แผนดำเนินการ
กรณีระบบเครือข่ายคอมพิวเตอร์ล่ม
(Business Continuity Plan - BCP)

กลุ่มงานศัลยกรรม
โรงพยาบาลอุดรธานี

สารบัญ

ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) กลุ่มงานศัลยกรรม โรงพยาบาลอุดรธานี
เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้
วันที่: 9 ธันวาคม 2566
แผนก: กลุ่มงานศัลยกรรม ประกอบด้วย 14 หอผู้ป่วย และ 2 หน่วยงาน ดังนี้

1. ศัลยกรรม 1 ผู้รับผิดชอบ พว.พวงผกา ไชยชมภู
2. ศัลยกรรมประสาท ผู้รับผิดชอบ พว.อโนชา พรหมจันทร์
3. หน่วยดูแลบาดแผล ผู้รับผิดชอบ พว.แสงเดือน มากมูล
4. ศัลยกรรมหญิง ผู้รับผิดชอบ พว.อาภา ศรีสร้อย
5. ศัลยกรรมระบบทางเดินปัสสาวะ ผู้รับผิดชอบ พว.ยุคลธร ทองตระกูล
6. ศัลยกรรมตกแต่งและเด็ก ผู้รับผิดชอบ พว.สุวาณี เตียนสำรวย
7. หน่วยไฟไหม้น้ำร้อนลวก ผู้รับผิดชอบ พว.มณีรัตน์ ศรีแก้ว
8. ศัลยกรรมชาย ผู้รับผิดชอบ พว.วริศรา ภู่ทวี
9. ศัลยกรรมพิเศษชั้น 7 ผู้รับผิดชอบ พว.กิตติ์รวี ประเสริฐจิตสรร
10. ศัลยกรรม 2 ผู้รับผิดชอบ พว.กรรณิการ์ ศุภกิจอนันต์คุณ
11. เคมีบำบัด ผู้รับผิดชอบ พว.ศิริพร คำศรี
12. ศัลยกรรมหลอดเลือดสมอง ผู้รับผิดชอบ พว.ศรีสุดา พรมสีชา
13. ศัลยกรรมหัวใจและทรวงอก ผู้รับผิดชอบ พว.ยุวดี คำพรมมาภิรักษ์
14. UDSC ผู้รับผิดชอบ พว.สุลัดดา โคตรประดา
15. ธุรการการพยาบาลผู้ป่วยศัลยกรรม ผู้รับผิดชอบ พว.จิราพร ศรีบูรพา
16. ธุรการแพทย์ศัลยกรรม ผู้รับผิดชอบ นพ.วรวิทย์ อินทนู

1. บทนำ

จากกรณี ransomware attack ในวันที่ 9 ธันวาคม 2566 กลุ่มงานศัลยกรรม ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้

ปัญหา

- ระบุบทเรียนปัญหาจากเหตุการณ์ ransomware attack :
  1. ระบบฐานข้อมูลของโรงพยาบาลต้องทำการสำรองข้อมูล back up ข้อมูลอย่างสม่ำเสมอ
  2. โรงพยาบาลไม่มีแผนการรับมือกรณีปัญหาระบบล่ม ทำให้ไม่สามารถใช้งานในระบบต่างต่างๆได้ ส่งผลให้เกิดความไม่ต่อเนื่องของงาน และทำให้ระบบการทำงานเกิดความล่าช้า ไม่เป็นตามเป้าหมายที่ตั้งไว้
- วิเคราะห์สาเหตุของปัญหา :
  1. ระบบเครือข่ายทั้งหมดของโรงพยาบาลหยุดชะงัก
  2. บุคลากรขาดความรู้ ความเข้าใจ กับเหตุการณ์ที่เกิดขึ้นและไม่มีแผนการรับมือต่อการเกิด ransomware
  3. มี / ไม่มี ระบบป้องกันการโจมตีจากทางไซเบอร์ ที่มีประสิทธิภาพ ในคอมพิวเตอร์ระบบเครือข่าย
  4. มีการโหลดไฟล์ที่ไม่ปลอดภัยเข้ามาในคอมพิวเตอร์โรงพยาบาล
  5. คอมพิวเตอร์เก่าใช้งานนานกว่า 10 ปี
- ระบุแนวทางการแก้ไขปัญหา :

