Business Continuity Plan (BCP) กลุ่มงานบัญชี โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack วันที่ 9 ธันวาคม 2566 ส่งผลให้ระบบบริการไม่สามารถดำเนินการได้

แผนก: กลุ่มงานบัญชี

ผู้รับผิดชอบ: นางวัฒนาพร กุลจิตติ์วิภาส หัวหน้ากลุ่มงานบัญชี

1. บทนำ

จากสถานกรณ์ระบบคอมพิวเตอร์ของโรงพยาบาลอุดรธานี โดนโจมตีจาก ransomware attack ในวันที่ 9 ธันวาคม 2566 ทำให้ Sever ล่ม ส่งผลกระทบต่อการให้บริการของโรงพยาบาล และส่งผลกระทบต่อระบบงานบัญชี จำเป็นต้องทบทวนและจัดทำแผนเพื่อเตรียมความพร้อมในการรับมือกับสถานการณ์ที่อาจเกิดขึ้นในอนาคตเพื่อให้เป็นแนวทางปฏิบัติในการรักษาความปลอดภัยของระบบข้อมูลที่อาจถูกโจมตีทางไซต์เบอร์ร่วมกับหน่ายงานต่าง ๆ ภายในโรงพยาบาลอีกครั้ง ซึ่งในยุคปัจจุบันระบบการทำงานและการรับส่งข้อมูลมีการพัฒนาอย่างมากมีการทำงานผ่านระบบอินเทอร์เน็ต ทำให้มีความเสี่ยงที่อาจเป็นช่องทางที่มิจฉาชีพสามารถเข้ามาโจมตีได้ง่าย ดังนั้นเพื่อปกป้องข้อมูลและรายงานที่สำคัญทางงานบัญชีและให้สามารถดำเนินงานได้อย่างต่อเนื่องเมื่อเกิดเหตุดังกล่าว จึงต้องมีแผน Business Continuity Plan (BCP) สำหรับหน่วยงานมาเป็นแนวทางป้องกันและแนวทางปฏิบัติหากเกิดเหตุวิกฤตในอนาคต

ปัญหา

ปัญหาที่เกิดขึ้นจากเหตุการณ์ ransomware attack: ดังนี้ ไม่สามารถบันทึกข้อมูลบัญชีและรายงานต่าง ๆ ได้ โปรแกรมบัญชีและข้อมูลทางบัญชีสูญหาย ไม่สามารถกู้ข้อมูลคืนกลับมาได้

วิเคราะห์สาเหตุของปัญหา

1. ระบบรักษาความปลอดภัยระบบป้องกันของโรงพยาบาลมีช่องโหว่ ทำให้แฮกเกอร์สามารถเข้าถึงระบบของโรงพยาบาล
2. โรงพยาบาลไม่มีระบบสำรองข้อมูลที่เพียงพอและไม่มีการสำรองข้อมูลในระบบที่ปลอดภัยที่เข้าถึงได้ยากกว่านี้ ทำให้ไม่สามารถกู้ข้อมูลคืนมาได้หลังจากถูกโจมตี
3. บุคลากรของโรงพยาบาลอาจไม่มีความรู้ความเข้าใจเกี่ยวกับ ransomware attack เพียงพอ เนื่องจากไม่เคยมีเหตุการณ์เช่นนี้เกิดขึ้นมาก่อน ทำให้ไม่สามารถปิดระบบและป้องกันภัยคุกคามได้ทันท่วงที

แนวทางการแก้ไขปัญหา

1. ผู้บริหารร่วมกับฝ่าย IT ปรับปรุงและพัฒนาระบบรักษาความปลอดภัยของโรงพยาบาลอย่างสม่ำเสมอ
2. พัฒนาจัดทำระบบสำรองข้อมูลที่ปลอดภัยอย่างเข้มแข็ง และมีการสำรองข้อมูลอย่างสม่ำเสมอ เก็บไว้ในที่ที่จะถูกโจมตีได้ยาก
3. มีพัฒนาบุคลากรให้มีการตื่นรู้และตระหนักกับปัญหาที่เกิดขึ้น
4. มีการจำกัดสิทธิการเข้าถึงข้อมูลการใช้ระบบตามระดับความจำเป็น

