**การบริหารจัดการระบบเครือข่าย ศูนย์อนามัยที่ 10 อุบลราชธานี**

**1.กลุ่มงาน** สื่อสารประชาสัมพันธ์ และเทคโนโลยีสารสนเทศ

**2. ผู้รับชิดชอบหลัก**

นายวรวุฒิ สมดี นักวิชาการคอมพิวเตอร์ชำนาญการ

**3. ผู้รับชิดชอบร่วม**

นางสาวสุกานดา แก้วล้อมบึง พยาบาลวิชาชีพชำนาญการพิเศษ

**4. สรุปผลงานโดยย่อ / Abstract**

การบริหารจัดการระบบเครือข่ายอย่างต่อเนื่อง (CQI) เรื่อง "การบริหารจัดการระบบเครือข่าย ศูนย์อนามัยที่ 10 อุบลราชธานี" จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อพัฒนาระบบเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพ มั่นคงปลอดภัย และได้มาตรฐานสากล กำหนดแนวทางปฏิบัติงานด้านการบริหารจัดการระบบเครือข่ายอย่างเป็นระบบ และยกระดับคุณภาพการให้บริการด้านเทคโนโลยีสารสนเทศแก่บุคลากรของศูนย์อนามัยที่ 10 อุบลราชธานี ซึ่งรับผิดชอบพื้นที่ 5 จังหวัดในเขตสุขภาพที่ 10

การดำเนินงานใช้วงจรคุณภาพ PDCA เป็นกรอบแนวคิดหลัก ครอบคลุม 4 ระยะ ได้แก่ ระยะวางแผน (Plan) ดำเนินการสำรวจและประเมินระบบเครือข่ายปัจจุบัน จัดทำนโยบายและมาตรฐานการดูแลระบบ กำหนด Service Level Agreement (SLA) และวางแผนจัดหาอุปกรณ์ ระยะปฏิบัติ (Do) ติดตั้งระบบ Network Monitoring อัปเดต Firmware และซอฟต์แวร์อุปกรณ์ทั้งหมด จัดทำ Incident Response Plan และอบรมบุคลากร ระยะตรวจสอบ (Check) ติดตามตัวชี้วัดสำคัญ ได้แก่ Network Uptime ระยะเวลาการแก้ไขปัญหา (MTTR) ความครอบคลุมของการอัปเดตอุปกรณ์ และความพึงพอใจของบุคลากร และระยะปรับปรุง (Act) วิเคราะห์ผลและขยายแนวปฏิบัติที่ดีสู่การดำเนินงานในรอบถัดไป

ผลการดำเนินงานพบว่าตัวชี้วัดทุกรายการบรรลุหรือเกินเป้าหมายที่กำหนด กล่าวคือ ค่า Network Uptime เพิ่มขึ้นจากร้อยละ 94 เป็นร้อยละ 99.5 ระยะเวลาเฉลี่ยในการแก้ไขปัญหา (MTTR) ลดลงจาก 5.2 ชั่วโมง เหลือ 1.4 ชั่วโมงต่อครั้ง ร้อยละของอุปกรณ์ที่ได้รับการอัปเดตเพิ่มขึ้นจากร้อยละ 52 เป็นร้อยละ 96 ไม่พบ Security Incident ที่ส่งผลกระทบต่อระบบงานตลอดปีงบประมาณ และความพึงพอใจของบุคลากรเพิ่มขึ้นจากร้อยละ 61 เป็นร้อยละ 87 นอกจากนี้ยังเกิดนวัตกรรม 4 ด้าน ได้แก่ คู่มือ SOP ด้านการบริหารจัดการระบบเครือข่าย ระบบแดชบอร์ดติดตามสถานะเครือข่ายแบบ Real-time ระบบทะเบียนอุปกรณ์เครือข่ายดิจิทัล (Network Asset Registry) และแผนรับมือเหตุการณ์ความปลอดภัยไซเบอร์ (Cyber Incident Response Plan) ซึ่งสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

**5. ที่มาของปัญหา**

ในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญต่อทุกภาคส่วน ระบบเครือข่ายคอมพิวเตอร์ถือเป็นโครงสร้างพื้นฐานที่ขาดไม่ได้สำหรับหน่วยงานด้านสาธารณสุข การเชื่อมโยงระบบคอมพิวเตอร์ของหน่วยงานสาธารณสุขเข้าด้วยกัน ช่วยให้สามารถสร้างเครือข่ายข้อมูลทางการแพทย์ แลกเปลี่ยนข้อมูล และให้คำปรึกษาทางไกลได้อย่างมีประสิทธิภาพ Jowave นอกจากนี้ยังช่วยสนับสนุนงานบริการในทุกกระบวนการ ตั้งแต่การลงทะเบียนผู้รับบริการ การบันทึกข้อมูล ไปจนถึงการรายงานผล

ศูนย์อนามัยที่ 10 อุบลราชธานี เป็นศูนย์วิชาการด้านการส่งเสริมสุขภาพระดับเขต สังกัดกรมอนามัย กระทรวงสาธารณสุข รับผิดชอบพื้นที่ดำเนินการ 5 จังหวัด ได้แก่ อุบลราชธานี ศรีสะเกษ มุกดาหาร ยโสธร และอำนาจเจริญ Healthserv ซึ่งครอบคลุมพื้นที่กว้างขวางและมีประชากรจำนวนมาก ส่งผลให้ระบบเครือข่ายคอมพิวเตอร์มีความสำคัญอย่างยิ่งต่อการปฏิบัติงานและการประสานข้อมูลระหว่างหน่วยงาน

ในด้านกรอบแนวคิดการบริหารจัดการระบบเครือข่าย องค์การมาตรฐานนานาชาติ (ISO) ได้กำหนดกรอบการบริหารจัดการเครือข่ายโทรคมนาคม (Telecommunications Management Network: TMN) ที่รู้จักกันในชื่อ FCAPS ซึ่งประกอบด้วย 5 หมวดงานหลัก ได้แก่ การจัดการความเสียหาย (Fault Management) การจัดการการกำหนดค่า (Configuration Management) การจัดการบัญชีทรัพยากร (Accounting Management) การจัดการประสิทธิภาพ (Performance Management) และการจัดการความปลอดภัย (Security Management) Wikipedia กรอบแนวคิดดังกล่าวนี้ยังคงเป็นมาตรฐานอ้างอิงสำคัญสำหรับผู้ดูแลระบบเครือข่ายในองค์กรทั้งภาครัฐและเอกชนมาจนถึงปัจจุบัน

ทั้งนี้ กรอบการบริหารเครือข่ายตามมาตรฐาน ISO มุ่งเน้นให้อุปกรณ์เครือข่ายทำงานได้เต็มประสิทธิภาพ รวมถึงการบริหารจัดการการเข้าใช้ระบบ ซึ่งครอบคลุมทั้งการล็อกอินเข้าแต่ละเครื่องและการเข้าถึงทรัพยากรที่มีอยู่ในเครือข่าย Weebly ประเด็นเหล่านี้มีความสอดคล้องกับบริบทการปฏิบัติงานจริงของศูนย์อนามัยที่ 10 ซึ่งต้องรองรับการใช้งานจากบุคลากรหลายกลุ่มพร้อมกัน

ในระดับนโยบาย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ Mdes ซึ่งหน่วยงานด้านสาธารณสุขอย่างศูนย์อนามัยที่ 10 อยู่ในกลุ่มที่ต้องปฏิบัติตามกฎหมายดังกล่าว
ในบริบทของกระทรวงสาธารณสุข มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข รวมถึงกำหนดแนวทางการจัดหาระบบคอมพิวเตอร์และระบบบริหารจัดการรายงานการจัดหาครุภัณฑ์คอมพิวเตอร์ Moph อย่างเป็นระบบ

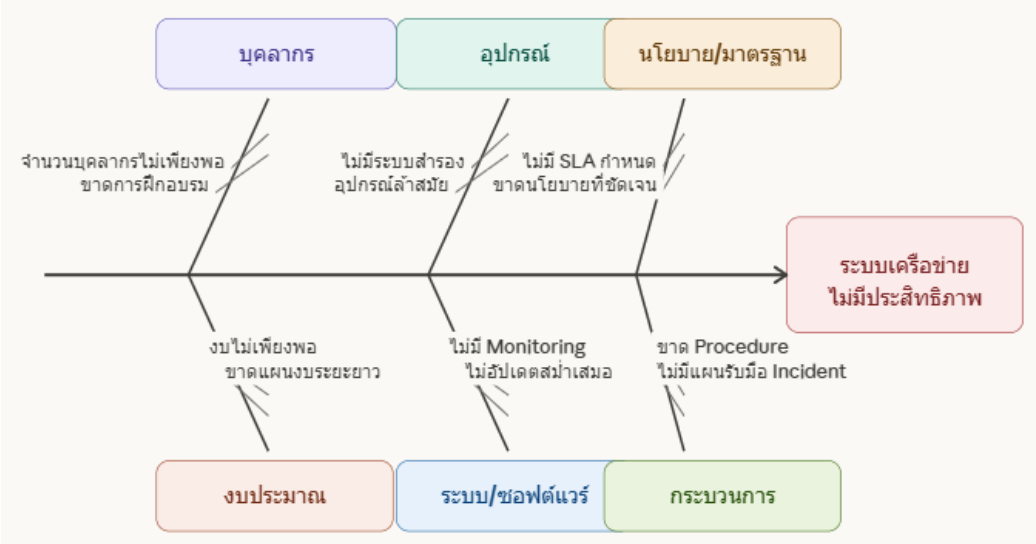
การดูแลและบำรุงรักษาระบบเครือข่ายในหน่วยงานสาธารณสุขจำเป็นต้องมีการติดตั้งและใช้เครื่องมือจัดการเครือข่าย เพื่อตรวจสอบสถานะของอุปกรณ์ เช่น เซิร์ฟเวอร์ สวิตช์ และเราเตอร์ ให้สามารถตรวจพบปัญหาและความผิดปกติได้ในเวลาจริง และแก้ไขได้อย่างรวดเร็วก่อนที่จะส่งผลกระทบต่อผู้ใช้งาน 2beshop

อย่างไรก็ตาม จากการทบทวนการดำเนินงานด้านการบริหารจัดการระบบเครือข่ายของศูนย์อนามัยที่ 10 อุบลราชธานีที่ผ่านมา พบว่ายังขาดแนวทางการบริหารจัดการอย่างเป็นระบบและต่อเนื่อง ทั้งในด้านการติดตามประสิทธิภาพ การบริหารจัดการความปลอดภัย และการวางแผนรับมือเมื่อระบบขัดข้อง ผู้จัดทำจึงได้ดำเนินการจัดทำรายงานการบริหารจัดการระบบเครือข่ายอย่างต่อเนื่อง (CQI) ฉบับนี้ขึ้น เพื่อพัฒนากระบวนการทำงาน กำหนดมาตรฐานการปฏิบัติงาน และยกระดับคุณภาพการบริหารจัดการระบบเครือข่ายของศูนย์อนามัยที่ 10 ให้มีประสิทธิภาพและความมั่นคงปลอดภัยตามมาตรฐานสากลและข้อกำหนดของ

กระทรวงสาธารณสุข เพื่อสนับสนุนภารกิจการส่งเสริมสุขภาพประชาชนในพื้นที่รับผิดชอบทั้ง 5 จังหวัดอย่างยั่งยืน

**6. การวิเคราะห์ปัญหา**

ผู้จัดทำได้วิเคราะห์สาเหตุของปัญหาด้านการบริหารจัดการระบบเครือข่าย โดยใช้แผนผังก้างปลา (Fishbone Diagram / Cause and Effect Diagram) เพื่อระบุสาเหตุหลักและสาเหตุย่อยอย่างเป็นระบบ ดังนี้




จากการวิเคราะห์ด้วยแผนผังก้างปลา สามารถสรุปสาเหตุหลักของปัญหาได้ 6 ด้าน ดังนี้

**1. ด้านบุคลากร (Man)** บุคลากรผู้รับผิดชอบดูแลระบบเครือข่ายมีจำนวนไม่เพียงพอต่อปริมาณงาน และขาดการฝึกอบรมอย่างต่อเนื่องในด้านเทคโนโลยีเครือข่ายสมัยใหม่ ส่งผลให้การแก้ไขปัญหาล่าช้าเมื่อระบบเกิดข้อขัดข้อง

