แผนบริหารความต่อเนื่อง (Business Continuity Plan : BCP)
ด้านเทคโนโลยีสารสนเทศ หน่วยงาน งานกฎหมาย กลุ่มงานบริหารทั่วไป โรงพยาบาลอุดรธานี

แผนบริหารความต่อเนื่อง (BCP) ด้านเทคโนโลยีสารสนเทศของงานกฎหมาย จัดทำขึ้นเพื่อให้บุคคลากรของงานกฎหมายสามารถนำไปใช้ตอบสนองและปฏิบัติงานในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน โดยไม่ให้สภาวะวิกฤตหรือเหตุการณ์ดังกล่าวส่งผลให้หน่วยงานต้องหยุดการดำเนินงาน

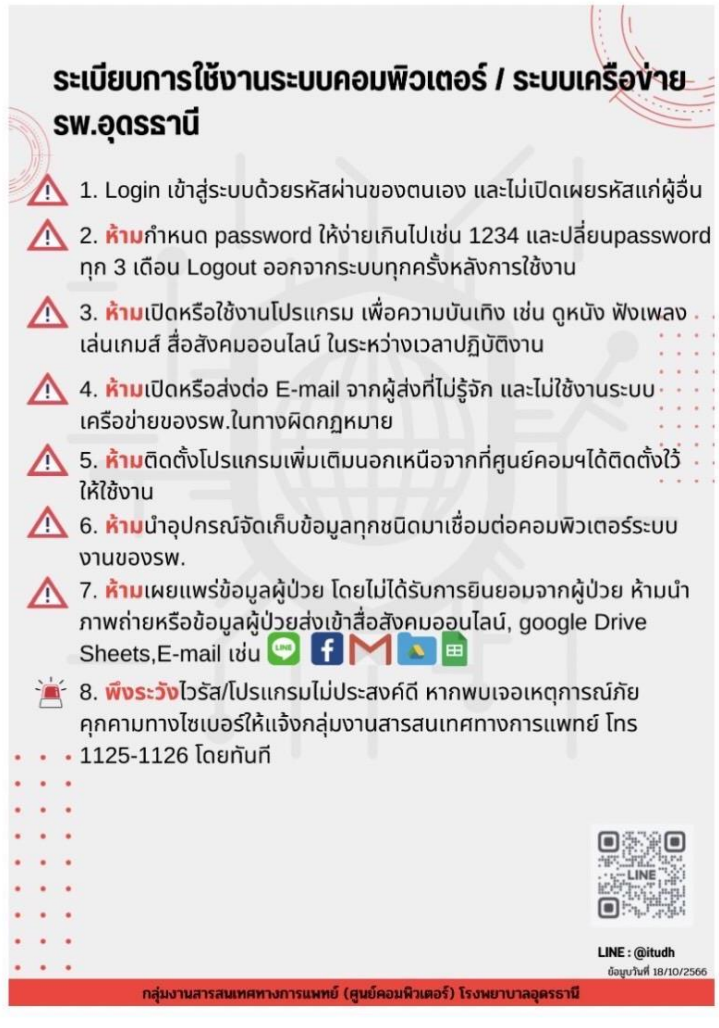
ผู้รับผิดชอบ :

1. นายวัชระ ชื่นชมน้อย เจ้าพนักงานวิทยาศาสตร์การแพทย์ชำนาญงานปฏิบัติหน้าที่หัวหน้างานกฎหมาย
2. นายถาวร มณีโรจน์ เจ้าพนักงานสถิติชำนาญงานปฏิบัติหน้าที่นิติกร
3. นายวุฒิเดช นิราสคำ นิติกรชำนาญการ
4. นายอธิป แก้วคูณเมือง นิติกร
5. นายพงศ์ศิริ สันติภาษิต นิติกร
6. นางสาวศศิโสภา รัศมิทัศ นิติกร
7. นางสาวสิริภา ค้าขาย นิติกร
8. นางสาววิไล จันนาวัน เจ้าพนักงานธุรการ

