แผนกู้คืนระบบเทคโนโลยีสารสนเทศ
(Disaster Recovery Plan: DRP)
โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

จัดทำโดย

กลุ่มงานเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗
ฉบับ พ.ศ. ๒๕๖๙

คำนำ

แผนกู้คืนระบบสารสนเทศจากสภาวะวิกฤต (Disaster Recovery Plan: DRP) ฉบับนี้ จัดทำขึ้นเพื่อให้โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีแนวทางปฏิบัติงานที่ชัดเจนและเป็นระบบ ในการตอบโต้กับสถานการณ์ฉุกเฉินทางเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น ไม่ว่าจะเป็นภัยคุกคามทางไซเบอร์ เหตุขัดข้องจากอุปกรณ์หลัก หรือภัยพิบัติต่าง ๆ ซึ่งอาจส่งผลกระทบโดยตรงต่อความต่อเนื่องในการให้บริการทางการแพทย์และความปลอดภัยของข้อมูลผู้ป่วย

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ตระหนักถึงความสำคัญของการบริหารจัดการความเสี่ยงในยุคดิจิทัล จึงได้ออกแบบแผนฉบับนี้ให้สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมุ่งเน้นที่การกู้คืนระบบสำคัญให้กลับมาพร้อมใช้งานภายในระยะเวลาที่กำหนด (RTO) และรักษาความสมบูรณ์ของข้อมูลให้สูญหายน้อยที่สุด (RPO) เพื่อให้บุคลากรทางการแพทย์สามารถปฏิบัติหน้าที่ได้อย่างต่อเนื่อง และสร้างความเชื่อมั่นให้แก่ผู้รับบริการว่าข้อมูลสุขภาพจะได้รับการปกป้องและกู้คืนได้อย่างทันท่วงทีตามมาตรฐานความมั่นคงปลอดภัยทางสารสนเทศ

หวังเป็นอย่างยิ่งว่า แผนฉบับนี้จะเป็นกลไกสำคัญในการบริหารจัดการสภาวะวิกฤตของโรงพยาบาล และเป็นคู่มือปฏิบัติงานที่ทรงประสิทธิภาพสำหรับเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อสร้างความมั่นคงปลอดภัยและความยั่งยืนให้กับระบบสารสนเทศของโรงพยาบาลต่อไป

กลุ่มงานเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗
มิถุนายน ๒๕๖๙

สารบัญ

แผนกู้คืนระบบสารสนเทศจากสภาวะวิกฤต
(Information Technology Disaster Recovery Plan: DRP)
โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

แผนกู้คืนระบบสารสนเทศจากสภาวะวิกฤต (Disaster Recovery Plan: DRP) จัดทำขึ้นเพื่อให้กลุ่มงานเทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มีขั้นตอนการตอบสนองและปฏิบัติงานที่เป็นระบบในการกู้คืนระบบสารสนเทศและฐานข้อมูลสำคัญ เมื่อเกิดเหตุการณ์วิกฤตหรือสถานการณ์ฉุกเฉิน ทั้งจากภัยคุกคามทางไซเบอร์ อุบัติภัยต่อโครงสร้างพื้นฐาน หรือความผิดพลาดร้ายแรงของระบบ โดยมุ่งเน้นการลดระยะเวลาที่ระบบหยุดชะงักและป้องกันการสูญหายของข้อมูลผู้ป่วย การที่หน่วยงานขาดแผนกู้คืนระบบที่มีประสิทธิภาพ อาจส่งผลกระทบอย่างรุนแรงต่อการให้บริการทางการแพทย์ เช่น การไม่สามารถเข้าถึงประวัติการรักษาในระบบสารสนเทศสำหรับให้บริการผู้ป่วย (HOSxP) การหยุดชะงักของระบบจัดการภาพถ่ายทางการแพทย์ (PACS) หรือระบบเอกสารอิเล็กทรอนิกส์ (IPD Paperless) ดังนั้น การจัดทำแผน DRP จึงเป็นหัวใจสำคัญในการนำระบบสารสนเทศที่เสียหายกลับมาให้บริการได้อย่างปกติภายในระยะเวลาที่กำหนด เพื่อรองรับการทำงานของแผนบริหารความต่อเนื่อง (BCP) และลดระดับความรุนแรงของผลกระทบต่อความปลอดภัยของผู้ป่วย

กรอบแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต ๔ ขั้นตอน คือ

๑. การป้องกันและเฝ้าระวัง

การจัดทำระบบสำรองข้อมูลหลายระดับ (Multi-tier Backup) และการตรวจสอบความพร้อมของระบบแม่ข่ายเป็นประจำ

๒. การเตรียมความพร้อมทางเทคนิค

การจัดเตรียมโครงสร้างพื้นฐานสำรองและเครื่องมือในการกู้คืนระบบ (Recovery Tools) เพื่อรองรับสถานการณ์วิกฤตตามบทบาทหน้าที่อย่างเป็นระบบ

๓. การซักซ้อมและทดสอบการกู้คืน

การจัดกิจกรรมทดสอบการกู้คืนข้อมูล (Restore Test) และการซ้อมแผนจำลองสถานการณ์ (DRP Drill) เพื่อยืนยันว่าแผนงานสามารถปฏิบัติได้จริง

๔. การกู้คืนและปรับปรุง

การดำเนินการกู้คืนระบบตามลำดับความสำคัญ และการวิเคราะห์หาสาเหตุเพื่อพัฒนาระบบป้องกันให้ดียิ่งขึ้น

โดยแนวคิดการกู้คืนระบบสารสนเทศของกลุ่มงานเทคโนโลยีสารสนเทศ คือ การบริหารจัดการทรัพยากรดิจิทัลและฐานข้อมูลให้มีความมั่นคงปลอดภัยและพร้อมกู้คืนได้ทันท่วงที เพื่อรักษามาตรฐานการบริการและความเชื่อมั่นของผู้รับบริการเป็นสำคัญ

หมวดที่ ๑ วัตถุประสงค์และขอบเขต

๑.๑ วัตถุประสงค์

๑. เพื่อกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ ให้สามารถกลับสู่สภาวะปกติได้อย่างเป็นระบบ เมื่อเกิดเหตุภัยพิบัติหรืออุบัติการณ์ที่ส่งผลกระทบอย่างรุนแรงต่อโครงสร้างพื้นฐานด้านไอที

๒. เพื่อควบคุมระยะเวลาและปริมาณการสูญเสียข้อมูล ให้เป็นไปตามค่าเป้าหมาย RTO (≤ ๔ ชั่วโมง) และ RPO (≤ ๒๔ ชั่วโมง) ตามที่ระบุไว้ในวิธีปฏิบัติมาตรฐาน (SOP) การสำรองและกู้คืนข้อมูล

๓. เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของทีมกู้คืนระบบ (IT Disaster Recovery Team) ให้มีความชัดเจน รวดเร็ว และลดความสับสนในสภาวะวิกฤต

๔. เพื่อสร้างความสอดคล้องและเชื่อมโยง ระหว่างแผนกู้คืนระบบ (DRP) กับแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) และวิธีปฏิบัติมาตรฐาน (SOP) ที่เกี่ยวข้องอย่างเป็นรูปธรรม

๕. เพื่อใช้เป็นแนวทางในการทดสอบ (Drill) ซักซ้อม และทบทวนแผน ให้มีความพร้อมต่อสถานการณ์ปัจจุบันและมีประสิทธิภาพในการใช้งานจริงอยู่เสมอ

๑.๒ ขอบเขต

แผนกู้คืนระบบฉบับนี้ครอบคลุมระบบสารสนเทศและโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของโรงพยาบาล โดยแบ่งออกเป็น ๔ กลุ่มหลัก ดังนี้

กลุ่มที่ ๑ ระบบแอปพลิเคชันและฐานข้อมูลหลัก (Core Application & Database)

- ระบบสารสนเทศโรงพยาบาล (HIS) เช่น ระบบ HOSxP ระบบบันทึกข้อมูลผู้ป่วยอิเล็กทรอนิกส์ (IPD Paperless) และ Virtual Machine (VM) ที่เกี่ยวข้องทั้งหมด
- ระบบสนับสนุนการรักษาเฉพาะทาง เช่น ระบบห้องปฏิบัติการ (LIS) และระบบจัดเก็บภาพถ่ายทางรังสี (PACS)

กลุ่มที่ ๒ ระบบสำรองข้อมูลและสื่อบันทึกข้อมูล (Data Backup & Storage)

- ระบบ NAS Storage (Network Attached Storage) สำหรับการสำรองข้อมูลภายใน (On-site Backup)
- External Storage Drive (Offline Backup) สำหรับการสำรองข้อมูลออฟไลน์ (Offline Backup)

กลุ่มที่ ๓ ระบบเครือข่ายและโครงสร้างพื้นฐาน (Network & IT Infrastructure)

- อุปกรณ์เครือข่ายหลัก (Core Switch, Firewall, Access Point) และระบบจัดการเครือข่ายภายในโรงพยาบาล

กลุ่มที่ ๔ ระบบสนับสนุนด้านกายภาพและพลังงาน (Physical Support & Power Supply)

- ระบบสำรองไฟฟ้าต่อเนื่อง (UPS) และเครื่องกำเนิดไฟฟ้าสำรอง (Generator) เพื่อรักษาเสถียรภาพของห้องแม่ข่ายคอมพิวเตอร์

๑.๓ความสัมพันธ์ระหว่าง BCP, DRP และ SOP

เอกสาร	จุดประสงค์หลัก	ผู้ใช้งาน
BCP (แผนบริหารความต่อเนื่อง)	**ภาพรวมการบริการ** กำหนดแนวทางให้โรงพยาบาลดำเนินงานต่อได้ (เช่น ใช้ระบบ Paper/Manual) เมื่อระบบ IT ล่ม	เจ้าหน้าที่ทุกหน่วยงาน
DRP (แผนกู้คืนระบบ)	**การตอบโต้ด้าน IT** ขั้นตอนการกู้คืนระบบ Infrastructure และฐานข้อมูลให้กลับมาใช้งานได้ตามค่า RTO	ทีมกลุ่มงานเทคโนโลยีสารสนเทศ
SOP (วิธีปฏิบัติมาตรฐาน)	เทคนิครายขั้นตอน: รายละเอียดเชิงลึก เช่น วิธี Backup ข้อมูล, วิธี Restore VM หรือวิธีสลับสาย Network	เจ้าหน้าที่ IT ผู้รับผิดชอบ

หมวดที่ SOP ตาม (RTO / RPO) เป้าหมายการกู้คืน ๒

๒.๑ตัวชี้วัดและเป้าหมายการกู้คืน)Metrics & Objectives)

ตัวชี้วัด	ความหมาย	ค่าเป้าหมาย (ตาม SOP)
RPO (Recovery Point Objective)	จุดที่ข้อมูลสูญหายได้สูงสุด (ปริมาณข้อมูลสูงสุดที่ยอมสูญหายได้)	≤ ๒๔ ชั่วโมง
RTO (Recovery Time Objective)	ระยะเวลาสูงสุดที่ยอมรับได้ สำหรับการกู้คืนระบบให้กลับมาพร้อมใช้งาน	≤ ๔ ชั่วโมง
MTD (Maximum Tolerable Downtime)	ระยะเวลาหยุดทำงานสูงสุดก่อนผลกระทบร้ายแรง	≤ ๘ ชั่วโมง

๒.๒เป้าหมายการกู้คืนรายระบบ (System Recovery Objectives)

ระบบงาน	ระดับความสำคัญ	RPO	RTO	แหล่ง Backup อ้างอิง SOP
HOSxP (HIS หลัก)	วิกฤต	≤ ๒๔ ชม.	≤ ๔ ชม.	Server ⟶ NAS ⟶ External Drive
IPD Paperless	วิกฤต	≤ ๒๔ ชม.	≤ ๖ ชม.	VM Backup ⟶ NAS
Virtual Machine (VM)	วิกฤต	≤ ๒๔ ชม.	≤ ๔ ชม.	VM Backup ⟶ NAS
LIS (ห้องปฏิบัติการ)	สูง	≤ ๒๔ ชม.	≤ ๖ ชม.	Server ⟶ NAS ⟶ External Drive
PACS (รังสีวิทยา)	สูง	≤ ๒๔ ชม.	≤ ๖ ชม.	NAS Storage (RAID)
NAS Storage	วิกฤต	N/A	ทันที	External Drive (Offline)
ระบบเครือข่าย (Network)	วิกฤต	N/A	≤ ๑ ชม.	Config Backup บน NAS
Thairefer / อินเทอร์เน็ต	ปานกลาง	≤ ๒๔ ชม.	≤ ๘ ชม.	Server Backup

หมวดที่ ๓โครงสร้าง ๓ Backupระดับชั้น (SOP ตาม)

เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญของโรงพยาบาลจะมีความพร้อมใช้งานและสามารถกู้คืนได้ในทุกสถานการณ์ โรงพยาบาลจึงกำหนดสถาปัตยกรรมข้อมูลสำรองตามวิธีปฏิบัติมาตรฐาน (SOP) ไว้ ๓ ระดับ ดังนี้

Backup ภาพรวมสถาปัตยกรรม ๓.๑

ระดับ	ประเภทการสำรองข้อมูล	สื่อบันทึกข้อมูล	ความถี่ (Frequency)	บทบาทหน้าที่ในแผน DRP
ระดับ ๑	Hot Backup / VM Snapshot การสำรอง Server Backup (Full + VM Snapshot)	Server หลัก / Host VM	ทุกวัน (Daily)	ใช้กู้คืนระบบอย่างรวดเร็วเป็นอันดับแรก (Primary Restore)
ระดับ ๒	Warm Backup (On-site) การสำรอง NAS Storage Backup	Network Attached Storage (NAS)	ทุกวัน (Sync/Daily)	ใช้กู้คืนกรณีเครื่องแม่ข่ายหลักเสียหาย หรือระบบ VM ผิดปกติ (ระดับ ๑ ล้มเหลว)
ระดับ ๓	Cold Backup (Offline) การสำรอง External Storage	External Storage Drive	สัปดาห์ละ ๑ ครั้ง / ตามกำหนด	ใช้กู้คืนกรณีเกิดภัยพิบัติร้ายแรง, NAS เสียหาย หรือถูกโจมตีด้วย Ransomware

๓) นโยบายการเก็บรักษาข้อมูลสำรอง ๒.Backup Retention Policy)

ระดับ	ระยะเวลาเก็บ (Retention)	เหตุผลและความจำเป็น
ระดับ ๑ (Server/VM)	๗ - ๓๐ วัน	เพื่อใช้กู้คืนอุบัติการณ์ที่เพิ่งเกิดขึ้น (Immediate Recovery) เน้นความรวดเร็ว
ระดับ ๒ (NAS)	๑ - ๓ เดือน	เพื่อเป็นประวัติข้อมูลย้อนหลัง กรณีตรวจพบความผิดปกติของข้อมูลในภายหลัง
ระดับ ๓ (Offline)	๑ - ๑๐ ปี	ตามระเบียบงานสารบรรณ/กฎหมาย (ข้อมูลเวชระเบียนต้องเก็บอย่างน้อย ๕-๑๐ ปี)

๓.๓ รายละเอียดการปฏิบัติงานในแต่ละระดับ

ระดับที่ ๑ Server/VM Backup (Primary Recovery)

(๑) ดำเนินการสำรองข้อมูลแบบเต็มรูปแบบ (Full Backup) ทุกวัน หลังเวลา ๐๐.๐๐ น.

(๒) จัดทำ VM Snapshot สำหรับระบบ HOSxP และระบบวิกฤตอื่น ๆ เป็นประจำทุกวัน

(๓) กำหนดระยะเวลาจัดเก็บข้อมูลอย่างน้อย ๓๐ วัน บนระบบเครื่องแม่ข่ายหลัก

(๔) เจ้าหน้าที่ผู้รับผิดชอบดำเนินการตรวจสอบความสมบูรณ์ของไฟล์สำรองข้อมูลทุกเช้าตามที่ระบุใน SOP

ระดับที่ ๒ NAS Storage (Secondary Recovery)

(๑) ดำเนินการคัดลอกข้อมูล (Synchronization) จากเครื่องแม่ข่ายไปยังระบบ NAS ทุกวัน

(๒) ทำหน้าที่เป็นแหล่งข้อมูลสำรองลำดับที่ ๒ กรณีเครื่องแม่ข่ายหลักหรือระบบ VM เกิดความขัดข้อง

(๓) ตรวจสอบสถานะการเชื่อมต่อ (Sync Status) และพื้นที่จัดเก็บข้อมูลอย่างสม่ำเสมอตาม SOP

ระดับที่ ๓ External Drive (Disaster Recovery & Offline Backup)

(๑) ดำเนินการสำรองข้อมูลลงสื่อบันทึกข้อมูลภายนอก (External Storage Drive) ตามรอบที่กำหนด (รายวัน/รายสัปดาห์/รายเดือน)

(๒) จัดเก็บสื่อบันทึกข้อมูลไว้ในตู้นิรภัยหรือสถานที่ปลอดภัยภายนอกห้องแม่ข่าย (Off-site Storage)

(๓) สงวนไว้สำหรับการกู้คืนกรณีฉุกเฉินร้ายแรง (เช่น การถูกโจมตีด้วย Ransomware หรือภัยพิบัติทางกายภาพ)

(๔) ข้อกำหนดความปลอดภัย ห้ามเชื่อมต่อสื่อบันทึกข้อมูลระดับ ๓ ค้างไว้กับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังข้อมูลสำรองชุดสุดท้าย

๓.๔ การตรวจสอบความพร้อมของระบบสำรองข้อมูลประจำวัน (Daily Inspection)

เจ้าหน้าที่เทคโนโลยีสารสนเทศผู้รับผิดชอบ ต้องดำเนินการตรวจสอบความพร้อมตามขั้นตอนที่ระบุในวิธีปฏิบัติมาตรฐาน (SOP) เป็นประจำทุกวัน ดังนี้

(๑) ตรวจสอบสถานะระบบบริการ

ตรวจสอบความพร้อมใช้งานของเครื่องแม่ข่าย (Server Health) และระบบสารสนเทศโรงพยาบาล (HOSxP XE) ในช่วงเวลา ๐๐.๐๐ น. หรือตามรอบเวรปฏิบัติงานที่กำหนด

(๒) ตรวจสอบความสมบูรณ์ของไฟล์สำรอง

ตรวจสอบ Error Log และขนาดไฟล์ (File Size) ของการสำรองข้อมูลจากคืนที่ผ่านมา เพื่อยืนยันว่ากระบวนการสำรองข้อมูลเสร็จสมบูรณ์และไม่มีไฟล์เสียหาย

(๓) ตรวจสอบการเชื่อมต่อข้อมูล (Sync Status)

ตรวจสอบสถานะการคัดลอกข้อมูลระหว่างเครื่องแม่ข่าย (Server) และระบบจัดเก็บข้อมูลเครือข่าย (NAS) ให้เป็นปัจจุบันและไม่มีการหยุดชะงัก

(๔) การรายงานผลและแก้ไข

บันทึกผลการตรวจสอบลงในแบบฟอร์ม Log Book ทุกวัน และรายงานหัวหน้าทีมกู้คืนระบบ (DRP Coordinator) ทันทีหากพบความผิดปกติ เพื่อดำเนินการแก้ไขให้แล้วเสร็จภายในระยะเวลาที่กำหนด

หมวดที่ ๔ทีมกู้คืนระบบ)DR Team) และบทบาทหน้าที่

เพื่อให้การดำเนินงานกู้คืนระบบสารสนเทศเป็นไปด้วยความรวดเร็วและมีประสิทธิภาพ โรงพยาบาลจึงกำหนดโครงสร้างทีมกู้คืนระบบ (IT Disaster Recovery Team) ดังนี้

๔.๑โครงสร้างและบทบาทหน้าที่ของทีม DRP

ตำแหน่งในทีม DRP	ผู้รับผิดชอบ	เหตุผลและความจำเป็น
ผู้อำนวยการแผน (DRP Coordinator)	หัวหน้ากลุ่มภารกิจด้านดิจิทัลสุขภาพ / หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ	-ประเมินความรุนแรงของสถานการณ์ - ตัดสินใจประกาศใช้แผน DRP และรหัส **"คุณเทคโน ๒"** -จั ดตั้งศูนย์ปฏิบัติการชั่วคราว (War Room) และรายงาน CIO และรายงานผู้บริหาร - ควบคุมดูแลภาพรวมการกู้คืนให้เป็นไปตาม RTO
ทีมกู้คืนระบบแม่ข่าย (Server & Virtualization Team)	เจ้าหน้าที่ IT กลุ่มงานเทคโนโลยีสารสนเทศ	ดำเนินการกู้คืนระบบระดับ ๑ (Server/VM Snapshot) และตรวจสอบความสมบูรณ์ VM - กู้คืนระบบฐานข้อมูล HOSxP และ IPD Paperless หรือระบบอื่นๆ - ทดสอบฟังก์ชันการทำงานก่อนเปิดให้ใช้งานจริง
ทีมกู้คืนข้อมูลสำรอง (Storage & Backup Team)	เจ้าหน้าที่ IT กลุ่มงานเทคโนโลยีสารสนเทศ	-ดำเนินการกู้คืนข้อมูลระดับ ๒ (NAS Storage) และระดับ ๓ (External Drive) -ตรวจสอบความถูกต้องของข้อมูลสำรอง (Data Integrity) - จัดการระบบสำรองข้อมูลกรณีถูกโจมตีด้วย Ransomware
ทีมกู้คืนระบบเครือข่าย (Network Infrastructure Team)	เจ้าหน้าที่ IT กลุ่มงานเทคโนโลยีสารสนเทศ	-กู้คืนระบบเครือข่ายหลัก (Core Switch/Firewall) - ตรวจสอบความปลอดภัยไซเบอร์และปิดช่องโหว่ก่อนกู้ข้อมูล - เป้าหมายกู้คืนระบบเครือข่ายภายใน **๑ ชั่วโมง**
ศูนย์ประสานงานรับแจ้งเหตุ (IT Help Desk)	เจ้าหน้าที่ IT - ชั้น ๑A อาคารวินิจฉัยโรคผ่าตัด และผู้ป่วยหนัก	-รับแจ้งเหตุผ่านสายด่วน ๘๒๐๗ -ประสานงานกับผู้ใช้งาน (User) -บันทึกเหตุการณ์ (Incident Log) -แจ้งความคืบหน้าให้หน่วยงานที่เกี่ยวข้องทราบ

๔.๒รหัสปฏิบัติการสื่อสารในภาวะวิกฤต (Crisis Action Codes)

เพื่อให้การประสานงานระหว่างทีมเทคโนโลยีสารสนเทศและหน่วยงานต่างๆ เป็นไปอย่างรวดเร็ว โรงพยาบาลกำหนดให้ใช้รหัสปฏิบัติการสื่อสาร ดังนี้

รหัสปฏิบัติการ	**สถานการณ์และระดับความรุนแรง**	**แนวทางปฏิบัติ (Action Plan)**
คุณเทคโน ๑	**ระดับเฝ้าระวัง** . ระบบขัดข้องบางส่วน คาดว่าจะแก้ไขให้กลับมาเป็นปกติได้ภายใน ๓๐ นาที	แจ้ง Help Desk IT (โทร ๘๒๐๗) เพื่อให้ทีม IT เร่งแก้ไข หากเกิน ๓๐ นาที ให้ยกระดับเป็น **"คุณเทคโน ๒"**
คุณเทคโน ๒	**ระดับวิกฤต** ระบบขัดข้องรุนแรง ไม่สามารถแก้ไขได้ภายใน ๓๐ นาที หรือส่งผลกระทบต่อการบริการหลัก	**ประกาศใช้แผน BCP และ DRP อย่างเป็นทางการ** โดยทีม IT เริ่มขั้นตอนการกู้คืนระบบและรายงาน CIO/ผู้บริหารโรงพยาบาลทันที
คุณเทคโน ๓	**ระดับสิ้นสุดเหตุการณ์** ระบบสารสนเทศกู้คืนสำเร็จและกลับมาทำงานได้ตามปกติ	ประกาศยกเลิก BCP/DRP แจ้งทุกหน่วยงานให้บันทึกข้อมูลย้อนหลัง และจัดทำรายงานสรุปเหตุการณ์ (Incident Report)

หมวดที่ การประเมินสถานการณ์และขั้นตอนการกู้คืน ๕

เพื่อให้การตัดสินใจประกาศใช้แผนกู้คืนระบบ (DRP) เป็นไปอย่างรวดเร็วและมีขั้นตอนปฏิบัติที่ชัดเจน โรงพยาบาลกำหนดเกณฑ์การดำเนินงาน ดังนี้

๕.๑เกณฑ์การประกาศใช้แผน DRP

ระดับความรุนแรง	ลักษณะเหตุการณ์	รหัสปฏิบัติการ	แนวทางดำเนินการ
ปานกลาง	ระบบหยุดชะงักบางส่วน คาดว่าจะแก้ไขให้เป็นปกติได้ภายใน ๓๐ นาที	คุณเทคโน ๑	ทีม IT ดำเนินการแก้ไขทันทีโดยไม่ต้องประกาศใช้แผน BCP
สูง	ระบบขัดข้องรุนแรง ไม่สามารถแก้ไขได้ภายใน ๓๐ นาที หรือมีแนวโน้มข้อมูลเสียหาย	คุณเทคโน ๒	**ประกาศใช้แผน BCP และ DRP** เริ่มการกู้คืนระดับ ๑ (Snapshot) หรือระดับ ๒ (NAS) ตามความเหมาะสม
วิกฤต	ระบบเสียหายทั้งหมด ภัยพิบัติร้ายแรง หรือถูกโจมตีด้วย Ransomware	คุณเทคโน ๒	**ประกาศใช้แผน BCP และ DRP** เริ่มการกู้คืนระดับ ๓ (Offline Backup) จากหน่วยเก็บข้อมูลภายนอกทันที

๕.๒ขั้นตอนการกู้คืนระบบแอปพลิเคชันและฐานข้อมูลหลัก

กู้คืนระบบ เช่น ระบบ HOSxP หรือ IPD Paperless (กรณีทั่วไป)

ขั้น	รายการ	ผู้รับผิดชอบ	เวลาเป้าหมาย
๑	ยืนยันสถานะความล้มเหลวของเครื่องแม่ข่ายหลัก และประเมินว่าไม่สามารถกู้คืนโดยวิธีปกติได้	ทีมกู้คืนระบบแม่ข่าย (Server Team)	๐–๑๕ นาที
๒	รายงาน DRP Coordinator เพื่อขออนุมัติเปิดศูนย์ปฏิบัติการ (War Room) ณ ชั้น ๑A และแจ้ง CIO	DRP Coordinator	๑๕ นาที
๓	ตรวจสอบความสมบูรณ์ (Integrity Check) ของไฟล์สำรองระดับ ๑ หรือ ๒ ที่จะนำมากู้คืน	ทีมกู้คืนระบบแม่ข่าย	๑๕–๓๐ นาที
๔	ดำเนินการ Failover ไปยัง Server สำรอง หรือ Restore ข้อมูลระบบ (HOSxP หรือ IPD Paperless)	ทีมกู้คืนระบบแม่ข่าย / Storage Team	๓๐–๑๒๐ นาที
๕	ทดสอบการเข้าถึงฐานข้อมูลและการใช้งานฟังก์ชันหลักจากเครื่องทดสอบ (System Verification)	ทีมกู้คืนระบบแม่ข่าย	๑๒๐–๑๘๐ นาที
๖	เมื่อระบบพร้อมใช้งาน ประกาศรหัส **"คุณเทคโน ๓"** เพื่อแจ้งทุกหน่วยงานให้ยกเลิก BCP	DRP Coordinator	≤ ๔ ชม. (RTO)
๗	บันทึกรายละเอียดเหตุการณ์ ระยะเวลากู้คืน และปัญหาที่พบลงใน DRP Incident Log	DRP Coordinator	ทันทีหลังเหตุการณ์สงบ

๕.๓ขั้นตอนกู้คืนกรณีถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware Recovery)

กรณีนี้เป็นเหตุวิกฤตระดับสูง **ห้าม** เชื่อมต่อสื่อบันทึกข้อมูลระดับ ๑ และ ๒ จนกว่าจะมั่นใจว่าปลอดภัย และให้เน้นการกู้คืนจาก Offline Backup (ระดับ ๓) เป็นลำดับแรก

ขั้นตอน	รายการปฏิบัติการ	ผู้รับผิดชอบ
๑	ดำเนินการ **"Isolate & Contain"** เพื่อตัดการเชื่อมต่อเครื่องแม่ข่ายและ Segment เครือข่ายที่ติดเชื้อออกจากระบบทันทีเพื่อหยุดการแพร่กระจาย	ทีมกู้คืนระบบเครือข่าย
๒	รายงานเหตุการณ์ต่อ ผู้อำนวยการแผน DRP Coordinator เพื่อแจ้ง CIO และผู้อำนวยการโรงพยาบาล และประกาศใช้แผน BCP สำหรับทุกหน่วยงาน ประกาศ **"คุณเทคโน ๒"**	ศูนย์ประสานงานรับแจ้งเหตุ (Help Desk)
๓	ดำเนินการ **"Forensic & Assessment"** ประเมินขอบเขตความเสียหายและตรวจสอบว่า Backup ระดับ ๑ (Snapshot) และ ๒ (NAS) ถูกเข้ารหัส (Encrypted) หรือไม่	ทีมกู้คืนระบบแม่ข่าย
๔	จัดเตรียมสื่อบันทึกข้อมูลระดับ ๓ External Storage Drive (Offline Backup) และตรวจสอบความสมบูรณ์ของไฟล์สำรองบนเครื่องที่ตัดการเชื่อมต่อเครือข่าย	ทีมกู้คืนข้อมูลสำรอง (Storage & Backup)
๕	ดำเนินการ **"System Rebuild"** ล้างข้อมูล (Format) และติดตั้งระบบปฏิบัติการ (OS) ใหม่ทั้งหมดบนเครื่องแม่ข่ายเป้าหมาย	ทีมกู้คืนระบบแม่ข่าย
๖	ดำเนินการ **"Data Restore"** กู้คืนฐานข้อมูลและไฟล์ระบบจาก Offline Backup พร้อมตรวจสอบความถูกต้องของข้อมูล (Integrity)	ทีมกู้คืนข้อมูลสำรอง (Storage & Backup)
๗	ดำเนินการ **"Security Scan"** ตรวจสอบระบบด้วยเครื่องมือความปลอดภัย (Antivirus/EDR) ให้มั่นใจ ๑๐๐% ก่อนเชื่อมต่อกลับเข้าสู่เครือข่ายหลัก	ทีมกู้คืนระบบแม่ข่าย
๘	ปิดช่องโหว่ (Patching) และประกาศ **"คุณเทคโน ๓"** เมื่อระบบพร้อมใช้งาน และรายงานผู้บริหารทราบ	ผู้อำนวยการแผน (DRP Coordinator)
๙	ดำเนินการ **"External Reporting"** รายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงานกำกับดูแลตามลำดับชั้น (ภายใน ๒๔ ชม.)	ผู้อำนวยการแผน (DRP Coordinator)

๕.๔ขั้นตอนการกู้คืนข้อมูลสำรองทั่วไป (Standard Data Recovery)

ใช้สำหรับกรณีข้อมูลบางส่วนสูญหาย ไฟล์ฐานข้อมูลเสียหาย หรือระบบขัดข้องที่ไม่ได้เกิดจากมัลแวร์เรียกค่าไถ่ โดยเน้นความเร็วในการกู้คืนตามลำดับชั้น Backup