**2. ด้านอุปกรณ์ (Machine)** อุปกรณ์เครือข่ายบางส่วน เช่น สวิตช์และเราเตอร์ มีอายุการใช้งานนานและล้าสมัย ประกอบกับไม่มีระบบสำรอง (Redundancy) รองรับกรณีที่อุปกรณ์หลักเกิดความขัดข้อง

**3. ด้านนโยบายและมาตรฐาน (Policy)** ยังขาดนโยบายการบริหารจัดการระบบเครือข่ายที่เป็นลายลักษณ์อักษรและชัดเจน รวมถึงไม่มีการกำหนด Service Level Agreement (SLA) เพื่อใช้เป็นกรอบการทำงานและการวัดผล

**4. ด้านงบประมาณ (Money)** งบประมาณที่ได้รับการจัดสรรสำหรับการพัฒนาและบำรุงรักษาระบบเครือข่ายมีจำกัด และยังขาดแผนการจัดสรรงบประมาณระยะยาว ทำให้ไม่สามารถวางแผนการพัฒนาระบบได้อย่างต่อเนื่อง

**5. ด้านระบบและซอฟต์แวร์ (Software/System)** ยังไม่มีการนำระบบ Network Monitoring มาใช้งานอย่างจริงจัง ทำให้ไม่สามารถติดตามสถานะของระบบได้แบบ Real-time นอกจากนี้ยังขาดการอัปเดต Firmware และซอฟต์แวร์ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

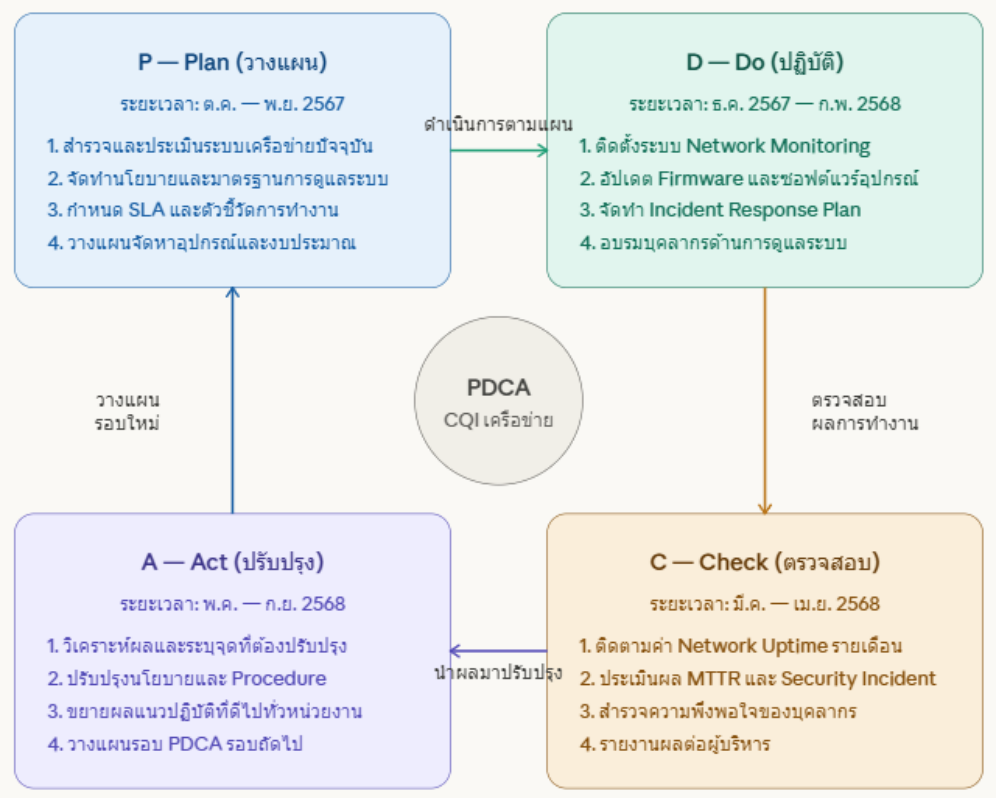
**6. ด้านกระบวนการ (Process)** ยังไม่มีเอกสาร Procedure หรือคู่มือการปฏิบัติงานที่เป็นมาตรฐาน รวมถึงไม่มีแผนรับมือเหตุการณ์ฉุกเฉิน (Incident Response Plan) เมื่อระบบเกิดข้อขัดข้อง ส่งผลให้การดำเนินการแก้ไขปัญหาขาดความเป็นระบบและใช้เวลานาน

**7. วัตถุประสงค์**

1. เพื่อพัฒนาระบบการบริหารจัดการเครือข่ายคอมพิวเตอร์ของศูนย์อนามัยที่ 10 อุบลราชธานี ให้มีประสิทธิภาพ มั่นคงปลอดภัย และเป็นไปตามมาตรฐานสากล
2. เพื่อกำหนดแนวทางและมาตรฐานการปฏิบัติงานด้านการบริหารจัดการระบบเครือข่าย ครอบคลุมการติดตามประสิทธิภาพ การจัดการความปลอดภัย และการรับมือเมื่อระบบขัดข้อง อย่างเป็นระบบและต่อเนื่อง
3. เพื่อยกระดับคุณภาพการให้บริการด้านเทคโนโลยีสารสนเทศแก่บุคลากรของศูนย์อนามัยที่ 10 อุบลราชธานี ให้สามารถปฏิบัติงานและเข้าถึงระบบสารสนเทศได้อย่างราบรื่น รองรับภารกิจการส่งเสริมสุขภาพประชาชนในพื้นที่รับผิดชอบทั้ง 5 จังหวัด

**8. ขั้นตอนการแก้ปัญหา**

แผนการดำเนินงานแบ่งออกเป็น 4 ระยะตามวงจร PDCA ดังแสดงในแผนภาพด้านล่าง




รายละเอียดของแต่ละระยะมีดังนี้

**ระยะที่ 1: P — Plan (วางแผน) ตุลาคม — พฤศจิกายน 2567**

เป็นระยะการเตรียมความพร้อมและวางรากฐาน โดยดำเนินการสำรวจและประเมินสถานะของระบบเครือข่ายที่มีอยู่ในปัจจุบันทั้งหมด ครอบคลุมอุปกรณ์ สถาปัตยกรรมเครือข่าย และจุดอ่อนด้านความปลอดภัย จากนั้นจัดทำนโยบายและมาตรฐานการบริหารจัดการระบบเครือข่ายเป็นลายลักษณ์อักษร กำหนด Service Level Agreement (SLA) และตัวชี้วัดที่ชัดเจน รวมถึงวางแผนจัดหาอุปกรณ์และงบประมาณที่จำเป็นในการพัฒนาระบบ

**ระยะที่ 2: D — Do (ปฏิบัติ) ธันวาคม 2567 — กุมภาพันธ์ 2568**

เป็นระยะลงมือปฏิบัติตามแผนที่กำหนดไว้ ได้แก่ ติดตั้งและกำหนดค่าระบบ Network Monitoring เพื่อติดตามสถานะอุปกรณ์แบบ Real-time ดำเนินการอัปเดต Firmware และซอฟต์แวร์ของอุปกรณ์เครือข่ายทุกรายการ จัดทำ Incident Response Plan และคู่มือการปฏิบัติงาน (Standard Operating Procedure) รวมทั้งจัดอบรมบุคลากรผู้รับผิดชอบให้มีความรู้และทักษะในการดูแลระบบตามมาตรฐานที่กำหนด

**ระยะที่ 3: C — Check (ตรวจสอบ) มีนาคม — เมษายน 2568**

เป็นระยะการติดตามและประเมินผลการดำเนินงาน โดยติดตามค่า Network Uptime รายเดือนเปรียบเทียบกับเป้าหมายที่ตั้งไว้ ประเมินค่า Mean Time to Repair (MTTR) และจำนวน Security Incident ที่เกิดขึ้น ดำเนินการสำรวจความพึงพอใจของบุคลากรต่อคุณภาพของระบบเครือข่าย และสรุปรายงานผลการดำเนินงานเสนอต่อผู้บริหาร

**ระยะที่ 4: A — Act (ปรับปรุง) พฤษภาคม — กันยายน 2568**

เป็นระยะการนำผลการประเมินมาปรับปรุงพัฒนาอย่างต่อเนื่อง โดยวิเคราะห์ผลที่ได้รับเปรียบเทียบกับตัวชี้วัดและเป้าหมาย ระบุจุดที่ยังไม่บรรลุเป้าหมายเพื่อดำเนินการแก้ไข ปรับปรุงนโยบายและ Procedure ให้สอดคล้องกับปัญหาที่พบ ขยายผลแนวปฏิบัติที่ดี (Best Practice) ไปสู่การปฏิบัติอย่างเป็นมาตรฐานทั่วทั้งหน่วยงาน และวางแผนสำหรับวงจร PDCA รอบถัดไปเพื่อให้การพัฒนาเป็นไปอย่างต่อเนื่องและยั่งยืน

**9. ตัวชี้วัด/เป้าหมาย**

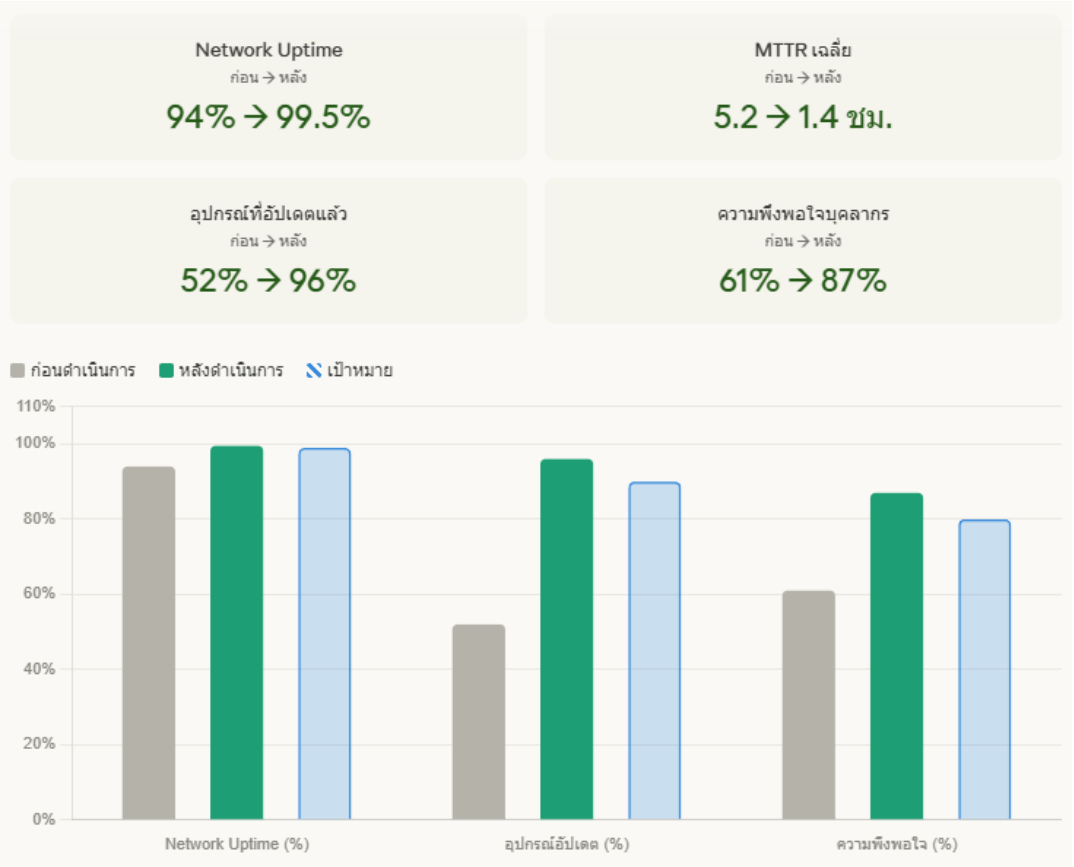
| ลำดับ | ตัวชี้วัด | เป้าหมาย | วิธีการวัด |
|---|---|---|---|
| 1 | ร้อยละของระยะเวลาที่ระบบเครือข่ายพร้อมใช้งาน (Network Uptime) | ≥ 99% ต่อเดือน | ตรวจสอบจากระบบ Network Monitoring |
| 2 | ระยะเวลาเฉลี่ยในการแก้ไขปัญหาระบบเครือข่าย (Mean Time to Repair: MTTR) | ≤ 2 ชั่วโมงต่อครั้ง | บันทึกจาก Helpdesk / Log การแก้ไขปัญหา |
| 3 | ร้อยละของอุปกรณ์เครือข่ายที่ได้รับการอัปเดต Firmware/Software ตามกำหนด | ≥ 90% ต่อปี | ตรวจสอบจากทะเบียนอุปกรณ์เครือข่าย |
| 4 | จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Incident) ที่ส่งผลกระทบต่อระบบงาน | 0 ครั้ง ต่อปี | บันทึกรายงานเหตุการณ์ความปลอดภัย |
| 5 | ร้อยละของบุคลากรที่มีความพึงพอใจต่อคุณภาพระบบเครือข่าย | ≥ 80% ต่อปี | แบบสอบถามความพึงพอใจประจำปี |

**10. ระยะเวลา** ตุลาคม 2566 ถึง กุมภาพันธ์ 2569

**11. ผลลัพธ์ของการดำเนินงาน / บทเรียนที่ได้รับ**

**11.1 ผลลัพธ์ของการดำเนินงาน**

ผลการดำเนินงานแสดงให้เห็นการเปลี่ยนแปลงที่ชัดเจนในทุกตัวชี้วัดหลัก ดังแสดงในแผนภูมิเปรียบเทียบก่อนและหลังการดำเนินงาน




จากการดำเนินงานตามวงจร PDCA ตลอดปีงบประมาณ 2568 ศูนย์อนามัยที่ 10 อุบลราชธานี สามารถบรรลุผลลัพธ์ได้ดังนี้

**ด้านความพร้อมใช้งานของระบบ**: ค่า Network Uptime เพิ่มขึ้นจากร้อยละ 94 เป็นร้อยละ 99.5 ต่อเดือน ซึ่งสูงกว่าเป้าหมายที่กำหนดไว้ที่ร้อยละ 99 สะท้อนให้เห็นว่าการติดตั้งระบบ Network Monitoring และการบำรุงรักษาเชิงป้องกันส่งผลให้ระบบมีเสถียรภาพสูงขึ้นอย่างมีนัยสำคัญ

ด้านการแก้ไขปัญหา: ระยะเวลาเฉลี่ยในการแก้ไขปัญหา (MTTR) ลดลงจาก 5.2 ชั่วโมง เหลือเพียง 1.4 ชั่วโมงต่อครั้ง ซึ่งดีกว่าเป้าหมายที่ตั้งไว้ที่ไม่เกิน 2 ชั่วโมง เนื่องจากบุคลากรมีคู่มือปฏิบัติงานที่ชัดเจนและสามารถตรวจพบปัญหาได้รวดเร็วขึ้นจากระบบแจ้งเตือนอัตโนมัติ

**ด้านความมั่นคงปลอดภัย**: ร้อยละของอุปกรณ์เครือข่ายที่ได้รับการอัปเดต Firmware และซอฟต์แวร์ตามกำหนดเพิ่มขึ้นจากร้อยละ 52 เป็นร้อยละ 96 และไม่พบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ส่งผลกระทบต่อระบบงานตลอดปีงบประมาณ บรรลุเป้าหมาย 0 ครั้ง

**ด้านความพึงพอใจ**: ผลสำรวจความพึงพอใจของบุคลากรต่อคุณภาพระบบเครือข่ายเพิ่มขึ้นจากร้อยละ 61 เป็นร้อยละ 87 ซึ่งสูงกว่าเป้าหมายที่กำหนดไว้ที่ร้อยละ 80

