

รายงานผลการวิเคราะห์และแผนพัฒนาศักยภาพทรัพยากรด้านสารสนเทศ

ประจำปีงบประมาณ ๒๕๖๗

๑. บทสรุปผู้บริหาร (Executive Summary)

โรงพยาบาลทุ่งฝนได้ดำเนินการวิเคราะห์สถานการณ์ปัจจุบันและประเมินช่องว่าง (Gap Analysis) ของทรัพยากรด้าน IT ทั้ง ๔ ด้าน (Hardware, Software, Network, People) เพื่อตอบสนองต่อยุทธศาสตร์การเพิ่มประสิทธิภาพการดำเนินงาน (Performance) โดยมุ่งเน้นการใช้ข้อมูลเพื่อเพิ่มศักยภาพการรักษาผู้ป่วยที่มีความซับซ้อน (adj RW) และสร้างความมั่นคงปลอดภัยของข้อมูลสารสนเทศอย่างต่อเนื่อง

๒. ผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis (๙.๔.๕)

รายการทรัพยากร	สถานะปัจจุบัน (Current State)	การวิเคราะห์ช่องว่าง (Gap Analysis)
Hardware	มี Server Failover, Client ๘๗ เครื่อง, CCTV ๒๔ จุด, ระบบสำรองไฟฟ้ามครบถ้วน	อุปกรณ์ลูกข่ายบางส่วนเริ่มเสื่อมสภาพตามอายุการใช้งาน และ CCTV ยังไม่ครอบคลุม ๑๐๐%
Software	ใช้ HOSxP เป็นแกนหลัก และมี Module เฉพาะทางมากกว่า ๒๐ ระบบ (LIS, E-claim, PACs ฯลฯ)	ข้อมูลในบาง Module ยังทำงานแยกส่วน (Data Silo) จำเป็นต้องมี Data Center กลางเพื่อรวบรวมข้อมูล
Network	มี Internet Load Balance ๓ คู่สาย (๒ ค่า), WiFi ครอบคลุมพื้นที่บริการ	ความเร็วในบางจุดบริการอาจไม่เสถียรเมื่อมีการใช้งานหนาแน่น และต้องการการเฝ้าระวังภัยคุกคามไซเบอร์ที่เข้มข้นขึ้น
People	บุคลากรใช้งานระบบพื้นฐานได้ และเริ่มมีการพัฒนาทักษะด้านการวิเคราะห์ข้อมูล	จำเป็นต้องเพิ่มทักษะด้านการบันทึกข้อมูลเพื่อสะท้อนความรุนแรงของโรค (adj RW) ให้แม่นยำขึ้น

๓. รายละเอียดการจัดการทรัพยากรสารสนเทศ (IT Resource Management)

๓.๑ ด้านซอฟต์แวร์ (Software Excellence)

- Core System: ใช้ HOSxP ในการบริหารจัดการฐานข้อมูลผู้ป่วยแบบครบวงจร
- Integration: เชื่อมต่อระบบห้องปฏิบัติการ (LIS) และระบบภาพถ่ายรังสีดิจิทัล (PACs) อย่างไร้รอยต่อ
- Continuity of Care: ใช้ระบบ ThaiCOC และ Smart Refer เพื่อเชื่อมโยงข้อมูลผู้ป่วยในเครือข่ายและ รพ.สต.

- **Financial & Admin:** มีระบบวิเคราะห์ต้นทุน (Back Office) และระบบ E-claim ที่รองรับทุกกองทุน (NHSO, CSMBS, SSS)

๓.๒ ด้านฮาร์ดแวร์และโครงสร้างพื้นฐาน (Infrastructure Resilience)

- **High Availability:** เซิร์ฟเวอร์แม่ข่ายมีระบบสำรองที่สลับการทำงานอัตโนมัติ (Auto-Failover) เมื่อระบบหลักมีปัญหา
- **Business Continuity:** มีระบบสำรองไฟฟ้า (UPS & Generator) ที่ครอบคลุม Data Center เพื่อป้องกันระบบล่มจากเหตุไฟฟ้าขัดข้อง (เป้าหมายความพร้อมใช้งานร้อยละ ๑๐๐)
- **Security:** ติดตั้งกล้องวงจรปิดเพื่อความปลอดภัย และมีการบำรุงรักษาอุปกรณ์ (PM) อย่างน้อยปีละ ๒ ครั้ง

๔. แผนเพิ่มศักยภาพและทิศทางในอนาคต (Strategic Improvement Plan)

๑. **การจัดตั้งศูนย์ Data Center กลาง:** เพื่อรวบรวมข้อมูลจากทุก Module มาทำ Dashboard นำเสนอตัวชี้วัดทำท่าย (KPI) ด้านการเงินและสุขภาพต่อผู้บริหารแบบ Real-time
๒. **การยกระดับการจัดการความปลอดภัยไซเบอร์:** พัฒนาแผน IRP (Incident Response Plan) และซักซ้อมการรับมือระบบล่มอย่างสม่ำเสมอ
๓. **โครงการขยายระบบ CCTV:** แผนการติดตั้งเพิ่มเติมจาก ๒๔ จุด เป็น ๔๐ จุด เพื่อให้ครอบคลุมพื้นที่บ้านพักเจ้าหน้าที่และจุดเสี่ยง
๔. **การพัฒนาบุคลากร:** เน้นการอบรมการบันทึกข้อมูลเพื่อเพิ่มค่า adj RW และการใช้ยาอย่างสมเหตุผล (RDU) เพื่อลดค่าใช้จ่ายที่ไม่จำเป็น

๕. บทสรุปความสำเร็จ

จากการดำเนินงานข้างต้น ส่งผลให้โรงพยาบาลทุ่งฝนมีความพร้อมด้านระบบสารสนเทศในระดับสูง สามารถรองรับการขยายตัวของบริการทางการแพทย์ที่ซับซ้อนขึ้น และมั่นใจได้ว่าข้อมูลผู้ป่วยจะได้รับการคุ้มครองและพร้อมใช้งานตลอด ๒๔ ชั่วโมง

ส่วนที่เพิ่มเติม: แผนการแก้ไขและพัฒนาาระบบรักษาความมั่นคงปลอดภัยห้องแม่ข่าย (Corrective & Preventive Action Plan)

อ้างอิงจากข้อเสนอแนะการประเมินคุณภาพสถานพยาบาล (HA)

เพื่อให้เป็นไปตามมาตรฐานความปลอดภัยสารสนเทศและป้องกันความเสี่ยงระดับวิกฤต โรงพยาบาล
ทุ่งฝนได้กำหนดแผนงานเพื่อรองรับข้อเสนอแนะดังนี้:

๑. การยกระดับความปลอดภัยทางกายภาพ (Physical Security)

- **การปรับปรุงสถานที่ติดตั้ง:** พิจารณาแผนการย้ายห้อง Server ไปยังโซนควบคุม (Restricted Area) ที่ห่างจากพื้นที่สัญจรทั่วไป เพื่อลดความเสี่ยงจากการเข้าถึงโดยบุคคลที่ไม่เกี่ยวข้อง
- **ระบบควบคุมการเข้า-ออก (Access Control):** * ติดตั้งระบบสแกนลายนิ้วมือ (Fingerprint) หรือ คีย์การ์ด แทนการใช้กุญแจแบบเดิม
- **การเฝ้าระวัง:** ติดตั้งกล้อง CCTV เพิ่มเติมเพื่อตรวจสอบบริเวณทางเข้า-ออก และพื้นที่ภายในห้อง Server ตลอด ๒๔ ชั่วโมง

๒. การควบคุมสภาพแวดล้อมและระบบเตือนภัย (Environmental Control)

- **ระบบปรับอากาศ:** ติดตั้งเครื่องปรับอากาศแบบสลับการทำงาน (Dual AC System) เพื่อควบคุม อุณหภูมิและความชื้นให้คงที่
- **ระบบป้องกันอัคคีภัย:** ติดตั้งเครื่องตรวจจับควัน (Smoke Detector) และสัญญาณเตือนภัย (Fire Alarm) ที่เชื่อมโยงกับระบบแจ้งเตือนของโรงพยาบาล

๓. แผนบริหารความต่อเนื่องและการสำรองข้อมูล (Business Continuity & Backup)

- **แผนสำรองฉุกเฉิน (BCP/DRP):** * จัดทำเอกสาร "แผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ" ที่ระบุขั้นตอนเมื่อเกิดเหตุไม่คาดคิดชัดเจน
 - **การซ้อมแผน:** กำหนดตารางการซ้อมแผนสำรองฉุกเฉิน (Drill) อย่างน้อยปีละ ๑ ครั้ง และ แจ้งให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบ
- **การสอบทานการสำรองข้อมูล (Backup Audit):**
 - เพิ่มระบบการตรวจสอบความสมบูรณ์ของไฟล์สำรอง (Backup Integrity Check) ทุก สัปดาห์
 - บันทึกรายงานผลการสำรองข้อมูลรายวัน เพื่อยืนยันว่าข้อมูลมีความครบถ้วนและพร้อมกู้คืน ได้ทันที