  1. ซักซ้อมและวางแผนรองรับของหน่วยงานให้ชัดเจน
  2. มีระบบสำรองข้อมูลต่างๆที่เกี่ยวข้องของตึก ลงในโปรแกรม excel หรือ e-mail ทุกๆ 1 เดือน
  3. มีระบบเอกสารสำรอง ที่สามารถปริ้นจากคอมพิวเตอร์ทั่วไปได้โดยการทำเป็น QR code ไว้ เพื่อใช้ในการทำเวชระเบียนผู้ป่วยได้เมื่อเกิดปัญหา
  4. มีระบบการบันทึกข้อมูลสำรองที่ คอมพิวเตอร์ โปรแกรม excel ของหน่วยงานเอง

อุปสรรค

- ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack :
  1. หน่วยงานไม่มีแผนรับมือกรณีปัญหาระบบล่ม
  2. หน่วยงานไม่มีการสำรองข้อมูลอย่างสม่ำเสมอ
- วิเคราะห์สาเหตุของอุปสรรค:

  1. หน่วยงานไม่มีการอัพเดตโปรแกรมสแกนไวรัส
  2. หน่วยงานไม่มี ระบบป้องกันการโจมตีจากทางไซเบอร์ที่มีประสิทธิภาพ
  3. มีการโหลดไฟล์ที่ไม่ปลอดภัยเข้ามาในคอมพิวเตอร์โรงพยาบาล
- ระบุแนวทางการแก้ไขอุปสรรค:
  1. ซักซ้อมและวางแผนรองรับของหน่วยงานให้ชัดเจนทุกๆ 3 เดือน
  2. มีการสื่อสารและให้ข้อมูลที่ชัดเจน รายงานสถานการณ์อย่างต่อเนื่องจนกว่าสถานการณ์จะคลี่คลาย
  3. มีการใช้เครื่องมือในการสำรองข้อมูลแทนโปรแกรม เช่น excel หรือ e-mail ทุกๆ 1 เดือน
  4. มีระบบเอกสารสำรอง ที่สามารถปริ้นจากคอมพิวเตอร์ทั่วไปได้โดยการทำเป็น QR code ไว้ เพื่อใช้ในการทำเวชระเบียนผู้ป่วยได้เมื่อเกิดปัญหา
  5. มีระบบการบันทึกข้อมูลสำรองที่ คอมพิวเตอร์ โปรแกรม excel ของหน่วยงานเอง

ฟอร์มนี้จัดทำขึ้นเพื่อให้แต่ละแผนกในโรงพยาบาลอุดรธานีสามารถจัดทำแผนรับมือ Business Continuity Plan (BCP) กรณีเกิดเหตุการณ์ ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้ แผน BCP นี้จะช่วยให้แต่ละแผนกสามารถดำเนินงานต่อเนื่องได้อย่างมีประสิทธิภาพ แม้จะเผชิญกับเหตุการณ์วิกฤต

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ระบุผลกระทบของ ransomware attack ที่มีต่อกลุ่มงานศัลยกรรม
  1. ไม่สามารถจัดทำเอกสารเวชระเบียนผู้ป่วยรับใหม่และต่อเนื่องได้
  2. ไม่สามารถตรวจสอบผลการตรวจทางห้องปฏิบัติการ ผลเอกซเรย์ ประวัติเดิม ประวัติการใช้ยาของผู้ป่วยได้
  3. ไม่สามารถลงบันทึกข้อมูลต่าง ๆ ในเวชระเบียน ได้
  4. กระบวนการขั้นตอนการทำงานที่เกี่ยวเนื่องกับระบบคอมพิวเตอร์ และระบบ IT หยุดชะงัก
- ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
  1. เกิดความล่าช้าในการรับบริการของผู้ป่วย และญาติ เพิ่มระยะเวลารอคอย ในการปริ้นเอกสารที่ต้องใช้ปริ้นเอกสารในระบบเครือข่าย
  2. ผู้ป่วยต้องเสียเวลารอคอยการรับยากลับบ้าน เพราะใช้เวลาในการตรวจสอบข้อมูล และมีความเสี่ยงที่ผู้ป่วยจะเกิดการแพ้ยาซ้ำ เนื่องจากไม่มีประวัติแจ้งเตือนการแพ้ยาในระบบ
  3. เพิ่มภาระงาน เพิ่มขั้นตอนการทำงานของเจ้าหน้าที่

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack
  1. จัดตั้งทีมสั่งการในสถานการณ์ฉุกเฉินและผู้ประสานงานหลัก
- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น

1. พยาบาลหัวหน้าตึก / พยาบาลหัวหน้าเวร แจ้งเจ้าหน้าที่ศูนย์คอมพิวเตอร์ ในเวลาติดต่อ **1125 – 6** นอกเวลาติดต่อ **1126**
2. พยาบาลหัวหน้าตึก / พยาบาลหัวหน้าเวร ประเมิน,ติดตามสถานการณ์ และเตรียมแนวทางแก้ไขเบื้องต้น
3. พยาบาลหัวหน้าตึก / พยาบาลหัวหน้าเวร รายงานหัวหน้า
   ในเวลา หัวหน้าตึก รายงานหัวหน้างาน
   นอกเวลา หัวหน้าเวร รายงานหัวหน้าตึก หัวหน้าตึก รายงานหัวหน้างาน ตามลำดับขั้น เบื้องต้น
4. ผู้อำนวยการ EOC ประกาศใช้แผนปฏิบัติการฉุกเฉินกรณีเครือข่ายคอมพิวเตอร์ล่ม ดำเนินการตามแผนฯ
5. พยาบาลหัวหน้าตึก / พยาบาลหัวหน้าและรายงานใน ไลน์กลุ่มงานศัลยกรรม เพื่อร่วมหาแนวทางแก้ไขปัญหาที่จะกระทบเบื้องต้น

<u>ผู้ป่วย</u>

1. ตรวจสอบเวชระเบียน ในส่วนที่ต้องมีเอกสารเพิ่ม ใช้เอกสาร ตาม QR Code ของแผนกศัลยกรรม (ตามเอกสารแนบ) เพื่อให้กระบวนการบันทึกข้อมูลต่างๆ เป็นไปตามปกติ

2. แบบบันทึกคำสั่งแพทย์ โรงพยาบาลอุดรธานี และ ใบบันทึกประวัติและการตรวจวินิจฉัยผู้ป่วย (admission form) หากยังลงรายละเอียดไม่ครบถ้วน ให้ประสานแพทย์เจ้าของไข้เป็นกรณีไป
3. Chart ผู้ป่วยใน แพทย์บันทึกคำสั่งการรักษาได้ปกติ สั่งยา พยาบาลรับคำสั่ง ลงนามการทำหัตถการประเมินและบันทึกความคืบหน้าของแพทย์ (progress note) และพยาบาล (nurse note) ตามปกติในเวชระเบียน ยกเว้นลงข้อมูลในระบบคอมพิวเตอร์ เมื่อระบบกลับมาดำเนินการได้ตามปกติ สามารถพิมพ์ข้อมูลระบุเวลาย้อนหลัง หรือสแกนสำเนาแนบลงในฟอร์มได้
4. ระบบสแกนยา สแกน Set ผ่าตัด ให้ใช้ระบบ manual ตามที่ต้นเรื่องของระบบกำหนดขึ้นมา
    4.1 กรณีผู้ป่วยต้องได้รับการผ่าตัด เขียนใบส่ง setเตรียมผ่าตัดส่งห้องผ่าตัดทุกครั้งและห้องผ่าตัดเซ็นตรับใบsetผ่าตัดทุกครั้ง โดยพนง.ช่วยเหลือคนไข้หรือพนักงานช่วยการพยาบาล นำส่งเอกสาร
    4.2 กรณีส่งตรวจทางห้องปฏิบัติการ ส่งสิ่งส่งตรวจพร้อมใบRequest ไปที่ห้องปฏิบัติการ พร้อมรับผลตามที่ห้องปฏิบัติการกำหนด นำผลติดใน Chart ผู้ป่วย
    4.3 กรณีส่งตรวจรังสีวินิจฉัย ให้บันทึกลงในแบบฟอร์มของรังสีวินิจฉัย พร้อมรับผลตามหน่วยงานกำหนด
    4.4 การเบิกอาหาร ส่งเบิกตามแบบฟอร์มที่โภชนาการ กำหนด เช่นระบบไลน์
    4.5 การส่งขอเปลในการเคลื่อนย้ายผู้ป่วย ส่งขอตามหน่วยงาน Porter กำหนด เช่น ระบบไลน์และทางโทรศัพท์ (กรณีเร่งด่วน)
    4.6 การเบิกยาเพื่อรักษาผู้ป่วย โดยการถ่ายเอกสารใบสั่งยา นำส่งห้องยาเพื่อให้เภสัชกร จัดยาและนำส่งหอผู้ป่วยบริหารยาต่อไป
5. กรณีส่งปรึกษาระหว่างแผนก ให้แพทย์เจ้าของไข้เขียนรายละเอียดการส่งปรึกษาลงในใบส่งปรึกษาระหว่างแผนกและให้เจ้าหน้าที่(พนง.ช่วยเหลือคนไข้หรือพนักงานช่วยการพยาบาล) นำส่งใบปรึกษาไปแผนกที่ต้องการปรึกษา และให้แพทย์ที่มารับปรึกษาตอบลงในใบเดียวกัน รวมทั้งลงชื่อ วันที่และเวลากำกับทุกครั้ง
6. เมื่อผู้ป่วยสิ้นสุดการรักษา เวชระเบียนของผู้ป่วย แพทย์เจ้าของไข้สรุปข้อมูลลงในเวชระเบียน เสมียนตึกเก็บเวชระเบียนไว้ที่ตึก รอแนวทางการส่งเก็บเวชระเบียน จากหน่วยงานเวชระเบียนกำหนด

2.3 แผนปฏิบัติการ

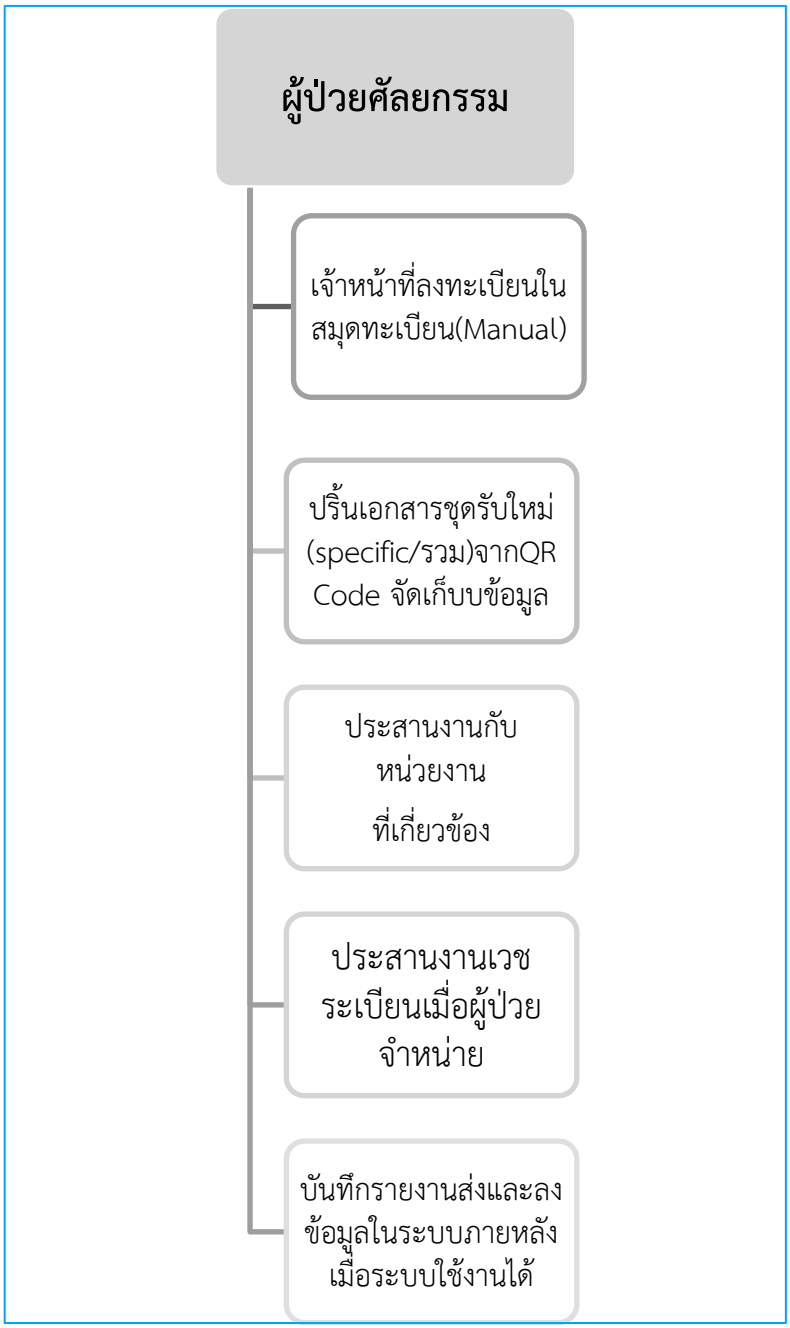
ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack

1. แจ้งเหตุการณ์ให้หัวหน้าตึก และไลน์กลุ่มงานการพยาบาลผู้ป่วยศัลยกรรม และงาน IT ทราบ
2. ปิดระบบที่ถูกโจมตีเพื่อป้องกันการแพร่กระจาย
3. ฝ่าย IT ประเมินและแก้ไขระบบ
4. หากข้อมูลและโปรแกรมสูญหายเริ่มการกู้คืนข้อมูลจากข้อมูลสำรอง
5. ทดสอบระบบเพื่อความปลอดภัยก่อนใช้งาน

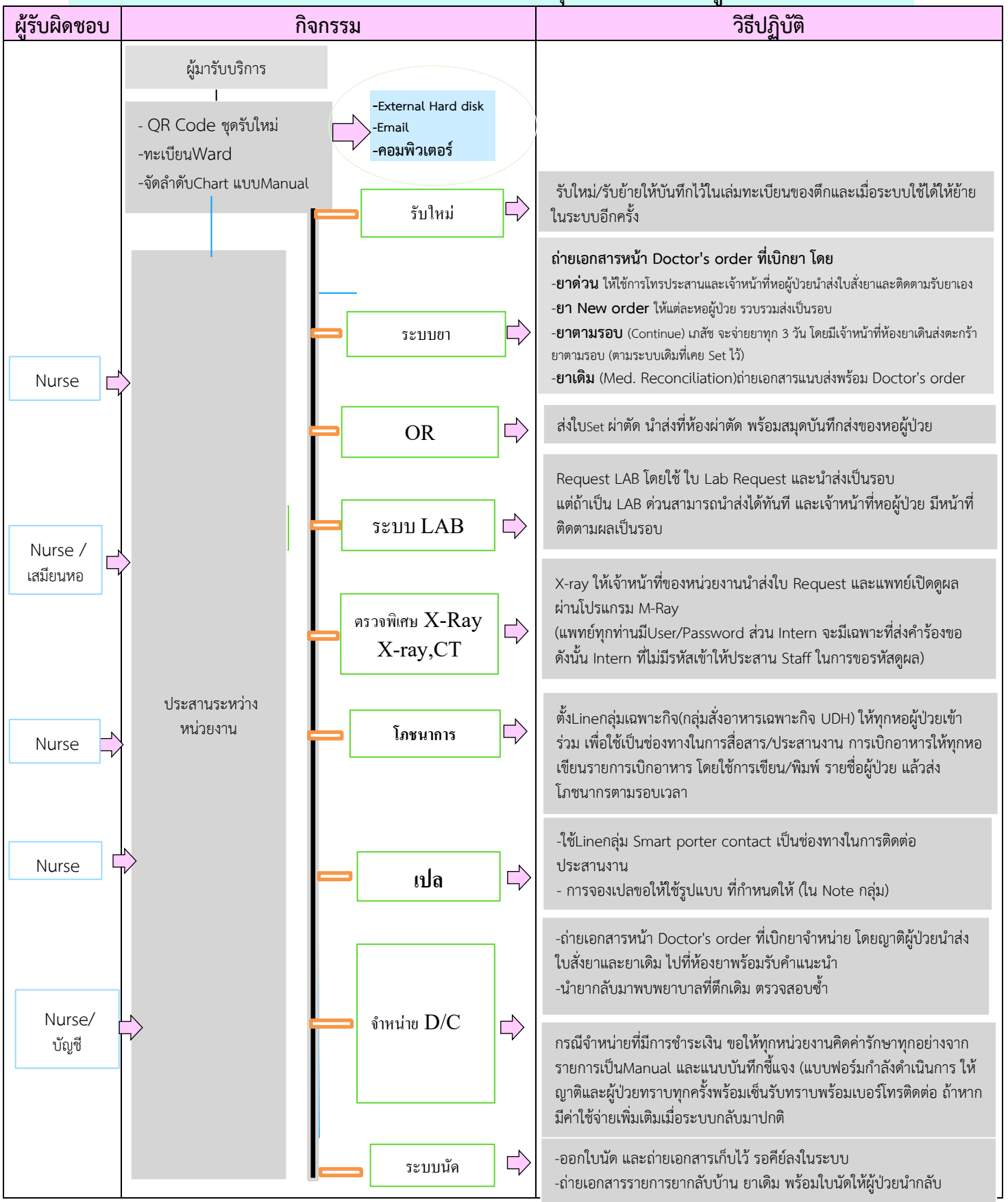
ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน

หัวหน้าเวร เป็นผู้รับผิดชอบรายงานและมอบหมายงานให้เจ้าหน้าที่ผู้ปฏิบัติปฏิบัติงานตามแผนงาน และรายงานต่อ หัวหน้าตึก หัวหน้าตึกรายงานหัวหน้ากลุ่มงาน หัวหน้ากลุ่มงานรายงานหัวหน้าพยาบาล ตามลำลับขั้น เมื่อประเมินจากฝ่าย IT ว่าเกิดเหตุการณ์ถูกโจมตี หัวหน้าเวรรายงานให้ผู้บังคับบัญชาลำดับขั้น

Flow Chart กลุ่มงานศัลยกรรม เมื่อระบบคอมพิวเตอร์ขัดข้อง



Flow chart เมื่อระบบ คอมพิวเตอร์ขัดข้อง กลุ่มงานศัลยกรรม ผู้ป่วยใน (IPD)



2.4 ทรัพยากร

วัสดุอุปกรณ์

1. คอมพิวเตอร์แบบ Stand Alone ที่มีระบบความปลอดภัย มีการลงโปรแกรม Antivirus และ Anti-malware
2. แอปพลิเคชัน เช่น ไลน์ (Line)
3. โทรศัพท์สำรอง 1 เลขหมาย

ระบุแหล่งที่มาของทรัพยากร :

1. บุคลากรในหน่วยงาน
2. ระบบ Cloud ที่มีความน่าเชื่อถือ เช่น Google Drive, OneDrive, iCloud หรือ Dropbox
3. การอัพเดตและติดตั้งซอฟต์แวร์และระบบปฏิบัติการที่ทันสมัย

2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP : การจำลองภัยคุกคามช่วยให้ทีมงานได้ทดสอบการตอบสนองต่อการโจมตี ransomware ในสภาวะจริง ซึ่งสามารถทดสอบการสำรองข้อมูล, กระบวนการกู้คืนข้อมูล, และการทำความเข้าใจของทีมงาน
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้ : การฝึกอบรมพร้อมจัดทำการทดสอบประจำปีเพื่อปรับปรุงความรู้, ทักษะ,และความเข้าใจของบุคลากรในสถานการณ์และเทคโนโลยีที่เปลี่ยนแปลง

3.เอกสารแนบ

- Flow Chart
- QR code เอกสารเวชระเบียน

4. การอนุมัติ

หัวหน้าแผนก: นางจิราพร ศรีบูรพา พยาบาลวิชาชีพชำนาญการพิเศษ

วันที่: 26 กันยายน พ.ศ. 2567

5. บทสรุป

ฟอร์มนี้เป็นแนวทางสำหรับหน่วยงานในกลุ่มงานศัลยกรรม และแต่ละแผนกในการจัดทำแผน BCP แผน BCP ที่ดี จะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ 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. ไม่เข้าเว็บไซต์ที่ไม่ปลอดภัยในคอมพิวเตอร์ของโรงพยาบาล			/
2. ไม่โหลดข้อมูล หรือไฟลที่ไม่ปบอดภัยเข้าคอมพิวเตอร์ของโรงพยาบาล			/
3. Back up ข้อมูลสม่ำเสมอ			/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1. ประชุมชี้แจง ทำหนังสือ และมีแผนรับมือ Business Continuity Plan (BCP) ของโรงพยาบาล		/	/
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1. การทำเอกสารเวชระเบียน ต่างๆ		/	
2. เอกสารเฉพาะทางศัลยกรรมชาย	/		
3. ทะเบียนงานต่าง ๆที่เกี่ยวกับข้อมูลศัลยกรรมชาย	/		
การปฏิบัติหลังระบบกลับสู่ปกติ			
1. ส่งสแกนเวชระเบียนทันทีที่ระบบใช้งานได้	/		

U =ดำเนินการได้เองระดับหน่วยงาน
S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน
I = ต้องได้รับการสนับสนุนจาก IT

แก้ไขข้อมูลล่าสุด วันที่ 26 กันยายน 2567

เอกสารแนบ QR Code เวชระเบียน