แผนการกู้คืนข้อมูลสารสนเทศ (Disaster Recovery Plan: DRP)

โรงพยาบาลปากช่องนานา

กลุ่มงานภารกิจสุขภาพดิจิทัล

สารบัญ

1. บทนำ

ปัจจุบันโรงพยาบาลปากช่องนานาได้นำเทคโนโลยีสารสนเทศมาใช้ในการเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร และอำนวยความสะดวกในการให้บริการประชาชนมากยิ่งขึ้น ส่งผลให้มีข้อมูลสารสนเทศเป็นจำนวนมาก อาทิ ข้อมูลพื้นฐานของผู้รับบริการ ข้อมูลประวัติการรักษา ประวัติการแพ้ยา ข้อมูลการนัดหมาย รวมถึงข้อมูลค่าใช้จ่ายต่าง ๆ ซึ่งล้วนเป็นข้อมูลที่มีความสำคัญต่อการวางแผนการรักษา การพัฒนาองค์กร และการบริหารจัดการในด้านต่าง ๆ อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการโจมตีของผู้ไม่หวังดี เช่น ไวรัสคอมพิวเตอร์ การโจมตีด้วย Ransomware การเจาะระบบข้อมูลสารสนเทศ ภัยพิบัติทางธรรมชาติ หรือปัจจัยอื่น ๆ ทั้งจากภายในและภายนอกองค์กร ซึ่งอาจก่อให้เกิดผลกระทบต่อการให้บริการประชาชน และการดำเนินงานของโรงพยาบาล

ดังนั้น เพื่อเป็นการป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้น จึงมีความจำเป็นต้องจัดทำแผนกู้คืนข้อมูลสารสนเทศ โดยเฉพาะฐานข้อมูลสำคัญของโรงพยาบาล (Hospital Information System - HIS) ให้สามารถกลับมาดำเนินการได้ตามปกติโดยเร็วที่สุด เพื่อลดผลกระทบต่อการให้บริการและข้อมูลที่สำคัญของโรงพยาบาล

2. วัตถุประสงค์

เพื่อกู้คืนระบบ Hospital Information System (HIS) และบริการที่สำคัญให้กลับมาใช้งานได้ตามปกติอย่างรวดเร็วและต่อเนื่อง

2.1 กู้คืนระบบ: กู้คืนระบบ HIS, ฐานข้อมูล และเครื่องมือสำคัญให้สามารถทำงานได้ตามระดับปกติที่กำหนดไว้ (RTO: Recovery Time Objective)

2.2 ปกป้องข้อมูล: จำกัดวงความเสียหายเพื่อป้องกันการสูญหายหรือถูกทำลายของข้อมูลผู้ป่วยและข้อมูลสำคัญของโรงพยาบาล

2.3 ลดผลกระทบ: ลดผลกระทบต่อการให้บริการทางการแพทย์และการดำเนินงานของโรงพยาบาลให้เหลือน้อยที่สุด

2.4 ปฏิบัติตามกฎหมาย: ป้องกันความเสียหายทางกฎหมายที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

3. ขอบเขต

แผนนี้ครอบคลุมการจัดการเหตุการณ์ Ransomware ที่ส่งผลกระทบต่อ:

3.1 HIS Server: ทั้ง Application Server, Database Server และ Storage

3.2 ระบบเครือข่าย: Network Infrastructure, Firewall และอุปกรณ์เชื่อมต่อ

3.3 เครื่อง Client: เครื่องคอมพิวเตอร์ที่ใช้ในหน่วยงานต่าง ๆ เช่น OPD, IPD, ห้องยา, ห้องปฏิบัติการ, และห้องฉุกเฉิน ฯลฯ

โดยครอบคลุมทั้งกรณีที่ Server ถูกโจมตีโดยตรง และกรณีที่ Client เป็นจุดเริ่มต้นของการแพร่ระบาด

4. การวิเคราะห์ความสำคัญของระบบ

4.1 HIS Server (Application + Database):

- ระดับความสำคัญ: Critical
- RTO: ≤ 6 ชั่วโมง (เป้าหมายในการกู้คืนระบบให้กลับมาทำงานได้)
- RPO: ≤ 1 วัน (เป้าหมายในการยอมรับการสูญเสียข้อมูลล่าสุด)

4.2 Network/Firewall:

- ระดับความสำคัญ: Critical
- RTO: ≤ 3 ชั่วโมง
- RPO: N/A

4.3 Client PC (OPD, IPD, ห้องยา):

- ระดับความสำคัญ: High
- RTO: ≤ 8 ชั่วโมง
- RPO: N/A

5. มาตรการป้องกันล่วงหน้า (Pre-Emptive Measures)

การป้องกันที่มีประสิทธิภาพเป็นหัวใจสำคัญในการลดความเสี่ยง

5.1 กลยุทธ์การสำรองข้อมูล (Backup Strategy)

- Daily Backup: ทำการสำรองข้อมูลทั้งหมดของ HIS Server ทุกวัน ไปยังที่จัดเก็บ Onsite และ Offsite/Cloud
- Daily Offline Backup: ทำการสำรองข้อมูลแบบออฟไลน์ทุกวัน ซึ่งไม่สามารถเข้าถึงได้จากเครือข่ายหลัก เพื่อป้องกันการเข้ารหัสจาก Ransomware โดยเฉพาะ
- Immutable Backup: ใช้เทคโนโลยี Immutable Storage ที่ทำให้ไม่สามารถแก้ไขหรือลบไฟล์สำรองได้

5.2 ความปลอดภัยระบบเครือข่าย

- Network Segmentation: แบ่งเครือข่ายภายในออกเป็นส่วนย่อย ๆ เช่น เครือข่ายสำหรับ Server, เครือข่ายสำหรับ Client, เครือข่ายสำหรับอุปกรณ์ทางการแพทย์ เพื่อจำกัดการแพร่กระจายของมัลแวร์
- Firewall & IDS/IPS: ใช้ Firewall ที่มีการตั้งกฎอย่างเข้มงวด และติดตั้ง Intrusion Detection/Prevention System (IDS/IPS) เพื่อตรวจจับและป้องกันการบุกรุก.

5.3 การป้องกัน Endpoint (Endpoint Protection):

- ติดตั้ง Antivirus/EDR (Endpoint Detection and Response) บนเครื่อง Client และ Server ทุกเครื่อง
- Patch Management: หมั่นอัปเดตระบบปฏิบัติการและแอปพลิเคชันอย่างสม่ำเสมอเพื่ออุดช่องโหว่ด้านความปลอดภัย

5.4 การสร้างความตระหนักรู้:

- จัดอบรมให้ความรู้แก่บุคลากรอย่างต่อเนื่องเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น Phishing และอันตรายจากการใช้อุปกรณ์ USB

6. ขั้นตอนการกู้คืนระบบ (Recovery Process)

แผนการกู้คืนระบบจะแบ่งตามสถานการณ์หลักที่ตรวจพบ เพื่อให้ทีมงานสามารถรับมือได้อย่างรวดเร็วและเป็นระบบ

6.1 กรณี HIS Server ถูกโจมตีโดยตรง

ผู้รับผิดชอบหลัก: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

1. การกักกันและประเมินสถานการณ์ (Containment & Assessment)

- ตรวจพบและแยกเครื่องทันที: เมื่อได้รับแจ้งว่า HIS Server ถูกโจมตี ให้รีบตัดการเชื่อมต่อออกจากเครือข่ายทั้งหมด (ถอดสาย LAN) เพื่อป้องกันการแพร่กระจายของ Ransomware

- ประกาศใช้ระบบสำรอง: แจ้งผู้บริหารและผู้ใช้งานที่เกี่ยวข้องทันทีให้เปลี่ยนไปใช้ขั้นตอนการทำงานแบบ Manual Process เช่น การบันทึกเวชระเบียนกระดาษ

- ประเมินความเสียหาย: ตรวจสอบว่าระบบปฏิบัติการหรือ VM มีความเสียหายระดับใด (เช่น ไฟล์ถูกเข้ารหัส, OS ไม่สามารถบูตได้) เพื่อตัดสินใจแนวทางการกู้คืนที่เหมาะสมที่สุด

2. การเตรียมการกู้คืนระบบ (Recovery Preparation)

- จัดหาเครื่องใหม่: จัดหาเครื่องแม่ข่ายใหม่ที่มีคุณสมบัติเพียงพอหรือสร้าง Virtual Machine (VM) ใหม่บนระบบ Hyper-Converged Infrastructure (HCI)

- เตรียมโปรแกรมและตั้งค่า: เตรียมไฟล์โปรแกรมติดตั้งระบบปฏิบัติการและแอปพลิเคชัน HIS รวมถึงไฟล์บันทึกการตั้งค่า (Configuration) ของ Server เดิม เช่น IP Address, Hostname, และสิทธิ์การเข้าถึง

3. การกู้คืนและติดตั้งระบบ (System Restoration)

- ติดตั้งระบบปฏิบัติการ: ติดตั้ง OS บนเครื่องแม่ข่ายใหม่ พร้อมกำหนดค่าเครือข่ายและอัปเดต Patch ที่จำเป็นทั้งหมด

- ติดตั้งฐานข้อมูลและกู้คืนข้อมูล: ติดตั้ง Database Management System (DBMS) และกู้คืน (Restore) ฐานข้อมูลล่าสุดจากไฟล์สำรองที่ปลอดภัย (Offline Backup)

- ติดตั้งแอปพลิเคชัน HIS: ติดตั้งโปรแกรม HIS และกำหนดค่าการเชื่อมต่อฐานข้อมูลให้เรียบร้อย.

4. การทดสอบและเปิดใช้งาน (Testing & Go-Live)

- ทดสอบระบบ: ทดสอบการทำงานภายในระบบ HIS และการเชื่อมโยงกับระบบภายนอก (เช่น ห้องแล็บ, ห้องยา ฯลฯ) เพื่อให้มั่นใจว่าข้อมูลถูกต้องและระบบทำงานได้ปกติ

- อนุมัติและประกาศใช้งาน: เมื่อมั่นใจว่าระบบกลับมาใช้งานได้ครบถ้วน ให้ผู้บริหารอนุมัติการเปิดใช้งาน และแจ้งให้ผู้ใช้งานทราบเพื่อกลับมาใช้งานระบบ HIS ตามปกติ

- เฝ้าระวัง: เฝ้าระวังการทำงานของระบบอย่างใกล้ชิดหลังการกู้คืน เพื่อตรวจจับปัญหาที่อาจเกิดขึ้น

5. การฟื้นฟูและปรับปรุง (Post-Incident Review)

- ป้อนข้อมูลย้อนหลัง: ให้เจ้าหน้าที่เวชระเบียนป้อนข้อมูลที่บันทึกไว้ในเวชระเบียนกระดาษกลับเข้าสู่ระบบ HIS

- วิเคราะห์หาสาเหตุ: จัดทำ Root Cause Analysis (RCA) เพื่อหาสาเหตุที่แท้จริงของการโจมตีและช่องโหว่ที่ต้องแก้ไข

- จัดทำรายงานและแจ้งหน่วยงาน: จัดทำ Incident Report และแจ้งผู้บริหาร รวมถึงหน่วยงานกำกับดูแลที่เกี่ยวข้อง (เช่น กรมคุ้มครองข้อมูลส่วนบุคคล) หากพบการรั่วไหลของข้อมูล

6.2 กรณี Client ติด Ransomware และแพร่เข้าสู่ Server

ผู้รับผิดชอบหลัก: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

1. การกักกันและการตรวจสอบ (Containment & Investigation)

- ตรวจจับ: ตรวจสอบและยืนยันการแจ้งเตือนจากระบบรักษาความปลอดภัย เช่น Antivirus, EDR (Endpoint Detection and Response) หรือระบบ SIEM (Security Information and Event Management) รวมถึงการแจ้งจากผู้ใช้งาน

- ระบุและแยกเครื่อง: ค้นหาและระบุเครื่องลูกข่ายที่ติดเชื้อ จากนั้นให้ ตัดการเชื่อมต่อเครือข่าย (ถอดสาย LAN/ปิด Wi-Fi) ของเครื่องนั้นทันที เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังเครื่องอื่น ๆ และ Server

- ตรวจสอบ Server: ตรวจสอบสถานะการทำงานของ HIS Server อย่างละเอียด และทำการสแกนหา Malware หากพบการแพร่กระจาย ให้ดำเนินการกู้คืนระบบตามขั้นตอน 6.1 ทันที

2. การกู้คืนเครื่องลูกข่าย (Client Restoration)

- ล้างเครื่อง (Reimage): ล้างข้อมูลในเครื่อง Client ที่ติดเชื้อทั้งหมดและติดตั้งระบบปฏิบัติการใหม่ เพื่อให้แน่ใจว่ามัลแวร์ถูกกำจัดอย่างสมบูรณ์

- อัปเดตระบบป้องกัน: ตรวจสอบและอัปเดตระบบ Antivirus/EDR บนเครื่อง Client ทุกเครื่องในเครือข่ายให้เป็นปัจจุบัน

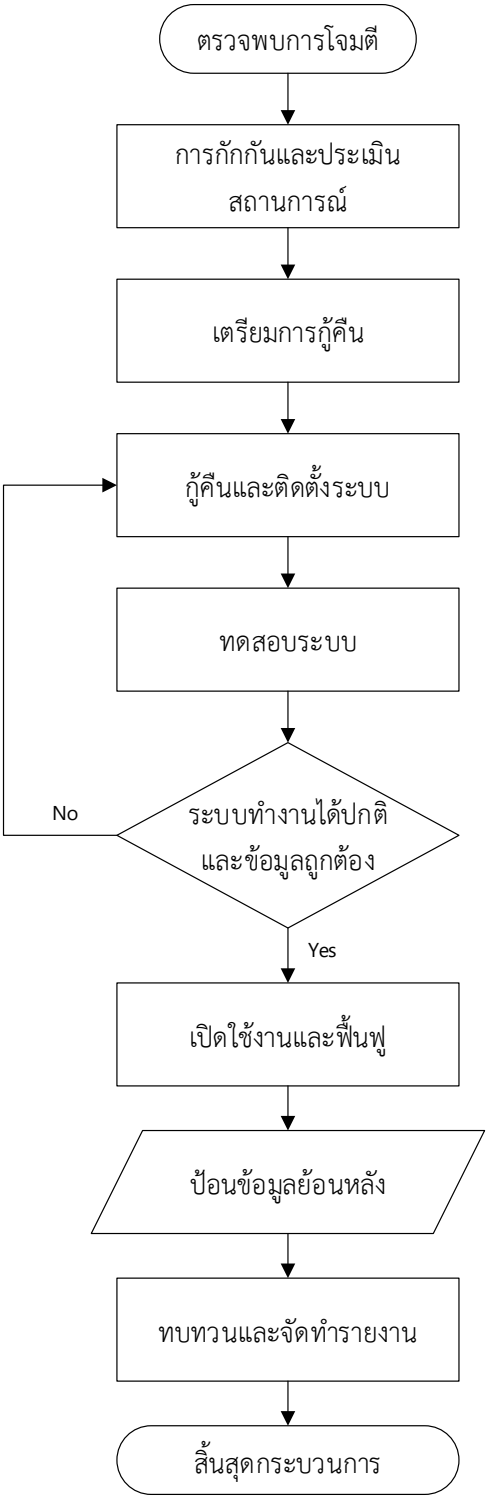
3. การป้องกันและเฝ้าระวังหลังเกิดเหตุ (Prevention & Monitoring)

- ทบทวนนโยบายความปลอดภัย: ทบทวนและปรับปรุงนโยบายการสำรองข้อมูล, นโยบายการใช้รหัสผ่าน, และสิทธิ์การเข้าถึงเครือข่าย