5. มีการแยกระบบที่ให้บริการ ระบบข้อมูลต่าง ๆ ในการใช้ Internet ตามความจำเป็นและเหมาะสม
6. มีการแยก Server ของระบบงานบัญชีออกจากระบบอื่น ๆ ของโรงพยาบาล
7. สำรองข้อมูลระบบงานบัญชีแยกต่างหากจากระบบอื่น
8. กำหนดสิทธิ์การเข้าถึง Server ของระบบงานบัญชีเฉพาะผู้ที่เกี่ยวข้อง

อุปสรรค

1. ระบบของโรงพยาบาลไม่มี server เฉพาะระบบงานบัญชี ไม่มีแหล่งสำรองข้อมูลที่แยกออกมาชัดเจน มีการสำรองแบบ Server รวม หากเกิดความผิดพลาดทำให้ล้มทั้งระบบ
2. กลุ่มงานไม่มีแหล่งสำรอง เนื่องจากข้อมูลมีจำนวนมากเกินไปกว่าจะเก็บไว้ที่ตัวเครื่องที่ใช้ทำงาน หากเครื่องชำรุดก็อาจทำให้ข้อมูลสูญหายทั้งหมด
3. ไม่ได้รับการสนับสนุนในด้าน Sever และคอมพิวเตอร์เครื่องเครื่องใหม่เพื่อเพิ่มประสิทธิภาพการทำงานความปลอดภัยเพราะไม่ได้ให้บริการกับคนไข้โดยตรง
4. งบประมาณที่จะจัดหาวัสดุอุปกรณ์อาจมีจำกัด

แนวทางการแก้ไขอุปสรรค

1. เสนอให้ผู้บริหารและทีม IT จัดให้มีระบบ Server ของระบบงานบัญชีแยกออกจากระบบอื่น ๆ ของโรงพยาบาล
2. ขอเครื่อง Server เพื่อให้มีการสำรองข้อมูลประจำวันภายในกลุ่มงานบัญชี
3. ขอทดแทนเครื่องคอมพิวเตอร์เครื่องใหม่แทนเครื่องคอมพิวเตอร์ที่ใช้งานมานาน เพื่อเพิ่มประสิทธิภาพการทำงานและลดความเสี่ยงในเรื่องการชำรุด
4. โรงพยาบาลต้องจัดหางบประมาณในการพัฒนาด้านเทคโนโลยีและสนับสนุนวัสดุอุปกรณ์ที่จำเป็น เช่น จัดทำแผนของบประมาณ หรือรับบริจาคจากแหล่งเงินอื่น ๆ

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ระบุผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก
  - ไม่สามารถบันทึกข้อมูลทางการเงินและบัญชี
  - ไม่สามารถออกรายงานทางการเงิน
  - ขอมูลทางบัญชีของโรงพยาบาลอุดรธานีสูญหาย
- ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
  ไม่สามารถค้นหาข้อมูลใบเสร็จ และข้อมูลให้บริการต่าง ๆ

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack

  <u>ป้องกัน ตรวจจับ และฟื้นฟู</u>

  1. มีระบบติดตั้งและอับเดท Antivirus เครื่องคอมพิวเตอร์แต่ละเครื่อง
  2. ขอเครื่องคอมพิวเตอร์ใหม่ทดแทนเครื่องเก่าที่อายุการใช้งานมานาน ซึ่งเสี่ยงต่อการชำรุด อาจทำให้ข้อมูลที่เก็บไว้สูญหาย
  3. จำกัดการเข้าถึงระบบ Lan แยกออกจากระบบ Internet หรือให้ใช้ได้แบบจำกัดเว็ปไซต์เท่านั้น
  4. อบรมให้ความรู้เจ้าหน้าที่ให้ตระหนักถึงภัยคุกคามและวิธีการป้องกันต่าง ๆ
  5. มีการสำรองข้อมูลเป็นประจำวัน และมีการสำรองข้อมูลหลาย ๆ แหล่งเก็บไว้ในที่ปลอดภัย เพื่อหากเกิดข้อผิดพลาดไม่สามารถกู้ข้อมูลได้ให้นำข้อมูลที่สำนรองไว้ในที่ปลอดภัยมาใช้
  6. หากเกิดเหตุภัยคุกคาม ให้ดำเนินการตามกระบวนการตามแผน BCP จนพ้นวิกฤต ตลอดจนแผนการฟื้นฟูข้อมูลให้สมบูรณ์และเป็นปัจจุบัน

- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น
  1. แยก Server ระบบบัญชีออกจากระบบอื่น ๆ
  2. มีระบบการสำรองข้อมูลเป็นประจำจาก กลุ่มงาน IT
  3. ให้สำรองข้อมูลประจำวันโดยกล่มงานบัญชี

- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
  รวบรวมข้อมูลจากเอกสารที่มีอยู่ เพื่ออำนวยความสะดวกต่อผู้มาติดต่องาน เช่น กรณีใบเสร็จสูญหาย เป็นต้น

2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack
  1. แจ้งเหตุการณ์ให้หัวหน้ากลุ่มงานบัญชี และงาน IT ทราบ
  2. ปิดระบบที่ถูกโจมตีเพื่อป้องกันการแพร่กระจายของมัลแวร์
  3. ฝ่าย IT ประเมินและแก้ไขระบบ
  4. หากข้อมูลและโปรแกรมสูญหายเริ่มการกู้คืนข้อมูลจากข้อมูลสำรอง
  5. ทดสอบระบบเพื่อความปลอดภัยก่อนใช้งาน

- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน

  หากเกิดเหตุเจ้าหน้าที่ผู้ปฏิบัติงานในกลุ่มงาน แจ้งฝ่าย IT ทันทีเพื่อตรวจสอบ และรายงานให้หัวหน้ากลุ่มงานบัญชีทราบ

  เมื่อประเมินจากฝ่าย IT ว่าเกิดเหตุการณ์ถูกโจมตี หัวหน้ากลุ่มงานรายให้ให้ผู้บังคับบัญชาลำดับขั้นต่อไป

ลำดับผู้ที่เกี่ยวข้อง	หน้าที่
ผู้ประสบเหตุ หรือพบเกิดสถานการณ์ - เจ้าหน้าที่บัญชี ผู้ปฏิบัติงาน ขณะนั้น	1. แจ้งเหตุ ประสานไปที่งาน IT หรือ เวร ผู้รับผิดชอบด้าน IT 2. รายงาน นางวัฒนาพร กุลจิตติ์วิภาส หัวหน้ากลุ่มงานบัญชี ให้รับทราบ
นางวัฒนาพร กุลจิตติ์วิภาส หัวหน้ากลุ่มงานบัญชี	1.ประสานหัวหน้ากลุ่มงานด้าน IT หรือ รองผู้อำนวยการด้านสารสนเทศ (หากมีเหตุขัดข้อง เช่น เจ้าหน้าที่ไม่สามารถติดต่อฝ่าย IT ได้ หรือมีเหตุอื่นที่จำเป็น) 2.รายงานผู้บังคับบัญชีเหนือขึ้นไป นายมนตรี ดวงจันทร์ทอง รองผู้อำนวยการกลุ่มภารกิจด้านอำนวยการ

- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน
  1.หากเกิดเหตุ ให้รีบปิดระบบทันที ใช้เวลาในการประสานฝ่าย IT (ภายใน 5 นาที)
  2.รายงานให้หัวหน้ากลุ่มงาน ประมาณ 5 – 10 นาที

2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP
  1. Server สำหรับสำรองข้อมูลและโปรแกรมบัญชี ที่มีระบบจัดเก็บข้อมูลที่เข้าถึงได้ยาก เพื่อให้สามารถกู้คืนได้เมื่อเกิดเหตุการณ์
  2. เครื่องคอมพิวเตอร์ที่มีระบบความปลอดภัย มีการลงโปรแกรม Antivirus และ Anti-malware

- ระบุแหล่งที่มาของทรัพยากร
  เงินบำรุงของโรงพยาบาลและงบประมาณที่อาจได้รับการสนับสนุนจากส่วนกลาง หรือเงินบริจาค