เบอร์โทรศัพท์ภายใน 3612

งานกฎหมายมีคอมพิวเตอร์สำหรับใช้ปฏิบัติงานจำนวน 9 เครื่อง ซึ่งเป็นระบบปฏิบัติการแบบเดี่ยว (Stand – alone OS) ไม่มีการเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องอื่นและไม่ได้มีการเชื่อมต่อระบบเครือข่ายของโรงพยาบาล (ระบบ LAN) แต่จะมีการเชื่อมต่อกับระบบอินเตอร์เน็ตผ่านเครือข่ายไร้สาย Wi-Fi ของโรงพยาบาล

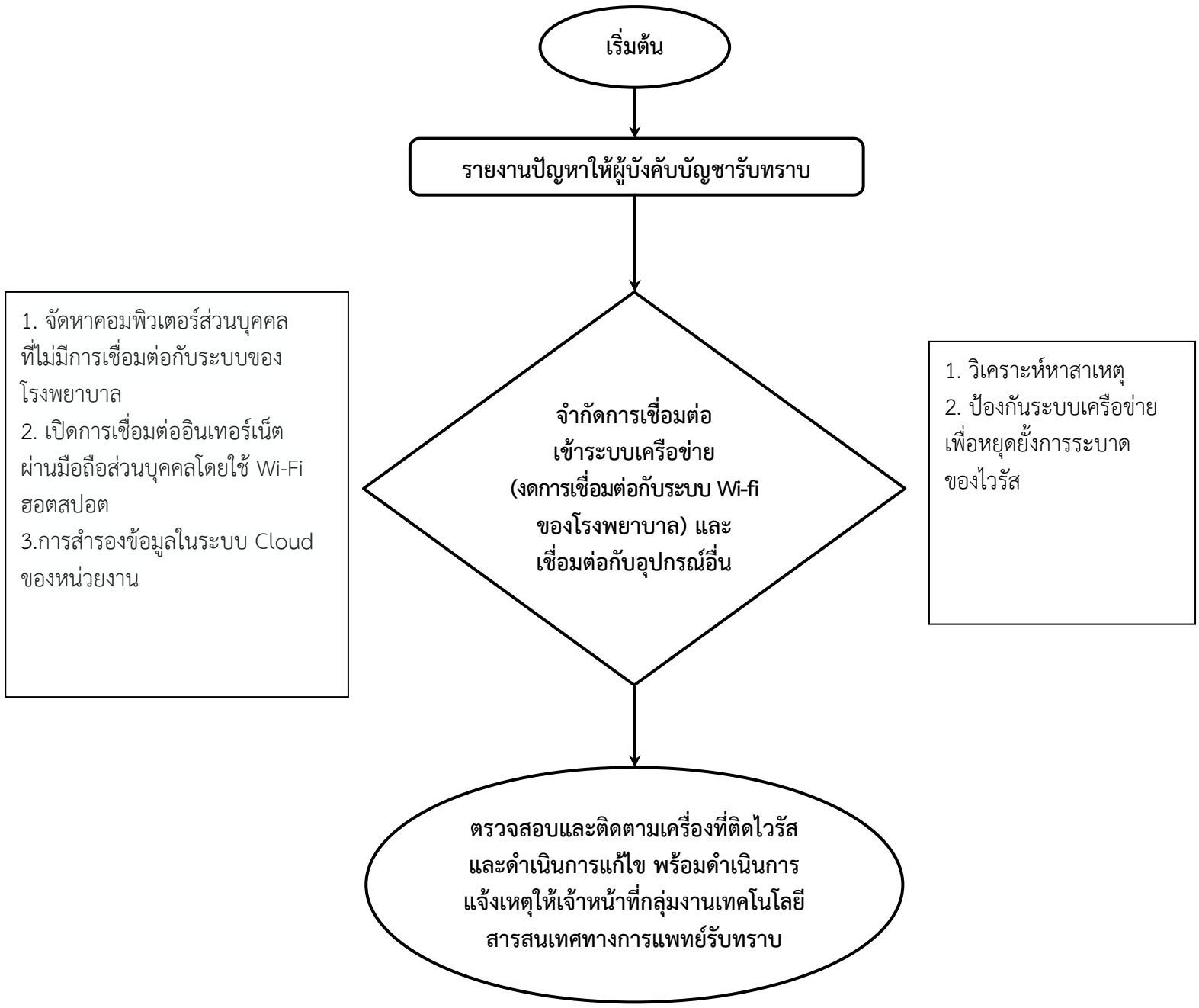
ระเบียบการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายโรงพยาบาลอดรธานี



1. เหตุการณ์: กรณีการป้องกันไวรัสล้มเหลว โดยถูกไวรัสหรือมีผู้บุกรุกให้ดำเนินการ ดังนี้

- รายงานเหตุให้ผู้บังคับบัญชาทราบ และให้จำกัดการเชื่อมต่อคอมพิวเตอร์เครื่องที่ติดไวรัสเข้ากับระบบเครือข่าย และห้ามนำอุปกรณ์อื่นใด เช่น USB Drive, External Harddisk เป็นต้น มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ดังกล่าวแล้วนำไปเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น
- แจ้งให้กลุ่มงานเทคโนโลยีสารสนเทศทราบถึงปัญหาเพื่อดำเนินการแก้ไข
- วิเคราะห์หาสาเหตุและป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องคอมพิวเตอร์ที่ติดไวรัสและดำเนินการแก้ไข
- ระหว่างรอการแก้ไขจากกลุ่มงานเทคโนโลยีสารสนเทศ จัดหาคอมพิวเตอร์ส่วนบุคคลที่ไม่มีการเชื่อมต่อกับระบบของโรงพยาบาล

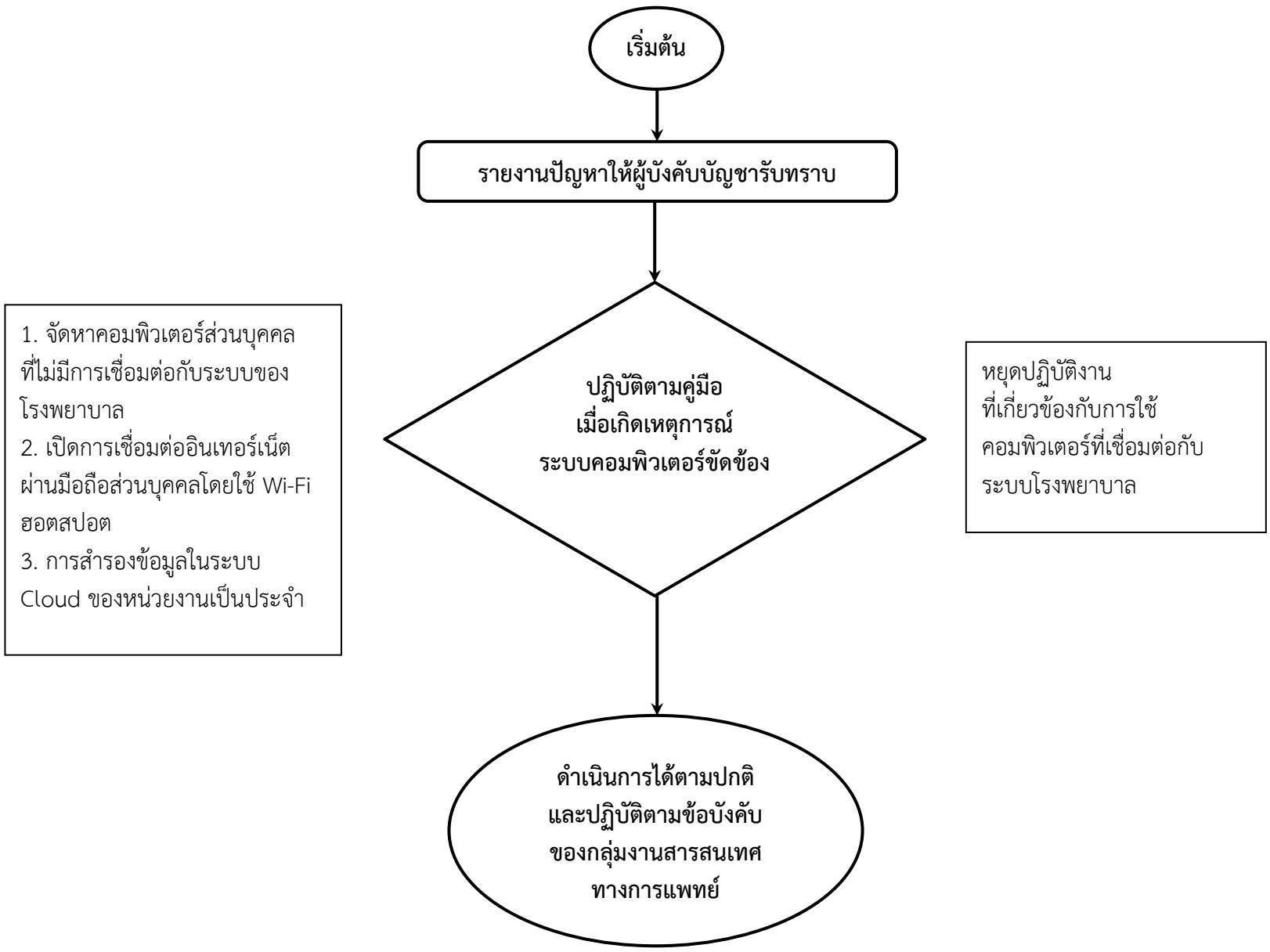
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



2. เหตุการณ์ : กรณีระบบคอมพิวเตอร์ขัดข้อง ให้ดำเนินการ ดังนี้

- รายงานปัญหาให้ผู้บังคับบัญชารับทราบ
- จัดหาคอมพิวเตอร์ส่วนบุคคลมาใช้ไปพลางก่อน และเปิดการเชื่อมต่ออินเทอร์เน็ตผ่านมือถือส่วนบุคคลโดยใช้ Wi-Fi ฮอตสปอต
- ให้สำรองข้อมูลในระบบ Cloud ของหน่วยงาน เช่น Google Drive, OneDrive, iCloud หรือ Dropbox เป็นประจำ

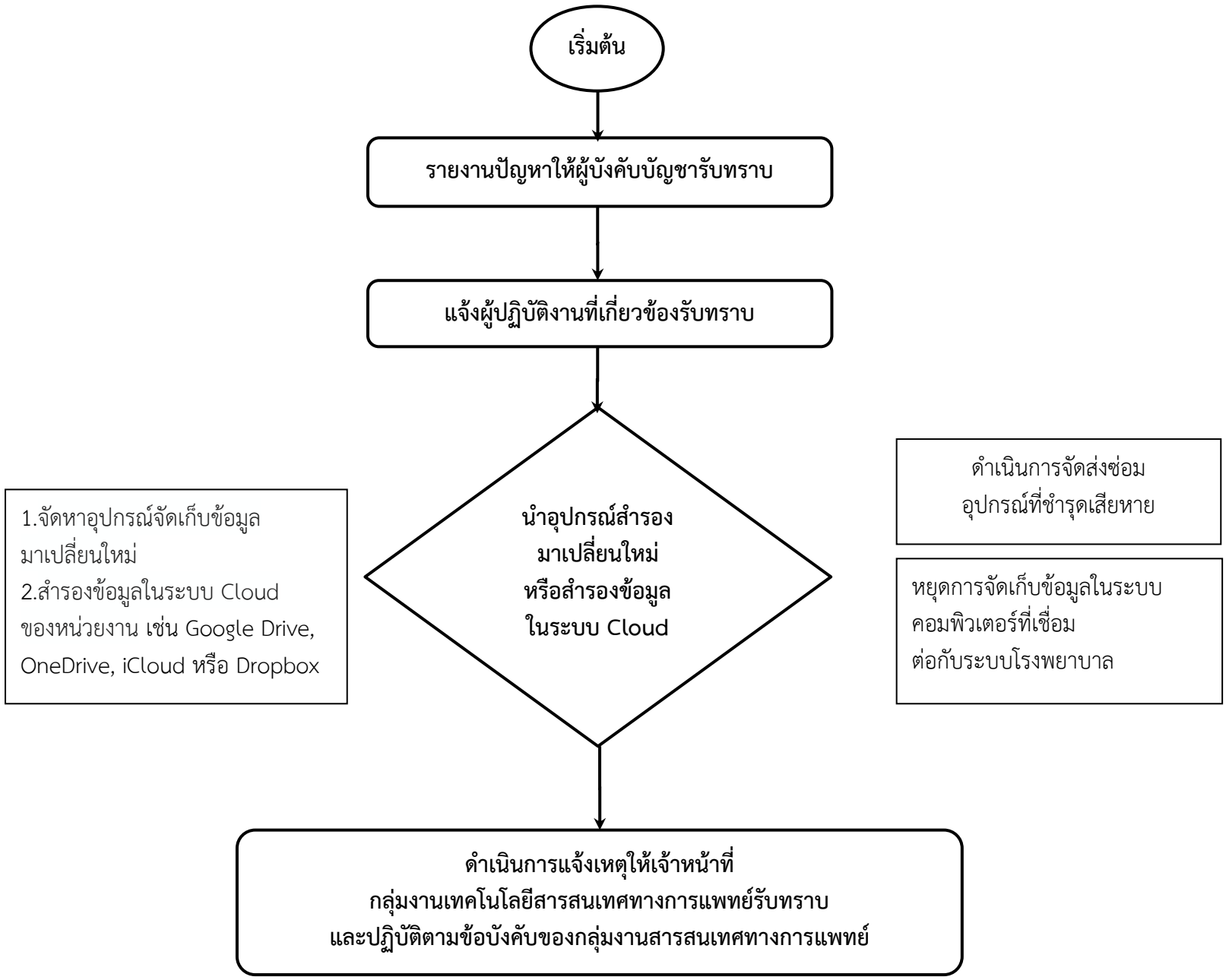
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีระบบคอมพิวเตอร์ขัดข้อง



3. เหตุการณ์ : กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้ดำเนินการ ดังนี้

- รายงานปัญหาให้ผู้บังคับบัญชารับทราบ
- แจ้งผู้ปฏิบัติงานที่เกี่ยวข้อง และหยุดการจัดเก็บข้อมูลในระบบคอมพิวเตอร์ที่เชื่อมต่อกับระบบโรงพยาบาล
- ดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ หรือสำรองข้อมูลในระบบ Cloud ของหน่วยงาน เช่น Google Drive, OneDrive, iCloud หรือ Dropbox
- ดำเนินการแจ้งเหตุ ให้เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์รับทราบและปฏิบัติตามข้อบังคับของกลุ่มงานสารสนเทศทางการแพทย์

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



แผน BCP

ขั้นตอนที่ 1 : การป้องกัน

1) ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่อัปเดตล่าสุด

2) ใช้ Firewall เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

3) อัปเดตระบบปฏิบัติการและซอฟต์แวร์เป็นประจำ

4) ให้การฝึกอบรมด้านความปลอดภัยแก่เจ้าหน้าที่ พนักงานทุกระดับ

5) สำรองข้อมูลอย่างสม่ำเสมอ

ขั้นตอนที่ 2 : การตรวจจับ

1) ใช้ระบบตรวจจับการบุกรุก (IDS) เพื่อตรวจจับกิจกรรมที่น่าสงสัย

2) ตรวจสอบล็อกระบบเป็นประจำเพื่อหาสัญญาณของการโจมตี

3) ติดตามข่าวสารเกี่ยวกับภัยคุกคามด้านความปลอดภัยล่าสุด

ขั้นตอนที่ 3 : การตอบโต้

1) แยกอุปกรณ์ที่ติดไวรัสออกจากเครือข่าย

2) แจ้งหน่วยงานบังคับใช้กฎหมาย

3) ติดต่อผู้เชี่ยวชาญด้านความปลอดภัยเพื่อขอความช่วยเหลือ

4) กู้คืนข้อมูลจากการสำรองข้อมูล

ขั้นตอนที่ 4 : การฟื้นฟู

1) ติดตั้งระบบปฏิบัติการใหม่และซอฟต์แวร์ที่อัปเดตล่าสุด

2) กู้คืนข้อมูลจากการสำรองข้อมูล

3) ตรวจสอบระบบเพื่อหาช่องโหว่ด้านความปลอดภัย

4) ปรับปรุงแผน BCP เพื่อป้องกันการโจมตีในอนาคต

ขั้นตอนที่ 5 : การเรียนรู้

1) วิเคราะห์การโจมตีเพื่อระบุช่องโหว่ด้านความปลอดภัย

2) ปรับปรุงแผน BCP และมาตรการป้องกันตามความจำเป็น

3) แบ่งปันข้อมูลเกี่ยวกับการโจมตีกับองค์กรอื่นๆ

สิ่งที่ต้องการเพิ่มเติม

1) ใช้การรับรองความถูกต้องแบบหลายปัจจัย (MFA)

2) จำกัดสิทธิ์การเข้าถึงข้อมูลและระบบ

3) สร้างแผนการสื่อสารสำหรับกรณีฉุกเฉิน

4) ทดสอบแผน BCP เป็นประจำ

1. แผนการควบคุม ป้องกันการเข้าถึงและการใช้งานระบบสารสนเทศ

ขั้นตอนการดำเนินงาน	ผู้รับผิดชอบ	ความเสี่ยง	จุดควบคุม	ระยะเวลา
กำหนดช่องทางการเข้าถึงข้อมูลและระบบเครือข่าย	- เจ้าหน้าที่ผู้รับผิดชอบงานสารสนเทศและตรวจสอบระบบภายในหน่วยงาน (IT ประจำหน่วยงาน), ประสานงาน IT	ผู้บุกรุก,ไวรัสคอมพิวเตอร์และระบบอินเทอร์เน็ตใช้งานไม่ได้	ตรวจสอบระบบข้อมูลและเครือข่ายให้สามารถใช้งานได้ปกติ	เมื่อมีระบบใหม่/ทุกวัน
ภายในหน่วยงาน (Lan, Wi-fi บลูทูธ) ภายนอกหน่วยงาน (Firewall, IP)	- เจ้าหน้าที่ที่อยู่เวรหรือประจำเครื่องที่เปิดทำงาน	ไม่สามารถเข้าถึงและใช้งานระบบอินเทอร์เน็ต, เว็บไซต์ และระบบงานได้	ตรวจสอบการเข้าถึงอินเทอร์เน็ต เว็บไซต์และระบบงาน	ทุกวัน
Login Authentication Firewall	- เจ้าหน้าที่ที่อยู่เวรหรือประจำเครื่องที่เปิดทำงาน	การใช้งานที่ผิดปกติ ผิดระบบ ผิดแนวปฏิบัติ	ตรวจสอบการใช้งานที่ผิดปกติ/ไม่ถูกต้อง	ทุกวัน
จัดเก็บข้อมูลผู้เข้าถึงและใช้งาน	- เจ้าหน้าที่ที่อยู่เวรหรือประจำเครื่องที่เปิดทำงาน - ผู้รับผิดชอบงาน IT จัดเก็บข้อมูลทุกวัน	ไม่สามารถบันทึกข้อมูลใน Storage	ตรวจสอบระบบจัดเก็บข้อมูลผู้ใช้งาน	ทุกวัน

2. การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

ขั้นตอนการดำเนินงาน	ผู้รับผิดชอบ	ความเสี่ยง	จุดควบคุม	ระยะเวลา
กำหนดข้อมูลสำคัญที่ต้องรักษาความปลอดภัยและสำรองข้อมูล	- ผู้รับผิดชอบงาน ITของแต่ละหน่วยงานหรือผู้ที่รับมอบหมาย	ข้อมูลติดไวรัส ข้อมูลสูญหาย	ตรวจสอบไวรัสก่อนสำรองข้อมูล	ปีละครั้ง/เมื่อมีระบบใหม่
ติดตั้งโปรแกรมป้องกันไวรัสและตรวจสอบความผิดปกติ	- ผู้รับผิดชอบงาน ITของแต่ละหน่วยงานหรือผู้ที่รับมอบหมาย	ผู้บุกรุก,ไวรัสคอมพิวเตอร์	Update โปรแกรมป้องกันไวรัส	ทุกเดือน/ ตามเวลาที่กำหนด
สำรองข้อมูลที่สำคัญใน Storage/ Cloud	- ผู้รับผิดชอบงาน ITของแต่ละหน่วยงานหรือผู้ที่รับมอบหมาย	สำรองข้อมูลไม่ครบถ้วนไม่ตามเวลาที่กำหนด	ตรวจสอบการสำรองข้อมูลให้ครบถ้วนตามเวลาที่กำหนด	ทุกเดือน/ ตามเวลาที่กำหนด
ตรวจสอบปัญหา	- ผู้รับผิดชอบงาน ITของแต่ละหน่วยงานหรือผู้ที่รับมอบหมาย - เจ้าหน้าที่ที่อยู่เวรหรือประจำเครื่องที่เปิดทำงาน	ผู้บุกรุก, ไวรัสคอมพิวเตอร์	ตรวจสอบอย่างสม่ำเสมอ	ทุกเดือน/ตามเวลาที่กำหนด
แก้ไขและกู้คืนข้อมูล	- ผู้รับผิดชอบงาน ITของแต่ละหน่วยงานหรือผู้ที่รับมอบหมาย	ไม่สามารถบันทึกข้อมูลใน Storage/Cloud ได้	ตรวจสอบอุปกรณ์และระบบอินเทอร์เน็ต	ทุกเดือน/ ตามเวลาที่กำหนด

2.4 ทรัพยากร ***ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP**

1) บุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ
2) อุปกรณ์คอมพิวเตอร์และระบบเครือข่ายที่ทันสมัย
3) ระบบโปรแกรมป้องกัน Spyware, Malwares ที่เหมาะสมให้กับทุกหน่วยงานทุกเครื่อง
4) งบประมาณในการดูแลระบบสารสนเทศ การบำรุงรักษา

แผนงาน

แผนระยะ	กิจกรรม	ผู้รับผิดชอบ	ระยะเวลา/มาตรการ	หมายเหตุ
ขั้นตอนที่ 1: การป้องกัน	1.ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่อัปเดตล่าสุด 2.ใช้ Firewall เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต 3.อัปเดตระบบปฏิบัติการและซอฟต์แวร์เป็นประจำ 4.ให้การฝึกอบรมด้านความปลอดภัยแก่พนักงาน 5.สำรองข้อมูลอย่างสม่ำเสมอ	ผู้รับผิดชอบงาน IT ของแต่ละหน่วยงาน หรือผู้ที่รับมอบหมาย	เมื่อมีเครื่องตรวจสอบและอัปเดตทุกสัปดาห์	โปรแกรมลิขสิทธิ์ต่ออายุเสมอตามข้อกำหนด -ใช้การรับรองความถูกต้องแบบหลาย ปัจจัย (MFA) -จำกัดสิทธิ์การเข้าถึงข้อมูลและระบบ -สร้างแผนการสื่อสารสำหรับกรณีฉุกเฉิน -ทดสอบแผน BCP เป็นประจำ
ขั้นตอนที่ 2: การตรวจจับ	1.ใช้ระบบตรวจจับการบุกรุก (IDS) เพื่อตรวจจับกิจกรรมที่น่า สงสัย 2.ตรวจสอบล็อกระบบเป็นประจำเพื่อหาสัญญาณของการโจมตี 3.ติดตามข่าวสารเกี่ยวกับภัยคุกคามด้านความปลอดภัยล่าสุด	ผู้รับผิดชอบงาน IT ของแต่ละหน่วยงาน หรือผู้ที่รับมอบหมาย	ทบทวนตรวจสแกนทุกสัปดาห์	
ขั้นตอนที่ 3: การตอบโต้	1.แยกอุปกรณ์ที่ติดไวรัสออกจากเครือข่าย 2.แจ้งหน่วยงานบังคับใช้กฎหมาย 3.ติดต่อผู้เชี่ยวชาญด้านความปลอดภัยเพื่อขอความช่วยเหลือ 4.กู้คืนข้อมูลจากการสำรองข้อมูล	ผู้รับผิดชอบงาน IT ของแต่ละหน่วยงาน หรือผู้ที่รับมอบหมาย	1.แยกอุปกรณ์ที่ติดไวรัสออกจากเครือข่ายทันที 2.แจ้งผู้ใช้ทั้งหมดให้ทราบถึงการโจมตีและให้หยุดใช้ระบบที่ได้รับผลกระทบ 3.ติดต่อทีมไอทีและหน่วยงานบังคับใช้กฎหมาย	
ขั้นตอนที่ 4: การฟื้นฟู	1.ติดตั้งระบบปฏิบัติการใหม่และซอฟต์แวร์ที่อัปเดตล่าสุด 2.กู้คืนข้อมูลจากการสำรองข้อมูล 3.ตรวจสอบระบบเพื่อหาช่องโหว่ด้านความปลอดภัย 4.ปรับปรุงแผน BCP เพื่อป้องกันการโจมตีในอนาคต	ผู้รับผิดชอบงาน IT ของแต่ละหน่วยงาน หรือผู้ที่รับมอบหมาย	หลังระบบได้รับการดูแลทำต่อเนื่องทันที	
ขั้นตอนที่ 5: การเรียนรู้	1.วิเคราะห์การโจมตีเพื่อระบุช่องโหว่ด้านความปลอดภัย 2.ปรับปรุงแผน BCP และมาตรการป้องกันตามความจำเป็น 3.แบ่งปันข้อมูลเกี่ยวกับการโจมตีกับองค์กรอื่น	ผู้รับผิดชอบงาน IT ของแต่ละหน่วยงาน หรือผู้ที่รับมอบหมาย	เรียนรู้ตลอดเพราะมีการพัฒนาต่อเนื่องเสมอในระบบสาร สนเทศ	

สรุปแผนดำเนินการ

สรุปประเด็นที่ควรดำเนินการ	U (/)	S (/)	I (/)
การป้องกัน			
1. ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่อัปเดตล่าสุด และเปิด Firewall ประจำ	/	/	/
2. อัปเดตระบบปฏิบัติการและซอฟต์แวร์เป็นประจำ	/		
3. สำรองข้อมูลอย่างสม่ำเสมอ	/		
4. ให้การฝึกอบรมด้านความปลอดภัยแก่พนักงาน	/	/	/
การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ			
1. ติดตามข่าวสารเกี่ยวกับภัยคุกคามด้านความปลอดภัยล่าสุด	/		
2. สำรองข้อมูลอย่างสม่ำเสมอ	/		
การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้			
1. แยกอุปกรณ์ที่ติดไวรัสออกจากเครือข่าย	/		/
2. แจ้งหน่วยงานบังคับใช้กฎหมาย		/	/
3. ติดต่อผู้เชี่ยวชาญด้านความปลอดภัยเพื่อขอความช่วยเหลือ		/	/
4. กู้คืนข้อมูลจากการสำรองข้อมูล			/
การปฏิบัติหลังระบบกลับสู่ปกติ			
1. ติดตั้งระบบปฏิบัติการใหม่และซอฟต์แวร์ที่อัปเดตล่าสุด			/
2. กู้คืนข้อมูลจากการสำรองข้อมูล	/		
3. ตรวจสอบระบบเพื่อหาช่องโหว่ด้านความปลอดภัย	/		/
4. ปรับปรุงแผน BCP เพื่อป้องกันการโจมตีในอนาคต		/	/

U = ดำเนินการได้เองระดับหน่วยงาน

S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน

I = ต้องได้รับการสนับสนุนจาก IT