แผนบริหารความต่อเนื่อง กรณีระบบ เทคโนโลยีสารสนเทศขัดข้อง
(BUSINESS COMTINUITY PLAN – BCP FOR IT SYSTEM FAILURE)
ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์
งานเทคโนโลยีสารสนเทศ ปีงบประมาณ 2568

วัตถุประสงค์ของแผนความต่อเนื่องในการดำเนินงาน

1. เพื่อจัดทำแนวทางในการบริหารความต่อเนื่องของการเรียนการสอนอย่างมีประสิทธิภาพ
2. เพื่อเตรียมความพร้อมล่วงหน้าในการรับมือกับสถานการณ์วิกฤติหรือเหตุการณ์ฉุกเฉินที่อาจส่งผลกระทบต่อการจัดการเรียนการสอน
3. เพื่อลดผลกระทบจากการหยุดชะงักในการเรียนการสอน
4. เพื่อลดความเสียหายให้การเรียนการสอนดำเนินต่อไปได้อย่างมีคุณภาพตามมาตรฐานของหลักสูตร

สมมติฐานในการจัดทำแผนบริหารความต่อเนื่อง (BCP Assumptions)

1. ความเสี่ยงที่อาจเกิดขึ้น

   1.1 มีความเป็นไปได้ที่จะเกิดเหตุการณ์ขัดข้องทางเทคโนโลยีสารสนเทศจากหลายสาเหตุ เช่น การโจมตีทางไซเบอร์ ความผิดพลาดของฮาร์ดแวร์หรือซอฟต์แวร์ ไฟฟ้าขัดข้อง ภัยธรรมชาติ เป็นต้น

   1.2 ความเสี่ยงดังกล่าวอาจส่งผลกระทบต่อการดำเนินงานของศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์ ทำให้ไม่สามารถให้บริการได้ตามปกติ
2. ความสำคัญของระบบเทคโนโลยีสารสนเทศ

   2.1 ระบบเทคโนโลยีสารสนเทศเป็นส่วนสำคัญในการสนับสนุนการดำเนินงานของศูนย์ฯ ทั้งในด้านการเรียนการสอน การจัดเก็บข้อมูล และการสื่อสารกับหน่วยงานต่าง ๆ

2.2 หากระบบเทคโนโลยีสารสนเทศขัดข้อง จะส่งผลกระทบโดยตรงต่อการดำเนินงาน ซึ่งอาจส่งผลให้การให้บริการทางการแพทย์และการศึกษาหยุดชะงัก

3. ทรัพยากรและบุคลากร

   3.1 ทีมงานเทคโนโลยีสารสนเทศมีความเชี่ยวชาญเพียงพอที่จะรับมือกับเหตุการณ์ขัดข้อง และสามารถแก้ไขปัญหาได้ตามลำดับความสำคัญของเหตุการณ์

   3.2 มีทรัพยากรที่เพียงพอ เช่น ระบบสำรองข้อมูล ศูนย์ข้อมูลสำรอง (Disaster Recovery Site) และเครื่องมือในการตรวจสอบและแก้ไขปัญหา เพื่อสนับสนุนการฟื้นฟูระบบในกรณีฉุกเฉิน

4. การสนับสนุนจากผู้บริหาร

   4.1 ผู้บริหารของศูนย์แพทยศาสตรศึกษาชั้นคลินิกให้การสนับสนุนแผนบริหารความต่อเนื่องนี้ และพร้อมที่จะจัดสรรทรัพยากรที่จำเป็นในกรณีที่เกิดเหตุการณ์ขัดข้อง

   4.2 มีการสื่อสารและประสานงานที่ดีระหว่างทีมงานเทคโนโลยีสารสนเทศกับผู้บริหารและผู้ใช้บริการ เพื่อให้การดำเนินงานตามแผนเป็นไปอย่างมีประสิทธิภาพ

5. การบูรณาการแผนบริหารความต่อเนื่อง

   5.1 แผนบริหารความต่อเนื่องนี้บูรณาการเข้ากับแผนความปลอดภัยทางไซเบอร์และแผนจัดการภัยพิบัติของโรงพยาบาล เพื่อให้การจัดการเหตุการณ์ขัดข้องเป็นไปอย่างมีประสิทธิภาพและครอบคลุมทุกด้าน

   5.2 แผนนี้มีการทดสอบและปรับปรุงเป็นระยะ เพื่อให้สามารถตอบสนองต่อเหตุการณ์ขัดข้องได้ตามสถานการณ์ที่อาจเกิดขึ้นจริง

6. ความสามารถในการกู้คืน

   6.1 ระบบเทคโนโลยีสารสนเทศที่สำคัญมีการจัดเตรียมสำรองข้อมูลและแผนกู้คืนระบบ (Disaster Recovery Plan) ที่สามารถนำมาใช้ได้ทันทีในกรณีที่เกิดเหตุการณ์ขัดข้อง

   6.2 ระยะเวลาการฟื้นฟูระบบ (Recovery Time Objective: RTO) และความทนทานของข้อมูล (Recovery Point Objective: RPO) ถูกกำหนดไว้ให้สอดคล้องกับความต้องการของการดำเนินงาน

7. การยอมรับจากผู้ใช้บริการ

   7.1 ผู้ใช้บริการและบุคลากรภายในศูนย์ฯ ได้รับการฝึกอบรมเกี่ยวกับแผนบริหารความต่อเนื่อง และมีความเข้าใจในบทบาทหน้าที่ของตนเมื่อเกิดเหตุการณ์ขัดข้อง

8. ความพร้อมของระบบสื่อสารและการแจ้งเตือน

   8.1 มีระบบสื่อสารและการแจ้งเตือนที่มีประสิทธิภาพ เพื่อให้สามารถแจ้งเหตุขัดข้องและสื่อสารกับผู้ที่เกี่ยวข้องได้อย่างรวดเร็วและครอบคลุม

ขอบเขต (Scope)

แผนบริหารความต่อเนื่องกรณีระบบเทคโนโลยีสารสนเทศขัดข้องนี้ครอบคลุม

1. ระบบที่เกี่ยวข้องกับการดำเนินงานหลักของศูนย์แพทยศาสตรศึกษาชั้นคลินิก

   1.1 ระบบการจัดการเรียนการสอน: รวมถึงแพลตฟอร์มการเรียนการสอนออนไลน์ ระบบจัดการหลักสูตร ระบบประเมินผลการเรียนรู้ และระบบสนับสนุนการสอนอื่น ๆ

   1.2 ระบบจัดการข้อมูลผู้ป่วยและนักศึกษา: ครอบคลุมการจัดเก็บข้อมูลทางการแพทย์ ข้อมูลส่วนบุคคลของนักศึกษา และข้อมูลที่เกี่ยวข้องอื่น ๆ

   1.3ระบบการสื่อสารภายใน: ระบบอีเมลภายใน ระบบสื่อสารผ่านเครือข่ายภายใน และเครื่องมือการสื่อสารอื่น ๆ ที่ใช้ในการประสานงานระหว่างบุคลากร

2. ระบบเครือข่ายและการเชื่อมต่อ

   2.1 เครือข่ายภายใน: รวมถึงระบบเครือข่ายที่ใช้ในการเชื่อมต่อระหว่างอาคารและหน่วยงานต่าง ๆ ภายในโรงพยาบาล

   2.2 การเชื่อมต่ออินเทอร์เน็ต: ครอบคลุมการเข้าถึงอินเทอร์เน็ตสำหรับการดำเนินงานของศูนย์ฯ และการสนับสนุนการเรียนการสอน

3. ระบบจัดเก็บข้อมูลและการสำรองข้อมูล

   3.1 ระบบจัดเก็บข้อมูล (Data Storage): ครอบคลุมระบบจัดเก็บข้อมูลหลักและระบบสำรองข้อมูลที่ใช้ในการจัดเก็บข้อมูลสำคัญต่าง ๆ ของศูนย์ฯ

   3.2 การสำรองข้อมูล (Backup Systems): รวมถึงการสำรองข้อมูลที่ดำเนินการอย่างสม่ำเสมอ และการจัดเก็บข้อมูลสำรองในสถานที่ที่ปลอดภัย

4. ระบบความปลอดภัยทางไซเบอร์

   4.1 ระบบป้องกันการโจมตีทางไซเบอร์: รวมถึงการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การป้องกันมัลแวร์ และการควบคุมการเข้าถึงข้อมูล

   4.2 การตรวจสอบและเฝ้าระวัง: ระบบตรวจสอบและเฝ้าระวังการดำเนินงานของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันและรับมือกับเหตุการณ์ที่อาจเกิดขึ้น

5. การประสานงานและการสื่อสารในกรณีฉุกเฉิน

   5.1 การประสานงานระหว่างหน่วยงาน: การจัดการและสื่อสารระหว่างทีมเทคโนโลยีสารสนเทศ ผู้บริหาร และผู้ใช้บริการในกรณีที่เกิดเหตุขัดข้อง

   5.2 การแจ้งเตือนและการรายงานเหตุการณ์: การแจ้งเตือนผู้ที่เกี่ยวข้องและการรายงานสถานการณ์เมื่อเกิดเหตุขัดข้อง

6. การฟื้นฟูและการทดสอบแผน
    6.1 การฟื้นฟูระบบหลังเกิดเหตุขัดข้อง: รวมถึงกระบวนการฟื้นฟูระบบที่ถูกหยุดทำงานให้กลับมาทำงานได้ตามปกติ
    6.2 การทดสอบแผน: การทดสอบและฝึกอบรมตามแผนบริหารความต่อเนื่อง เพื่อให้แน่ใจว่าแผนสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ
7. ระบบที่เกี่ยวข้องอื่น ๆ
    7.1 อุปกรณ์ฮาร์ดแวร์: รวมถึงเซิร์ฟเวอร์ คอมพิวเตอร์ และอุปกรณ์ที่จำเป็นในการดำเนินงานของระบบเทคโนโลยีสารสนเทศ
    7.2 ซอฟต์แวร์ที่ใช้งาน: ระบบปฏิบัติการ ซอฟต์แวร์บริหารจัดการ และแอปพลิเคชันที่ใช้สนับสนุนการดำเนินงานของศูนย์ฯ

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นขั้นตอนสำคัญในการระบุและจัดลำดับความสำคัญของความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์ โดยแบ่งการประเมินความเสี่ยงออกเป็นส่วนต่าง ๆ ดังนี้:

ประเภทของความเสี่ยง

1. ความเสี่ยงทางกายภาพ (Physical Risks)
    1.1 ไฟฟ้าขัดข้อง: การสูญเสียพลังงานไฟฟ้าอาจทำให้ระบบเทคโนโลยีสารสนเทศหยุดทำงาน
    1.2 ภัยธรรมชาติ: เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหว อาจทำลายอุปกรณ์ฮาร์ดแวร์และศูนย์ข้อมูล
    1.3 การเข้าถึงโดยไม่ได้รับอนุญาต: การเข้าถึงสถานที่จัดเก็บอุปกรณ์หรือข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาตอาจนำไปสู่การโจรกรรมหรือการทำลายข้อมูล
2. ความเสี่ยงทางเทคนิค (Technical Risks)
    2.1 ความผิดพลาดของฮาร์ดแวร์: การทำงานผิดพลาดของเซิร์ฟเวอร์ คอมพิวเตอร์ หรืออุปกรณ์เครือข่าย
    2.2 ความล้มเหลวของซอฟต์แวร์: ปัญหาซอฟต์แวร์ เช่น บั๊กหรือการทำงานที่ไม่ถูกต้อง อาจทำให้ระบบหยุดชะงัก
    2.3 การโจมตีทางไซเบอร์: การโจมตีจากแฮกเกอร์ การติดมัลแวร์ หรือการโจมตีแบบ Distributed Denial of Service (DDoS)

3. ความเสี่ยงจากมนุษย์ (Human Risks)
   3.1 ความผิดพลาดจากผู้ใช้งาน: การใช้งานระบบผิดพลาด การลบข้อมูลโดยไม่ตั้งใจ หรือการตั้งค่าที่ไม่ถูกต้อง
   3.2 การขาดบุคลากรที่มีความเชี่ยวชาญ: การขาดแคลนบุคลากรที่มีทักษะเพียงพอในการดูแลและแก้ไขปัญหาของระบบเทคโนโลยีสารสนเทศ
   3.3 การละเมิดนโยบายความปลอดภัย: การไม่ปฏิบัติตามนโยบายและขั้นตอนความปลอดภัยของระบบ
4. ความเสี่ยงจากกระบวนการ (Process Risks)
   4.1 กระบวนการสำรองข้อมูลที่ไม่เพียงพอ: การสำรองข้อมูลที่ไม่เป็นระเบียบหรือล้มเหลว อาจทำให้การกู้คืนข้อมูลหลังเกิดเหตุการณ์เป็นไปได้ยาก
   4.2 การบำรุงรักษาระบบที่ไม่เพียงพอ: การขาดการบำรุงรักษาและอัปเดตระบบอย่างสม่ำเสมอ อาจนำไปสู่ความล้มเหลวของระบบ
   4.3 การจัดการความเปลี่ยนแปลงที่ไม่เหมาะสม: การเปลี่ยนแปลงในระบบโดยไม่มีการวางแผนหรือการทดสอบ อาจทำให้เกิดปัญหาหรือความเสี่ยงที่ไม่คาดคิด

การวิเคราะห์ผลกระทบ (Impact Analysis)

1. ความเสี่ยงสูง (High Risk): ความเสี่ยงที่อาจส่งผลกระทบอย่างรุนแรงต่อการดำเนินงานของศูนย์ฯ หากเกิดขึ้น อาจทำให้การบริการทางการแพทย์หยุดชะงัก ข้อมูลสำคัญสูญหาย หรือส่งผลเสียต่อความปลอดภัยของผู้ป่วย
   - เช่น: การโจมตีทางไซเบอร์ที่ทำให้ข้อมูลผู้ป่วยรั่วไหล, ระบบฐานข้อมูลล้มเหลว
2. ความเสี่ยงกลาง (Medium Risk): ความเสี่ยงที่อาจส่งผลกระทบปานกลางต่อการดำเนินงาน แต่สามารถฟื้นฟูได้ในระยะเวลาที่สั้น
   - เช่น: ความผิดพลาดของซอฟต์แวร์ในระบบการเรียนการสอน, การสูญเสียการเชื่อมต่ออินเทอร์เน็ตชั่วคราว
3. ความเสี่ยงต่ำ (Low Risk): ความเสี่ยงที่มีผลกระทบต่ำต่อการดำเนินงาน หรือสามารถจัดการได้อย่างรวดเร็วและมีผลกระทบน้อย
   - เช่น: ปัญหาการเข้าถึงอินเทอร์เน็ตของบางอุปกรณ์, การขาดแคลนบุคลากรในช่วงเวลาสั้น

การจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization)

จัดลำดับความสำคัญของความเสี่ยงโดยพิจารณาจากทั้งความเป็นไปได้ในการเกิดเหตุการณ์ (Probability) และผลกระทบที่อาจเกิดขึ้น (Impact) โดยระบบและกระบวนการที่มีความเสี่ยงสูงจะถูกจัดการและได้รับการป้องกันก่อน

มาตรการการจัดการความเสี่ยง (Risk Mitigation Measures)

1. การสำรองข้อมูลอย่างสม่ำเสมอ: กำหนดแผนสำรองข้อมูลเพื่อให้แน่ใจว่ามีข้อมูลสำรองที่สามารถกู้คืนได้ในกรณีที่ข้อมูลหลักสูญหาย โดยสำรองข้อมูล Snapshot 1 เดือนต่อครั้ง
2. การบำรุงรักษาและอัปเดตระบบ: บำรุงรักษาอุปกรณ์และซอฟต์แวร์อย่างสม่ำเสมอ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในระยะยาว จัดทำ 1 เดือนต่อครั้ง
3. การฝึกอบรมบุคลากร: จัดอบรมเกี่ยวกับการใช้ระบบเทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัยให้กับบุคลากรทั้งหมด
4. การทดสอบแผนฉุกเฉิน: ทดสอบแผนบริหารความต่อเนื่องอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนสามารถนำไปปฏิบัติได้จริงและมีความพร้อมเมื่อต้องใช้ในกรณีฉุกเฉิน

การดำเนินการเมื่อเกิดเหตุขัดข้อง (Incident Response Actions)

เมื่อเกิดเหตุขัดข้องในระบบเทคโนโลยีสารสนเทศ ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์ จะต้องดำเนินการตามขั้นตอนดังต่อไปนี้เพื่อฟื้นฟูระบบและลดผลกระทบที่อาจเกิดขึ้น

1. การตรวจสอบและแจ้งเหตุขัดข้อง (Incident Detection and Reporting)

1. **การตรวจพบเหตุขัดข้อง:**
    - **การตรวจสอบอัตโนมัติ:** ระบบตรวจสอบการทำงานอัตโนมัติ (Monitoring System) แจ้งเตือนเมื่อเกิดปัญหาขึ้นในระบบ เช่น ความล้มเหลวของเซิร์ฟเวอร์หรือการเชื่อมต่อเครือข่ายขาดหาย ทาง Email ของ IT และ Line
    - **การรายงานจากผู้ใช้:** หากผู้ใช้พบปัญหาในการใช้งานระบบ ควรรายงานไปยังฝ่ายเทคโนโลยีสารสนเทศทันทีผ่านช่องทางที่กำหนด เช่น สแกน QR Code แจ้งปัญหา IT หรือโทรศัพท์สายด่วน 056219870
2. **การประเมินเหตุการณ์เบื้องต้น:**
    - ทีมเทคโนโลยีสารสนเทศจะทำการประเมินสถานการณ์เบื้องต้น เพื่อระบุประเภทและความรุนแรงของเหตุขัดข้องที่เกิดขึ้น
3. **การแจ้งเหตุ:**
    - แจ้งเหตุขัดข้องต่อผู้บริหารที่เกี่ยวข้องและทีมงานที่เกี่ยวข้องทันที พร้อมทั้งสื่อสารกับผู้ใช้บริการเกี่ยวกับสถานะของเหตุการณ์

2. การควบคุมสถานการณ์ (Incident Containment)

1. **การจำกัดขอบเขตของปัญหา:**

- ดำเนินการตามขั้นตอนที่กำหนดไว้ล่วงหน้าเพื่อจำกัดขอบเขตของเหตุขัดข้อง การแยกส่วนระบบที่ได้รับผลกระทบออกจากเครือข่ายหลัก เพื่อลดความเสี่ยงในการกระจายของปัญหา

2. **การระบุสาเหตุ:**
    - ทำการวิเคราะห์เพื่อระบุสาเหตุของเหตุขัดข้อง การตรวจสอบบันทึก (Logs) หรือการทดสอบระบบที่เกี่ยวข้อง
3. **การจัดสรรทรัพยากร:**
    - จัดสรรบุคลากรและทรัพยากรที่จำเป็นเพื่อจัดการกับปัญหา โดยให้ความสำคัญกับระบบที่มีผลกระทบสูงสุดต่อการดำเนินงาน

3. การฟื้นฟูและกู้คืนระบบ (System Recovery)

1. **การฟื้นฟูระบบ:**
    - ทำการแก้ไขปัญหาที่ทำให้เกิดเหตุขัดข้อง เช่น การซ่อมแซมฮาร์ดแวร์ การกู้คืนข้อมูลจากระบบสำรอง หรือการรีเซ็ตซอฟต์แวร์
2. **การกู้คืนข้อมูล:**
    - หากข้อมูลสำคัญสูญหายหรือเสียหาย ให้ดำเนินการกู้คืนข้อมูลจากแหล่งสำรองที่มีอยู่
3. **การตรวจสอบความเสถียรของระบบ:**
    - ทำการทดสอบระบบที่ฟื้นฟูแล้วเพื่อให้แน่ใจว่าระบบกลับมาทำงานได้ตามปกติและมีความเสถียรเพียงพอ

4. การสื่อสารและรายงาน (Communication and Reporting)

1. **การสื่อสารกับผู้ใช้:**
    - แจ้งสถานะและการดำเนินการในการแก้ไขปัญหาให้ผู้ใช้บริการทราบเป็นระยะ พร้อมให้ข้อมูลเกี่ยวกับการคาดการณ์เวลาที่ระบบจะกลับมาใช้งานได้
2. **การรายงานเหตุการณ์:**
    - จัดทำรายงานสรุปเหตุการณ์ขัดข้อง รวมถึงสาเหตุ ผลกระทบ และการดำเนินการแก้ไขที่เกิดขึ้นเพื่อนำเสนอแก่ผู้บริหารและหน่วยงานที่เกี่ยวข้อง

5. การป้องกันการเกิดซ้ำ (Post-Incident Review and Prevention)

1. **การทบทวนเหตุการณ์:**
    - หลังจากเหตุขัดข้องได้รับการแก้ไขแล้ว ให้มีการประชุมทบทวนเหตุการณ์เพื่อวิเคราะห์การดำเนินการทั้งหมด หาจุดอ่อนและข้อบกพร่องในการจัดการเหตุการณ์
2. **การปรับปรุงแผนและกระบวนการ:**

- ปรับปรุงแผนบริหารความต่อเนื่องและกระบวนการการจัดการเหตุขัดข้องตามผลการทบทวน เพื่อป้องกันการเกิดเหตุซ้ำและเพิ่มประสิทธิภาพในการตอบสนองในอนาคต

3. **การฝึกอบรมและเตรียมความพร้อม:**
    - ดำเนินการฝึกอบรมบุคลากรเพิ่มเติมตามบทเรียนที่ได้จากเหตุการณ์ เพื่อเพิ่มความพร้อมในการรับมือกับเหตุขัดข้องในอนาคต

แผนการฟื้นฟู (Recovery Plan)

แผนการฟื้นฟูมีวัตถุประสงค์เพื่อให้ระบบเทคโนโลยีสารสนเทศของศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์ กลับมาทำงานได้อย่างเต็มประสิทธิภาพหลังจากเกิดเหตุขัดข้อง โดยแบ่งแผนการฟื้นฟูออกเป็นขั้นตอนต่าง ๆ ดังนี้:

1. การจัดลำดับความสำคัญในการฟื้นฟู (Recovery Prioritization)

1. **การระบุระบบที่สำคัญ:**
    - ระบุระบบที่มีความสำคัญสูงสุดต่อการดำเนินงาน เช่น ระบบจัดการข้อมูลผู้ป่วย ระบบการเรียนการสอน และระบบการสื่อสารภายใน เพื่อให้ระบบเหล่านี้ได้รับการฟื้นฟูเป็นลำดับแรก
2. **การจัดลำดับความสำคัญของงาน:**
    - กำหนดลำดับความสำคัญของงานในการฟื้นฟูตามผลกระทบและความต้องการของผู้ใช้ โดยให้ความสำคัญกับงานที่ส่งผลกระทบต่อผู้ป่วยและนักศึกษามากที่สุด

2. ขั้นตอนการฟื้นฟู (Recovery Steps)

1. **การกู้คืนข้อมูล (Data Recovery):**
    - **การสำรองข้อมูล:** ใช้ข้อมูลสำรอง (Backup) ที่ได้จัดทำไว้ก่อนหน้าเพื่อกู้คืนข้อมูลที่สูญหายหรือเสียหาย
    - **การยืนยันความสมบูรณ์ของข้อมูล:** ตรวจสอบข้อมูลที่กู้คืนมาเพื่อให้แน่ใจว่ามีความสมบูรณ์และถูกต้อง
2. **การฟื้นฟูระบบฮาร์ดแวร์ (Hardware Recovery):**
    - **การซ่อมแซมและเปลี่ยนอุปกรณ์:** ซ่อมแซมหรือเปลี่ยนอุปกรณ์ฮาร์ดแวร์ที่เสียหาย เช่น เซิร์ฟเวอร์ คอมพิวเตอร์ หรืออุปกรณ์เครือข่าย
    - **การติดตั้งฮาร์ดแวร์สำรอง:** ในกรณีที่ไม่สามารถซ่อมแซมได้ ให้ติดตั้งฮาร์ดแวร์สำรองที่เตรียมไว้เพื่อให้ระบบกลับมาทำงานได้
3. **การฟื้นฟูระบบซอฟต์แวร์ (Software Recovery):**
    - **การติดตั้งซอฟต์แวร์ใหม่:** ติดตั้งซอฟต์แวร์ที่จำเป็นใหม่หากซอฟต์แวร์เดิมเสียหายหรือไม่สามารถใช้งานได้

- **การอัปเดตและตั้งค่าซอฟต์แวร์:** อัปเดตซอฟต์แวร์และตั้งค่าตามที่กำหนดไว้ล่วงหน้าเพื่อให้ระบบทำงานได้ตามปกติ

4. **การตรวจสอบและทดสอบระบบ (System Verification and Testing):**
    - **การทดสอบระบบ:** ทดสอบระบบทั้งหมดที่ได้รับการฟื้นฟูเพื่อให้แน่ใจว่าทำงานได้อย่างถูกต้องและมีความเสถียร
    - **การตรวจสอบความเข้ากันได้:** ตรวจสอบให้แน่ใจว่าระบบทั้งหมดสามารถทำงานร่วมกันได้อย่างสมบูรณ์โดยไม่มีข้อขัดแย้งหรือปัญหา

3. การสื่อสารระหว่างการฟื้นฟู (Communication During Recovery)

1. **การแจ้งสถานะการฟื้นฟู:**
    - สื่อสารกับผู้ใช้บริการอย่างสม่ำเสมอเกี่ยวกับสถานะการฟื้นฟู รวมถึงการคาดการณ์เวลาที่ระบบจะกลับมาใช้งานได้
2. **การรายงานผลการฟื้นฟู:**
    - รายงานผลการฟื้นฟูต่อผู้บริหารและหน่วยงานที่เกี่ยวข้อง เพื่อให้ทราบถึงสถานะของระบบและความสำเร็จในการกู้คืนระบบ

4. การปรับปรุงและทบทวน (Post-Recovery Improvement and Review)

1. **การทบทวนกระบวนการฟื้นฟู:**
    - หลังจากระบบกลับมาทำงานได้อย่างสมบูรณ์ ให้ทบทวนกระบวนการฟื้นฟูที่ดำเนินการไป เพื่อระบุจุดอ่อนและข้อบกพร่องที่อาจเกิดขึ้น
2. **การปรับปรุงแผนฟื้นฟู:**
    - ปรับปรุงแผนฟื้นฟูตามบทเรียนที่ได้จากเหตุการณ์ที่เกิดขึ้น เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการฟื้นฟูระบบในอนาคต
3. **การฝึกอบรมเพิ่มเติม:**
    - จัดฝึกอบรมเพิ่มเติมสำหรับบุคลากรที่เกี่ยวข้อง เพื่อเพิ่มความพร้อมและความสามารถในการฟื้นฟูระบบหากเกิดเหตุการณ์ซ้ำ

การประเมินผลและปรับปรุงแผน (Evaluation and Plan Improvement)

การประเมินผลและการปรับปรุงแผนเป็นขั้นตอนสำคัญในการสร้างความมั่นใจว่าแผนบริหารความต่อเนื่อง (BCP) จะยังคงมีประสิทธิภาพในการตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้นและสามารถปรับตัวตามสถานการณ์และเทคโนโลยีที่เปลี่ยนแปลงได้ โดยแบ่งออกเป็นขั้นตอนต่าง ๆ ดังนี้:

1. การประเมินผลการดำเนินการ (Performance Evaluation)

1. **การทบทวนหลังเหตุการณ์ (Post-Incident Review):**
    - หลังจากการฟื้นฟูระบบจากเหตุการณ์ขัดข้องเสร็จสิ้น ควรมีการทบทวนการดำเนินการทั้งหมด โดยมีการประชุมกับทีมงานที่เกี่ยวข้องเพื่อวิเคราะห์ขั้นตอนที่ดำเนินการ และผลลัพธ์ที่ได้ว่ามีประสิทธิภาพเพียงพอหรือไม่
2. **การวัดผลสำเร็จ (Success Metrics):**
    - ใช้เกณฑ์วัดผลสำเร็จ (Key Performance Indicators - KPIs) เช่น ระยะเวลาที่ใช้ในการฟื้นฟูระบบ (Recovery Time Objective - RTO), ระดับความเสียหายที่เกิดขึ้น และความพึงพอใจของผู้ใช้งาน เพื่อประเมินประสิทธิภาพของแผน BCP
3. **การวิเคราะห์ความสำเร็จและความล้มเหลว (Success and Failure Analysis):**
    - วิเคราะห์สิ่งที่ทำได้ดีและสิ่งที่ต้องปรับปรุง โดยเฉพาะในด้านการตอบสนองต่อเหตุการณ์ ความเร็วในการฟื้นฟู และการสื่อสารกับผู้ใช้บริการและผู้มีส่วนได้ส่วนเสีย

2. การทดสอบแผนเป็นประจำ (Regular Plan Testing)

1. **การทดสอบแผน (Plan Testing):**
    - ทดสอบแผน BCP อย่างสม่ำเสมอโดยการจำลองเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น เช่น การโจมตีทางไซเบอร์ หรือการขัดข้องของฮาร์ดแวร์ เพื่อทดสอบความพร้อมของระบบและบุคลากร
    - การทดสอบควรรวมถึงสถานการณ์ที่ซับซ้อนและไม่คาดคิด เพื่อให้แน่ใจว่าแผนสามารถตอบสนองต่อทุกสถานการณ์ได้อย่างมีประสิทธิภาพ
2. **การประเมินผลการทดสอบ (Test Evaluation):**
    - ประเมินผลการทดสอบเพื่อหาจุดอ่อนและข้อบกพร่องในแผน รวมถึงการระบุส่วนที่ต้องปรับปรุงและเพิ่มประสิทธิภาพ

3. การปรับปรุงแผน (Plan Improvement)

1. **การอัปเดตแผนตามการเปลี่ยนแปลง (Plan Updates Based on Changes):**
    - ปรับปรุงแผน BCP ตามการเปลี่ยนแปลงของเทคโนโลยี กระบวนการทำงาน หรือการเปลี่ยนแปลงโครงสร้างองค์กร เพื่อให้แผนยังคงสอดคล้องกับสภาพแวดล้อมที่เป็นปัจจุบัน
2. **การรวมบทเรียนที่ได้รับ (Incorporation of Lessons Learned):**
    - บทเรียนที่ได้รับจากการทดสอบและการตอบสนองต่อเหตุการณ์จริง ควรถูกนำมาใช้ในการปรับปรุงแผนให้มีความครบถ้วนและพร้อมรับมือกับเหตุการณ์ในอนาคต
3. **การรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสีย (Stakeholder Feedback):**
    - รับฟังความคิดเห็นจากผู้ใช้บริการ ผู้บริหาร และบุคลากรที่เกี่ยวข้อง เพื่อพัฒนาและปรับปรุงแผนให้สอดคล้องกับความต้องการและความคาดหวัง

4. การฝึกอบรมและเตรียมความพร้อม (Training and Readiness)

1. **การฝึกอบรมต่อเนื่อง (Ongoing Training):**
    - จัดการฝึกอบรมให้กับบุคลากรอย่างต่อเนื่องเพื่อให้พวกเขามีความพร้อมและความรู้ในการตอบสนองต่อเหตุการณ์ขัดข้อง รวมถึงการใช้เครื่องมือและกระบวนการที่เกี่ยวข้อง
2. **การฝึกซ้อมและทบทวนแผน (Drills and Plan Review):**
    - จัดการฝึกซ้อมตามแผน BCP อย่างน้อยปีละ 1-2 ครั้ง โดยจำลองเหตุการณ์ขัดข้องที่อาจเกิดขึ้น เพื่อให้แน่ใจว่าบุคลากรทุกคนทราบบทบาทและหน้าที่ของตน

5. การตรวจสอบและอนุมัติแผน (Plan Review and Approval)

1. **การตรวจสอบแผนประจำปี (Annual Plan Review):**
    - แผน BCP ควรถูกตรวจสอบและปรับปรุงเป็นประจำทุกปี โดยผู้บริหารและผู้มีส่วนได้ส่วนเสีย เพื่อให้แผนมีความเหมาะสมและพร้อมใช้งาน
2. **การอนุมัติแผนโดยผู้บริหาร (Management Approval):**
    - หลังจากการปรับปรุงแผนแล้ว แผนใหม่จะต้องได้รับการอนุมัติจากผู้บริหารระดับสูงเพื่อให้มั่นใจว่าแผนเป็นที่ยอมรับและสามารถนำไปปฏิบัติได้จริง

การฝึกอบรมและทดสอบ (Training and Testing)

การฝึกอบรมและการทดสอบเป็นองค์ประกอบสำคัญของแผนบริหารความต่อเนื่อง (BCP) ที่ช่วยเสริมสร้างความพร้อมและความสามารถในการตอบสนองต่อเหตุการณ์ขัดข้องได้อย่างมีประสิทธิภาพ โดยมุ่งเน้นทั้งการเพิ่มพูนความรู้ของบุคลากรและการตรวจสอบความพร้อมของระบบและกระบวนการ ดังนี้:

1. การฝึกอบรมบุคลากร (Employee Training)

1. **การฝึกอบรมเบื้องต้น (Initial Training):**
    - **วัตถุประสงค์:** เพื่อให้บุคลากรทุกคนมีความเข้าใจในแผนบริหารความต่อเนื่อง รวมถึงบทบาทและความรับผิดชอบของตนเองเมื่อเกิดเหตุขัดข้อง
    - **เนื้อหา:** แผนการฟื้นฟูขั้นพื้นฐาน, การรายงานเหตุขัดข้อง, ขั้นตอนการสื่อสารในสถานการณ์วิกฤต และการใช้เครื่องมือและระบบที่เกี่ยวข้อง
2. **การฝึกอบรมต่อเนื่อง (Ongoing Training):**
    - **วัตถุประสงค์:** เพื่อให้บุคลากรมีความรู้และความเข้าใจในกระบวนการที่ปรับปรุงใหม่ และเตรียมพร้อมรับมือกับสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้น
    - **เนื้อหา:** การอัปเดตแผน BCP, การฝึกการตัดสินใจในสถานการณ์วิกฤต, การใช้เทคโนโลยีใหม่ ๆ ที่เกี่ยวข้องกับการจัดการเหตุขัดข้อง

3. **การฝึกอบรมเฉพาะทาง (Specialized Training):**
    - **วัตถุประสงค์:** เพื่อให้บุคลากรที่มีบทบาทเฉพาะในการตอบสนองต่อเหตุการณ์ขัดข้อง เช่น ทีมเทคนิค หรือผู้จัดการวิกฤต มีความรู้และทักษะเฉพาะทางที่จำเป็น
    - **เนื้อหา:** การแก้ไขปัญหาด้านเทคนิคขั้นสูง, การจัดการวิกฤตและการสื่อสารในสถานการณ์ฉุกเฉิน, การกู้คืนระบบและข้อมูล

2. การทดสอบแผน (Plan Testing)

1. **การทดสอบระบบเป็นประจำ (Regular System Testing):**
    - **วัตถุประสงค์:** เพื่อทดสอบว่าแผน BCP สามารถใช้งานได้จริงและมีประสิทธิภาพเมื่อเกิดเหตุขัดข้อง รวมถึงตรวจสอบความพร้อมของระบบและบุคลากร
    - **ประเภทของการทดสอบ:**
        - **Tabletop Exercise:** การจำลองเหตุการณ์ขัดข้องและให้ทีมงานหารือถึงวิธีการตอบสนองที่เหมาะสม
        - **Simulation Exercise:** การทดสอบสถานการณ์ที่จำลองขึ้นจริง เช่น การปิดระบบเครือข่ายชั่วคราว หรือการกู้คืนข้อมูลจากระบบสำรอง
        - **Full-scale Exercise:** การทดสอบเต็มรูปแบบที่ครอบคลุมทุกส่วนของแผน โดยจำลองเหตุการณ์วิกฤตทั้งหมดและให้บุคลากรทุกคนมีส่วนร่วม
2. **การประเมินผลการทดสอบ (Test Evaluation):**
    - **การวิเคราะห์ผลการทดสอบ:** หลังจากการทดสอบ ควรมีการประเมินว่าการตอบสนองเป็นไปตามแผนที่กำหนดหรือไม่ รวมถึงระบุจุดอ่อนและข้อผิดพลาดที่พบเจอ
    - **การรายงานและข้อเสนอแนะ:** จัดทำรายงานสรุปผลการทดสอบ รวมถึงข้อเสนอแนะสำหรับการปรับปรุงแผน BCP ให้มีประสิทธิภาพยิ่งขึ้น

3. การปรับปรุงจากผลการทดสอบ (Improvement Based on Testing)

1. **การปรับปรุงแผนตามผลการทดสอบ (Plan Update Based on Test Results):**
    - **การแก้ไขข้อบกพร่อง:** ปรับปรุงแผน BCP ตามข้อบกพร่องและจุดอ่อนที่พบในการทดสอบ เพื่อให้แผนมีความสมบูรณ์และมีประสิทธิภาพมากขึ้น
    - **การปรับปรุงกระบวนการ:** ปรับปรุงกระบวนการทำงานหรือการสื่อสารระหว่างเหตุขัดข้อง เพื่อเพิ่มความรวดเร็วและลดผลกระทบที่อาจเกิดขึ้น
2. **การทดสอบใหม่หลังปรับปรุง (Re-testing):**
    - **การทดสอบซ้ำ:** หลังจากปรับปรุงแผน ควรมีการทดสอบซ้ำเพื่อให้แน่ใจว่าการปรับปรุงนั้นได้ผลและแผนใหม่สามารถใช้งานได้จริงในสถานการณ์ฉุกเฉิน

4. การบันทึกและรายงานผล (Documentation and Reporting)

1. **การบันทึกการฝึกอบรมและการทดสอบ (Training and Testing Documentation):**
    - **การบันทึกผล:** บันทึกผลการฝึกอบรมและการทดสอบ รวมถึงการปรับปรุงที่เกิดขึ้น เพื่อใช้เป็นข้อมูลในการปรับปรุงแผนในอนาคต
    - **การรายงานต่อผู้บริหาร:** สรุปผลการฝึกอบรมและการทดสอบ รวมถึงข้อเสนอแนะในการปรับปรุงแผน นำเสนอให้กับผู้บริหารเพื่อการอนุมัติและดำเนินการต่อไป

รายชื่อผู้รับผิดชอบ (Responsible Personnel)

ในการจัดทำแผนบริหารความต่อเนื่อง (BCP) สำหรับระบบเทคโนโลยีสารสนเทศของศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์ จำเป็นต้องมีการกำหนดบุคลากรที่รับผิดชอบในแต่ละด้านของการจัดการเหตุการณ์ขัดข้อง เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว โดยมีรายชื่อผู้รับผิดชอบดังนี้:

1. ผู้รับผิดชอบหลัก (Primary Responsible Personnel)

1. **ผู้อำนวยการศูนย์แพทยศาสตรศึกษาชั้นคลินิก**
    - **บทบาท:** ผู้รับผิดชอบสูงสุดในการตัดสินใจและให้การอนุมัติแผนบริหารความต่อเนื่อง รวมถึงการจัดสรรทรัพยากรที่จำเป็นสำหรับการฟื้นฟูระบบ
    - **หน้าที่:** ให้การสนับสนุนและอนุมัติแผน BCP, กำหนดนโยบายการดำเนินงานในสถานการณ์วิกฤต
2. **หัวหน้างานเทคโนโลยีสารสนเทศ**
    - **บทบาท:** ผู้นำทีมรับผิดชอบในการดำเนินการตามแผน BCP และการฟื้นฟูระบบเทคโนโลยีสารสนเทศหลังเกิดเหตุขัดข้อง
    - **หน้าที่:** ควบคุมและบริหารจัดการทีม IT, ประสานงานกับผู้บริหารและหน่วยงานอื่น ๆ, ตัดสินใจเกี่ยวกับการกู้คืนระบบและข้อมูล
3. **ผู้จัดการฝ่ายสนับสนุนเทคโนโลยีสารสนเทศ**
    - **บทบาท:** ผู้รับผิดชอบในการดำเนินการตามแผนฟื้นฟูระบบในด้านเทคนิคและสนับสนุนการดำเนินงานของทีม IT
    - **หน้าที่:** นำทีมในการกู้คืนระบบและข้อมูล, ตรวจสอบความสมบูรณ์ของข้อมูลและระบบที่กู้คืนมา, จัดการและรายงานผลการฟื้นฟู

2. ทีมปฏิบัติการ (Operational Teams)

1. **ทีมเทคนิค (Technical Team)**
    - **สมาชิก:** วิศวกรระบบ, ผู้เชี่ยวชาญด้านเครือข่าย, ผู้เชี่ยวชาญด้านฐานข้อมูล

- **บทบาท:** รับผิดชอบในการดำเนินการฟื้นฟูระบบเทคโนโลยีสารสนเทศในด้านต่าง ๆ
- **หน้าที่:** ตรวจสอบและซ่อมแซมฮาร์ดแวร์และซอฟต์แวร์, กู้คืนข้อมูลจากระบบสำรอง, ติดตั้งและตั้งค่าระบบใหม่ตามที่กำหนดในแผน BCP

2. **ทีมสื่อสาร (Communication Team)**
    - **สมาชิก:** เจ้าหน้าที่ฝ่ายสื่อสาร, ผู้จัดการฝ่ายประชาสัมพันธ์
    - **บทบาท:** ดูแลการสื่อสารภายในและภายนอกระหว่างสถานการณ์วิกฤต
    - **หน้าที่:** แจ้งเตือนผู้ใช้บริการเกี่ยวกับสถานะของระบบ, รายงานสถานการณ์และการฟื้นฟูให้กับผู้บริหารและผู้ใช้บริการ, ประสานงานกับสื่อมวลชน (ถ้าจำเป็น)
3. **ทีมสนับสนุนผู้ใช้บริการ (User Support Team)**
    - **สมาชิก:** เจ้าหน้าที่บริการลูกค้า, ทีมสนับสนุน IT
    - **บทบาท:** ให้การสนับสนุนและแก้ไขปัญหาให้กับผู้ใช้บริการเมื่อเกิดเหตุขัดข้อง
    - **หน้าที่:** ตอบคำถามและให้ความช่วยเหลือผู้ใช้บริการ, แก้ไขปัญหาเบื้องต้นที่เกิดจากการขัดข้องของระบบ, ประสานงานกับทีมเทคนิคเพื่อแก้ไขปัญหาที่ซับซ้อน

3. คณะกรรมการบริหารแผน (BCP Steering Committee)

1. **คณะกรรมการบริหารแผน (Steering Committee Members):**
    - ประกอบด้วยผู้แทนจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง เช่น ฝ่ายบริหาร, ฝ่ายเทคโนโลยีสารสนเทศ, ฝ่ายวิชาการ
    - **บทบาท:** ให้คำแนะนำและควบคุมการดำเนินงานตามแผน BCP, ประเมินผลและปรับปรุงแผนตามความเหมาะสม
2. **เลขานุการคณะกรรมการบริหารแผน (BCP Coordinator):**
    - **บทบาท:** รับผิดชอบในการจัดเตรียมการประชุมของคณะกรรมการบริหารแผน และจัดการเอกสารที่เกี่ยวข้องกับแผน BCP
    - **หน้าที่:** จัดการประชุม, บันทึกการประชุม, ดูแลการปรับปรุงแผนตามคำแนะนำของคณะกรรมการบริหารแผน

4. บุคลากรสำรอง (Backup Personnel)

1. **บุคลากรสำรองในแต่ละตำแหน่ง (Backup for Key Positions):**
    - กำหนดบุคลากรสำรองในทุกตำแหน่งหลัก เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่องหากบุคลากรหลักไม่สามารถปฏิบัติงานได้
    - **หน้าที่:** เตรียมพร้อมและทบทวนแผน BCP อย่างสม่ำเสมอ เพื่อให้สามารถปฏิบัติงานได้ทันทีเมื่อเกิดเหตุขัดข้อง

การกำหนดบุคลากรผู้รับผิดชอบ

ในแผนบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ได้มีการระบุบุคลากรที่รับผิดชอบเพิ่มเติมในด้านต่าง ๆ ดังนี้

1. นายปารมินทร์ ทิมแก้ว (นักวิชาการคอมพิวเตอร์)

- รับผิดชอบหลักด้านระบบแม่ข่าย (Server) ระบบเครือข่าย (Network) และระบบ IT ทุกระบบของศูนย์ฯ
- มีบทบาทในการควบคุม ดูแล และแก้ไขปัญหาเมื่อเกิดเหตุขัดข้อง พร้อมประสานงานในการฟื้นฟูระบบทั้งหมด
- เป็นบุคลากรลำดับที่ 1 ในงานระบบ และลำดับที่ 2 สำหรับงานซ่อมบำรุงอุปกรณ์

2. นายณัฐวุฒิ ทับทิมศรี (นายช่างเทคนิค)

- รับผิดชอบหลักในด้านการติดตั้งและซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศภายในศูนย์ฯ
- เป็นบุคลากรลำดับที่ 1 สำหรับงานซ่อมบำรุง และลำดับที่ 2 สำหรับระบบเครือข่าย
- ให้การสนับสนุนในภารกิจสำรองข้อมูลและฟื้นฟูระบบกรณีเกิดเหตุขัดข้อง

การบริหารจัดการระบบศูนย์ข้อมูล (DC) และระบบสำรองฉุกเฉิน (DR)

เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินงานต่อเนื่องได้แม้ในกรณีเกิดเหตุขัดข้องรุนแรง ได้มีการจัดเตรียมแนวทางด้านศูนย์ข้อมูล (Data Center – DC) และระบบกู้คืนจากภัยพิบัติ (Disaster Recovery – DR) ดังนี้

1. ระบบศูนย์ข้อมูลหลัก (Primary DC)

- ตั้งอยู่ภายในศูนย์แพทยศาสตรศึกษาชั้นคลินิกโรงพยาบาลสวรรค์ประชา รักษ์โดยมีระบบไฟฟ้าสำรองและการควบคุมอุณหภูมิที่เหมาะสม

- นายปารมินทร์ ทิมแก้ว เป็นผู้ดูแลรับผิดชอบหลักในการตรวจสอบและควบคุมความพร้อมของระบบ

2. ระบบสำรอง DR (Disaster Recovery Site)

- ขณะนี้อยู่ระหว่างดำเนินการจัดซื้ออุปกรณ์เพิ่มเติม ได้แก่ Server และ SAN สำหรับใช้เป็น DR Site

- ระบบ DR จะถูกออกแบบให้สามารถใช้งานต่อเนื่องได้โดยไม่ต้องหยุดประมวลผล (Non-stop operation)

3. แนวทางการทดสอบและฟื้นฟู

- มีการทดสอบระบบ DR อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินความพร้อมของระบบสำรอง

- ในกรณีที่ระบบหลักขัดข้อง จะสามารถเปลี่ยนการประมวลผลไปยัง DR Site ได้ภายใน 2 ชั่วโมง โดยมีเป้าหมาย RTO ไม่เกิน 4 ชั่วโมง และ RPO ไม่เกิน 1 ชั่วโมง