โรงพยาบาลแม่ลาว

แผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต

(Business Continuity Plan : BCP)

สารบัญ

แผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต
(Business Continuity Plan : BCP)

1. Introduction

1.1 Title of Plan

แผน BCP ฉบับนี้จัดทำขึ้นเพื่อให้โรงพยาบาลแม่ลาว สามารถดำเนินธุรกิจด้านการบริการประชาชน ได้อย่างต่อเนื่อง แม้เกิดเหตุการณ์ฉุกเฉิน เช่น ความล้มเหลวของระบบเครือข่าย, ภัยธรรมชาติ, หรือการโจมตีทางไซเบอร์ โดยมุ่งเน้นการฟื้นฟูกระบวนการ (Recovery) และลดผลกระทบต่อบริการหลักขององค์กร เป็นหลัก อีกทั้งการจัดทำแผนนี้ยังช่วยสร้างความมั่นใจให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียว่าโรงพยาบาลแม่ลาวมีความพร้อมในการรับมือกับสถานการณ์ฉุกเฉินต่าง ๆ ได้อย่างมีประสิทธิภาพและรวดเร็วมากแค่ไหน

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

1.2 Purpose

1. วัตถุประสงค์

1. เพื่อรับประกันความต่อเนื่องของบริการแอปพลิเคชั่นหลัก ที่สำคัญ เช่น HOSxPXE4ซึ่งเป็นส่วนสำคัญหลักของธุรกิจ
2. ลดผลกระทบที่อาจเกิดขึ้นกับข้อมูลและโครงสร้างพื้นฐานในกรณีฉุกเฉิน
3. ฟื้นฟูกระบวนการดำเนินงานให้กลับมาทำงานได้ภายในเวลาที่กำหนด เพื่อไม่ให้ส่งผลกระทบต่อภาพลักษณ์ขององค์กร
4. สร้างความเชื่อมั่นให้แก่ลูกค้าและผู้มีส่วนได้ส่วนเสีย โดยแสดงถึงความสามารถในการจัดการกับเหตุการณ์วิกฤติ
5. ส่งเสริมการบริหารจัดการที่โปร่งใสและเป็นระบบในช่วงเวลาฉุกเฉิน รวมถึงการรายงานความคืบหน้าแก่ฝ่ายบริหารและผู้เกี่ยวข้อง
6. ส่งเสริมการฝึกซ้อมและการปรับปรุงแผนอย่างต่อเนื่อง เพื่อให้แผนมีความเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลง

2. ขอบเขต

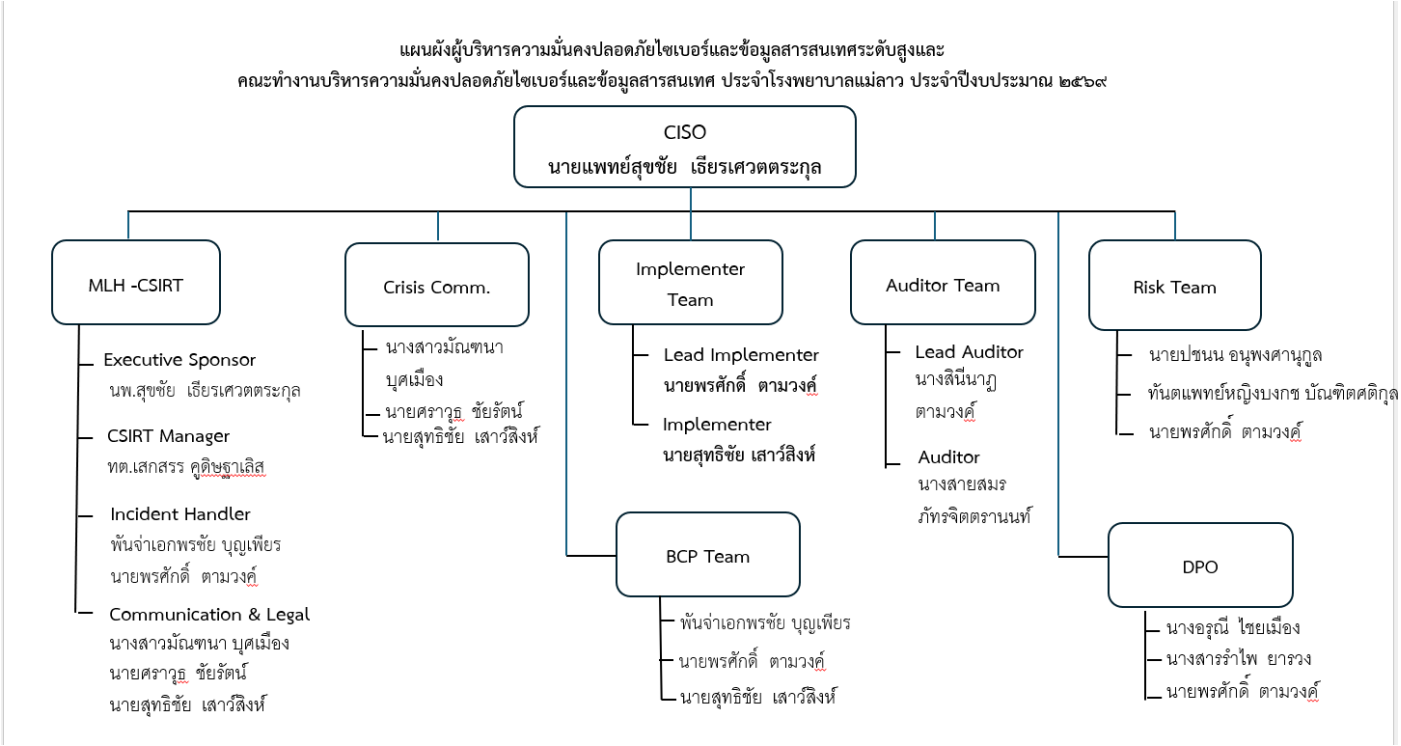
แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) ฉบับนี้ ใช้สำหรับเป็นแนวทางในการปฏิบัติ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน เหตุการณ์ที่มีผลกระทบต่อกิจกรรมหลักของโรงพยาบาลแม่ลา ซึ่งประกอบด้วยเหตุการณ์ต่อไปนี้

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

ให้ใส่ชื่อผู้ที่เกี่ยวข้องทั้งหมด มาวางใส่ในตาราง เพื่อขึ้นระบบใหม่ ให้ไวที่สุด

No	Name	Position	Department	Tel / Mobile Phone
1	นพ.สุขชัย เธียรเศวตตระกูล	CISO	Management	053-603100 ต่อ 2014
2	ทต.เสกสรร คูดิษฐาเสิศ	CSIRT Manager	CSIRT Manager	053-603100 ต่อ 3116
3	พันจ่าเอกพรชัย บุญเพียร	Incident Handler	Incident Handler	053-603100 ต่อ 2015
4	น.ส มัณฑนา บุศเมือง	Communication & Crisis Comm	Communication & Crisis Comm	053-603100 ต่อ 3114
5	นายศราวุธ ชัยรัตน์	Communication & Crisis Comm	Communication & Crisis Comm	053-603100 ต่อ 3144
6	นางอรุณี ไชยเมือง	DPO	DPO	053-603100 ต่อ 3102
7	นางสาวรำไพ ยารวง	DPO	DPO	053-603100 ต่อ 3144
8	นายพรศักดิ์ ตามวงค์	หัวหน้า IT Support	IT Support	081-4733415
9	นายสุทธิชัย เสาว์สิงห์	เจ้าหน้าที่ IT Support	IT Support	061-3061590
10	ภก.ปชนน อนุพงศานุกูล	Risk Team	Risk Team	053-603100 ต่อ 3115
11	ทต.ญ บงกช บัณฑิตศติกุล	Risk Team	Risk Team	053-603100 ต่อ 3116

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/**

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 ที่ทาง**โรงพยาบาลแม่ลาว** ได้ใช้พร้อมกับบริการ IT หลักและแอปพลิเคชันหลักสำหรับระบบธุรกิจตามที่ระบุด้านล่างและขั้นตอนระดับสูงที่จำเป็นในการดำเนินการ Fail over ในกรณีที่เกิดภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์จริง
ข้างล่างนี้คือ บริการ IT หลักที่รวมอยู่ในแผนนี้ ได้แก่

1. ระบบ HOSXPEX4
2. ระบบ LIS
3. ระบบ Pacs

3. Communications Plan

3.1 Who Can Declare a Business continuity Plan

การประกาศภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศดำเนินการโดย**โรงพยาบาลแม่ลาว** 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 มีบทบาทสำคัญในการดำเนินการตามคู่มือแผนความต่อเนื่องทางธุรกิจจะถูกนำมาใช้งานทันทีหลังจากที่มีการประกาศเหตุภัยพิบัติ

- 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
หจก.เชียงรายเทคโนคอม	บริการด้าน Hard ware	086-420-1849	25 ถนนเรืองนคร ตำบลเวียง อำเภอเมือง จังหวัด เชียงราย 57000

3.5 Customers/Authorities/Media/Press Communications

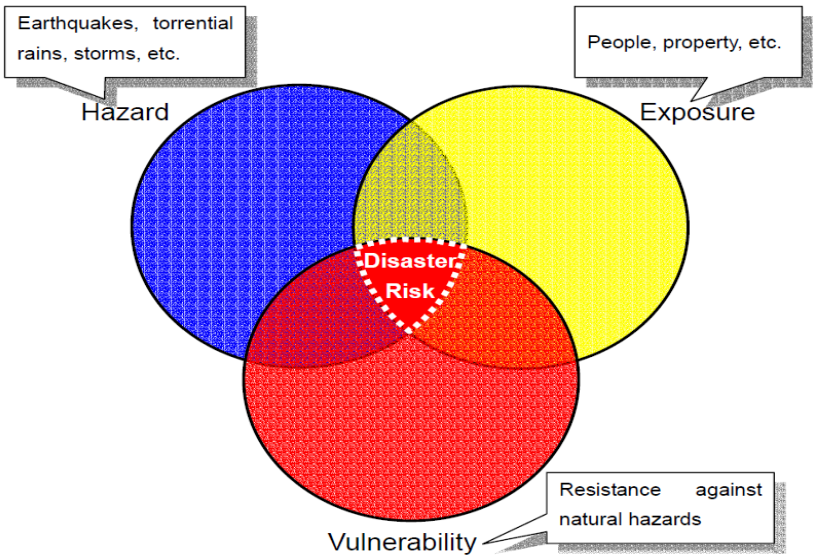
สำหรับการสื่อสารกับหน่วยงานภายนอก (ลูกค้า, หน่วยงานราชการ, สื่อมวลชน) ควรใช้ขั้นตอนต่อไปนี้ตามแนวทางของ**โรงพยาบาลแม่ลาว** สำหรับการสื่อสารในภาวะวิกฤต (Crisis Communication)

Company name	Contact Person	Contact Information
หัวหน้าทีมดับเพลิง (นายวิชาญ)	083-5772287	
รถดับเพลิงเทศบาลป่าก่อดำ		0 5366 6694
รถดับเพลิง อบต.ป่าก่อดำ		0 5377 8011
รถดับเพลิงเทศบาลแม่ลาว		0 53729074
สถานีตำรวจภูธรแม่ลาว		0 5377 8191
กฟภ.แม่ลาว		0 5318 3850-1
โรงพยาบาลพาน	06 4086 1450	
สสจ.เชียงราย		0 5391 0300

4. Risk Assessment

4.1 Risk Definitions

จำนวนภัยพิบัติทางธรรมชาติเกิดเพิ่มขึ้นพร้อมกับผลกระทบที่เกิดขึ้น เนื่องจากการเปลี่ยนแปลงภายนอก เช่น การรวมตัวของประชากรและทรัพย์สินในพื้นที่อันตราย และการขยายตัวของเมืองอย่างรวดเร็ว ภาพด้านล่างแสดงให้เห็นว่า "อันตราย" ตัวอย่างเช่น แผ่นดินไหวที่เกิดขึ้นบนเกาะร้างไม่ก่อให้เกิดภัยพิบัติเนื่องจากไม่มีประชากร 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	แผ่นดินไหวอาจเกิดขึ้นที่ตำแหน่งที่ส่งผลกระทบต่อความพร้อมใช้งานของบริการที่จัดหาโดยศูนย์ข้อมูลภูมิภาคและผู้ให้บริการโทรคมนาคม ตำแหน่งนี้เป็นศูนย์กลางหลักที่ให้บริการ IT ในประเทศรวมถึงประเทศอื่น ๆ	Very Low 1	Rare 5	ยอมรับได้	Data Center	**โรงพยาบาลแม่ลาว** ไม่ได้ตั้งอยู่ในพื้นที่เสี่ยงต่อแผ่นดินไหว	ไม่เคยเกิดขึ้นในช่วง 25 ปีที่ผ่านมา
Cyclone	พายุไซโคลนอาจพัดกระหน่ำในพื้นที่ ส่งผลกระทบต่อสายการสื่อสารของวงจรทั้งในระดับภูมิภาคและระดับสากลที่เชื่อมต่อกับศูนย์ข้อมูล พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงบริการไปยังประเทศอื่น ๆ	Very Low 1	Rare 1	ยอมรับได้	Data Center	**โรงพยาบาลแม่ลาว** มีความเสี่ยงต่ำต่อการเกิดฟ้าผ่า	ไม่เคยเกิดขึ้นในช่วง 25 ปีที่ผ่านมา

Flooding	น้ำท่วมอาจทำให้ระบบจ่ายไฟฟ้าล้มเหลวและนำไปสู่การขัดข้องของกระแสไฟฟ้าพื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	Medium 2	Unlikely 2	ยอมรับได้	Data Center	ศูนย์ข้อมูลตั้งอยู่บนชั้นสองของอาคาร OPD เป็นพื้นที่ไม่เสี่ยงต่อน้ำท่วม	เคยเกิดขึ้นในช่วง 15 ปีที่ผ่านมา
Power Failure	การขัดข้องของกระแสไฟฟ้าอาจทำให้ระบบที่ศูนย์ข้อมูล/ห้องสื่อสารหยุดทำงานพื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	Low 1	Rare 1	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/เซิร์ฟเวอร์/เครือข่ายที่โฮสต์นอกพื้นที่นี้เกิดความขัดข้อง พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ	Low 1	Rare 1	ยอมรับได้	Data Center	มีการจัดหาเส้นทางสื่อสารจากผู้ให้บริการโทรคมนาคมสองรายได้แก่ True, AIS เพื่อให้สามารถสื่อสารกับภายนอกได้โดยไม่เกิดการขัดข้อง	ไม่มี
Toxic release	การปล่อยสารพิษในพื้นที่อาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูลและห้องสื่อสารได้ พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ	Low 1	Rare 1	ยอมรับได้	Data Center	ศูนย์ข้อมูลอยู่ห่างจากพื้นที่เคมีภัณฑ์/อุตสาหกรรมประมาณ 250 กิโลเมตร โอกาสที่จะได้รับผลกระทบจากการปล่อยสารพิษมีน้อยมาก และส่วนใหญ่จะสลายตัวก่อนที่จะมาถึงอาคาร	ไม่เคยเกิดขึ้นในช่วง 25 ปีที่ผ่านมา