2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP
  - ทำการทดสอบการสำรองข้อมูลและการกู้คืนข้อมูลจากSever สำรอง
  - ตรวจสอบความปลอดภัยของโปรแกรม Antivirus และ Anti-malware
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้
  - ให้เจ้าหน้าที่เข้าร่วมอบรมในโครงการของโรงพยาบาลเพื่อให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับ ransomware และวิธีการป้องกัน
  - ทบทวนการปฏิบัติตามแผน BCP
  - จำลองเหตุการณ์ทดสอบระบบ การกู้คืนข้อมูล

3. เอกสารแนบ

<u>แนวทางรักษาข้อมูลงานบัญชี</u> <u>เพื่อเตรียมตัวรับมือกับสถานการณ์</u>

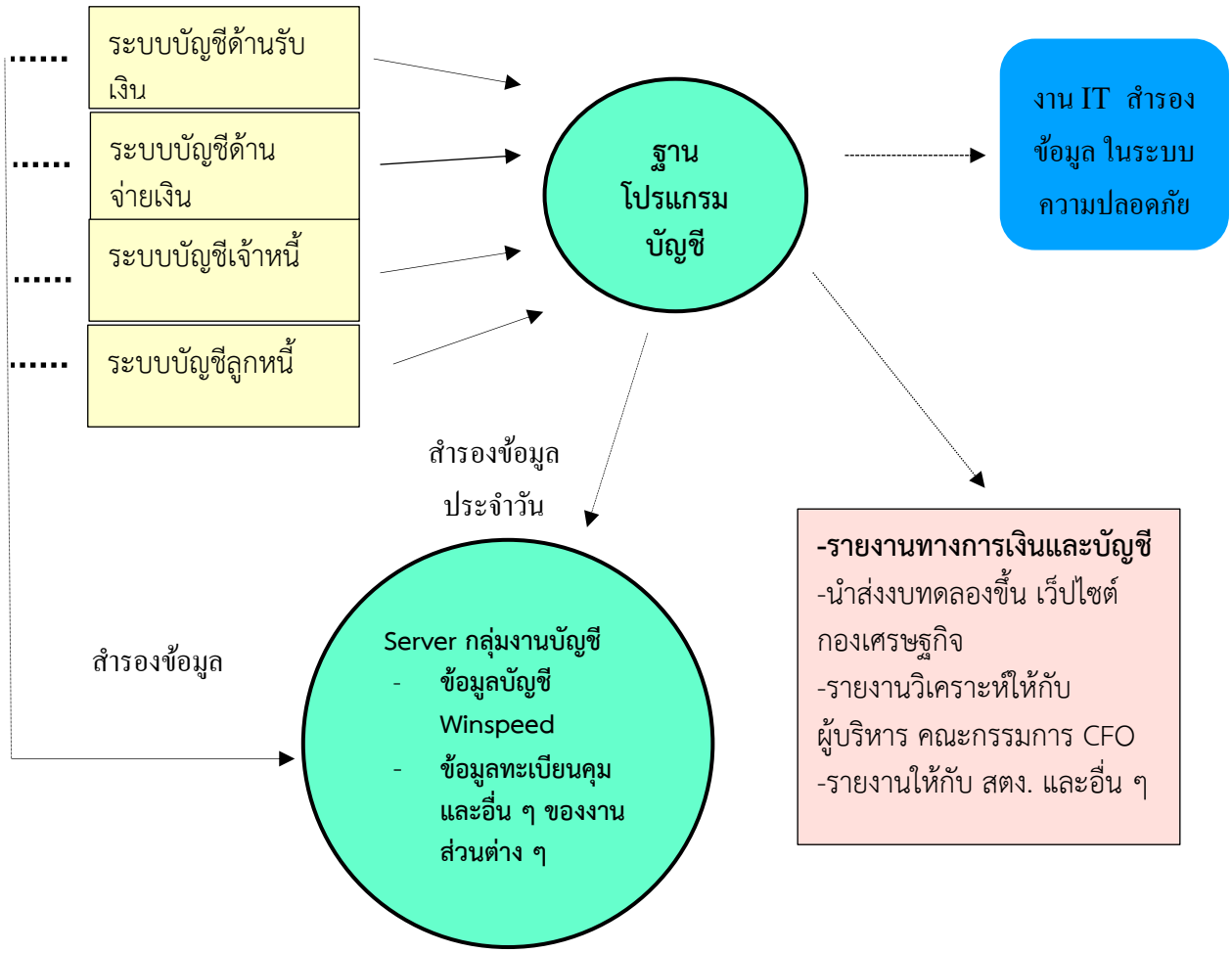
แนวทางปฏิบัติ

1. ฝ่าย IT ทำการสำรอง ข้อมูลโปรแกรมบัญชี นำเก็บในระบบ Sever ที่ปลอดภัยต่าง ๆ ตามระบบความปลอดภัยทางไซเบอร์

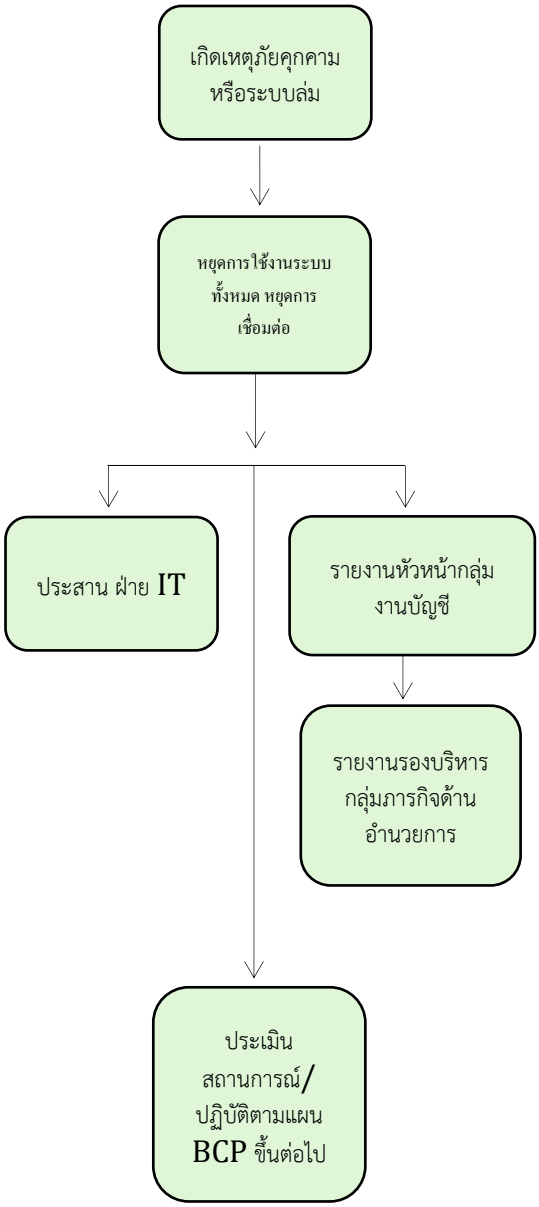
2. จัดให้มีผู้ดูแลระบบโปรแกรมของกลุ่มงานทำการสำรองข้อมูลและโปรแกรมทุกสิ้นวัน เพื่อเก็บรักษาและนำมาใช้หากระบบใหญ่เกิดเหตุไม่สามารถดำเนินการได้ ใน Server ของกลุ่มงาน