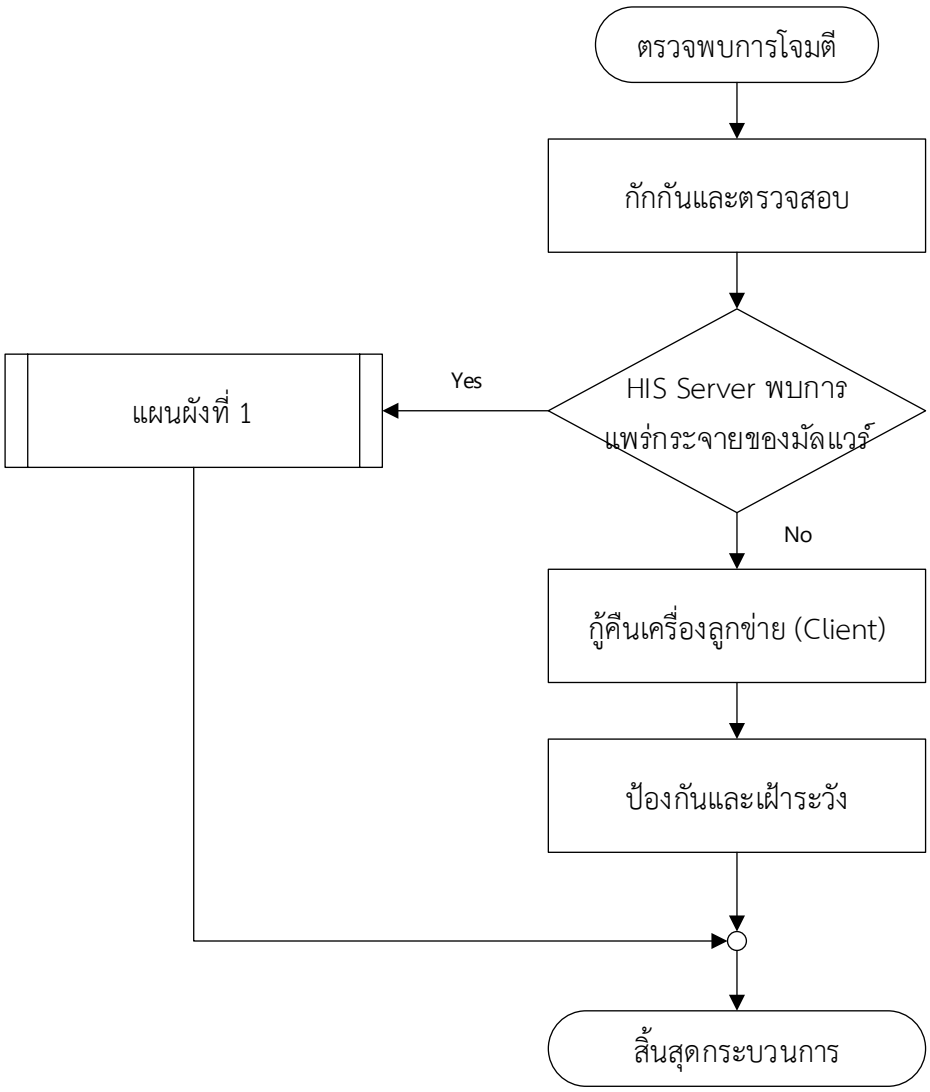
- ให้ความรู้บุคลากร: จัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการป้องกัน Ransomware และภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง

- เฝ้าระวัง: เฝ้าระวังการทำงานของระบบเครือข่ายและ Server อย่างใกล้ชิด เพื่อตรวจจับความผิดปกติที่อาจเกิดขึ้นอีกในอนาคต

6.3 Flow Chart แผนการกู้คืนข้อมูล



แผนผังที่ 1 กรณี HIS Server ถูกโจมตีโดยตรง



แผนผังที่ 2 กรณี Client ติด Ransomware

7. **บทบาทและหน้าที่**

- ทีม IT/IT Security: มีหน้าที่หลักในการตรวจจับ, กักกัน, กู้คืนระบบ Server, ติดตั้ง Patch/EDR และวิเคราะห์หาสาเหตุ

- เจ้าหน้าที่เวชระเบียน: มีหน้าที่จัดการบันทึกข้อมูลระหว่างระบบล่ม และรับผิดชอบการป้อนข้อมูลย้อนหลังเมื่อระบบกลับมาใช้งาน

- แพทย์/พยาบาล: มีหน้าที่ใช้เวชระเบียนกระดาษเพื่อรักษาผู้ป่วยและประสานงานกับเจ้าหน้าที่เวชระเบียน

- ผู้บริหาร: มีหน้าที่ตัดสินใจในภาวะวิกฤติ เช่น การประกาศใช้ DR Site หรือการแจ้งหน่วยงานภายนอก

ภาคผนวก

แบบฟอร์มบันทึกการทดสอบกู้คืนข้อมูล Hosxp

ทะเบียน Restore Hosxp

ลำดับ	วัน เดือน ปี	เวลา	เจ้าหน้าที่	สถานะ	ผู้ตรวจสอบ	หมายเหตุ
1	4 เม.ย. 68	16.30	วิศาล	☑ สำเร็จ ☐ ไม่สำเร็จ	อภัสรา	
2	7 พ.ค. 68	09.10	[illegible]	☑ สำเร็จ ☐ ไม่สำเร็จ	นิพรา	
3	6 มิ.ย. 68	09.35	[illegible]	☑ สำเร็จ ☐ ไม่สำเร็จ	[illegible]	
4	1 ก.ค. 68	09.30	[illegible]	☑ สำเร็จ ☐ ไม่สำเร็จ	[illegible]	
5	5 ส.ค. 68	09.22	ปวินท์	☑ สำเร็จ ☐ ไม่สำเร็จ	อภัสรา	
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ		
				☐ สำเร็จ ☐ ไม่สำเร็จ