

แผน Business Continuity Plan (BCP) กลุ่มงานสุขศึกษา โรงพยาบาลอุดรธานี

เหตุการณ์: โดน ransomware attack ส่งผลให้ระบบบริการไม่สามารถดำเนินได้

วันที่: 30 สิงหาคม 2567

แผนก: สุขศึกษา

ผู้รับผิดชอบ: น.ส.จิราวรรณ สีสภาพพัฒนาพาณิชย์, น.ส.เพ็ญภักดี พวงมาลา และ น.ส.สุพาภรณ์ คนองเดช

1. บทนำ

กลุ่มงานสุขศึกษา ได้จัดทำแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) เพื่อใช้ในกรณีที่เกิดวิกฤติ ransomware attack เข้าโจมตีเมื่อวันที่ 9 ธันวาคม 2566 หรือเหตุการณ์ฉุกเฉินต่างๆ ที่อาจจะเกิดขึ้นในอนาคต จากระบบเซิร์ฟเวอร์ ระบบเน็ตเวิร์คขัดข้อง ระบบล่มจากไวรัสคอมพิวเตอร์ เพื่อให้กลุ่มงานสามารถนำไปใช้เพื่อตอบสนองการปฏิบัติงานภายใต้ภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ได้ทันท่วงที โดยสถานการณ์ฉุกเฉินที่เกิดขึ้นไม่ส่งผลกระทบต่อการใช้บริการผู้ป่วย เพื่อสร้างความมั่นใจให้กับผู้ป่วยและลดผลกระทบที่อาจเกิดขึ้นกับโรงพยาบาลผู้ป่วย และทำให้กระบวนการสำคัญขององค์กร(Critical Business Process) สามารถกลับมาดำเนินงานได้อย่างปกติโดยใช้เวลาน้อยที่สุดในกานฟื้นฟู ซึ่งจะช่วยลดระดับความรุนแรงของผลกระทบที่จะเกิดขึ้นกับองค์กร ดังนั้น กลุ่มงานจึงได้วิเคราะห์ถึงปัญหาและอุปสรรคในการให้บริการผู้ป่วย

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

ปัญหา

- ระบุทเรียนปัญหาจากเหตุการณ์ ransomware attack: ปัญหา คือ การให้บริการคลินิก DPAC ไม่สามารถดูประวัติการรักษาย้อนหลังได้
- วิเคราะห์สาเหตุของปัญหา:
 - 1.เครื่องคอมพิวเตอร์ในกลุ่มงานสุขศึกษา เป็นเครื่องที่อายุการใช้งานนาน
 - 2.ระบบปฏิบัติการเป็นเวอร์ชันเก่า
 - 3.โปรแกรมป้องกัน มัลแวร์(Anti-malware) ที่ไม่อัปเดต
 - 4.ขาดความระมัดระวังการดาวน์โหลดไฟล์จากอินเทอร์เน็ต
- ระบุแนวทางการแก้ไขปัญหา: คือ
 - 1.สำรองข้อมูลผู้มารับบริการและผู้ป่วยไว้ในรูปแบบกระดาษ (opd card)
 - 2.ใช้ Notebook ปฏิบัติงานแทนคอมพิวเตอร์
 - 3.จัดทำแฟ้มทะเบียนประวัติผู้ป่วย
 - 4.สำรองข้อมูลเก็บไว้ในฐานข้อมูลอื่นๆ

อุปสรรค

- ระบุอุปสรรคที่เกิดขึ้นในการรับมือกับ ransomware attack: คือ
 - 1.เกิดความล่าช้าในการหาเอกสาร (opd card) ของผู้มารับบริการและผู้ป่วย
 - 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.การออกแบบสื่อสุขภาพ เผยแพร่ประชาสัมพันธ์ ข้อมูลข่าวสารด้านสุขภาพ ของกลุ่มงานหยุดชะงัก
 - 2.การให้บริการคลินิก DPAC ไม่สามารถดูประวัติการรักษาย้อนหลังได้
- ระบุผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
 - 1.ประวัติการรักษาเดิมของผู้ป่วยหายจากระบบ
 - 2.ตรวจสอบจำนวนการนัดผู้ป่วยไม่ได้
 - 3.การให้บริการล่าช้า เนื่องจากไม่สามารถดูประวัติการรักษาเดิมได้
 - 4.เวลาในการให้บริการผู้ป่วยแต่ละรายเพิ่มมากขึ้น