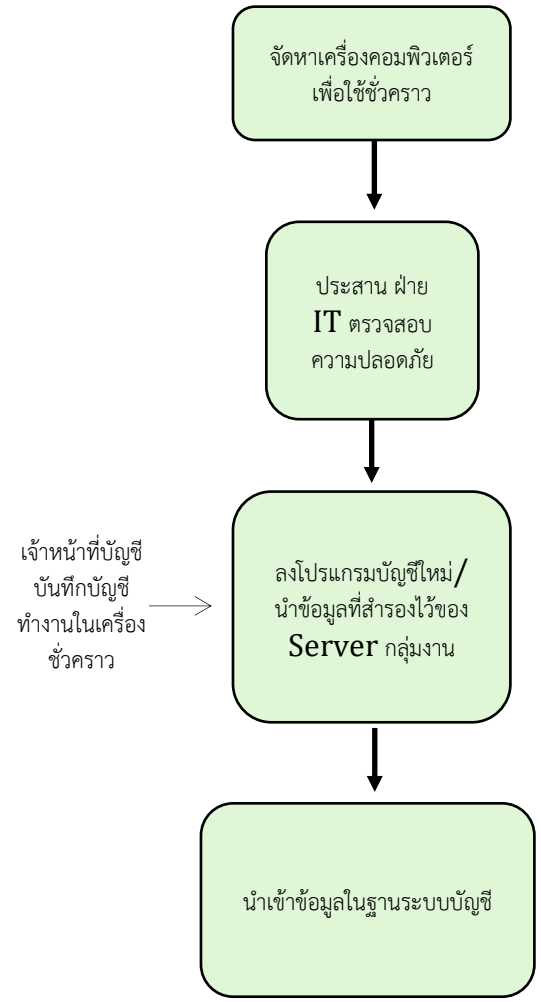
3. สำรองข้อมูลในเครื่องคอมพิวเตอร์ของงานบัญชีฝ่ายต่าง ๆ ทุก สัปดาห์ และทุกสิ้นเดือน ใน Server ของกลุ่มงาน หากเกิดการชำรุดเสียหายของข้อมูลในเครื่องคอมพิวเตอร์

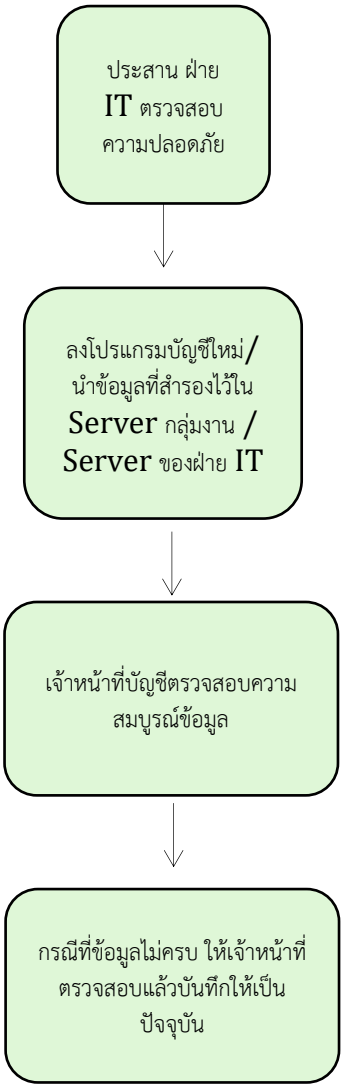
แผนผังแสดงแนวทางการปฏิบัติการระบบงานบัญชี



Flow Chart แผนปฏิบัติการ กลุ่มงานบัญชี
กรณีเกิดเหตุระบบคอมพิวเตอร์ล่มหรือมีภัยคุกคามทางไซเบอร์

ผู้รับผิดชอบ	กิจกรรม	วิธีปฏิบัติ
ผู้เจ้าหน้าบัญชี หัวหน้ากลุ่มงานบัญชี ฝ่าย IT / เวรประจำของฝ่าย IT	**เมื่อพบเหตุการณ์**  	- หากเกิดเหตุ ให้เจ้าหน้าที่ผู้ปฏิบัติงาน ปิดระบบการใช้งานคอมพิวเตอร์ การเชื่อต่อต่าง ๆ - ประสานฝ่าย IT / เวร IT - รายงานให้หัวหน้ากลุ่มงานทราบ - หัวหน้ากลุ่มงานรายงานผู้บังคับบัญชาลำดับต่อไป - ประเมินสถานการณ์ร่วมปฏิบัติตามแผน BCP ที่วางแนวทางไว้

ผู้รับผิดชอบ	กิจกรรม	วิธีการปฏิบัติ
ผู้เจ้าหน้าที่บัญชี หัวหน้ากลุ่มงานบัญชี ฝ่าย IT	**กรณี ระบบยังไม่สามารถกลับมาใช้ได้**  	กรณีเร่งด่วน แต่สถานการณ์ยังไม่ คลีคลาย ไม่ทันต่อการใช้งาน ดำเนินการดังนี้ 1. จัดหาคอมพิวเตอร์ที่ปลอดภัย (ตรวจสอบจากฝ่าย IT) 2. เพื่อลงโปรแกรมและนำเข้าข้อมูลที่สำรองไว้เพื่อใช้ไปพลางก่อน (อาจไม่ครบทุกงาน) เพื่อบันทึกข้อมูลทางบัญชี ไม่ให้งานคั่งค้าง หรือส่งข้อมูลได้ทันกำหนด 3. เมื่อระบบและเครื่องใช้งานได้ตามปกติให้นำเข้าข้อมูลในระบบใหญ่เพื่อใช้งานต่อไป

ผู้รับผิดชอบ	กิจกรรม	วิธีปฏิบัติ
ผู้เจ้าหน้าที่บัญชี หัวหน้ากลุ่มงานบัญชี ฝ่าย IT	**กรณี ระบบใช้งานได้ตามปกติ แต่ไม่สามารถกู้คืนข้อมูลได้**  	หลังจากระบบกลับมาใช้ได้แต่ไม่สามารถกู้คืนโปรแกรมหรือข้อมูลทางบัญชีได้ ให้ดำเนินการดังนี้ 1. ให้นำเข้าข้อมูลจาก Sever ของกลุ่มงานที่สำรองไว้ เลือกเป็นอันดับแรก เนื่องจากมีการสำรองไว้เป็นประจำวัน 2. หากไม่สามารถนำข้อมูลจาก Sever กลุ่มงานบัญชี ให้นำข้อมูลที่สำรองของฝ่าย IT ที่สำรองไว้ 3. เจ้าหน้าที่บัญชีดำเนินการตรวจสอบความสมบูรณ์ของข้อมูลในฐานโปรแกรมบัญชี และข้อมูลงานของตนเอง 4. หากข้อมูลไม่ครบ ไม่สมบูรณ์ให้เร่งดำเนินการบันทึกให้ครบถ้วนและเป็นปัจจุบัน

4. การอนุมัติ

หัวหน้าแผนก: นางวัฒนาพร กุลจิตติ์วิภาส

นักวิชาการเงินและบัญชีชำนาญการ

5. บทสรุป

การจัดทำแผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่นๆ ได้อย่างมีประสิทธิภาพ และแผน BCP ของกลุ่มงานบัญชีเป็นแผนของกลุ่มงานภายในร่วมกับ งาน ITจัดทำขึ้นเพื่อรับมือกับเหตุการณ์ ภัยคุกคามทางไซต์เบอร์ที่ถอดบทเรียนจาก ransomware attack

หมายเหตุ:

- ฟอร์มนี้สามารถปรับแต่งให้เหมาะกับแต่ละแผนกได้
- แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

แหล่งข้อมูล

คำแนะนำ

- ควรจัดทำแผน BCP ร่วมกับผู้เชี่ยวชาญด้านไอที
- ควรทดสอบแผน BCP เป็นประจำ
- ควรฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
มีการแยก Server ของระบบงานบัญชีออกจากระบบอื่น ๆ		/	/
มีการสำรอง ในส่วนของกลุ่มงานบัญชี	/	/	
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
การสำรองข้อมูลของงานบัญชีทุกวัน เพื่อนำมาใช้หากเกิดเหตุขึ้นอีก	/		/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
จัดหาโปรแกรมบัญชีเพื่อติดตั้งระบบใหม่	/		/
จัดหาคอมพิวเตอร์เครื่องที่ปลอดภัยเพื่อทำงานชั่วคราว	/		/
การปฏิบัติหลังระบบกลับสู่ปกติ			
กรณีข้อมูลไม่สามารถกู้คืน ดำเนินการนำเข้าข้อมูลสำรองมาใช้	/		/
ข้อมูลที่คืนมาอาจไม่ครบ อาจขาดช่วงก่อนสำรอง ให้ระดมกำลังเจ้าหน้าที่บัญชีเร่งบันทึกให้ครบถ้วน	/		
ดำเนินการบันทึกข้อมูลบัญชีให้เป็นปัจจุบัน	/		

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT