ฟอร์มสำหรับทำแผนรับมือ Business Continuity Plan (BCP) โรงพยาบาลอุดรธานี
หอผู้ป่วยวิกฤตเด็ก (PICU)

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 5 มีนาคม 2567

แผนก: กลุ่มงานกุมารเวชกรรม

ผู้รับผิดชอบ: หัวหน้ากลุ่มงานกุมารเวชกรรม, IT nurse ประจำกลุ่มงานและหอผู้ป่วย

1. บทนำ

จากการโดน ransomware attack ในวันที่ 9 ธันวาคม 2566 แผนกกุมารเวชกรรม ได้วิเคราะห์ปัญหาและอุปสรรคจากการรับมือ ransomware attack ในครั้งนี้

ปัญหา

ปัญหาที่ 1 ผู้ปฏิบัติไม่รู้ถึงผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้น

วิเคราะห์ปัญหา

1. ขาดการสื่อสารจากผู้บริหารหรือศูนย์คอมพิวเตอร์ไม่ได้แจ้งข้อมูลเกี่ยวกับผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้นอย่างครบถ้วน ชัดเจน หรือทันท่วงที
2. โรงพยาบาลไม่มีแผนและเตรียมการซ้อมแผน

แนวทางการแก้ปัญหา

1. พัฒนาการสื่อสาร
    1.1 แจ้งข้อมูลเกี่ยวกับผลกระทบรุนแรงจากเหตุการณ์ที่เกิดขึ้นอย่างครบถ้วน ชัดเจน ทันท่วงที และเข้าใจง่าย
    1.2 ใช้ช่องทางการสื่อสารที่หลากหลายและเข้าถึงผู้ปฏิบัติได้ครบถ้วน
    1.3 จัดกิจกรรมถาม-ตอบเพื่อตอบข้อสงสัยของผู้ปฏิบัติ
2. จัดทำแนวปฏิบัติอุบัติภัยทางไซเบอร์
3.ซ้อมแผนอุบัติภัยทางไซเบอร์

ปัญหาที่ 2 ศูนย์คอมไม่แจ้งปัญหาที่แท้จริงเมื่อได้รับแจ้งปัญหาในการใช้งานระบบ

วิเคราะห์ปัญหา

1. ปัญหาทางเทคนิค
    1.1ศูนย์คอมพิวเตอร์อาจไม่มีเครื่องมือหรือความเชี่ยวชาญเพียงพอในการวินิจฉัยปัญหาที่แท้จริง
    1.2.ระบบการตรวจสอบอาจมีข้อบกพร่อง ทำให้ไม่สามารถระบุสาเหตุของปัญหาได้
2. ปัญหาการสื่อสาร
    2.1 ศูนย์คอมพิวเตอร์อาจไม่ได้แจ้งข้อมูลเกี่ยวกับปัญหาให้ผู้ใช้ทราบอย่างครบถ้วน
3. ปัญหาด้านนโยบาย
    3.1 ศูนย์คอมพิวเตอร์อาจมีนโยบายไม่แจ้งรายละเอียดเกี่ยวกับปัญหาที่แท้จริงแก่ผู้ใช้
    3.2 ศูนย์คอมพิวเตอร์อาจกังวลว่าการแจ้งปัญหาที่แท้จริงอาจสร้างความตื่นตระหนกให้กับผู้ใช้
4. ศูนย์คอมพิวเตอร์อาจขาดแคลนบุคลากรที่มีสมรรถนะ

แนวทางการแก้ปัญหา

1. เพิ่มจำนวนและพัฒนาสมรรถนะบุคลากรด้าน IT
2. ควรมีระบบการแจ้งภาวะฉุกเฉินที่เกิดขึ้น ให้ผู้ปฏิบัติงานได้รับทราบอย่างรวดเร็ว และบอกแนวทางการปฏิบัติอย่างชัดเจน เช่น งดใช้คอมพิวเตอร์ ถอดสาย Lan เป็นต้น
3. จัดทำแผนงานและขั้นตอนเพื่อรองรับหรือเรียกคืนการดำเนินให้กลับสู่ภาวะปกติ พร้อมมีแผนสำรองระหว่างรอเรียกคืนแผนหลัก

ปัญหาที่ 3 เครื่องคอมพิวเตอร์ไม่เพียงพอ บางหน่วยงานต้องใช้ระบบ Internet ในการปฏิบัติงาน

วิเคราะห์ปัญหา

1. งบประมาณจำกัด: หน่วยงานอาจไม่มีงบประมาณเพียงพอที่จะจัดซื้อเครื่องคอมพิวเตอร์ใหม่หรืออัปเกรดเครื่องเก่า
2. การขาดการวางแผน: หน่วยงานอาจไม่ได้วางแผนการจัดซื้อคอมพิวเตอร์ล่วงหน้า

3. ประสิทธิภาพการทำงานลดลงเครื่องคอมพิวเตอร์ที่เก่าอาจมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์

แนวทางการแก้ปัญหา

1. ศูนย์คอมฯควรจัดทำแผนการจัดซื้อคอมพิวเตอร์ล่วงหน้า โดยพิจารณาถึงจำนวนผู้ใช้งาน งบประมาณ และประเภทของงาน
2. จัดสรรงบประมาณ: หน่วยงานควรจัดสรรงบประมาณให้เพียงพอสำหรับการจัดซื้อคอมพิวเตอร์ใหม่หรืออัปเกรดเครื่องเก่า
3. มีแผนการบำรุงรักษาและอัพเดตโปรแกรมเครื่องเก่า

ปัญหาที่ 4 ไม่มีการสำรองข้อมูลเมื่อเกิดปัญหากรณีคอมพิวเตอร์ทำงานไม่ได้

วิเคราะห์ปัญหา

1. ไม่มีแผนสำรองเอกสารแบบ manual ไว้

แนวทางการแก้ไขปัญหา

1. มีการสำรองเอกสารแบบฟอร์มที่ต้องใช้ในการปฏิบัติงานของแต่ละหน่วยงาน
2. หน่วยงานมีการสำรองข้อมูลในระบบ on cloud หรือจัดทำสมุดประจำตัวผู้ป่วยเรื้อรัง

2. รายละเอียดแผน BCP

2.1 ผลกระทบ

- ไม่สามารถดูประวัติการรักษาผู้ป่วยย้อนหลังได้
- เพิ่มภาระในการการดูแลรักษาผู้ป่วย
- ผู้ป่วยได้รับการรักษาล่าช้าและไม่ครบถ้วน

2.2 กลยุทธ์

กลยุทธ์รับมือกับ Ransomware Attack

1. การป้องกัน

- **สำรองข้อมูล**: สำรองข้อมูลสำคัญอย่างสม่ำเสมอ โดยใช้ระบบสำรองข้อมูลแบบออฟไลน์ (Offline Backup)
- **อัปเดตซอฟต์แวร์**: อัปเดตซอฟต์แวร์และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
- **ติดตั้งโปรแกรมป้องกันไวรัส**: ติดตั้งโปรแกรมป้องกันไวรัสและไฟร์วอลล์ที่มีประสิทธิภาพ
- **ฝึกอบรมพนักงาน**: ฝึกอบรมพนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกัน Ransomware Attack
- **ใช้การยืนยันตัวตนแบบหลายชั้น**: ใช้การยืนยันตัวตนแบบหลายชั้น (MFA) เพื่อเพิ่มความปลอดภัย

2. การตรวจจับ

- **ใช้เครื่องมือตรวจจับ**: ใช้เครื่องมือตรวจจับ Ransomware เฉพาะทางอย่างสม่ำเสมอ

3. การตอบสนอง

- **แยกระบบที่ติดเชื้อ**: แยกระบบที่ติดเชื้อออกจากเครือข่าย

4. การฟื้นฟู

- **อัปเดตระบบ**: อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และโปรแกรมป้องกันไวรัส
- **เปลี่ยนรหัสผ่าน**: เปลี่ยนรหัสผ่านทุก3เดือน
- **ฝึกอบรมพนักงาน**: ฝึกอบรมพนักงานเกี่ยวกับวิธีการป้องกัน Ransomware Attack

วิธีการรักษางานบริการและลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร

1. มีการสำรองเอกสารแบบฟอร์มที่ต้องใช้ในการปฏิบัติงานของแต่ละหน่วยงาน
2. หน่วยงานมีการสำรองข้อมูลในระบบ on cloud หรือจัดทำสมุดประจำตัวผู้ป่วยเรื้อรัง

2.3 แผนปฏิบัติการ

เป้าหมาย	วัตถุประสงค์	กิจกรรม/ขั้นตอน	ผู้รับผิดชอบ	ระยะเวลา
เพื่อให้ระบบบริการสามารถดำเนินได้เมื่อเกิดปัญหา Ransomware attack	1. เพื่อให้เจ้าหน้าที่สามารถปฏิบัติงานได้อย่างต่อเนื่องเมื่อเกิด Ransomware attack 2. เพื่อให้ผู้ป่วยได้รับการรักษาที่ปลอดภัย และต่อเนื่อง	ระบุและแยกตัวเครื่องที่ติดเชื้อ	ทีม IT	ภายใน 1 ชั่วโมง
		สำรองข้อมูล	ผู้ใช้, ทีม IT	ภายใน 1 ชั่วโมง
		แจ้งหน่วยงานไอทีภายในองค์กร	ผู้ใช้	ภายใน 1 ชั่วโมง
		วิเคราะห์สายพันธุ์ของ ransomware	ทีม IT	ภายใน 1 ชั่วโมง
		กู้คืนระบบจากสำเนาสำรอง	ทีม IT	ภายใน 24 ชั่วโมง
		แจ้งหน่วยงานด้านความปลอดภัยทางไซเบอร์	ผู้บริหาร	ภายใน 24 ชั่วโมง
		หาวิธีแก้ไขเพิ่มเติม	ทีม IT	ภายใน 24 ชั่วโมง
		กู้คืนข้อมูล	ทีม IT	ภายใน 1 สัปดาห์
		ป้องกันการโจมตีในอนาคต	ทีม IT, ผู้ใช้	ภายใน 1 สัปดาห์
		แจ้งหน่วยงานบังคับใช้กฎหมาย	ผู้บริหาร	ภายใน 1 สัปดาห์

3. เอกสารแนบ

-

4. การอนุมัติ

หัวหน้าแผนก: _____

(นางสาววนิดา ฉัตรชมชื่น)
นายแพทย์ชำนาญการพิเศษ
หัวหน้ากลุ่มงานกมารเวชกรรม
วันที่ 6 มีนาคม 2567

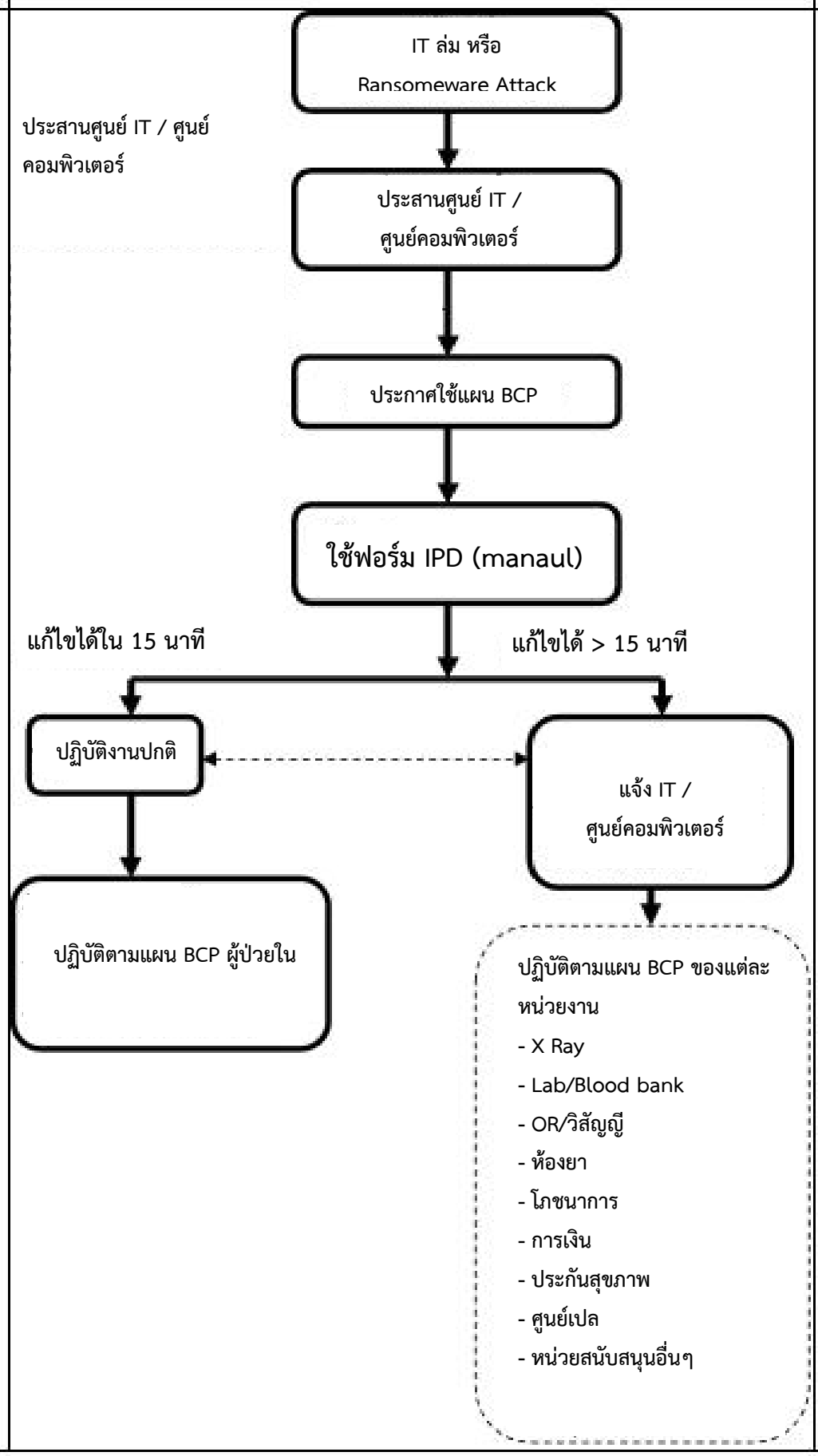
สรุปประเด็นที่ควรดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1. แจ้งศูนย์คอมให้รับทราบว่ามีปัญหาเกิดขึ้นที่หน่วยงาน	/		
2. ไม่ใช้คอมพิวเตอร์ระบบ Lan ร่วมกับ Internet	/		
3. ใช้เอกสารแบบ manual มาใช้ในการปฏิบัติงานแทนโปรแกรมที่ใช้ไม่ได้	/		
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุหน่วยงาน มีการจัดเตรียมเอกสาร แบบ manual ให้พร้อมใช้กรณีที่เกิดภาวะฉุกเฉินทาง cyber	/		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้ IT ควรมีหน่วยกลางเก็บเอกสารฟอร์ม manual ของทุกกลุ่มงานเป็นต้นฉบับ แยกไฟล์ไว้ต่างหากกับโปรแกรมที่ปริ้นท์จากคอมพิวเตอร์			/
การปฏิบัติหลังระบบกลับสู่ปกติ			
1. ทบทวนการใช้งานคอมพิวเตอร์ในการปฏิบัติงานอย่างสม่ำเสมอ	/	/	/
2. หัวหน้างาน /หัวหน้าหอ ควบคุมกำกับ นิเทศติดตาม การใช้งานคอมพิวเตอร์ของผู้ปฏิบัติงาน	/	/	/
3. มีการสื่อสารนโยบายลงสู่ผู้ปฏิบัติ 100%	/	/	/

U =ดำเนินการได้เองระดับหน่วยงาน, S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน, I = ต้องได้รับการสนับสนุนจาก IT

Flow Chart กรณีเกิดปัญหา IT ล้ม หรือ Ransomware Attack

กลุ่มงานกุมารเวชกรรม โรงพยาบาลอุดรธานี

ผู้รับผิดชอบ	กิจกรรม	วิธีปฏิบัติ
IT / ศูนย์คอมพิวเตอร์ **ในเวลา** แจ้งหัวหน้ากลุ่มงาน **นอกเวลา** แจ้งพยาบาลตรวจการ/เวรบริหาร		ประชาสัมพันธ์แจ้งผู้ป่วยและญาติ ระบบคอมพิวเตอร์ขัดข้องอาจทำให้การบริการล่าช้า IT/ ศูนย์คอมพิวเตอร์ โทร. 1125 ใช้แบบฟอร์ม IPD manual ได้แก่ 1. เอกสารชุดรับใหม่ 2. ใบเบิกอาหาร 3. ใบตามผลแล็บ /เลือด/ x - ray 4. ใบ MAR 5. ใบสั่งยา 6. เอกสารตรวจสอบสิทธิ์ 7. ใบส่งผู้ป่วยผ่าตัด 8. ใบเบิกพัสดุ 9. ใบสื่อสารหน่วยงานที่เกี่ยวข้อง