2.2 กลยุทธ์

- ระบุกลยุทธ์ที่จะใช้ในการรับมือกับ ransomware attack
 - 1.แจ้งเจ้าหน้าที่ศูนย์คอมพิวเตอร์ ให้ทราบเหตุการณ์เกิดขึ้น
 - 2.แจ้งบุคลากรในกลุ่มงานสุขศึกษา รับทราบเหตุการณ์
 - 3.ปฏิบัติตามแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของกลุ่มงานสุขศึกษา
- ระบุวิธีการที่จะรักษางานบริการที่จำเป็น
 - 1.แจ้งผู้มารับบริการเกี่ยวกับปัญหาด้านระบบคอมพิวเตอร์ให้เข้าใจ
 - 2.เตรียมใบ OPD card ไว้สำหรับเขียนและบันทึกการซักประวัติ ตรวจร่างกาย
 - 3.บันทึกผลการให้บริการในคลินิก DPAC และคำแนะนำต่างลงใน OPD card และใบสั่งยา
 - 4.ลงค่าใช้จ่ายทุกรายการในใบสั่งยาแล้วนำไปคืนที่ห้องการเงิน
 - 5.กรณีมีการนัดหมายให้ออกใบนัดแก่ผู้มารับบริการ(แบบกระดาษและในlineOA)และลงข้อมูลย้อนหลัง
 - 6.หลังจากระบบใช้งานได้ปกติให้ลงข้อมูลการซักประวัติ ตรวจร่างกาย การวินิจฉัย คำแนะนำการดูแล สุขภาพ ค่าบริการทุกอย่าง ของผู้ป่วย และสแกนเอกสารทุกอย่างเข้าในระบบเพื่อเป็นหลักฐานอ้างอิง
- ระบุวิธีการที่จะลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากร
 - 1.อธิบายผู้ป่วยเกี่ยวกับปัญหาด้านระบบคอมพิวเตอร์ให้เข้าใจ
 - 2.ให้บริการผู้ป่วยที่มาตรงนัดและผิคนัด
 - 3.โทรศัพท์ประสานผู้ป่วยก่อนวันนัดหมายและแจ้งรายละเอียดเกี่ยวกับเอกสารที่ต้องนำติดตัวมาเมื่อมารับบริการที่โรงพยาบาลตามนัด

2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับ ransomware attack
- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน
- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน

ข้อมูล/ผู้รับผิดชอบ	วันที่	รอ
1.ถอดสายตัวเชื่อมระบบ (น.ส.เพ็ญกัณฑ์ พวงมาลา)	/	
	(5 นาที)	
2.สำรองข้อมูล (น.ส.เพ็ญกัณฑ์ พวงมาลา, น.ส.นลิสสา ลาเสือ)	/	
	(1 ชม.)	
3.ประสานเจ้าหน้าที่ศูนย์คอมพิวเตอร์ทำการ update antivirus คอมพิวเตอร์ในหน่วยงาน (น.ส.จิราวรรณ ถีลาพัฒนาพาณิชย์, น.ส.สุพาภรณ์ คนองเดช)	/	
	(5 นาที)	
4.ประสานเจ้าหน้าที่ศูนย์คอมพิวเตอร์ทำการ update windows คอมพิวเตอร์ในหน่วยงาน (น.ส.จิราวรรณ ถีลาพัฒนาพาณิชย์, น.ส.สุพาภรณ์ คนองเดช)	/	
	(5 นาที)	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	หมายเหตุ
1.แจ้งหัวหน้ากลุ่มงานสุขศึกษาให้รับทราบ	เจ้าหน้าที่พบเห็นเหตุการณ์	-มีการซ้อมแผน อย่างน้อยเดือน ละ 1 ครั้ง
2.ประเมิน		
3.ทบทวนกระบวนการงาน		
4.รายงานผู้บริหาร		
5.ประสานศูนย์คอม		
6.สรุปผลการดำเนินงานแก้ไขสถานการณ์		
7.รายงานผลการ		

2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP คือ
 - 1.เจ้าหน้าที่กลุ่มงานสุขศึกษา
 - 2.เจ้าหน้าที่ศูนย์คอมพิวเตอร์
 - 3.เครื่องคอมพิวเตอร์
- ระบุแหล่งที่มาของทรัพยากร คือ
 - 1.กลุ่มงานสุขศึกษา โรงพยาบาลอุดรธานี
 - 2.ศูนย์คอมพิวเตอร์ โรงพยาบาลอุดรธานี

2.5 การทดสอบและฝึกอบรม

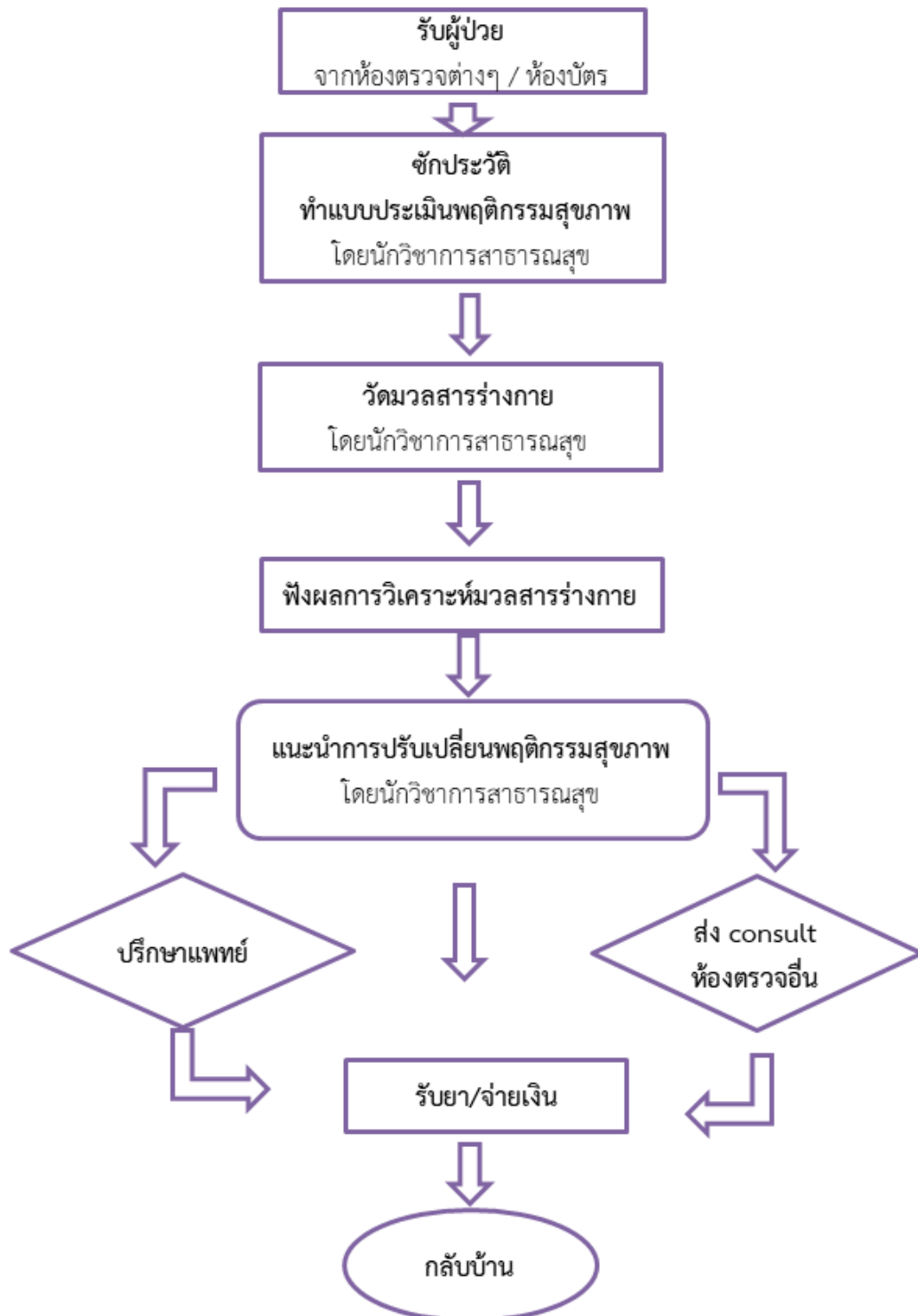
- ระบุวิธีการทดสอบแผน BCP
 - 1.แจ้งแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของกลุ่มงานสุขศึกษา ให้กับเจ้าหน้าที่ทุกคนทราบ
 - 2.ติด flow chart ให้เจ้าหน้าที่ในกลุ่มงานสุขศึกษาชัดเจน
 - 3.แจ้งแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของกลุ่มงานสุขศึกษา รับทราบเมื่อมีเจ้าหน้าที่ใหม่
 - 4.ซ้อมแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของกลุ่มงานสุขศึกษา ไตรมาสละ 1 ครั้ง
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

1. ตรวจสอบ firewall ได้เปิดอยู่ทุกครั้งที่ใช้งานคอมพิวเตอร์
2. สอนการใช้งานโปรแกรม scan virus แก่เจ้าหน้าที่ทุกคนในกลุ่มงาน
3. ซ้อมแผนบริหารความต่อเนื่อง Business Continuity Plan (BCP)

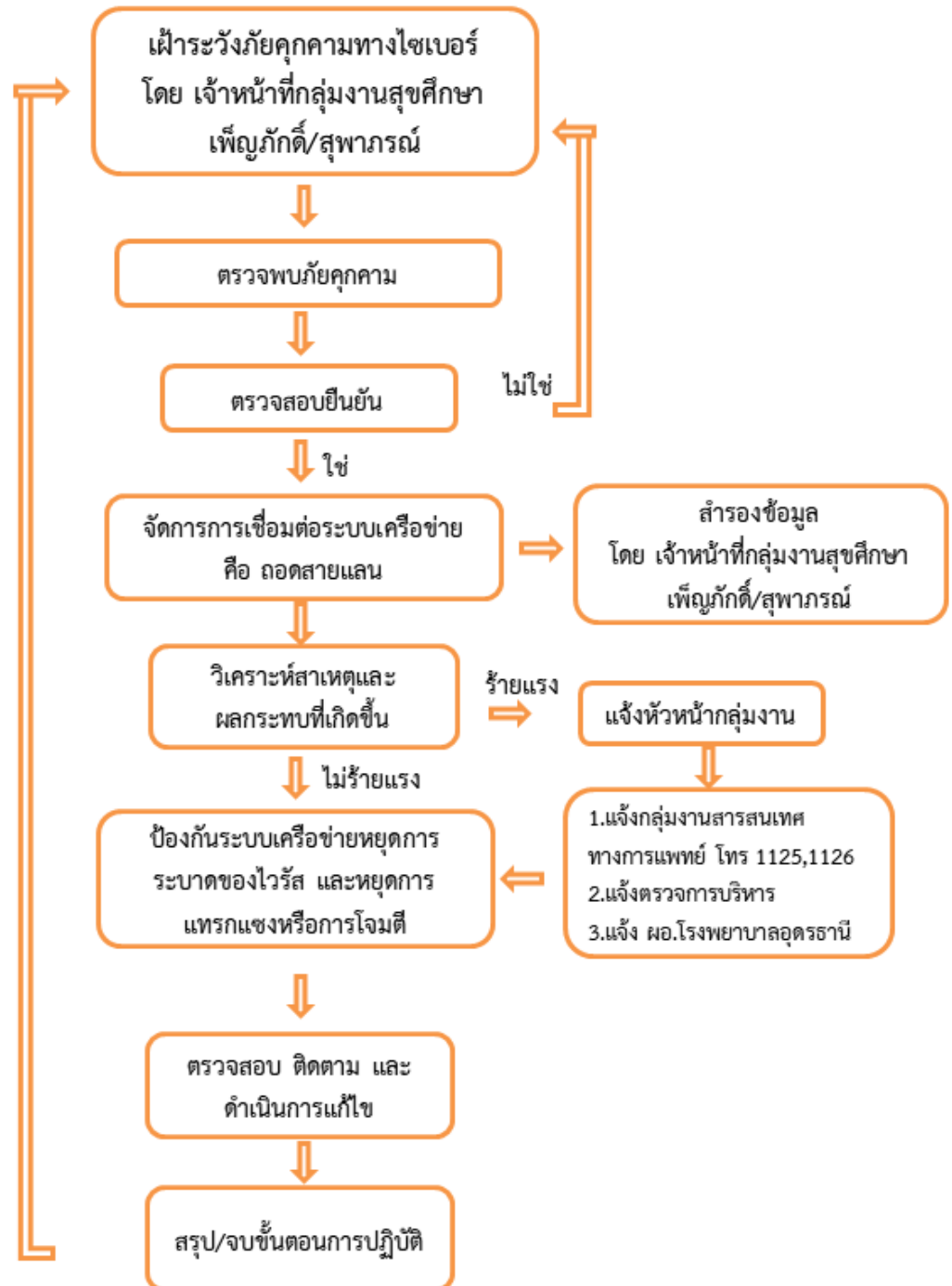
3. เอกสารแนบ

- แผนงาน flow chart ต่างๆ

แผนการดำเนินงานกลุ่มงานสุขศึกษา เมื่อระบบคอมพิวเตอร์ใช้งานไม่ได้ โดยใช้ระบบ MANUAL



แผนบริหารความต่อเนื่อง
(Business Continuity Plan : BCP) ของกลุ่มงานสุขศึกษา



4. การอนุมัติ

หัวหน้าแผนก: น.ส.จิราวรรณ ลีลาพัฒนาพาณิชย์

วันที่: 30 สิงหาคม 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)ที่นำเชื่อถือและอัปเดตเสมอ เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ที่ดาวน์โหลด			✓
3.ไม่เข้าใช้งานเว็บไซต์ที่ไม่เกี่ยวข้องกับการทำงาน	✓		
4.ระมัดระวังการเปิดอ่านไฟล์จาก E-mail ที่ไม่ทราบแหล่งที่มา	✓		
5.ระมัดระวังในการดาวน์โหลดไฟล์จากอินเทอร์เน็ต	✓		
6.หลีกเลี่ยงการใช้แชร์ไฟล์โดยไม่จำเป็น	✓		
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	✓		
การปฏิบัติหลังระบบกลับสู่ปกติ			

1.Format เครื่องคอมพิวเตอร์ใหม่ทั้งหมด			✓
2.กู้ข้อมูลจากฐานข้อมูลมาใช้งาน			✓
3.ตรวจสอบ firewall ได้เปิดอยู่ทุกครั้งที่ใช้งานคอมพิวเตอร์	✓		
4.ลงข้อมูลการให้บริการผู้ป่วยย้อนหลังในระบบและสแกนเอกสารเข้าระบบเพื่อเก็บไว้เป็นเอกสารอ้างอิง	✓		
5.อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ			✓

U =ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT