ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 27 กันยายน 2567

แผนก: เวชนิทัศน์และโสตทัศนศึกษา

ผู้รับผิดชอบ: นายชัยคม อธิชโย,อำไพ สาระสัตย์

1. บทนำ

งานเวชนิทัศน์และโสตทัศนศึกษา ได้จัดทำแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) เพื่อใช้ในกรณีที่เกิดวิกฤติ ransomware attack เข้าโจมตีเมื่อวันที่ 9 ธันวาคม 2566 หรือเหตุการณ์ฉุกเฉินต่างๆที่อาจจะเกิดขึ้นในอนาคต จากระบบเซิฟเวอร์ ระบบเนตเวิร์คขัดข้อง ระบบล่มจากไวรัสคอมพิวเตอร์ เพื่อให้หน่วยงานสามารถนำไปใช้เพื่อตอบสนองการปฏิบัติงานภายใต้ภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ได้ทันท่วงที โดยสถานการณ์ฉุกเฉินที่เกิดขึ้นไม่ส่งผลกระทบต่อการให้บริการบุคลากร เพื่อสร้างความมั่นใจและลดผลกระทบที่อาจเกิดขึ้นกับโรงพยาบาล และทำให้กระบวนงานสำคัญขององค์กร(Critical Business Process) สามารถกลับมาดำเนินงานได้อย่างปกติโดยใช้เวลาน้อยที่สุดในการฟื้นฟู ซึ่งจะช่วยลดระดับความรุนแรงของผลกระทบที่จะเกิดขึ้นกับองค์กร ดังนั้น หน่วยงานจึงได้วิเคราะห์ถึงปัญหาและอุปสรรคในการให้บริการบุคลากร

หมายเหตุ : งานเวชนิทัศน์และโสตทัศนศึกษาใช้คอมพิวเตอร์ 2 แบบ คือ Internet Only และ Lan only โดยแยกเครื่องกัน

ปัญหา

- ระบุบทเรียนปัญหาจากเหตุการณ์ ransomware attack: ปัญหา คือ
  1.ไม่สามารถเข้าใช้อินเตอร์เน็ตได้
  2.ไม่สามารถรับ-ส่งข้อมูลออนไลน์ได้
  3.การเผยแพร่ความรู้และข้อมูล ผ่านระบบออนไลน์ หยุดชั่วคราว เนื่องจากไม่สามารถสืบค้นข้อมูลจากระบบอินเตอร์เน็ตได้
  4.ประสานงานผ่านระบบออนไลน์ ต้องระงับการปฏิบัติงานนี้ไว้ชั่วคราว
- วิเคราะห์สาเหตุของปัญหา:
  1.เครื่องคอมพิวเตอร์ในงานเวชนิทัศน์ฯเป็นเครื่องที่อายุการใช้งานนาน
  2.ระบบปฏิบัติการเป็นเวอร์ชั่นเก่า
  3.โปรแกรมป้องกัน มัลแวร์(Anti-malware)ที่ไม่อัพเดต
  4.อาจจะมีการเปิดอ่านไฟล์จาก E-mail ที่ไม่ทราบแหล่งที่มา
  5.ขาดความระมัดระวังการดาวน์โหลดไฟล์จากอินเตอร์เน็ต
- ระบุแนวทางการแก้ไขปัญหา: คือ
  1.ใช้ Notebook ปฏิบัติงานแทนคอมพิวเตอร์
  2.สำรองข้อมูลเก็บไว้ในฐานข้อมูลอื่นๆ

อุปสรรค

- ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack: คือ
  1.เกิดความล้าช้าในการล่าช้าในการประสานงาน
  2.ประสิทธิภาพเครื่องคอมพิวเตอร์ Notebook ต่ำ ทำให้ปฏิบัติงานได้ล่าช้า
  3.ความเข้าใจของเจ้าหน้าที่เกี่ยวกับปัญหาที่เกิดขึ้น
- วิเคราะห์สาเหตุของอุปสรรค:
  1.เจ้าหน้าที่
  2.ระบบคอมพิวเตอร์
  3.ประสิทธิภาพของเครื่องคอมพิวเตอร์
- ระบุแนวทางการแก้ไขอุปสรรค:
  1.จัดเรียงเอกสารให้เป็นระบบ
  2.สำรองข้อมูลในฐานข้อมูลอื่นๆ
  3.ชี้แจงเจ้าหน้าที่เกี่ยวกับเหตุการณ์โดน ransomware attack ที่เกิดขึ้นและแนวทางการแก้ไขในภาพรวมของโรงพยาบาลและกลุ่มงาน

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ระบุผลกระทบของ ransomware attack ที่มีต่องานบริการของแผนก
  1.การเผยแพร่สื่อประชาสัมพันธ์ ข้อมูลข่าวสาร ของหน่วยงานหยุดชะงัก
  2.ไม่สามารถสืบค้นข้อมูลทางอินเตอร์เน็ตได้
  3.ไม่สามารถรับ-ส่งข้อมูล ทางออนไลน์ได้
- ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
  1. ไม่สามารถรับ-ส่ง ข้อมูลทางออนไลน์ได้
  2.การให้บริการล่าช้า เนื่องไม่สามารถประสานทางออนไลน์ได้
  3.เวลาในการให้บริการบุคลากรแต่ละรายเพิ่มมากขึ้น

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack
  1.แจ้งเจ้าหน้าที่ศูนย์คอมพิวเตอร์ ให้ทราบเหตุการณ์เกิดขึ้น
  2.แจ้งบุคลากรในงานเวชนิทัศน์ฯ รับทราบเหตุการณ์
  3.ปฏิบัติตามแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของงานเวชนิทัศน์ฯ
- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น
  1.แจ้งผู้มารับบริการเกี่ยวกับปัญหาด้านระบบคอมพิวเตอร์ให้เข้าใจ
  2.ผู้มาใช้บริการต้องมาประสานงานด้วยตนเอง หรือประสานงานโทรศัพท์
- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
  1.อธิบายผู้ป่วยเกี่ยวกับปัญหาด้านระบบคอมพิวเตอร์ให้เข้าใจ

2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack
- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน
- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน

ข้อมูล/ผู้รับผิดชอบ	ทันที	รอ
1.ถอดสายตัวเชื่อมระบบ (น.ส.อำไพ สาระสัตย์)	/ (5 นาที)	
2.สำรองข้อมูล (นายมารุต บุตรจำนงค์,นายณัฐพงศ์ หมอดี,นางสาวกาญจนา ศรีเฉลิม, นางสาวธัญทิพ หาญวงศ์,)	/ (1 ชม.)	
3.ประสานเจ้าหน้าที่ศูนย์คอมพิวเตอร์ทำการ update antivirus คอมพิวเตอร์ในหน่วยงาน (นายสรธร โมรา, นายณฐวรรต ไชยดี)	/ (5 นาที)	
4.ประสานเจ้าหน้าที่ศูนย์คอมพิวเตอร์ทำการ update windows คอมพิวเตอร์ในหน่วยงาน (นายนิตินันท์ ชุมดาวงษ์,นายศักดิ์สิทธิ์ ใจน้ำ)	/ (5นาที)	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	หมายเหตุ
1.แจ้งหัวหน้างานเวชนิทัศน์ฯให้รับทราบ	เจ้าหน้าที่พบเห็นเหตุการณ์	-มีการซ้อมแผนอย่างน้อยเดือนละ 1 ครั้ง
2.ประเมิน		
3.ทบทวนกระบวนงาน		
4.รายงานผู้บริหาร		
5.ประสานศูนย์คอม		
6.สรุปผลการดำเนินงานแก้ไขสถานการณ์		
7.รายงานผลการ		

2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP คือ

  1.เจ้าหน้าที่งานเวชนิทัศน์และโสตทัศนศึกษา

  2.เจ้าหน้าที่ศูนย์คอมพิวเตอร์

  3.เครื่องคอมพิวเตอร์

- ระบุแหล่งที่มาของทรัพยากร คือ

  1.งานเวชนิทัศน์และโสตทัศนศึกษา โรงพยาบาลอุดรธานี

  2.ศูนย์คอมพิวเตอร์ โรงพยาบาลอุดรธานี

2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP

  1.แจ้งแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของงานเวชนิทัศน์ฯ ให้กับเจ้าหน้าที่ทุกคนทราบ

  2.ติด flow chart ให้เจ้าหน้าที่ชัดเจน

  3.แจ้งแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของงานเวชนิทัศน์ฯ รับทราบเมื่อมีเจ้าหน้าที่ใหม่

- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

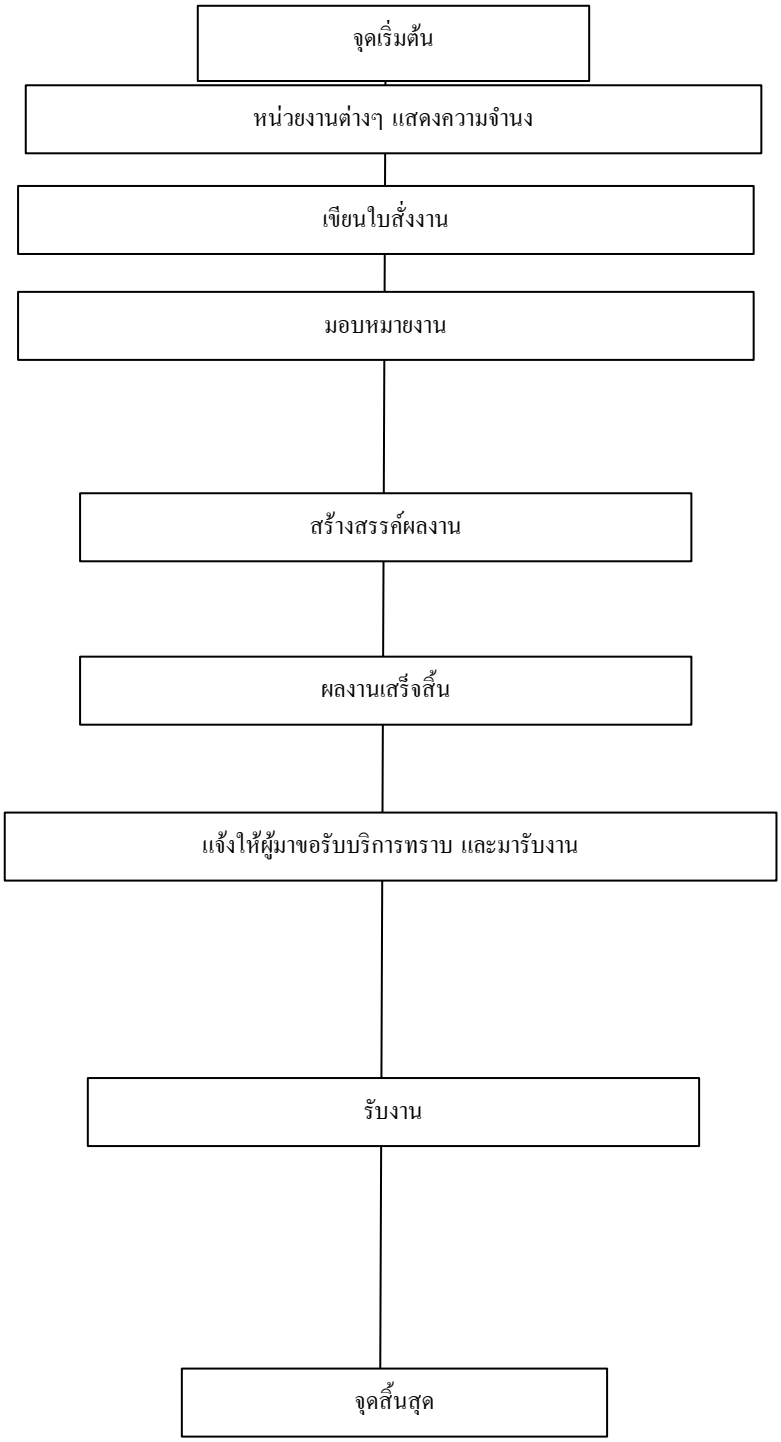
  1.ตรวจสอบ firewall ได้เปิดอยู่ทุกครั้งที่ใช้งานคอมพิวเตอร์

  2.สอนการใช้งานโปรแกรม scan virus แก่เจ้าหน้าที่ทุกคนในกลุ่มงาน

3. เอกสารแนบ

- แผนงาน flow chart ต่างๆ

แผนการดำเนินงานเวชนิทัศน์ฯ



4. การอนุมัติ

หัวหน้าแผนก: ชัยคม อธิชโย

วันที่: 27 กันยายน 2567

5. บทสรุป

ฟอร์มนี้เป็นแนวทางสำหรับแต่ละแผนกในการจัดทำแผน BCP แผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ ransomware attack และเหตุการณ์วิกฤตอื่นๆ ได้อย่างมีประสิทธิภาพ

หมายเหตุ:

- ฟอร์มนี้สามารถปรับแต่งให้เหมาะกับแต่ละแผนกได้
- แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

แหล่งข้อมูล

คำแนะนำ

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

สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1.แยกเครื่องคอมพิวเตอร์ที่ใช้งานให้บริการผู้ป่วย ออกจากเครื่องที่ใช้งาน internet			✓
2.ติดตั้งโปรแกรมป้องกันมัลแวร์(Anti-malware)ที่น่าเชื่อถือและอัพเดตเสมอ เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ที่ดาวน์โหลด			✓
3.ไม่เข้าใช้งานเว็บไซต์ที่ไม่เกี่ยวข้องกับการทำงาน	✓		
4.ระมัดระวังการเปิดอ่านไฟล์จาก E-mail ที่ไม่ทราบแหล่งที่มา	✓		
5.ระมัดระวังในการดาวน์โหลดไฟล์จากอินเตอร์เน็ต	✓		
6.หลักเลี่ยงการใช้แชร์ไฟล์โดยไม่จำเป็น	✓		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1.ตรวจสอบ firewall ได้เปิดอยู่ทุกครั้งที่ใช้งานคอมพิวเตอร์	✓		
2.เน้นย้ำความปลอดภัยเรื่องการ Identification ผู้ป่วยทุกขั้นตอนของการให้บริการ	✓		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1.ตัดเครื่องที่ติด Ransomware ออกจากระบบทันทีเพื่อป้องกันไม่ให้เครื่องอื่นติดด้วย			✓

2.ระงับการใช้ internet ของคอมพิวเตอร์ทุกเครื่อง		✓	
3.จัดทำทะเบียนผู้รับบริการในคลินิก DPAC	✓		
4.ใช้ระบบ OPD card เพื่อใช้ในการบันทึกข้อมูลการซักประวัติและการให้บริการผู้ป่วย	✓		
5.จัดทำสมุดนัดผู้ป่วยและใบนัดผู้ป่วยเพิ่มเติม	✓		
การปฏิบัติหลังระบบกลับสู่ปรกติ			
1.Format เครื่องคอมพิวเตอร์ใหม่ทั้งหมด			✓
2.กู้ข้อมูลจากฐานข้อมูลมาใช้งาน			✓
3.ตรวจสอบ firewall ได้เปิดอยู่ทุกครั้งที่ใช้งานคอมพิวเตอร์	✓		
4.ลงข้อมูลการให้บริการผู้ป่วยย้อนหลังในระบบและแสกนเอกสารเข้าระบบเพื่อเก็บไว้เป็นเอกสารอ้างอิง	✓		
5.อัพเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ			✓

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT