายการส่งยา ลงในแฟ้มเวชระเบียนผู้ป่วยนอก และใบส่งยา
6. พยาบาลหน้าห้องตรวจลงทะเบียนผู้ป่วยที่มารับบริการในคลินิก **ในสมุดทะเบียน**
7. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้พยาบาลหน้าห้องตรวจลงรายละเอียดการตรวจรักษาผู้ป่วยในโปรแกรม HOSxP จากสมุดทะเบียนที่ลงบันทึกไว้ และแฟ้มเวชระเบียนที่ลงบันทึกการรักษาไว้ ภายใน 24 ชั่วโมง

#### ห้องจ่ายยา

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. เภสัชกรจัดยา และจ่ายยาตามใบสั่งยา ของแพทย์ หากต้องการสืบค้นประวัติข้อมูลสุขภาพผ่านระบบ MOPH PHR viewer ผ่าน URL <https://phr1.moph.go.th/phr/> (หมอปพร้อม)
3. แยกใบสั่งยาไว้ลงข้อมูลย้อนหลัง
4. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้เจ้าหน้าที่เภสัชกรห้องจ่ายยาลงรายละเอียดการสั่งยาในโปรแกรม HOSxP จากใบสั่งยาที่แยกเก็บไว้ ภายใน 24 ชั่วโมง

#### ห้องการเงิน

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. เจ้าหน้าที่การเงินเก็บเงินค่าบริการตามใบสั่งยา โดยอ้างอิงค่าใช้จ่ายจากราคาการให้บริการของกรมบัญชีกลาง และออกใบเสร็จโดยเขียนรายละเอียดให้ครบถ้วนให้ผู้ป่วย
3. เจ้าหน้าที่การเงินลงทะเบียนรับเงิน และออกใบเสร็จ**ในสมุดทะเบียนการเงิน**
4. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้เจ้าหน้าที่การเงินลงรายละเอียดการรับเงินในโปรแกรม HOSxP จากสมุดทะเบียนการเงิน ภายใน 24 ชั่วโมง

### ห้องตรวจพยาธิวิทยาคลินิก (Lab)

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. เจ้าหน้าที่พยาธิวิทยาคลินิกรับรายการส่งตรวจ Lab จากใบส่งตรวจ หรือในแฟ้มเวชระเบียนผู้ป่วย
3. ลงทะเบียนการส่ง Lab พร้อมรายละเอียดการส่ง ในสมุดทะเบียนการส่ง Lab หากต้องการสืบค้นประวัติข้อมูลสุขภาพผ่านระบบ MOPH PHR viewer ผ่าน URL <https://phr1.moph.go.th/phr/> (หมอมพร้อม)
4. คำนวณ และบันทึกค่าบริการทางห้องปฏิบัติการตามมาตรฐานราคากรมบัญชีกลางทั้งหมดลงในใบส่งตรวจ
5. ดำเนินการเจาะเก็บตัวอย่าง Speciment ของผู้ป่วย จากนั้นดำเนินการตรวจวิเคราะห์ด้วยเครื่องตรวจทางห้องปฏิบัติการ LIS
6. พิมพ์รายงานผลการตรวจวิเคราะห์ พร้อมรับรองผลการตรวจวิเคราะห์ จากนั้นส่งให้แพทย์ ที่ห้องตรวจผู้ป่วยส่ง Lab มา
7. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้เจ้าหน้าที่พยาธิวิทยาคลินิกลงทะเบียนการส่ง Lab ในโปรแกรม HOSxP จากสมุดทะเบียนการส่ง Lab จากนั้นให้ตรวจสอบดูว่ามีการโอนข้อมูลผล Lab จากระบบ LIS กลับเข้ามาในระบบ HOSxP ครบถ้วนถูกต้องหรือไม่ ภายใน 24 ชั่วโมง

### ห้องตรวจเอกซเรย์ (X-Ray)

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. เจ้าหน้าที่ห้องเอกซเรย์รับรายการส่งตรวจ X-Ray จากใบส่งตรวจ หรือในแฟ้มเวชระเบียนผู้ป่วย
3. ลงทะเบียนการส่งตรวจ X-Ray พร้อมรายละเอียดการส่ง ในสมุดทะเบียนการส่ง X-Ray
4. คำนวณ และบันทึกค่าบริการทางห้องเอกซเรย์ตามมาตรฐานราคากรมบัญชีกลางทั้งหมดลงในใบส่งตรวจ
5. ส่งผู้ป่วยเข้าเครื่องถ่ายภาพเอกซเรย์
6. เจ้าหน้าที่ห้องเอกซเรย์ตรวจสอบคุณภาพฟิล์ม พร้อมรายงานส่งภาพถ่ายเอกซเรย์ในระบบ Pack หรือส่งฟิล์มเอกซเรย์ให้ผู้ป่วยเพื่อให้แพทย์ดูประกอบการวินิจฉัย
7. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้เจ้าหน้าที่เอกซเรย์ลงทะเบียนการส่งเอกซเรย์ในโปรแกรม HOSxP จากสมุดทะเบียนการส่ง ให้ครบถ้วนสมบูรณ์ ภายใน 24 ชั่วโมง

### หอผู้ป่วยใน (Ward)

1. แจ้งผู้ป่วยให้ทราบว่าระบบโปรแกรมการให้บริการผู้ป่วย HOSxP ไม่สามารถใช้งานได้
2. พยาบาลประจำหอผู้ป่วยลงรายละเอียดการตรวจรักษาตามมาตรฐานและให้ครบถ้วนในแฟ้มเวชระเบียนผู้ป่วยใน

3. ในกรณีมีผู้ป่วย Admit ใหม่ในระหว่างโปรแกรม HOSxP ใช้งานไม่ได้ เมื่อระบบโปรแกรม HOSxP ใช้งานได้ปกติ ให้ส่งข้อมูลผู้ป่วยในให้ศูนย์ Admit ขึ้นทะเบียนผู้ป่วยในย้อนหลัง
4. ในกรณีผู้ป่วยมีการสั่ง Lab,X-Ray,Set ผ่าตัด ให้เขียนลงในใบ Order แล้วจึงส่งผู้ป่วยไปตรวจตามคำสั่งแพทย์
5. เมื่อระบบโปรแกรมการให้บริการผู้ป่วย HOSxP สามารถใช้งานได้ปกติ ให้พยาบาลประจำหอผู้ป่วย ลงข้อมูลการให้บริการผู้ป่วยย้อนหลังในโปรแกรม HOSxP จากแฟ้มเวชระเบียนผู้ป่วยใน ให้ครบถ้วนสมบูรณ์ ภายใน 24 ชั่วโมง
6. หากต้องการสืบค้นประวัติข้อมูลสุขภาพผ่านระบบ MOPH PHR viewer ผ่าน URL <http://phr1.moph.go.th/phr/> (หมออพร้อม)

### แผนรองรับสถานการณ์ฉุกเฉินกลุ่มงานสุขภาพดิจิทัล

#### สถานการณ์ฉุกเฉินศูนย์คอมพิวเตอร์ที่เกิดจากความขัดข้องด้านเทคนิค

##### กรณีการป้องกันไวรัสลึ้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุเจ้าหน้าที่ITทราบ หรือกรณีมีเหตุอันทำให้ศูนย์คอมพิวเตอร์ไม่สามารถดำเนินการให้บริการด้านระบบเครือข่ายได้ก็จะต้องประกาศให้ทุกหน่วยงานได้รับทราบ

##### กรณีการเชื่อมโยงเครือข่ายลึ้มเหลว

- รับผิดชอบการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่ายเพื่อดำเนินการซ่อมแซมสายเคเบิลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

##### กรณีระบบเครือข่ายภายใน(LAN) ไม่สามารถใช้งานได้

- รับผิดชอบการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากการเชื่อมต่อใช้งานไม่ได้บางจุดให้ตรวจสอบอุปกรณ์ Swtich ของจุดบริการนั้นๆ ดำเนินการแก้ไข/หาอุปกรณ์มาเปลี่ยนทดแทนให้ระบบสามารถใช้งานได้

- หากการเชื่อมต่อใช้งานไม่ได้ทั้งโรงพยาบาลให้ตรวจสอบอุปกรณ์ Core Switch ในห้องคอมพิวเตอร์แม่ข่าย ดำเนินการแก้ไข/ดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

#### กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 30 นาที
- หากใกล้ครบ 30 นาทีแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้ากลุ่มงานสุขภาพดิจิทัล
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

กรณีเครื่องแม่ข่ายหลัก HOSxP ล่ม ไม่สามารถใช้งานได้ ให้ดำเนินการใช้เครื่องแม่ข่ายสำรอง HOSxP และดำเนินการซ่อมแซมเครื่องแม่ข่ายหลัก HOSxP ให้สามารถใช้งานได้ปกติโดยเร็ว

#### สถานการณ์ฉุกเฉินศูนย์คอมพิวเตอร์ที่เกิดจากภัยต่างๆ

##### กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานอาคาร สถานที่ (หัวหน้ากลุ่มงานบริหาร)
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

##### กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ห้อง ชั้น 2 หรือสถานที่ที่เหมาะสมต่อไป
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

- เจ้าหน้าที่ITตรวจสอบรายการทรัพย์สิน สํารวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้ต่อไป

### การทบทวนและติดตามการซ้อมแผนความต่อเนื่อง (Testing the Plan)

1. มีการทดสอบแผนบริหารความต่อเนื่องฯ บางส่วนหรือทั้งหมดเป็นประจำทุกปี เพื่อให้มั่นใจว่าหน่วยงานมีการเตรียมตัวและมีความสามารถในการกู้คืนระบบสำคัญภายในระยะเวลาที่กำหนดไว้

2. ทดสอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยการสร้างสถานการณ์จำลอง (Simulation Exercises) เป็นประจำทุกปี โดยต้องมีการปรับเปลี่ยนหมุนเวียนสถานการณ์จำลอง เพื่อให้แน่ใจว่าได้ มีการทดสอบความสูญเสีย/เสียหายของปัจจัยหลักที่เกี่ยวข้องทุกๆ 1 ปี

3. ข้อบกพร่องใด ๆ (GAP) ที่เกิดจากการทดสอบบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ จะต้องมีการติดตามให้เสร็จสิ้นภายใน 3 เดือน นับตั้งแต่วันที่ทดสอบ ถ้าไม่สามารถดำเนินการติดตามได้ตามเวลาที่กำหนดให้ หัวหน้าทีมบริหารและผู้ประสานงานความต่อเนื่องด้านเทคโนโลยีสารสนเทศได้แจ้งผู้บริหารระดับสูงเพื่อพิจารณาแนวทางแก้ไขข้อบกพร่องนั้น ๆ ให้หมดไปโดยเร็ว

การทบทวนการดำเนินงาน การจัดการกับเหตุการณ์เพื่อเตรียมการป้องกันของการเกิดเหตุในครั้งนี้อาจจะต้องปรับปรุงอย่างไรต่อไป

### การรายงานผล บันทึกข้อความสรุปรายงาน มีเนื้อหาประเด็นดังนี้

- ระบุสาเหตุของเหตุการณ์ที่เกิดขึ้น
- ประเมินค่าความเสียหายที่เกิดขึ้น
- ประเมินผลกระทบต่อระบบสารสนเทศ
- ระบุแนวทางการดำเนินการแก้ไข เพื่อป้องกันการเกิดขึ้นซ้ำอีกของเหตุการณ์นี้ในอนาคต
- ประเมินความเหมาะสมในการตัดสินใจดำเนินการ เพื่อรับมือและจัดการกับเหตุที่เกิดขึ้น
- ประเมินความเหมาะสมด้านระยะเวลาในการแก้ไข กระบวนการสำคัญและระบบสำคัญ เพื่อให้กลับคืนมาให้บริการได้
- ประเมินความเหมาะสมด้านสิ่งต่างๆ ที่ได้เตรียมการไว้ก่อนล่วงหน้า
- ทบทวนจากข้อมูลที่บันทึกไว้ระหว่างการเกิดเหตุ ว่ามีสิ่งใดที่มองข้ามไป คาดการณ์ผิดหรือเป็นข้อบกพร่องที่ต้องแก้ไข
- ทบทวนแผนการบริหารจัดการกับเหตุการณ์ความมั่นคงปลอดภัยนี้ ควรปรับปรุง ให้ครอบคลุมในจุดไหนมากขึ้น หรือเพื่อให้ใช้งานหรือรับมือในสถานการณ์ได้ดีขึ้น
- ทบทวนว่าจำเป็นต้องมีการอบรม ฝึกฝน หรือสร้างความตระหนักเพิ่มเติมหรือไม่
- ระบุสิ่งที่ต้องดำเนินการปรับปรุงหรือแก้ไขเพิ่มเติม เช่น นโยบาย ขั้นตอนการปฏิบัติหรืออื่นๆ



โรงพยาบาลเวียงป่าเป้า  
Wiang Pa Pao Hospital

แผนการดำเนินงานกู้คืนระบบสารสนเทศ  
โรงพยาบาลเวียงป่าเป้า  
(Disaster Recovery Plan : DRP)

จัดทำโดย

งานสารสนเทศกลุ่มงานสุขภาพดิจิทัล  
โรงพยาบาลเวียงป่าเป้า

## บทนำ

ด้วยโรงพยาบาลเวียงป่าเป้า ได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริการจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการทำงานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กรการบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรจึงจำเป็นต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าว ไปใช้งานได้อย่างต่อเนื่อง จึงได้จัดทำแผนการกู้คืนระบบสารสนเทศโรงพยาบาล จึงได้จัดทำแผนการกู้คืนระบบสารสนเทศโรงพยาบาลเวียงป่าเป้า Disaster Recovery Plan : DRP ขึ้นเพื่อเป็นการป้องกันการเสียหายของระบบและข้อมูลสารสนเทศในกรณีที่โรงพยาบาลเวียงป่าเป้าได้ประสบเหตุการณ์ไม่คาดขึ้น ไม่ว่าจะเป็นภัยธรรมชาติ ภัยจากมนุษย์ หรือเหตุอื่นใดที่ทำให้ระบบสารสนเทศของโรงพยาบาลได้รับความเสียหายหรือขัดข้อง เพื่อให้โรงพยาบาลเวียงป่าเป้าสามารถให้บริการ คาดหวังว่าแผนบริหารความต่อเนื่องเล่มนี้ จะเป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงานในสภาวะวิกฤต และสามารถปฏิบัติงานได้อย่างต่อเนื่องและสร้างความเชื่อมั่นให้กับผู้มารับบริการและญาติ

งานสารสนเทศกลุ่มงานสุขภาพดิจิทัล

**แผนการดำเนินการกู้คืนระบบกรณีระบบสารสนเทศล่มโรงพยาบาลเวียงป่าเป้า**  
(Disaster Recovery Plan : DRP)

แผนการกู้คืนระบบ Disaster Recovery Plan : DRP จัดทำขึ้น เพื่อให้โรงพยาบาลเวียงป่าเป้านำไปใช้ในการปฏิบัติงานในสภาวะวิกฤติ ที่ส่งผลให้ระบบสารสนเทศที่ใช้ปฏิบัติงานหลัก ไม่สามารถให้บริการได้ โดยแผนการกู้คืน ได้แนวทางการวิเคราะห์ความสำคัญของกระบวนการในภารกิจที่มีระบบสารสนเทศที่ใช้งานเป็นหลัก ซึ่งเมื่อมีการหยุดชะงักจะก่อให้เกิดผลกระทบต่อการทำงานการให้บริการผู้ป่วย และฐานข้อมูลหลักของโรงพยาบาลเวียงป่าเป้าคือระบบ HIS (โปรแกรม HOSxPXE4) จึงได้นำระบบฐานข้อมูลหลักของโรงพยาบาลมาจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสามารถกลับมาดำเนินการได้ตามปกติหรือให้บริการได้ในสภาวะฉุกเฉินในระยะเวลาที่เหมาะสม ลดความรุนแรงของเหตุการณ์ที่เกิดขึ้นได้

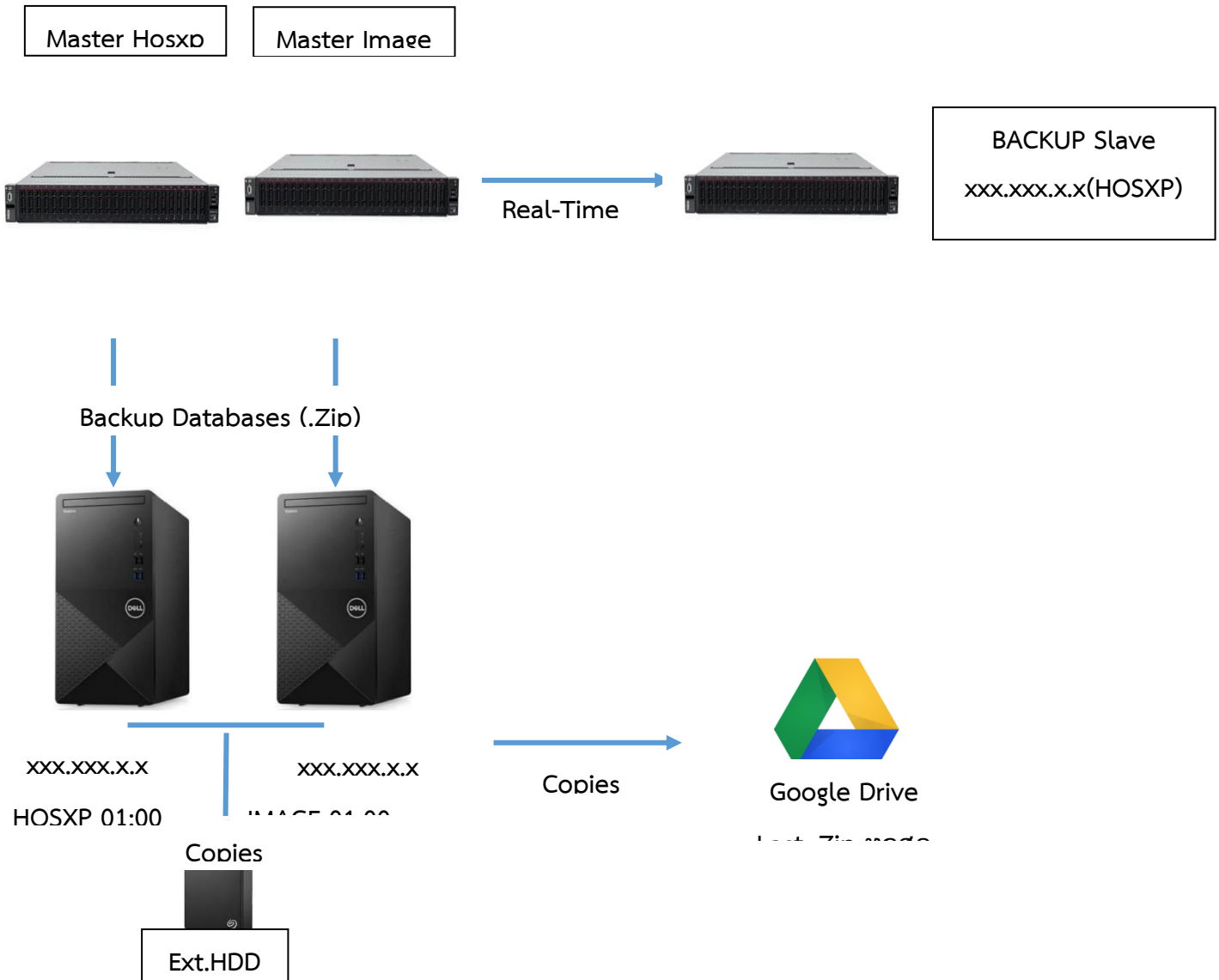
**1. วัตถุประสงค์**

- 1.1 จัดทำแผนกู้คืนระบบสารสนเทศเพื่อนำไปปฏิบัติใช้เมื่อเกิดเหตุการณ์ภัยพิบัติที่อาจส่งผลกระทบต่อการทำงานให้บริการผู้ป่วยในโรงพยาบาลเวียงป่าเป้า
- 1.2 เพื่อให้เจ้าหน้าที่งานสารสนเทศกลุ่มงานสุขภาพดิจิทัลหรือผู้เกี่ยวข้องทราบขั้นตอนการรับมือ
- 1.3 เพื่อลดผลกระทบจากการหยุดชะงักในการให้บริการ

**2. นโยบายในการจัดทำแผนกู้คืนระบบ**

ระยะเวลา	หน่วยให้บริการ	แผนกสารสนเทศโรงพยาบาล
< 30 นาที	1.ประกาศแจ้งผู้รับบริการ(ผู้ป่วย+ญาติ) ทราบ 2.ดำเนินการตามแผนBCP User ทุกระดับเหตุการณ์บันทึกข้อมูลเข้าระบบ	1.แจ้งผู้บังคับบัญชาตามลำดับ 2. ประกาศแจ้งผู้รับบริการและผู้ใช้งานทราบ 3.ตรวจสอบปัญหา 4.ดำเนินการแก้ไขเบื้องต้น
30 นาที – 60 นาที	1.ดำเนินการตามแผนBCP ทุกหน่วยงานดำเนินการตามแนวทางปฏิบัติ	1.แจ้งผู้บังคับบัญชาตามลำดับ 2.ประกาศใช้แผน BCP 3.ดำเนินการแก้ไขปัญหาต่อไป
> 60 นาที	1.ประกาศและปิดประกาศแจ้งผู้รับบริการ(ผู้ป่วย+ญาติ) ทราบ 1.1.งดให้บริการในส่วนของผู้ป่วยรายใหม่และผู้ป่วยที่ไม่ฉุกเฉิน 1.2.ผู้ป่วยฉุกเฉินให้บริการตามปกติ 2.ดำเนินการตามแผนBCP ทุกหน่วยงานดำเนินการตามแนวทางปฏิบัติ 3.เก็บข้อมูลต่างๆ ไว้ บันทึกเข้าระบบสารสนเทศโรงพยาบาลในภายหลัง	1.แจ้งผู้บังคับบัญชาตามลำดับ 2.ประกาศใช้แผน BCP 3.ดำเนินการแก้ไขปัญหาต่อไป

### 3. วิธีการสำรองข้อมูล



#### วิธีการสำรองข้อมูล

1. การสำรองข้อมูลแบบ Replication
  - 1.1 เครื่องคอมพิวเตอร์หลัก (Master) (IP:xxx.xxx.x.x) สำรองข้อมูลรูปแบบการจำลองข้อมูลแบบ Replication ไปยังเครื่องคอมพิวเตอร์แม่ข่ายสำรอง(Slave) Physical Server (IP:xxx.xxx.x.x) แบบเรียลไทม์
2. การสำรองฐานข้อมูล
  - 2.1 เครื่องคอมพิวเตอร์แม่ข่ายหลักจะสำรองข้อมูลอัตโนมัติ(Auto backup databases) ทุกวันเวลา 01.00 โดยเก็บไฟล์ไว้ในโฟลเดอร์ E:/BackupHosxp
  - 2.2 สำเนาไฟล์ข้อมูลแบบ OFFSITE เก็บไว้บน External HDD ย้อนหลังได้ 7วัน
  - 2.3 สำเนาไฟล์ล่าสุดข้อมูลแบบ OFFSITE จาก External HDD ลงใน Google Drive

## การกู้ข้อมูล (Recovery)

### 1. กรณีเครื่องลูกข่าย

1.1 ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้หนึ่งแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบหรือกรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้จะต้องประกาศให้ทุกงานในสังกัดทราบ

1.2 ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุชัดเจนให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

### 2. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟฟ้า

2.3 ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

2.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

2.5 ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และ ระบบเครือข่ายโดยเร็วที่สุด

2.6 ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รับหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

2.7 ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

### 3. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ให้ดำเนินการดังนี้

3.1 เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

3.2 สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

3.3 แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

4. หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากร สามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติดังนี้

4.1 ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

4.2 ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนี ไฟอย่างละเอียด

4.3 ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจาก ห้องทำงานตนเองไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

4.4 เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้เปิดสัญญาณเตือนเพลิงไหม้จากนั้นออก จากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

4.5 เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ให้รีบหาทางหนีออกจากอาคารทันที

4.6 หากเพลิงไหม้ในห้องทำงานให้ออกจากห้อง ปิดประตูแล้วแจ้งงานอาคารสถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

4.7 หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตูหาก ประตูมี ความเย็นอยู่ค่อยๆ เปิดประตูแล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

4.8 หากเพลิงไหม้อยู่บริเวณใกล้ประตูจะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วย ดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

4.9 เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

5. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มีมักจะเกิดขึ้นและยากต่อการหลีกเลี่ยง คือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

5.1 เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

5.2 เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ในภายหลังแผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติการคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายต้องอยู่ในสภาพที่พร้อมรองรับ การให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ต้องรีบกู้ระบบ คืนไฟได้เร็วที่สุดเพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะเดิม เมื่อระบบ เสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน 48 ชั่วโมง
4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ในการชั่วคราว
5. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน 48 ชั่วโมง
6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่

เกี่ยวข้อง

## ผู้รับผิดชอบ

1. ระดับนโยบาย ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของหน่วย (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

2. ระดับปฏิบัติ เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติศึกษา ทบทวนวางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้

- 2.1 ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ
- 2.2 ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ
- 2.3 ทีมกู้คืนแอปพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน
- 2.4 ทีมประเมินความเสียหาย เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อ

เตรียมจัดหาอุปกรณ์มาทดแทน

2.5 ทีมอาคารสถานที่ เป็นทีมที่จัดเตรียมสถานที่สำหรับใช้สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร เครื่องปรับอากาศให้พร้อมใช้งาน

2.6 ทีมจัดการทั่วไป เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน

2.7 ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง

2.8 ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไพพ์ระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรอง ข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่

2.9 ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบสูบน้ำออกจากห้องควบคุม ระบบและตรวจสอบการรั่วซึม

2.10 ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติรวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

2.11 ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วน สมบูรณ์

2.12 ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาเนินการประกาศสั่งการตามแผนที่เตรียมไว้และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ ควบคุมและศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป

2.13 ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อกวน ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชา ดำเนินการสั่งการตามแผนที่เตรียมไว้เมื่อการชุมนุมประท้วงและก่อกวนสิ้นสุดลงให้เจ้าหน้าที่ รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียดแล้วรายงานแก่ผู้ควบคุมและศูนย์เทคโนโลยีสารสนเทศเพื่อ ทราบและสั่งการต่อไป

#### การติดตามและรายงานผล

กำหนดให้หัวหน้างานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

#### รายชื่อผู้รับผิดชอบในการทำสำเนาข้อมูลและกู้คืนระบบ

ลำดับ	ชื่อ - สกุล	ตำแหน่ง	บทบาทหน้าที่
1	นายรังสิมันต์ ฉันทะ	นักวิชาการคอมพิวเตอร์	ทีมทำสำเนาข้อมูล/กู้คืนระบบ
2	น.ส.ศิริลักษณ์ ชัยชนะ	นักวิชาการคอมพิวเตอร์	ทีมทำสำเนาข้อมูล/กู้คืนระบบ
3	นายสุพงษ์ กันทา	เจ้าหน้าที่เครื่องคอมพิวเตอร์	ทีมเทคนิค Server

#### ผลการทดสอบการกู้คืนในแต่ละวิธี

- 1.กรณี เครื่องแม่ข่าย เสียหาย แต่เครื่องแบคอัพเรียลไทม์ไม่เสียหาย น้อยกว่า 5 นาที
- 2.กรณี เครื่องแม่ข่าย ไม่เสียหาย ฐานข้อมูลเสียหาย นำข้อมูลแบคอัพ ทำการกู้คืน 3 ชั่วโมง
- 3.กรณี เครื่องแม่ข่าย เสียหาย ฐานข้อมูลเสียหาย นำเครื่องสำรองมาตั้งค่าใช้งานและ ทำการ Restore ฐานข้อมูล ทำการกู้คืนภายใน 5 ชั่วโมง