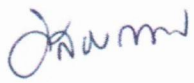
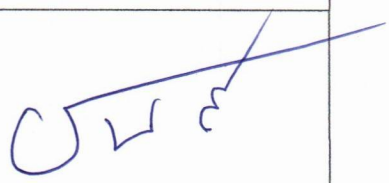
	กระบวนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)	**รหัสเอกสาร**	**NKH MOPH Recover -01**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**23 มี.ค. 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นายอิสระภาพ เบ้าน้อย	นางพรรณี วรธรรม	นายธนสันตชัย พรหมบุตร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	พยาบาลวิชาชีพชำนาญการพิเศษ (Lead Implementer)	นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโนนคูณ (CISO)
วันเดือนปี	16 มีนาคม 2569	20 มีนาคม 2569	23 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	23 มีนาคม 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

	กระบวนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)	รหัสเอกสาร	NKH MOPH Recover -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้	23 มี.ค. 2569
		ชั้นความลับของเอกสาร	ใช้ภายในเท่านั้น

สารบัญ

กระบวนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 25.1.1, ข้อ 25.1.2]

1. วัตถุประสงค์

กระบวนการนี้จัดทำขึ้นเพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการต่อไปได้อย่างต่อเนื่องในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้กระบวนการ ฟื้นฟูความเสียหายเป็นไปอย่างมีประสิทธิภาพและใช้เวลาสั้นในการฟื้นฟู

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) การทบทวนแผน BCP และการฝึกซ้อมแผน BCP เพื่อประเมินความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	บุคลากรที่เกี่ยวข้อง	เจ้าหน้าที่ของหน่วยงานต่าง ๆ ของ โรงพยาบาลโนนคูณที่เกี่ยวข้อง รวมถึงบุคลากรภายนอกสำนักงานปลัดกระทรวงที่เกี่ยวข้อง

2	ทีมรักษาความต่อเนื่องทางธุรกิจ	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลรักษาความต่อเนื่องทางธุรกิจ
3	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นปลอดภัยสารสนเทศขององค์กร

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	รับผิดชอบในการอนุมัติและสนับสนุนการจัดทำและการทบทวนแผน BCP รวมถึงการจัดสรรทรัพยากรที่จำเป็นสำหรับการฟื้นฟูความเสียหาย
2	ทีมรักษาความต่อเนื่องทางธุรกิจ (Business Continuity Team)	รับผิดชอบในการพัฒนาแผน BCP และการประสานงานกับผู้ให้บริการภายนอกเพื่อให้แน่ใจว่าแผน BCP ของผู้ให้บริการภายนอก สอดคล้องกับแผนขององค์กร
3	บุคลากรที่เกี่ยวข้อง (Relevant Personnel)	มีหน้าที่เข้าร่วมในการฝึกซ้อมแผน BCP และปฏิบัติตาม ขั้นตอนที่กำหนดไว้ในแผนเมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

5. ขั้นตอนปฏิบัติ

5.1 การจัดทำและทบทวนแผนความต่อเนื่องทางธุรกิจ (Development and Review of Business Continuity Plan)

1) การจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP)

ขั้นตอน: จัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) เพื่อให้บริการที่สำคัญขององค์กรหรือหน่วยงานสามารถดำเนินการต่อไปได้ในกรณีที่เกิดการหยุดชะงักจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีการกำหนดขอบเขตของแผน BCP ที่ครอบคลุมทุกส่วนที่เกี่ยวข้องกับบริการที่สำคัญ และการกำหนดระยะเวลาในการฟื้นฟู (RTO, RPO)

2) การทบทวนแผนของผู้ให้บริการภายนอก

ขั้นตอน: ทบทวนแผน BCP ของผู้ให้บริการภายนอกเพื่อให้แน่ใจว่ามีความสอดคล้องกับแผนความต่อเนื่องทางธุรกิจของหน่วยงาน อีกทั้ง เพื่อให้แน่ใจว่าการฟื้นฟูระบบสามารถดำเนินการได้ภายในระยะเวลาที่กำหนดในแผนความต่อเนื่องทางธุรกิจของหน่วยงาน

5.2 การฝึกซ้อมและการประเมินผล (Exercise and Evaluation)

1) การฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP)

ขั้นตอน: ดำเนินการฝึกซ้อมแผน BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนในการรับมือกับภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยการการจำลองสถานการณ์การโจมตีทางไซเบอร์และการทดสอบความสามารถของบุคลากรในการดำเนินการตามแผน BCP

2) การประเมินผลการฝึกซ้อม

ขั้นตอน: ประเมินผลการฝึกซ้อมแผน BCP เพื่อวิเคราะห์จุดแข็งและจุดอ่อนที่ต้องปรับปรุง ใน การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดทำรายงานผลการฝึกซ้อมที่สรุปผลการดำเนินงานพร้อมข้อเสนอแนะการปรับปรุงแผน BCP เพื่อเพิ่มประสิทธิภาพในการ ฟื้นฟูความเสียหายในอนาคต

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร
1		แผนเตรียมพร้อมกรณีฉุกเฉินระบบเทคโนโลยีสารสนเทศ ประจำปี
2		การฝึกซ้อมแผนความต่อเนื่องทางธุรกิจด้านระบบสารสนเทศ

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

	- การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)
2	แผนความต่อเนื่องทางธุรกิจ
3	แผนการสอบทานแผนของผู้ให้บริการภายนอก
4	ผลการฝึกซ้อมแผนตามแผนความต่อเนื่องทางธุรกิจ
5	คู่มือแผนความต่อเนื่องทางธุรกิจ
6	ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

หลักฐานจริง

โรงพยาบาลโนนคูณ

แผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต

(Business Continuity Plan : BCP)

รวมเหตุการณ์ กรณีเกิดภัยพิบัติ (Disaster) และการโจมตีทางไซเบอร์ที่ร้ายแรง

สารบัญ

แผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต
(Business Continuity Plan : BCP)

1. Introduction

1.1 Title of Plan

แผน BCP ฉบับนี้จัดทำขึ้นเพื่อให้โรงพยาบาลโนคูณ สามารถดำเนินธุรกิจด้านการบริการประชาชน ได้อย่างต่อเนื่อง แม้เกิดเหตุการณ์ฉุกเฉิน เช่น ความล้มเหลวของระบบเครือข่าย, ภัยธรรมชาติ, หรือการโจมตีทางไซเบอร์ โดยมุ่งเน้นการฟื้นฟูกระบวนการ (Recovery) และลดผลกระทบต่อบริการหลักขององค์กร เป็นหลัก อีกทั้งการจัดทำแผนนี้ยังช่วยสร้างความมั่นใจให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียว่าโรงพยาบาลโนนคูณ มีความพร้อมในการรับมือกับสถานการณ์ฉุกเฉินต่าง ๆ ได้อย่างมีประสิทธิภาพและรวดเร็วมากแค่ไหน

การดำเนินงานตามแผนนี้เน้นการวิเคราะห์ความเสี่ยง (Risk Analysis) การเตรียมความพร้อมของทรัพยากร (Resource Preparation) และกระบวนการฟื้นฟู (Recovery) รวมถึงกระบวนการที่สำคัญภายใต้กรอบเวลาที่กำหนด เพื่อให้มั่นใจว่าองค์กรสามารถกลับมาดำเนินงานตามปกติได้ในเวลาอันรวดเร็วที่สุด

1.2 Purpose

1. วัตถุประสงค์

1. เพื่อรับประกันความต่อเนื่องของบริการแอปพลิเคชั่นหลัก ที่สำคัญ เช่น HIMPRO ซึ่งเป็นส่วนสำคัญหลักของธุรกิจ
2. ลดผลกระทบที่อาจเกิดขึ้นกับข้อมูลและโครงสร้างพื้นฐานในกรณีฉุกเฉิน
3. ฟื้นฟูกระบวนการดำเนินงานให้กลับมาทำงานได้ภายในเวลาที่กำหนด เพื่อไม่ให้ส่งผลกระทบต่อภาพลักษณ์ขององค์กร
4. สร้างความเชื่อมั่นให้แก่ลูกค้าและผู้มีส่วนได้ส่วนเสีย โดยแสดงถึงความสามารถในการจัดการกับเหตุการณ์วิกฤติ
5. ส่งเสริมการบริหารจัดการที่โปร่งใสและเป็นระบบในช่วงเวลาฉุกเฉิน รวมถึงการรายงานความคืบหน้าแก่ฝ่ายบริหารและผู้เกี่ยวข้อง
6. ส่งเสริมการฝึกซ้อมและการปรับปรุงแผนอย่างต่อเนื่อง เพื่อให้แผนมีความเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลง

2. ขอบเขต

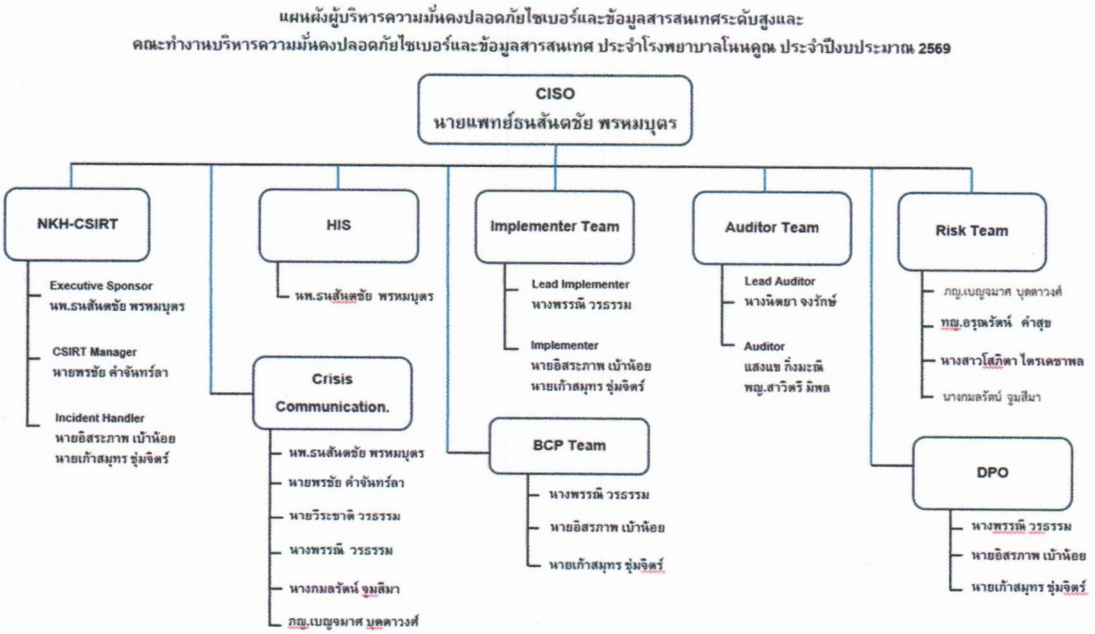
แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) ฉบับนี้ ใช้สำหรับเป็นแนวทางในการปฏิบัติ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน เหตุการณ์ที่มีผลกระทบต่อกิจกรรมหลักของโรงพยาบาลโนนคูณ ซึ่งประกอบด้วยเหตุการณ์ต่อไปนี้

1. ความล้มเหลวของระบบเทคโนโลยีสารสนเทศ เช่น เซิร์ฟเวอร์หลักล่ม, การโจมตีของไวรัส หรือการโจมตีไซเบอร์
2. ภัยธรรมชาติ เช่น อุทกภัย, แผ่นดินไหว, หรือพายุที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานและอุปกรณ์
3. เหตุการณ์อัคคีภัย
4. เหตุการณ์ชุมนุมประท้วง/จลาจล
5. การโจมตีทางไซเบอร์ เช่น การแฮ็กระบบที่สำคัญหรือการโจมตีแบบ Phishing, DDoS, Ransomware หรืออื่นๆ ที่ถือว่าเป็นภัยคุกคาม

3. ความรับผิดชอบ

1. หัวหน้า IT Support (IT Manager/ISMS/CSMR) : รับผิดชอบในการกำกับดูแลและตรวจสอบการดำเนินงานตามแผน BCM (Business Continuity Management) โดยใช้ทีมตอบสนองในการทำงาน
2. ทีม IT Support : รับผิดชอบในการดำเนินการตามแผน BCM (Business Continuity Management) และประสานงานกับหน่วยงานต่างๆ
3. ผู้ใช้ : ปฏิบัติตามแนวทางและขั้นตอนที่กำหนดในแผน BCM (Business Continuity Management)

BCM Organization Chart



BCM - Business Continuity Management Team

No	Name	Position	Department	Tel / Mobile Phone
1	นายอิสระภาพ เบ้าน้อย	หัวหน้า IT	IT	0640215121, 0800300641
2	นายเก้าสมุทร ซุ่มจิตร์	เจ้าหน้าที่ IT	IT	098-1111111

1.3 Executive Summary

ขั้นตอนการทำงานนี้ ถูกใช้ในกรณีที่เกิดภัยพิบัติที่ศูนย์ข้อมูล (Data Center) หรือเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศที่ทำให้ธุรกิจหยุดชะงัก ซึ่งขั้นตอนการทำงานนี้มีเป้าหมาย เพื่ออธิบายโครงสร้างการกู้คืนจากภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ วิธีการที่ใช้ในการกู้คืนและขั้นตอนสำหรับการนำบริการเทคโนโลยีสารสนเทศหลักและแอปพลิเคชัน ระบบธุรกิจที่สำคัญกลับมาใช้งาน โดยได้มาจากการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ณ สถานที่กู้คืนจากภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ และแผนนี้ยังกล่าวถึงทรัพยากรที่จำเป็นและลำดับการกู้คืนที่ต้องปฏิบัติตามเพื่อให้แผนประสบความสำเร็จ

1.4 Documentation and References (เอกสารประกอบ)

1. Application and vendor contact List (แอพพลิเคชั่นและรายชื่อของผู้ให้บริการ พร้อมเบอร์ติดต่อ)
2. Hardware and software inventory (รายการทรัพย์สิน ไม่ว่าจะเป็น ฮาร์ดแวร์และซอฟแวร์)
3. Backup and Restore Manual / Scheduling (เอกสารคู่มือในการติดตั้งระบบ ต่างๆ)

1.5 Document Location (ที่ตั้งในการเก็บเอกสารต่างๆ)

แผนนี้ถูกจัดเก็บไว้และจะถูกนำมาใช้จากเวอร์ชั่นที่อยู่ในโฟลเดอร์ "แผนการกู้คืนจากภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์หรือความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ" ที่อยู่ใน Google Drive และเอกสารที่เป็นต้นฉบับที่ตู้เก็บเอกสารในห้องแผนกไอที **Link : https://drive.google.com/drive/folders/1hlerkZwwmfDEGfXFQXoHkKubuhneWmL2?usp=sharing**

1.6 Document Security (ความปลอดภัยในการจัดเก็บเอกสารต่างๆ)

แผนนี้เป็นข้อมูลธุรกิจที่ถือว่าเป็นความลับ ออกแบบมาสำหรับกลุ่มงาน IT และกลุ่มงานตรวจสอบที่เหมาะสม เท่านั้น

2. Scope of the business continuity plan

2.1 Users of this Procedure

- BCM Org chart
- CSIRT Org chart (Incident Response Team)
- Crisis Communication Team

2.2 Participating Systems

เอกสารนี้อธิบายการออกแบบที่เหมาะสมต่อการเกิดภัยพิบัติและกิจกรรมการสำรองเพื่อรับมือกับภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ สำหรับเซิร์ฟเวอร์ ที่ทางโรงพยาบาลโนนคูณ ได้ใช้พร้อมกับบริการ IT หลักและแอปพลิเคชันหลักสำหรับระบบธุรกิจตามที่ระบุด้านล่างและขั้นตอนระดับสูงที่จำเป็นในการดำเนินการ Fail over ในกรณีที่เกิดภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์จริง
ข้างล่างนี้คือ บริการ IT หลักที่รวมอยู่ในแผนนี้ ได้แก่

1. ระบบ HIMPRO
2. ระบบ PACS
3. ระบบ GTW

3. Communications Plan

3.1 Who Can Declare a Business continuity Plan

การประกาศภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศดำเนินการโดยโรงพยาบาลโนนคูณ หากหัวหน้า IT Support (IT Manager/ISMS/CSMR) ไม่อยู่ สามารถรายงานตรงไปยังตัวแทนหน่วยงานแต่ละแผนก เพื่อทำการตัดสินใจโดยบุคลากรดังต่อไปนี้ จะเป็นผู้ตัดสินใจหลักอย่างต่อเนื่อง

- หัวหน้า IT Support
- เจ้าหน้าที่ IT Support
- หัวหน้า Implement
- เจ้าหน้าที่ Operation

3.2 Emergency Funding

อาจจำเป็นต้องใช้เงินทุนก่อนที่ระบบ Application หลักดังกล่าว จะกลับมาออนไลน์อีกครั้ง ดังนั้นจึงจำเป็นต้องนำเสนองบประมาณที่จำเป็น ต่อคณะผู้บริหารต่อไป

3.3 Key IT Staff & Alternates

โครงสร้างของบุคลากร IT Support มีบทบาทสำคัญในการดำเนินการตามคู่มือแผนความต่อเนื่องทางธุรกิจ จะถูกนำมาใช้งานทันทีหลังจากที่มีการประกาศเหตุภัยพิบัติ

- หัวหน้า IT Support (IT Manager/ISMS/CSMR)
  - จุดศูนย์กลางสำหรับการสื่อสารและแผนปฏิบัติการ จัดตารางเวลาและบันทึกเหตุการณ์
  - ตัดสินใจเกี่ยวกับการจัดลำดับความสำคัญและวิธีการกู้คืน สื่อสารกับผู้นำธุรกิจระดับสูง
  - ติดตั้งและกำหนดค่าแอปพลิเคชัน
  - ติดตั้งและกำหนดค่าแอปพลิเคชันบนเวิร์คสเตชัน
  - จัดเตรียมเครือข่ายที่เหมาะสม เป็นจุดติดต่อกับผู้ให้บริการเครือข่าย

- เจ้าหน้าที่ IT Support
  - รักษาความปลอดภัยและดำเนินการสร้างฐานของเซิร์ฟเวอร์ เตรียมอุปกรณ์สำหรับการติดตั้งแอปพลิเคชัน- ติดตั้งและกำหนดค่าแอปพลิเคชันบนเวิร์คสเตชัน
  - รับผิดชอบด้านการสื่อสารโทรคมนาคมในสถานที่สำรอง
  - รับผิดชอบการดำเนินงานในสถานที่สำรอง
  - รับผิดชอบด้านสิ่งอำนวยความสะดวกในสถานที่สำรอง

3.4 3rd Party/Service Provider Contacts

รายชื่อผู้ให้บริการภายนอกต่อไปนี้จะให้บริการเพิ่มเติม เช่น อุปกรณ์ และการสนับสนุน สำหรับกิจกรรมการกู้คืนจากภัยพิบัติ/ ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ ตามข้อตกลงในสัญญาที่มีร่วมกัน

Company/Organization Name	Services	Contact Person	Contact Information
บริษัท NT จำกัด	บริการ Internet	call center	Office : 18 อาคาร ทรู ทาวเวอร์ ถนนรัชดาภิเษก แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

บริษัท คิวรี่ดิจิตอล จำกัด	โปรแกรม Himpro บริการต่างๆภายใรโรงพยาบาล	099-0190195	เลขที่ 24/2 หมู่ 3 ตำบลห้วยทับทัน อำเภอห้วยทับทัน จังหวัดศรีสะเกษ
บริษัท PACS	โปรแกรม x-ray		
บริษัท นีโอ เน็ตเวิร์ค สแกน จำกัด (สำนักงานใหญ่)	โปรแกรมเรียกคิว	02-8667818	261/95 ถนนจรัญสนิทวงศ์ แขวงบางขุนศรี เขตบางกอกน้อย กรุงเทพฯ 10700
ห้างหุ้นส่วนจำกัด โปรเน็ตเวิร์ค เทเลคอม (สำนักงานใหญ่)	กล้องโทรทัศน์วงจรปิดชนิดเครือข่ายแบบมุมมองคงที่ / อุปกรณ์บันทึกภาพผ่านเครือข่าย แบบ 8 ช่อง อุปกรณ์กระจายสัญญาณแบบ PoE L2 Switch	089-9171125	341 หมู่ 17 ตำบลไร่น้อย อำเภอเมืองอุบลฯ จังหวัดอุบลราชธานี 34000
ห้างหุ้นส่วนจำกัด ศรีสะเกษ คอมพิวเตอร์ แอนด์ เทคโนโลยี	อุปกรณ์คอมพิวเตอร์ โน๊ตบุ๊ค,ปริ้นเตอร์	099-0190194	24/2 หมู่ 3 ตำบล ห้วยทับทัน อำเภอห้วยทับทัน จังหวัดศรีสะเกษ

3.5 Customers/Authorities/Media/Press Communications

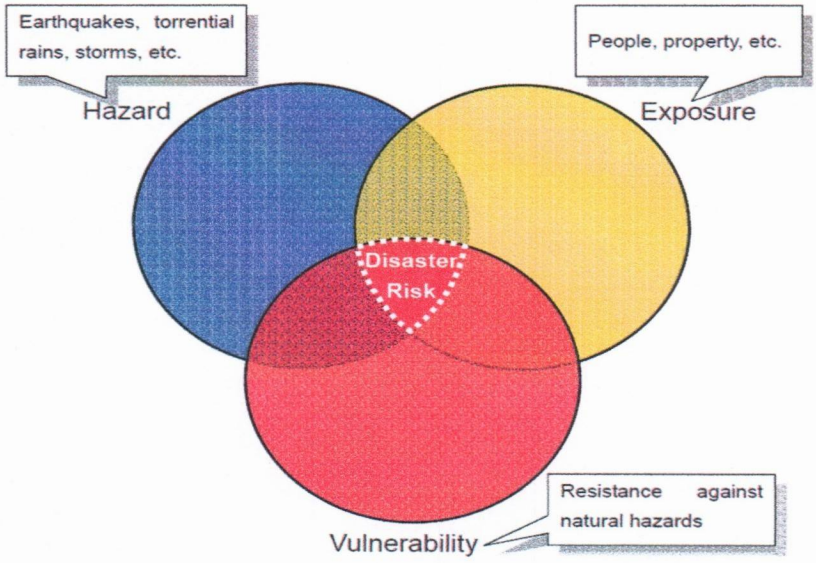
สำหรับการสื่อสารกับหน่วยงานภายนอก (ลูกค้า, หน่วยงานราชการ, สื่อมวลชน) ควรใช้ขั้นตอนต่อไปนี้ตามแนวทางของโรงพยาบาลโนนคูณ สำหรับการสื่อสารในภาวะวิกฤต (Crisis Communication)

Company name	Contact Person	Contact Information
แจ้งเหตุด่วน เหตุร้าย		Tel.: 191
ประปา		
ไฟฟ้า		
โรงพยาบาล		045 659 044

4. Risk Assessment

4.1 Risk Definitions

จำนวนภัยพิบัติทางธรรมชาติเกิดเพิ่มขึ้นพร้อมกับผลกระทบที่เกิดขึ้น เนื่องจากการเปลี่ยนแปลงภายนอก เช่น การรวมตัวของประชากรและทรัพย์สินในพื้นที่อันตราย และการขยายตัวของเมืองอย่างรวดเร็ว ภาพด้านล่างแสดงให้เห็นว่า "อันตราย" ตัวอย่างเช่น แผ่นดินไหวที่เกิดขึ้นบนเกาะร้างไม่ก่อให้เกิดภัยพิบัติ เนื่องจากไม่มีประชากร หรือทรัพย์สินที่ได้รับผลกระทบ นอกจากอันตรายแล้ว อาจจะต้องมี "ความเปราะบาง" บางประการต่อปรากฏการณ์"ธรรมชาติ เพื่อให้เหตุการณ์นั้นถือเป็นภัยพิบัติทางธรรมชาติ ""ความเปราะบาง"" หมายถึงสภาวะที่เกิดจากปัจจัยหรือกระบวนการทางกายภาพ สังคม เศรษฐกิจ และสิ่งแวดล้อม ซึ่งเพิ่มความเสี่ยงของชุมชนต่อผลกระทบของอันตราย"การสัมผัส" เป็นองค์ประกอบอีกประการหนึ่งของความเสี่ยงจากภัยพิบัติ และหมายถึงสิ่งที่ได้รับผลกระทบจากภัยพิบัติทางธรรมชาติ เช่น ผู้คนและทรัพย์สิน โดยทั่วไป "ความเสี่ยง" ถูกกำหนดให้เป็นค่าความคาดหวังของความสูญเสีย (การเสียชีวิต การบาดเจ็บ ทรัพย์สิน ฯลฯ) ที่เกิดจากอันตราย ความเสี่ยงจากภัยพิบัติสามารถมองเห็นได้ว่าเป็นฟังก์ชันของอันตราย การสัมผัส และความเปราะบาง ดังนี้: Disaster Risk = function (Hazard, Exposure, Vulnerability)การเพิ่มขึ้นของการเปิดรับและความล่าช้าในการลดความเปราะบาง ส่งผลให้จำนวนภัยพิบัติทางธรรมชาติเพิ่มขึ้นและระดับความสูญเสียมากขึ้น



4.1.1 Vulnerabilities, Threats and Exposure Identification for Business/Location

Threat	Risk Identified (Narrative)	Probability (low, med, high)	Severity (low, med, high)	Risk Score	Buildings Affected	Risk Mitigation measures and remarks	Notes on any actual past events
Earthquake	แผ่นดินไหวอาจเกิดขึ้นที่ตำแหน่งที่ส่งผลกระทบต่อความพร้อมใช้งานของบริการที่	1	5	ยอมรับได้	Data Center	โรงพยาบาลโนนคูณไม่ได้ตั้งอยู่ใน	ไม่เคยเกิดขึ้นในช่วง

	จัดหาโดยศูนย์ข้อมูลภูมิภาคและผู้ให้บริการโทรคมนาคม ตำแหน่งนี้เป็นศูนย์กลางหลักที่ให้บริการ IT ในประเทศรวมถึงประเทศอื่น ๆ					พื้นที่เสี่ยงต่อแผ่นดินไหว	25 ปีที่ผ่านมา
Cyclone	พายุไซโคลนอาจพัดกระหน่ำในพื้นที่ ส่งผลกระทบต่อสายการสื่อสารของวงจรทั้งในระดับภูมิภาคและระดับสากลที่เชื่อมต่อกับศูนย์ข้อมูล พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงบริการไปยังประเทศอื่น ๆ	1	4	ยอมรับได้	Data Center	**โรงพยาบาลโนนคูณ** มีความเสี่ยงต่ำต่อการเกิดฟ้าผ่า	ไม่เคยเกิดขึ้นในช่วง 25 ปีที่ผ่านมา
Flooding	น้ำท่วมอาจทำให้ระบบจ่ายไฟฟ้าล้มเหลวและนำไปสู่การขัดข้องของกระแสไฟฟ้าพื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	1	5	ยอมรับได้	Data Center	ศูนย์ข้อมูลตั้งอยู่บนชั้นหนึ่งของอาคาร HQ เป็นพื้นที่เสี่ยงต่อน้ำท่วม	
Power Failure	การขัดข้องของกระแสไฟฟ้าอาจทำให้ระบบที่ศูนย์ข้อมูล/ห้องสื่อสารหยุดทำงานพื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	1	3	ยอมรับได้	Data Center	มีเครื่องสำรองไฟ (UPS) สามารถให้พลังงานสำรองได้นาน 4 ชั่วโมง	มีการทดสอบระบบสำรองไฟตามข้อตกลงการบำรุงรักษา (MA Agreement)

Threat	Risk Identified (Narrative)	Probability (low, med, high)	Severity (low, med, high)	Risk Score	Buildings Affected	Risk Mitigation measures and remarks	Notes on any actual past events
Telecom. Failure	การล้มเหลวของบริการโทรคมนาคมอาจทำให้การเข้าถึงแอปพลิเคชัน/	1	3	ยอมรับได้	Data Center	มีการจัดหาเส้นทางสื่อสารจากผู้ให้บริการ	ไม่มี

	เซิร์ฟเวอร์/เครือข่ายที่โฮสต์นอกพื้นที่นี้เกิดความขัดข้อง พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ					โทรคมนาคมสองราย ได้แก่ True, AIS เพื่อให้สามารถสื่อสารกับภายนอกได้โดยไม่เกิดการขัดข้อง	
Toxic release	การปล่อยสารพิษในพื้นที่อาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูลและห้องสื่อสารได้ พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ	1	2	ยอมรับได้	Data Center	ศูนย์ข้อมูลอยู่ห่างจากพื้นที่เคมีภัณฑ์/อุตสาหกรรมประมาณ 250 กิโลเมตร โอกาสที่จะได้รับผลกระทบจากการปล่อยสารพิษมีน้อยมาก และส่วนใหญ่จะสลายตัวก่อนที่จะมาถึงอาคาร	ไม่เคยเกิดขึ้นในช่วง 25 ปีที่ผ่านมา
Nearby buildings	ในกรณีที่เกิดเหตุการณ์รุนแรง อาคารที่อยู่ใกล้เคียงอาจทำให้ศูนย์ข้อมูล/ห้องสื่อสารได้รับความเสียหาย พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ	1	3	ยอมรับได้	Data Center	พื้นที่นี้ไม่มีเหตุการณ์รุนแรง	ไม่มี
Fire	ในกรณีเกิดเหตุเพลิงไหม้ ศูนย์ข้อมูล/ห้องสื่อสารในพื้นที่นี้อาจได้รับความเสียหายทั้งทางกายภาพและทางตรรกะ พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	2	4	ยอมรับไม่ได้	Data Center	มีระบบตรวจจับและติดตั้งถังดับเพลิง การทดสอบประสิทธิภาพของอุปกรณ์ป้องกันอัคคีภัยจะดำเนินการเป็นระยะเพื่อให้มั่นใจว่า	ไม่มี

						อุปกรณ์พร้อมใช้งานตลอดเวลา	

Threat	Risk Identified (Narrative)	Probability (low, med, high)	Severity (low, med, high)	Risk Score	Buildings Affected	Risk Mitigation measures and remarks	Notes on any actual past events
Cyber security Hackers /Attack	เหตุการณ์การแฮ็ก/การโจมตีด้านความปลอดภัยทางไซเบอร์อาจนำไปสู่การสูญหาย/การขโมยข้อมูล เนื่องจากพื้นที่นี้เป็นศูนย์กลางหลักของประเทศไทยและมีข้อมูลที่เกี่ยวข้องทั้งในระดับภูมิภาคและระดับโลก	5	5	ยอมรับไม่ได้	Data Center	มีการติดตั้ง Firewall, PS/IDS,ซอฟต์แวร์ป้องกันไวรัส และทำการเฝ้าระวังและตรวจสอบอย่างต่อเนื่องเพื่อป้องกันข้อมูลจากการถูกขโมย ,รั่วไหล และการโจมตี	ไม่มี
Terrorists	การโจมตีของผู้ก่อการร้ายหรือผู้ไม่ประสงค์ดี อาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูล/ห้องสื่อสารได้ รวมถึงอาจเกิดการสูญเสียชีวิต พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศ	1	2	ยอมรับได้	Data Center	อาจเป็นเป้าหมายที่มีความเสี่ยงต่ำต่อการก่อการร้าย อย่างไรก็ตาม มีการเพิ่มความเข้มงวดด้านความปลอดภัยภายในโดยการติดตั้งและตรวจสอบสถานที่ด้วยกล้องวงจรปิด (CCTV) และมีการจัดเจ้าหน้าที่รักษาความปลอดภัยตลอด 24 ชั่วโมงเพื่อการเฝ้าระวังอย่างเข้มงวด	ไม่มี
Pandemic	เหตุการณ์การระบาดของโรคอาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูล/ห้องสื่อสารได้ รวมถึงอาจเกิดการสูญเสียชีวิต พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศ	1	2	ยอมรับได้	Data Center	ฝ่าย IT มีแผนฉุกเฉินสำหรับการระบาดใหญ่ที่ระบุไว้ในเอกสารแยกต่างหาก เอกสารอ้างอิงสามารถดูได้จากคู่มือความปลอดภัยสำหรับฐานข้อมูลของ	

						โรงพยาบาลโนนคูณ ภายใต้ชื่อแผนตอบสนองการระบาดของไข้หวัดใหญ่	

หมายเหตุ : - Risk Score 1-5 = ยอมรับได้ , ถ้า Risk Score > 5 = ยอมรับไม่ได้

4.1.2 Conclusions on Vulnerabilities, Threats and Exposure Identification

จากช่องโหว่, ภัยคุกคาม และการเปิดเผยที่ระบุไว้สำหรับศูนย์ข้อมูลส่วนกลางของ โรงพยาบาลโนนคูณ มีความเข้าใจถึงสาเหตุของการเกิดและสามารถจัดการกับความเสี่ยงที่เกี่ยวข้องกับเงื่อนไขดังต่อไปนี้

1. ข้อมูลที่เกี่ยวกับ Production ทั้งหมด จะไม่มีเก็บไว้ที่ศูนย์ข้อมูล ที่ศูนย์ข้อมูลจะมีเพียงระบบทดสอบเท่านั้น ซึ่งข้อมูลอื่นจะถูกสำรองข้อมูลไว้บน external harddisk ในทุกๆวัน
2. ธุรกิจได้ใช้การดำเนินการลดความเสี่ยงที่หลากหลายเพื่อให้ความเสี่ยงอยู่ในระดับที่เหมาะสม โดยหนึ่งในการดำเนินการในด้านนี้คือ
   - มีการทำbackup แบบ Real time (Slave Server of Himpro)
3. ผู้ใช้ที่สำคัญได้รับการติดตั้ง VPN และโทรศัพท์มือถือที่สามารถเข้าถึงเครือข่ายผ่านแอปพลิเคชันไคลเอ็นต์ที่ปลอดภัยซึ่งจะช่วยให้ผู้ใช้สามารถเข้าถึงแอปพลิเคชันจากศูนย์ข้อมูล Data Center HQ ได้อย่างราบรื่น
4. ข้อสรุปอื่น ๆ เกี่ยวกับการดำเนินการลดความเสี่ยงที่ระบุไว้ ได้แก่ การได้รับการจัดเตรียมสถานที่สำรอง เพื่อรับรองความถูกต้องและรองรับคำขอของผู้ใช้ในกรณีที่เกิดภัยพิบัติที่ไซต์หลัก ข้อมูลสำรอง (Backup) สำหรับแอปพลิเคชันที่สำคัญทั้งหมดถูกเก็บไว้ใน **Slave Server** (Himpro) เพื่อให้ผู้ใช้ดำเนินกิจกรรมทางธุรกิจได้อย่างราบรื่น
5. ได้มีการสร้างแผนการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินที่หลากหลาย ตามความสำคัญต่อธุรกิจ

4.2 Business Impact Analysis (BIA)

จากระบบที่ใช้งานในปัจจุบัน โดยมีศูนย์ข้อมูล Data Center HQ และผู้ให้บริการสนับสนุนบริการ IT ต่างๆ ซึ่งต่อไปนี้จะต้องถูกกู้คืนตามลำดับและความสำคัญที่แสดงในตารางด้านล่าง

Business Impact Analysis Summary Table

Application/ IT Service Name	Business Purpose	MTPD	RTO	RPO	Recovery Priority
ระบบ HIMPRO	ระบบบริการโรงพยาบาลโนนคูณ	12 ชั่วโมง	6 ชั่วโมง	15 ชั่วโมง	0
ระบบ PACS	ระบบ X-RAY	12 ชั่วโมง	6 ชั่วโมง	6ชั่วโมง	1

หมายเหตุ : ระดับความสำคัญในการกู้คืน 0 คือสูงสุด ลำดับการกู้คืนจะเริ่มต้นด้วยการกู้คืนระบบ HosXP ที่มีความสำคัญสูงสุดก่อน

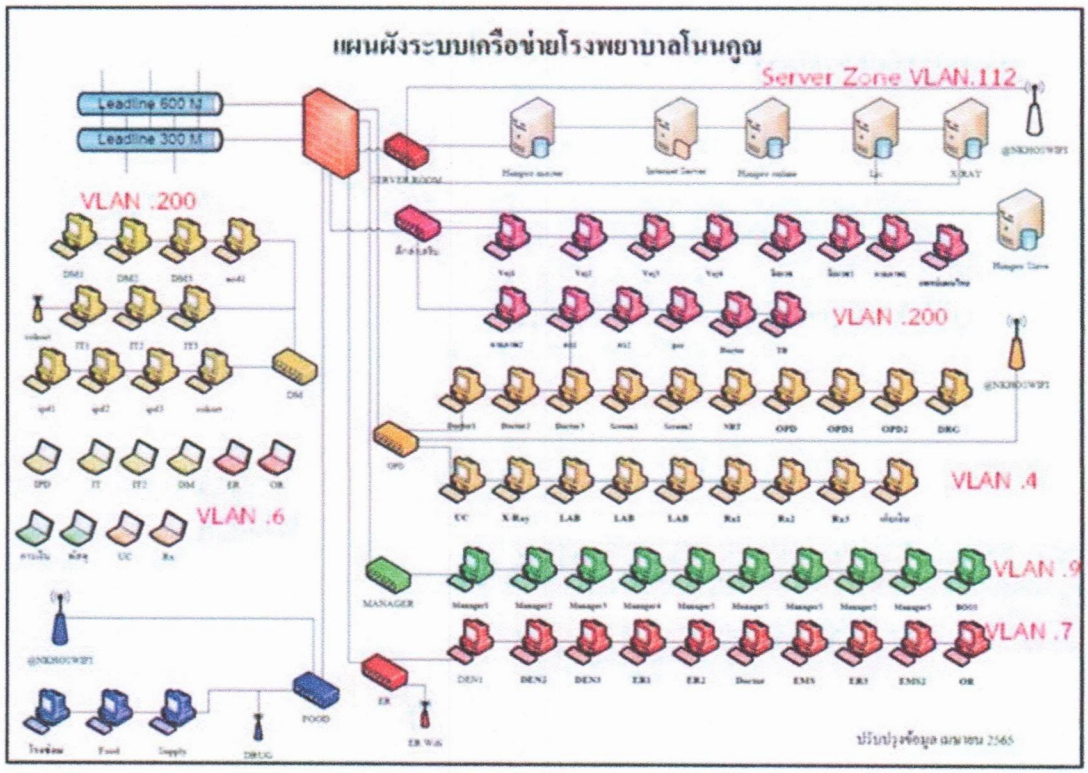
4.3. Recovery Assumptions

ข้อสมมุติฐานต่อไปนี้เป็นเงื่อนไขที่พิจารณาเมื่อพัฒนาลำดับความสำคัญในการกู้คืนและลำดับการกู้คืนสำหรับระบบที่อยู่ในขอบเขตของการกู้คืนจากภัยพิบัติที่มีผลต่อธุรกิจ

- การสำรองข้อมูลและกำหนดการถูกดำเนินการในลักษณะที่สอดคล้องกับข้อกำหนด RTO (Recovery Time Objective) ของธุรกิจ และได้รับการทดสอบเป็นระยะ เพื่อให้แน่ใจว่าอยู่ในสภาพที่สามารถกู้คืนได้ดี
- ผู้ให้บริการโทรคมนาคมได้รับการแจ้งเกี่ยวกับกระบวนการและขั้นตอนอย่างดี เพื่อให้สามารถขยายการสนับสนุนในกรณีที่เกิดภัยพิบัติ
- ผู้จำหน่ายฮาร์ดแวร์ได้รับการสื่อสารเกี่ยวกับข้อกำหนดของฮาร์ดแวร์และบริการในกรณีที่เกิดภัยพิบัติ