Nearby buildings	ในกรณีที่เกิดเหตุการณ์รุนแรง อาคารที่อยู่ใกล้เคียงอาจทำให้ศูนย์ข้อมูล/ห้องสื่อสารได้รับความเสียหาย พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศรวมถึงประเทศอื่น ๆ	Low 1	Rare 1	ยอมรับได้	Data Center	พื้นที่นี้ไม่มีเหตุการณ์รุนแรง	ไม่มี
Fire	ในกรณีเกิดเหตุเพลิงไหม้ ศูนย์ข้อมูล/ห้องสื่อสารในพื้นที่นี้อาจได้รับความเสียหายทั้งทางกายภาพและทางตรรกะ พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ ITภายในประเทศรวมถึงประเทศอื่น ๆ	Medium 2	Possible 2	ยอมรับได้	Data Center	มีระบบตรวจจับและติดตั้งถังดับเพลิง การทดสอบประสิทธิภาพของอุปกรณ์ป้องกันอัคคีภัยจะดำเนินการเป็นระยะเพื่อให้มั่นใจว่าอุปกรณ์พร้อมใช้งานตลอดเวลา	ไม่มี

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	High 5	Almost Certain 5	ยอมรับได้แบบมีเงื่อนไข	Data Center	มีการติดตั้ง Firewall, PS/IDS,ซอฟต์แวร์ป้องกันไวรัส และทำการเฝ้าระวังและตรวจสอบอย่างต่อเนื่องเพื่อป้องกันข้อมูลจากการถูกขโมย,รั่วไหล และการโจมตี	ไม่มี
Terrorists	การโจมตีของผู้ก่อการร้ายหรือผู้ไม่ประสงค์ดี อาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูล/ห้องสื่อสารได้ รวมถึงอาจเกิดการสูญเสียชีวิต พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศ	Low 1	Rare 1	ยอมรับได้	Data Center	อาจเป็นเป้าหมายที่มีความเสี่ยงต่ำต่อการก่อการร้าย อย่างไรก็ตาม มีการเพิ่มความเข้มงวดด้านความปลอดภัยภายในโดยการติดตั้งและตรวจสอบสถานที่ด้วยกล้องวงจรปิด (CCTV) และมีการจัดเจ้าหน้าที่รักษาความปลอดภัย	ไม่มี

						ตลอด 24 ชั่วโมงเพื่อการเฝ้าระวังอย่างเข้มงวด	
Pandemic	เหตุการณ์การระบาดของโรคอาจทำให้ไม่สามารถเข้าถึงศูนย์ข้อมูล/ห้องสื่อสารได้ รวมถึงอาจเกิดการสูญเสียชีวิต พื้นที่นี้เป็นศูนย์กลางหลักที่ให้บริการ IT ภายในประเทศ	Low 1	Rare 1	ยอมรับได้	Data Center	ฝ่าย IT มีแผนฉุกเฉินสำหรับการระบาดใหญ่ที่ระบุไว้ในเอกสารแยกต่างหาก เอกสารอ้างอิงสามารถดูได้จากคู่มือความปลอดภัยสำหรับฐานข้อมูลของ **โรงพยาบาลแม่ลาว**..... ภายใต้ชื่อแผนตอบสนองการระบาดของไข้หวัดใหญ่	

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

4.1.2 Conclusions on Vulnerabilities, Threats and Exposure Identification

จากช่องโหว่, ภัยคุกคาม และการเปิดเผยที่ระบุไว้สำหรับศูนย์ข้อมูลส่วนกลางของ **โรงพยาบาลแม่ลาว** มีความเข้าใจถึงสาเหตุของการเกิดและสามารถจัดการกับความเสี่ยงที่เกี่ยวข้องกับเงื่อนไขดังต่อไปนี้

1. ข้อมูลที่เกี่ยวกับ Production ทั้งหมด จะไม่มีเก็บไว้ที่ศูนย์ข้อมูล ที่ศูนย์ข้อมูลจะมีเพียงระบบทดสอบเท่านั้น
2. ธุรกิจได้ใช้การดำเนินการลดความเสี่ยงที่หลากหลายเพื่อให้ความเสี่ยงอยู่ในระดับที่เหมาะสม โดยหนึ่งในการดำเนินการในด้านนี้คือ
   - มีการทำbackup แบบ Real time (Slave Server of HOSxPeX4)
3. ผู้ใช้ที่สำคัญได้รับการติดตั้ง VPN และโทรศัพท์มือถือที่สามารถเข้าถึงเครือข่ายผ่านแอปพลิเคชันไคลเอ็นต์ที่ปลอดภัยซึ่งจะช่วยให้ผู้ใช้สามารถเข้าถึงแอปพลิเคชันจากศูนย์ข้อมูล Data Center HQ ได้อย่างราบรื่น
4. ข้อสรุปอื่น ๆ เกี่ยวกับการดำเนินการลดความเสี่ยงที่ระบุไว้ ได้แก่ การได้รับการจัดเตรียมสถานที่สำรอง เพื่อรับรองความถูกต้องและรองรับคำขอของผู้ใช้ในกรณีที่เกิดภัยพิบัติที่ไซต์หลัก ข้อมูลสำรอง (Backup) สำหรับแอปพลิเคชันที่สำคัญทั้งหมดถูกเก็บไว้ใน **Slave Server (HOSxPeX4)** 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	Recovery Sequence
ระบบ HOSXPEX4	ระบบการเงิน	6 ชม.	4 ชม.	2 ชม.	0	0
ระบบ LIS	การซัพพอร์ต	6 ชม.	2 ชม.	1 ชม.	1	1
ระบบ PACS	การซัพพอร์ต	6 ชม.	2 ชม.	1 ชม.	2	2

หมายเหตุ : ระดับความสำคัญในการกู้คืน 0 คือสูงสุด ลำดับการกู้คืนจะเริ่มต้นด้วยการกู้คืนระบบบัญชี ที่มีความสำคัญสูงสุดก่อน

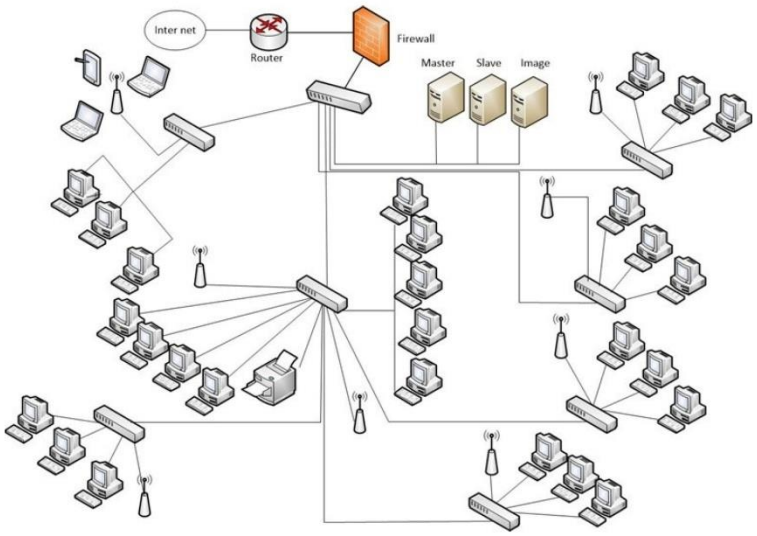
4.3. Recovery Assumptions

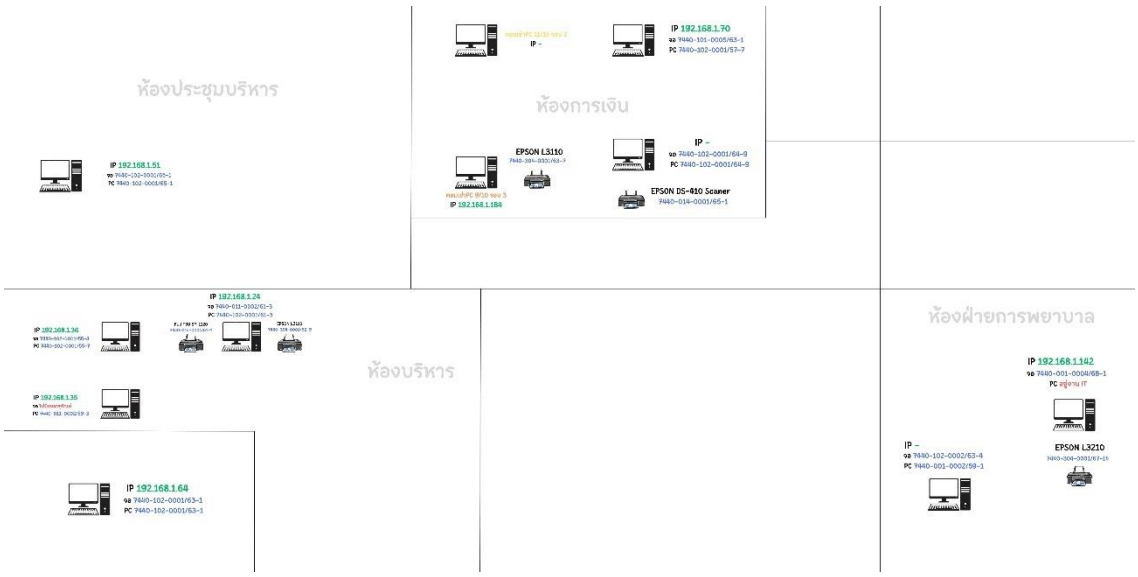
ข้อสมมุติฐานต่อไปนี้เป็นเงื่อนไขที่พิจารณาเมื่อพัฒนาลำดับความสำคัญในการกู้คืนและลำดับการกู้คืนสำหรับระบบที่อยู่ในขอบเขตของการกู้คืนจากภัยพิบัติที่มีผลต่อธุรกิจ

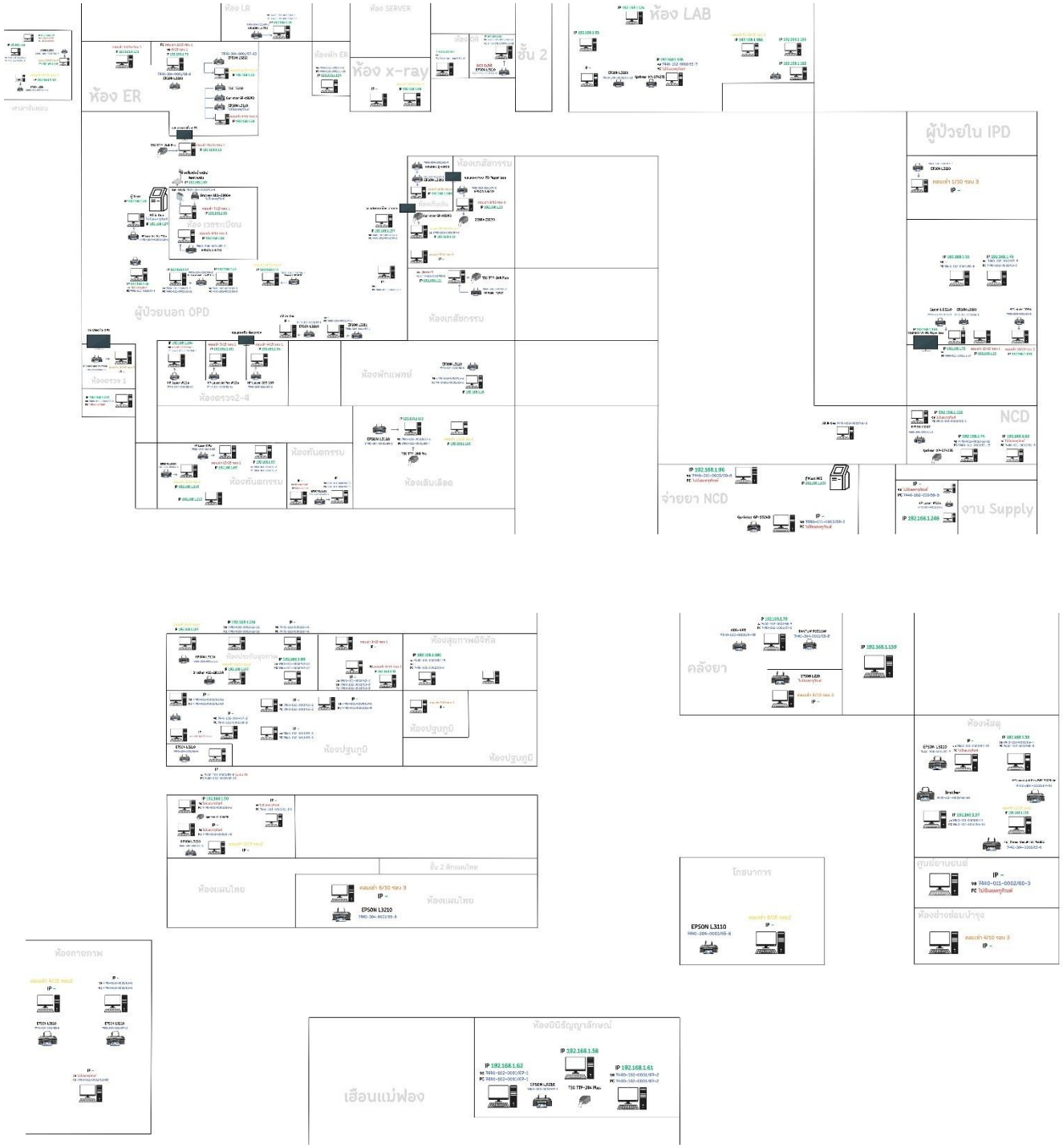
- การสำรองข้อมูลและกำหนดการถูกดำเนินการในลักษณะที่สอดคล้องกับข้อกำหนด RTO (Recovery Time Objective) ของธุรกิจ และได้รับการทดสอบเป็นระยะ เพื่อให้แน่ใจว่าอยู่ในสภาพที่สามารถกู้คืนได้ดี
- ผู้ให้บริการโทรคมนาคมได้รับการแจ้งเกี่ยวกับกระบวนการและขั้นตอนอย่างดี เพื่อให้สามารถขยายการสนับสนุนในกรณีที่เกิดภัยพิบัติ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

5. Business Continuity Recovery Process Overview

5.1 Business Continuity Recovery Architecture Overview







แสดง Network Diagram

1. สถานที่ตั้งทางกายภาพ – ศูนย์ข้อมูลหลักที่โรงพยาบาลแม่ลาว
ศูนย์ข้อมูลหลักตั้งอยู่ที่ ชั้น 2 ตึกผู้ป่วยนอกใหม่
โรงพยาบาลแม่ลาว
ที่อยู่ 309 ม. 3 ต.จอมหมอกแก้ว อ.แม่ลาว จ.เชียงราย 57250
ศูนย์ข้อมูลสำรองอยู่ที่
2. บริการโทรคมนาคม - ศูนย์ข้อมูลสำรองจะเชื่อมต่อกับอินเทอร์เน็ต
3. การสำรองฮาร์ดแวร์และการทำงานแบบสำรอง – ฮาร์ดแวร์สำรองจะถูกจัดเตรียมที่สถานที่สำรองในกรณีที่เกิดภัยพิบัติที่ไซต์หลัก

รายละเอียดการติดต่อของผู้ขายมีดังนี้

อุปกรณ์	รายละเอียด
Server Supplier หจก.เชียงราย เทคโนคอม Tel 086-420-1849	เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 1 ราคา 130,000 บาท คุณลักษณะพื้นฐาน - มีหน่วยประมวลผลกลาง (CPU) แบบ 10 แกนหลัก (10 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.2 GHz จำนวนไม่น้อยกว่า 1 หน่วย - หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 13 MB - มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า มีขนาดไม่น้อยกว่า 128 GB - สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5 - มีหน่วยจัดเก็บข้อมูลชนิด SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที ขนาดความจุไม่น้อยกว่า 1 TB หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 4 หน่วย - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง - มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

อุปกรณ์	รายละเอียด
Notebook Supplier หจก.เชียงราย เทคโนคอม Tel 086-420-1849	เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล ราคา 24,000 บาท คุณลักษณะพื้นฐาน - มีหน่วยประมวลผลกลาง (CPU) ที่มีแกนหลักรวมกันไม่น้อยกว่า 8 แกนหลัก (8 core) และแกนเสมือนรวมกันไม่น้อยกว่า 8 แกนเสมือน (8 Thread) และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.0 GHz จำนวน 1 หน่วย - หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level)เดียวกันขนาดไม่น้อยกว่า 12 MB - มีหน่วยความจำหลัก (RAM) ชนิด DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB - มีหน่วยจัดเก็บข้อมูลชนิด Solid State Drive ขนาดความจุไม่น้อยกว่า 500 GB จำนวน 1 หน่วย - มีจอภาพที่รองรับความละเอียดไม่น้อยกว่า 1,920 x 1,080 pixel และมีขนาดไม่น้อยกว่า 14 นิ้ว - มีกล้องความละเอียดไม่น้อยกว่า 1,280 x 720 pixel หรือ 720p - มีช่องเชื่อมต่อ (Interface) แบบ USB 2.0 หรือดีกว่า ไม่น้อยกว่า 3 ช่อง - มีช่องเชื่อมต่อแบบ HDMI หรือ VGA จำนวนไม่น้อยกว่า 1 ช่อง - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่าแบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวนไม่น้อยกว่า 1 ช่อง - สามารถใช้งานได้ไม่น้อยกว่า Wi-Fi (IEEE 802.11 ax) และ Bluetooth480 GB จำนวนไม่น้อยกว่า 2 หน่วย - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่าจำนวนไม่น้อยกว่า 2 ช่อง - มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

5.2 Core Services Recovery Overview

ส่วนนี้อธิบายขั้นตอนระดับสูงที่จำเป็นสำหรับการกู้คืนจากภัยพิบัติ ขั้นตอนเฉพาะจะอ้างอิงจากเอกสารที่มีอยู่แล้วในกรณีที่จำเป็น

- ระบบ HOSXPEX4 : จำเป็นสำหรับการดำเนินงานทางการบริการภาคประชาชน การจ่ายยา การชำระเงิน
- ระบบ LIS : มีความสำคัญต่อการให้บริการงลูกค้า ด้านการบริการตรวจทางห้องปฏิบัติการ
- ระบบ Pacs : มีความสำคัญต่อการให้บริการงลูกค้า ด้านการบริการดูภาพ X-ray

5.3 Application Recovery Overview

1. การกู้คืนแอปพลิเคชันจะดำเนินการที่สถานที่สำรองตามระดับความรุนแรงของภัยพิบัติที่ไซต์หลัก
   - ระบบ HOSXPEX4 จะถูกกู้คืนเมื่อมีการเชื่อมต่อเครือข่ายผ่าน VPN และทำการ Restore Backup
   - ระบบ LIS จะถูกกู้คืนเมื่อมีการเชื่อมต่อเครือข่ายผ่าน VPN และทำการ Restore Backup
   - ระบบ PACS จะถูกกู้คืนเมื่อมีการเชื่อมต่อเครือข่ายผ่าน VPN 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 HOSXPEX4					◯							
ระบบ Lis					◯							
ระบบ Pacs					◯							

7.3 กรณีทดสอบการขึ้นระบบ HOSxPeX4

1. ทำการติดตั้ง ระบบ Slave HOSxPeX4 Server (Hardware and Software) และติดตั้งให้อยู่คนละทีเดียวกับ Primary HOSxPeX4 Server
2. ทำการตั้งค่าให้มีการสำรองข้อมูลแบบต่อเนื่อง (Real Time)
3. ทำการตั้งค่าให้ Slave HOSxPeX4 Server อยู่คนละวงเดียวกับ Primary HOSxPeX4 Server
4. ทำการเชื่อมโยง 1 computer ให้เชื่อมโยงเข้ากับ Slave HOSxPeX4 Server
5. ดำเนินการทดสอบระบบ เช่น Access Test, Function Test และดูว่าข้อมูลเป็นปัจจุบันหรือไม่
6. จบขั้นตอนการทดสอบ ถ้าผลการทดสอบเป็นที่น่าพอใจ
7. ถ้าผลการทดสอบมีปัญหา ต้องทำการแก้ไขปัญหา หาสาเหตุหรือทำการ Restore ข้อมูลใหม่อีกครั้ง

7.4 กรณีทดสอบการขึ้นระบบ Lis

1. ทำการติดตั้ง ระบบ Slave Lis Server (Hardware and Software) และติดตั้งให้อยู่คนละทีเดียวกับ Primary GTW Server
2. ทำการตั้งค่าให้มีการสำรองข้อมูลแบบต่อเนื่อง (Real Time)
3. ทำการตั้งค่าให้ Slave Lis Server อยู่คนละวงเดียวกับ Primary Lis Server
4. ทำการเชื่อมโยง 1 computer ให้เชื่อมโยงเข้ากับ Slave Lis Server
5. ดำเนินการทดสอบระบบ เช่น Access Test, Function Test และดูว่าข้อมูลเป็นปัจจุบันหรือไม่
6. จบขั้นตอนการทดสอบ ถ้าผลการทดสอบเป็นที่น่าพอใจ
7. ถ้าผลการทดสอบมีปัญหา ต้องทำการแก้ไขปัญหา หาสาเหตุหรือทำการ Restore ข้อมูลใหม่อีกครั้ง

7.5 กรณีทดสอบการขึ้นระบบ PACS

ทำการติดตั้ง ระบบ Slave PACS Server (Hardware and Software) และติดตั้งให้อยู่คนละทีเดียวกับ Primary PACS Server

1. ทำการตั้งค่าให้มีการสำรองข้อมูลแบบต่อเนื่อง (Real Time)
2. ทำการตั้งค่าให้ Slave PACS Server อยู่คนละวงเดียวกับ Primary PACS Server
3. ทำการเชื่อมโยง 1 computer ให้เชื่อมโยงเข้ากับ Slave PACS Server
4. ดำเนินการทดสอบระบบ เช่น Access Test, Function Test และดูว่าข้อมูลเป็นปัจจุบันหรือไม่
5. จบขั้นตอนการทดสอบ ถ้าผลการทดสอบเป็นที่น่าพอใจ
6. ถ้าผลการทดสอบมีปัญหา ต้องทำการแก้ไขปัญหา หาสาเหตุหรือทำการ Restore ข้อมูลใหม่อีกครั้ง

8. Business Continuity Plan Business Approval

แผนการกู้คืนความต่อเนื่องทางธุรกิจที่บันทึกไว้ในขั้นตอนนี้และเอกสารสนับสนุนที่เกี่ยวข้อง ได้รับการตรวจสอบและอนุมัติโดยทีมผู้บริหารระดับสูงของโรงพยาบาลแม่ลาว... โดยสมาชิกในทีมได้ลงนามและอนุมัติเอกสารดังนี้

9. Related Document (เอกสารที่เกี่ยวข้อง)

รหัสเอกสาร	ชื่อเอกสาร
	รายงานการทดสอบระบบ

ลงชื่อ	ลงชื่อ	ลงชื่อ
นพ.สุขชัย เธียรเศวตตระกูช	นายพรศักดิ์ ตามวงค์	นายสุทธิชัย เสาว์สิงห์
CISO	HIS	Lead Implementer
วันที่ 25/12/2568	วันที่ 25/12/2568	วันที่ 25/12/2568