ขั้นตอน	รายการปฏิบัติการ	ผู้รับผิดชอบ	เวลาเป้าหมาย
๑	**ประเมินความเสียหาย** ระบุขอบเขตข้อมูลที่เสียหาย (เช่น เฉพาะตารางข้อมูล หรือทั้ง VM) และช่วงเวลาที่ข้อมูลยังสมบูรณ์ล่าสุด (Point in Time)	ทีมกู้คืนข้อมูลสำรอง	๑๕ นาที
๒	**เลือกแหล่งข้อมูล** พิจารณาเลือกใช้ Backup เริ่มจาก ระดับ ๑ (Snapshot) หากไม่ได้ผลจึงขยับไป ระดับ ๒ (NAS) ตามลำดับ เริ่มจากระดับ ๑ ⟶ ๒ ⟶ ๓ ตามลำดับ	ทีมกู้คืนข้อมูลสำรอง	๑๕ นาที
๓	**ตรวจสอบความพร้อม** ตรวจสอบความสมบูรณ์ของไฟล์สำรอง (Integrity Check) และขนาดไฟล์ให้ตรงตาม Log ใน SOP ก่อนเริ่ม Restore	ทีมกู้คืนข้อมูลสำรอง	๑๕ - ๓๐ นาที
๔	**ดำเนินการกู้คืน** Restore ข้อมูลหรือ Rollback VM กลับไปยังสถานะที่ใช้งานได้ และตรวจสอบความถูกต้องของโครงสร้างฐานข้อมูล	ทีมกู้คืนข้อมูลสำรอง	๓๐ - ๑๒๐ นาที
๕	**ทดสอบระบบ** ตรวจสอบการเชื่อมต่อระหว่างฐานข้อมูลและแอปพลิเคชัน (HOSxP/IPD Paperless) ว่าทำงานสัมพันธ์กันปกติ	ทีมกู้คืนข้อมูลสำรอง	๓๐ นาที
๖	**ประเมิน RPO** สรุปปริมาณข้อมูลที่สูญหาย (Data Loss) หากมีข้อมูลหายเกินกว่า RPO ๒๔ ชม. ให้รีบรายงานหัวหน้าทีมเพื่อวางแผนกู้คืนเพิ่มเติม	ผู้อำนวยการแผน (DRP)	ทันที
๗	**ประสานงานผู้ใช้** แจ้งหน่วยงานผ่าน Help Desk เพื่อให้เริ่มการบันทึกข้อมูลย้อนหลัง (Back-entry) ให้เสร็จสิ้นภายใน ๒๔ ชม. ตามแผน BCP	ศูนย์ประสานงาน (Help Desk)	ทันที
๘	บันทึกและสรุป บันทึกเวลาที่ใช้และผลการกู้คืนลงใน DRP Incident Log เพื่อใช้เป็นข้อมูลในการปรับปรุงแผนครั้งถัดไป	ผู้อำนวยการแผน (DRP)	๑ วันหลังเหตุการณ์

๕การรายงานเหตุการณ์ต่อหน่วยงานกำกับดูแลภายนอก ๕.

ในกรณีที่อุบัติการณ์สารสนเทศเข้าข่ายภัยคุกคามทางไซเบอร์ระดับ "ร้ายแรง" หรือ "วิกฤต" (เช่น การถูกโจมตีด้วย Ransomware หรือข้อมูลผู้ป่วยรั่วไหล) ผู้อำนวยการแผน (DRP Coordinator) มีหน้าที่ต้องดำเนินการรายงานต่อหน่วยงานภายนอกตามกำหนดระยะเวลาทางกฎหมาย ดังนี้

หน่วยงานที่รับรายงาน	ระยะเวลาที่ต้องแจ้ง	ช่องทางการติดต่อ / ข้อมูลที่ต้องระบุ
๑. ศูนย์ประสานงาน สสจ. และ MOPH-CERT	**ทันที** หรือภายใน ๒๔ ชม.	แจ้งเหตุเพื่อขอรับการสนับสนุนทางเทคนิค และประสานงานเฝ้าระวังภัยระดับจังหวัด
๒. สกมช. (NCSA)	ภายใน ๒๔ ชม.	รายงานตามแบบฟอร์มภัยคุกคามไซเบอร์ระดับร้ายแรง ตาม พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๓. สคส. (PDPC)	ภายใน ๗๒ ชม.	กรณีพบว่ามีการละเมิดข้อมูลส่วนบุคคล (Data Breach) ตามข้อกำหนดของ พรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

รายละเอียดข้อมูลที่ต้องรายงาน (Incident Brief)

(ก) วันและเวลาที่ตรวจพบเหตุการณ์

(ข) ประเภทของภัยคุกคาม (เช่น มัลแวร์เรียกค่าไถ่ หรือการเข้าถึงโดยไม่ได้รับอนุญาต)

(ค) ระบบสารสนเทศและจำนวนข้อมูลที่ได้รับผลกระทบ

(ง) มาตรการเบื้องต้นที่โรงพยาบาลได้ดำเนินการไปแล้ว (Containment)

(จ) ชื่อและเบอร์โทรศัพท์ของผู้ประสานงานหลักของทีม DRP

หมวดที่ การตรวจสอบและบำรุงรักษาเชิงป้องกัน ๖

เพื่อให้มั่นใจว่าแผนกู้คืนระบบสารสนเทศ (DRP) และข้อมูลสำรองมีความพร้อมใช้งานอยู่เสมอ โรงพยาบาลจึงกำหนดแนวทางการตรวจสอบและซักซ้อม ดังนี้

๖.๑การตรวจสอบประจำวัน (Daily Inspection - ตาม SOP)

ให้ดำเนินการตามรายละเอียดในข้อ ๓.๔ ของแผนฉบับนี้

๖.๒การตรวจสอบตามรอบและการซักซ้อมแผน (Testing Schedule)

กิจกรรม	ความถี่	ผู้รับผิดชอบ
ทดสอบการกู้คืนระบบระดับ ๑ (Restore from Snapshot)	ทุกเดือน	ทีมกู้คืนระบบแม่ข่าย
ทดสอบการกู้คืนระบบระดับ ๒ (Restore from NAS)	ทุก ๓ เดือน	ทีมกู้คืนข้อมูลสำรอง
ทดสอบการกู้คืนระบบระดับ ๓ (Restore from External Drive)	ทุก ๖ เดือน	ทีมกู้คืนข้อมูลสำรอง
ทดสอบระบบสำรอง (VM Failover) สำหรับ HOSxP XE	ทุก ๖ เดือน	ทีมกู้คืนระบบแม่ข่าย
การซักซ้อมแผนบนโต๊ะ (Tabletop Exercise) จำลองสถานการณ์	ปีละ ๑ ครั้ง	ผู้อำนวยการแผน (DRP Coordinator)
การซักซ้อมแผนกู้คืนเต็มรูปแบบ (Full DR Drill)	ปีละ ๑ ครั้ง	ทีม IT ทั้งหมด
ตรวจสอบเป้าหมาย RPO และ RTO ให้เป็นไปตามมาตรฐาน	ทุก ๖ เดือน	ผู้อำนวยการแผน (DRP Coordinator)
การทบทวนและปรับปรุงแผน DRP ให้ทันสมัย	ปีละ ๑ ครั้ง*	ผู้อำนวยการแผน (DRP Coordinator)

หมายเหตุ: ให้มีการทบทวนแผนทันทีหากมีการเปลี่ยนแปลงโครงสร้างระบบ IT ที่สำคัญ หรือพบข้อบกพร่องจากการซักซ้อมแผน

หมวดที่ ๗การทดสอบและซักซ้อมแผน DRP (DRP Testing & Drill)

เพื่อให้มั่นใจว่าบุคลากรมีความเข้าใจและระบบสำรองข้อมูลสามารถใช้งานได้จริงตามค่าเป้าหมาย RTO/RPO โรงพยาบาลจึงกำหนดรูปแบบการทดสอบ ดังนี้

๗.๑ประเภทการทดสอบและเกณฑ์การประเมินผล

ประเภทการทดสอบ	รายละเอียด	ความถี่	เกณฑ์ผ่าน
Restoration Test	ทดสอบสุ่มกู้คืนไฟล์ฐานข้อมูลจริง (Restore Backup) และตรวจความสมบูรณ์ (Integrity Check)	รายเดือน	กู้คืน(Restore) ได้สำเร็จและข้อมูลถูกต้อง ๑๐๐%
Failover Test (VM)	ทดสอบการสลับไปใช้ HOSxP บน VM สำรอง (ระดับ ๑)	ทุก ๖ เดือน	ระบบพร้อมใช้งานภายใน ๓๐ นาที
Offline Backup Drill	ทดสอบกู้คืนระบบจาก External Drive (ระดับ ๓) ตรวจสอบ Offline Backup ใช้ได้จริง กรณีจำลอง Ransomware	ทุก ๖ เดือน	เป็นไปตามเกณฑ์ RTO และ RPO ที่กำหนดไว้ในข้อ ๒.๒ ของแผนฉบับนี้
Tabletop Exercise	จำลองสถานการณ์วิกฤตบนโต๊ะ เพื่อซักซ้อมการตัดสินใจและรหัสสื่อสาร เช่นRansomware, ไฟไหม้ ฯลฯ	รายปี	ทีมงานเข้าใจบทบาทและขั้นตอนรหัส "คุณเทคโน"
Full DR Drill	ทดสอบกู้คืนระบบทั้งหมดแบบครบวงจร (End-to-End)	รายปี	เป็นไปตามเกณฑ์ RTO และ RPO ที่กำหนดไว้ในข้อ ๒.๒ ของแผนฉบับนี้

กระบวนการทดสอบ ๗.๒

เพื่อให้การทดสอบเป็นระบบและนำไปสู่การพัฒนา เจ้าหน้าที่ต้องปฏิบัติขั้นตอน ดังนี้

(๑) วางแผนและกำหนดขอบเขต โดยระบุวัตถุประสงค์และระบบที่จะทดสอบ พร้อมแจ้งหน่วยงานที่อาจได้รับผลกระทบ

(๒) ดำเนินการตามสถานการณ์จำลอง โดยปฏิบัติตามแผน DRP ในหมวดที่ ๕ และบันทึกเวลาที่ใช้ในแต่ละขั้นตอนอย่างละเอียด

(๓) ประเมินผลเปรียบเทียบ โดยนำผลการทดสอบมาเทียบกับค่าเป้าหมาย RTO/RPO ที่กำหนดไว้ในวิธีปฏิบัติมาตรฐาน (SOP)

(๔) สรุปรายงานผล โดยจัดทำรายงานสรุปปัญหาที่พบและข้อเสนอแนะเพื่อนำเสนอต่อผู้บริหาร

(๕) ปรับปรุงแผน โดยดำเนินการปรับปรุงแผน DRP หรือ SOP ตามผลการทดสอบให้เสร็จสิ้นภายใน ๓ เดือน

หมวดที่ ๘การรายงานและบันทึกเหตุการณ์ (Reporting & Documentation)

๘.๑รายงานหลังเกิดเหตุการณ์

เพื่อให้ผู้บริหารรับทราบสถานการณ์และนำไปสู่การปรับปรุงเชิงนโยบายต้องดำเนินการรายงาน ดังนี้

- รายงานเบื้องต้น (Preliminary Report)

ส่งภายใน ๒๔ ชั่วโมง หลังระบบกลับมาใช้งานปกติ (คุณเทคโน ๓) เพื่อสรุปสถานการณ์และผลกระทบเบื้องต้น

- รายงานฉบับสมบูรณ์ (Full Incident Report)

ส่งภายใน ๗ วันทำการ โดยต้องระบุสาเหตุรากเหง้า (Root Cause) ขั้นตอนการแก้ไขและบทเรียนที่ได้รับ (Lessons Learned)

- ผู้รับรายงาน คือ ผู้อำนวยการโรงพยาบาล CIO และคณะกรรมการบริหารโรงพยาบาล

DRP แบบบันทึกเหตุการณ์ ๘.๒

หัวข้อ	รายละเอียด (กรอกเมื่อเกิดเหตุ)
วันที่ / เวลาเกิดเหตุ	
สถานที่พบเหตุ	
ผู้รับแจ้ง / DRP Coordinator	
ลักษณะเหตุการณ์	
ระดับความรุนแรง	☐ ปานกลาง ☐ สูง ☐ วิกฤต
ระบบ/เครื่องแม่ข่ายที่ได้รับผลกระทบ	[ ] ห้องแม่ข่ายหลัก (ชั้น ๑A) [ ] ห้องแม่ข่ายสำรอง (อาคารเภสัชกรรม) [ ] อื่นๆ (ระบุ).. .....
รหัสที่ประกาศ	☐ คุณเทคโน ๑ ☐ คุณเทคโน ๒
Backup ระดับที่ใช้กู้คืน	☐ ระดับ ๑ (Server/VM) ☐ ระดับ ๒ (NAS) ☐ ระดับ ๓ (Offline Drive)
เวลาเริ่มดำเนินการกู้คืน	
เวลาระบบกลับมาทำงาน	
RTO ที่ทำได้จริง (ชั่วโมง)	
RPO ที่ทำได้จริง (ชั่วโมง)	
ข้อมูลที่สูญหาย (Data Loss)	
มาตรการที่ดำเนินการ	
ข้อเสนอแนะ / Lessons Learned	
ผู้รับผิดชอบ / ลงนาม	

ภาคผนวก

Emergency Checklist (IT Incident Response & DRP)

๑. Checklist เมื่อเกิดเหตุฉุกเฉินด้าน IT

ลำดับ	รายการตรวจสอบ (Action Items)	รายละเอียด/เป้าหมาย	เสร็จสิ้น
๑	ตรวจสอบสถานะเหตุการณ์	ระบุระบบที่ล่มและสาเหตุเบื้องต้น (Hardware / Network / Malware)	☐
๒	แจ้งประสานงานด่วน	แจ้ง Help Desk กลุ่มงาน IT (เบอร์ภายใน ๔๒๐๗) และทีมงาน IT ณ ชั้น ๑A อาคารวินิจฉัยโรคฯ	☐
๓	ประเมินระดับความรุนแรง	ประเมินระยะเวลาแก้ไขและระดับผลกระทบ (ปานกลาง / สูง / วิกฤต)	☐
๔	รายงานผู้บังคับบัญชา	รายงาน DRP Coordinator และ CIO ทันที (ภายใน ๑๕-๓๐ นาที)	☐
๕	ประกาศรหัสสื่อสาร	ประกาศ **"คุณเทคโน ๑"** (เฝ้าระวัง) หรือ **"คุณเทคโน ๒"** (ใช้แผน DRP/BCP)	☐
๖	ประชาสัมพันธ์ผู้ใช้งาน	แจ้งทุกหน่วยงานผ่านเสียงตามสาย หรือกลุ่ม Line เพื่อเริ่มใช้ระบบ Paper	☐
๗	กรณี Ransomware (Isolate)	**ตัดการเชื่อมต่อเครือข่ายทันที** และห้ามใช้ Backup ระดับ ๑ และ ๒	☐
๘	ตรวจสอบ Backup ระดับ ๑	ตรวจสอบ Snapshot บน Server/VM (Integrity Check)	☐
๙	ตรวจสอบ Backup ระดับ ๒	หากระดับ ๑ เสียหาย ให้เตรียมกู้คืนจาก NAS Storage	☐
๑๐	ตรวจสอบ Backup ระดับ ๓	กรณีวิกฤต/Ransomware ให้กู้จาก External Drive (Offline) เท่านั้น	☐
๑๑	ดำเนินการกู้คืนระบบ	Restore ข้อมูลและทดสอบฟังก์ชันการทำงาน (HOSxP / IPD Paperless)	☐
๑๒	รายงานหน่วยงานภายนอก	แจ้ง สสจ. / สกมช. ภายใน ๒๔ ชม. (กรณีเหตุร้ายแรง/ข้อมูลรั่วไหล)	☐
๑๓	ตรวจสอบเป้าหมายกู้คืน	ยืนยันผลการกู้คืนว่า RTO ≤ ๔ ชม. และ RPO ≤ ๒๔ ชม. (ตามข้อ ๒.๒)	☐
๑๔	ประกาศสถานะปกติ	เมื่อระบบพร้อม ๑๐๐% ให้ประกาศ **"คุณเทคโน ๓"** เพื่อยกเลิกแผนฉบับนี้	☐
๑๕	บันทึกและสรุปผล	บันทึก DRP Incident Log และเตรียมส่งรายงานฉบับสมบูรณ์ใน ๗ วัน	☐

๒. รายชื่อ และผู้ติดต่อฉุกเฉิน Vendor

ในกรณีที่ทีม IT ไม่สามารถแก้ไขปัญหาได้เอง ให้ติดต่อ Vendor ตามลำดับดังนี้

ระบบ / Vendor	บริษัท / หน่วยงาน	ผู้ติดต่อ	เบอร์โทร	ช่องทางสำรอง
HOSxP (HIS)	Bangkok Medical Software	BMS Call Center	๐-๒๔๒๗-๙๙๙๑ กด ๑ ๐๘๑-๘๑๑๘๑๗๓ ๐๘๑-๘๙๙๕๓๙๑ ๐๘๙-๙๒๔๖๒๐๗	bms.callcenter๙@gmail.com
เครื่องแม่ข่าย / Server	Vendor ผู้จำหน่าย Server	ช่างบริการ	ระบุตามสัญญา	ระบุตามสัญญา
NAS Storage	Vendor ผู้จำหน่าย NAS	ช่างบริการ	ระบุตามสัญญา	ระบุตามสัญญา
ระบบเครือข่าย (Network)	ISP / Vendor Network	NOC Support	ระบุตามสัญญา	ระบุตามสัญญา
ระบบ LIS	Vendor ผู้จำหน่าย LIS	ฝ่าย Support	ระบุตามสัญญา	ระบุตามสัญญา
ไฟฟ้า / UPS	กลุ่มงานวิศวกรรมฯ	ช่างไฟฟ้า	โทร ๔๑๘	โทร ๔๑๘

๓. แบบฟอร์มบันทึกผลการทดสอบแผน DRP

หัวข้อ	รายละเอียด (กรอกหลังการทดสอบ)
วันที่ทดสอบ	
ประเภทการทดสอบ	☐ Restoration Test ☐ Failover Test ☐ Offline Drill ☐ Tabletop ☐ Full DR Drill
ผู้ดำเนินการทดสอบ	
ผู้สังเกตการณ์ / ผู้ประเมิน	
ระบบที่ทดสอบ	
เวลาเริ่มทดสอบ	
เวลาสิ้นสุดการทดสอบ	
RTO ที่ทำได้จริง (ชั่วโมง)	
RPO ที่ทำได้จริง (ชั่วโมง)	
ผลการทดสอบ	☐ ผ่านเกณฑ์ ☐ ไม่ผ่านเกณฑ์ ☐ ผ่านบางส่วน
ปัญหาที่พบระหว่างทดสอบ	
ข้อเสนอแนะ / Lessons Learned	
แผนแก้ไขและระยะเวลา	
ผู้รับผิดชอบติดตาม	
วันที่ทดสอบครั้งต่อไป	
ผู้จัดทำรายงาน / ลงนาม	
DRP Coordinator อนุมัติ / ลงนาม	

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP) กรณีระบบสารสนเทศเสียหายฉบับนี้ ใช้เป็นแนวทางให้หน่วยงานภายในโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ สามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินต่าง ๆ เพื่อให้เจ้าหน้าที่ทราบและถือปฏิบัติต่อไป

ประกาศ ณ วันที่ ๑ กรกฎาคม พ.ศ. ๒๕๖๙

(นายจิรภัทร กัลยาณพจน์พร)

ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