5. Business Continuity Recovery Process Overview

5.1 Business Continuity Recovery Architecture Overview



1. สถานที่ตั้งทางกายภาพ – ศูนย์ข้อมูลหลักที่โรงพยาบาลโนนคูณ

ศูนย์ข้อมูลหลักตั้งอยู่ที่

โรงพยาบาลโนนคูณ

ที่อยู่ **57 หมู่12 ต.โนนค้อ อ.โนนคูณ จ.ศรีสะเกษ 33250**

ศูนย์ข้อมูลสำรองอยู่ที่

ตึกส่งเสริมสุขภาพ

2. บริการโทรคมนาคม - ศูนย์ข้อมูลสำรองจะเชื่อมต่อกับอินเทอร์เน็ต

3. การสำรองฮาร์ดแวร์และการทำงานแบบสำรอง – ฮาร์ดแวร์สำรองจะถูกจัดเตรียมที่สถานที่สำรองในกรณีที่เกิดภัยพิบัติที่ไซต์หลัก

รายละเอียดการติดต่อของผู้ขายมีดังนี้

อุปกรณ์	รายละเอียด
Server Supplier Name : ห้างหุ้นส่วนจำกัด ศรีสะเกษคอมพิวเตอร์ แอนด์เทคโนโลยี Tel : 099-0190194	Processor : 2x Intel Xeon Gold 6326 (2.9GHz up to 3.5GHz, 24MB Cache) Main Memory: 32GB (2x16GB) Dual Rank x8 DDR4-3200 CAS-22-22-22 Registered Smart Memory KitMemory Slot Storage 4 x 960GB SATA 6G Read Intensive SFF BC Multi Vendor SSD Storage Slot 8 x SFF (Hot Plug) Chassis Expansion Slots 1x HPE 96W Smart Storage Lithium-ion Battery with 145mm Cable Kit 1x HPE ProLiant DL380 Gen10 Plus x8/x16/x8 Primary FIO Riser Kit Special Feature RAID : MegaRAID MR416i-a x16 Lanes 4GB Cache NVMe/SAS 12G Controller System Management : HPE iLO Form Factor : 2U Rack Network Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T OCP3 Adapter for HPE Power Supply 2 x 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit

อุปกรณ์	รายละเอียด
Notebook Supplier Name : หุ้นส่วนจำกัด ศรีสะเกษคอมพิวเตอร์ แอนด์เทคโนโลยี Tel : 099-0190194	Intel® Core™ i5-1135G7 (up to 4.2 GHz with Intel® Turbo Boost Technology, 8 MB L3 cache, 4 cores) 16GB (2x8GB) DDR4 3200 (Memory Slots :2 SODIMM) 512GB PCIe NVMe Value Solid State Drive

อุปกรณ์	รายละเอียด
CCTV Supplier Name : ห้าง หุ้นส่วนจำกัด โปรเน็ตเวิร์ค เทเลคอม (สำนักงานใหญ่) Tel : 089-9171125	Intel® Core™ i5-1135G7 (up to 4.2 GHz with Intel® Turbo Boost Technology, 8 MB L3 cache, 4 cores) 16GB (2x8GB) DDR4 3200 (Memory Slots :2 SODIMM) 512GB PCIe NVMe Value Solid State Drive

5.2 Core Services Recovery Overview

ส่วนนี้อธิบายขั้นตอนระดับสูงที่จำเป็นสำหรับการกู้คืนจากภัยพิบัติ ขั้นตอนเฉพาะจะอ้างอิงจากเอกสารที่มีอยู่แล้วในกรณีที่จำเป็น

- ระบบ HIMPRO : จำเป็นสำหรับการดำเนินงานทางการบริการภาคประชาชน การจ่ายยา การชำระเงิน
- ระบบ PACS : มีความสำคัญต่อการทดสอบระบบ ในการขึ้นระบบใหม่ของลูกค้า
- ระบบ LIS : มีความสำคัญต่อการจัดเก็บ source code

5.3 Application Recovery Overview

1. การกู้คืนแอปพลิเคชันจะดำเนินการที่สถานที่สำรองตามระดับความรุนแรงของภัยพิบัติที่ไซต์หลัก
   - ระบบ HIMPRO จะถูกกู้คืนเมื่อมีการเชื่อมต่อเครือข่าย และทำการ Restore Backup

2. การสำรองข้อมูลจะถูกกำหนดเวลาให้สำรองข้อมูลแบบเต็มทุกวัน และข้อมูลสำรองจะถูกเก็บไว้ที่ Slave Server การสำรองข้อมูลจะได้รับการทดสอบรายไตรมาส เพื่อแน่ใจว่าระบบสำรองสามารถใช้งานได้และมีข้อมูลเป็นปัจจุบัน
3. การติดตั้งเซิร์ฟเวอร์พื้นฐานจะถูกดำเนินการโดยทีม IT Support
4. เมื่อได้รับข้อมูลสำรอง (Backup) กิจกรรมการกู้คืนจะถูกดำเนินการโดยทีม IT Support การสำรองข้อมูลและจะได้รับการทดสอบแอปพลิเคชัน เพื่อความสมบูรณ์และความถูกต้องของข้อมูล

6. Business Continuity Recovery Procedures

ตามลำดับความสำคัญและลำดับการดำเนินการที่กำหนดไว้ในตารางสรุปผลกระทบทางธุรกิจสำหรับโครงสร้างพื้นฐานและแอปพลิเคชันหลัก ขั้นตอนต่อไปนี้จะถูกดำเนินการตามลำดับที่แสดงในตารางต่อไปนี้ เพื่อให้สามารถใช้งานตามสภาพแวดล้อมสำรองได้ในกรณีที่มีการประกาศเหตุการณ์ระดับความต่อเนื่องทางธุรกิจ

No	Application/ IT Service Name Recovery Procedure	Recovery Procedure	Document Name	Version
1	Business Continuity Plan Manual	Business Continuity Plan Manual	Business Continuity Plan Manual	1.0

7. Business Continuity Plan Testing Requirements

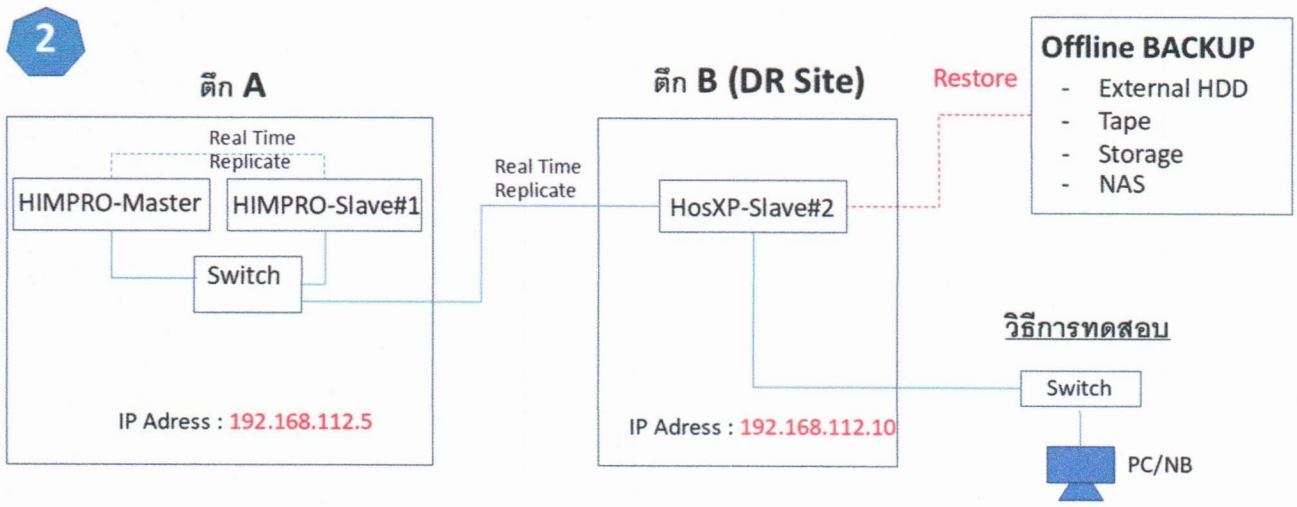
7.1 การทดสอบการกู้คืนความต่อเนื่องทางธุรกิจเป็นประจำทุกปี เพื่อให้แน่ใจว่าขั้นตอนนี้ได้รับการเข้าใจอย่างดีและกระบวนการมีความถูกต้อง

7.2 ข้อกำหนดพื้นฐานสำหรับการวางคู่มือแผนความต่อเนื่องทางธุรกิจ ในระหว่างขั้นตอนการวางแผนการทดสอบแอพพลิเคชั่นที่จะทดสอบจะถูกวิเคราะห์ เพื่อทำความเข้าใจว่ามีการใช้ส่วนประกอบต่างๆ ในแอปพลิเคชั่นทำงานปกติ

ด้านล่างนี้คือตารางการทดสอบโดยรวมที่จำเป็นสำหรับแอปพลิเคชันหลักที่อยู่ในขอบเขตเป็นส่วนหนึ่งของแผนการกู้คืนจากภัยพิบัตินี้

ต้องมีการกำหนดวันทดสอบ ระบบสำรองด้วยนะ เอาที่เราสะดวกเลย แต่ต้องทดสอบอย่างน้อย 1 ครั้งต่อปี

Application DR Plan	Year Test Schedule											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
ระบบ HIMPRO								○				
ระบบ GTW								○				
ระบบ PACS								○				



วิธีการทดสอบ : -

1. ตรวจสอบว่า HIMPRO-Slave#2 สามารถทำงานได้หรือไม่
2. ตรวจสอบว่า ข้อมูลที่ Restore จาก Media สามารถใช้งานได้หรือไม่

7.3 กรณีทดสอบการขึ้นระบบ Himpro **ครั้งที่ 1 :** ทดสอบว่าระบบมีการ Replicate Data แบบ Real Time ได้สมบูรณ์หรือไม่

1. ทำการติดตั้ง ระบบ Slave HIMPRO Server (Hardware and Software) และติดตั้งให้อยู่คนละทีหรือคนละอาคารเดียวกับ Primary HIMPRO Server เปรียบเสมือน DR Site
2. ทำการตั้งค่า (Configure) ให้มีการสำรองข้อมูลแบบต่อเนื่อง (Real Time)
3. ทำการตั้งค่าให้ Slave HIMPRO Server อยู่คนละวงเดียวกับ Primary HIMPRO Server
4. ทำการเชื่อมโยง 1 computer ให้เชื่อมโยงเข้ากับ Slave HIMPRO Server
5. ดำเนินการทดสอบระบบ เช่น Access Test, Function Test และดูว่าข้อมูลเป็นปัจจุบันหรือไม่
6. จบขั้นตอนการทดสอบ ถ้าผลการทดสอบเป็นที่น่าพอใจ
7. ถ้าผลการทดสอบมีปัญหา ต้องทำการแก้ไขปัญหา หาสาเหตุหรือทำการ Restore ข้อมูลใหม่อีกครั้ง

7.4 กรณีทดสอบการขึ้นระบบ HIMPRO **ครั้งที่ 2 :** ทดสอบว่าการ Restore จาก Media มีความสมบูรณ์หรือไม่

1. ทำการ Restore Data จาก Medie ลงไปใน ระบบ Slave HIMPRO Server
2. ทำการเชื่อมโยง 1 computer ให้เชื่อมโยงเข้ากับ Slave HIMPRO Server
3. ดำเนินการทดสอบระบบ เช่น Access Test, Function Test และดูว่าข้อมูลเป็นปัจจุบันหรือไม่
4. จบขั้นตอนการทดสอบ ถ้าผลการทดสอบเป็นที่น่าพอใจ
5. ถ้าผลการทดสอบมีปัญหา ต้องทำการแก้ไขปัญหา หาสาเหตุหรือทำการ Restore ข้อมูลใหม่อีกครั้ง

7.5 กรณีทดสอบการขึ้นระบบ LIS และระบบ PACS (สามารถประสานงานกับ Supplier ให้มาช่วยในการทดสอบได้ เนื่องจากมันเป็นทรัพย์สินของ Supplier นั้นๆ)

8. Business Continuity Plan Business Approval

แผนการกู้คืนความต่อเนื่องทางธุรกิจที่บันทึกไว้ในขั้นตอนนี้และเอกสารสนับสนุนที่เกี่ยวข้อง ได้รับการตรวจสอบและอนุมัติโดยทีมผู้บริหารระดับสูงของโรงพยาบาลโนนคูณ โดยสมาชิกในทีมได้ลงนามและอนุมัติเอกสารดังนี้

9. Related Document (เอกสารที่เกี่ยวข้อง)

รหัสเอกสาร	ชื่อเอกสาร
	รายงานการทดสอบระบบ

ลงชื่อ	ลงชื่อ	ลงชื่อ .....
นายแพทย์ธนสันตชัย พรหมบุตร	นายแพทย์ธนสันตชัย พรหมบุตร	นางพรรณี วรธรรม
CISO	HIS	Lead Implementer
วันที่ ____/____/____	วันที่ ____/____/____	วันที่ ____/____/____