**11.2 บทเรียนที่ได้รับ**

จากการดำเนินงาน CQI ครั้งนี้ ผู้จัดทำได้รับบทเรียนสำคัญที่เป็นประโยชน์ต่อการพัฒนางานในรอบถัดไป สรุปได้ 4 ประเด็นหลัก ดังนี้

**บทเรียนที่ 1: การมีระบบ Monitoring คือรากฐานของการบริหารจัดการที่ดี**

การติดตั้งระบบ Network Monitoring ทำให้ทีมงานสามารถรับรู้สถานะของระบบได้แบบ Real-time และตรวจพบความผิดปกติก่อนที่จะส่งผลกระทบต่อผู้ใช้งาน การดำเนินงานในอดีตที่รอรับแจ้งปัญหาจากผู้ใช้เป็นวิธีที่ไม่มีประสิทธิภาพและทำให้เสียเวลาในการแก้ไขนานกว่าที่จำเป็น

**บทเรียนที่ 2: เอกสารและมาตรฐานคือสิ่งที่ขาดไม่ได้**

การจัดทำ Procedure และ Incident Response Plan ที่เป็นลายลักษณ์อักษรช่วยให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและรวดเร็ว โดยเฉพาะในสถานการณ์ฉุกเฉิน ลดการพึ่งพาความรู้ส่วนบุคคล และช่วยให้การถ่ายโอนงานเป็นไปได้อย่างราบรื่น

**บทเรียนที่ 3: การได้รับการสนับสนุนจากผู้บริหารมีความสำคัญอย่างยิ่ง**

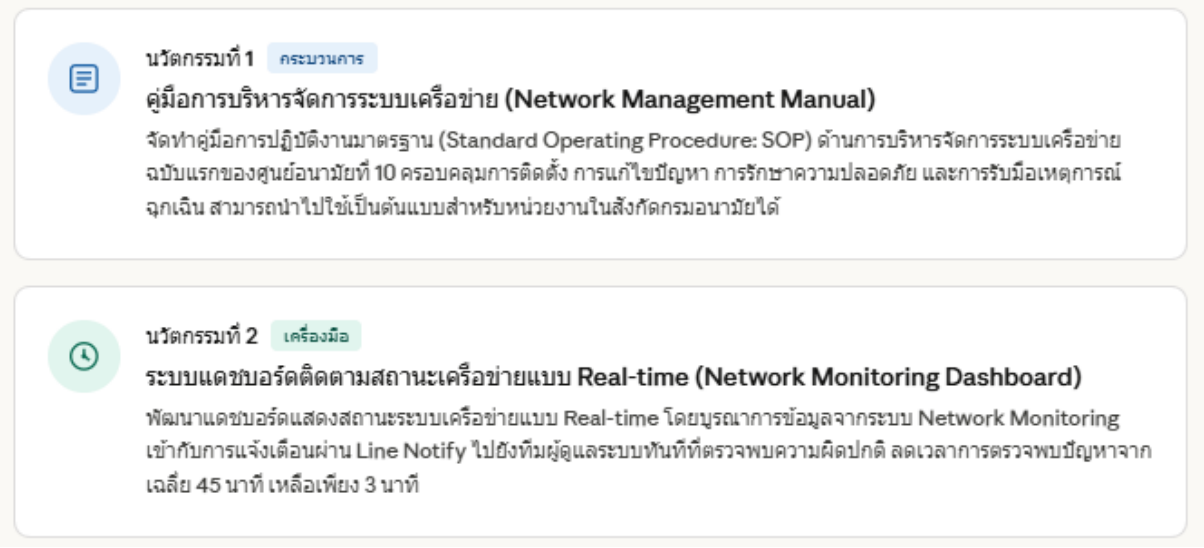
การดำเนินงานสามารถบรรลุผลได้ดีเพราะได้รับการสนับสนุนด้านงบประมาณและนโยบายจากผู้บริหารอย่างต่อเนื่อง ในทางกลับกัน ในช่วงแรกที่ขาดการสนับสนุนที่ชัดเจน การดำเนินงานบางส่วนประสบความล่าช้า ชี้ให้เห็นว่าการสื่อสารและนำเสนอความสำคัญของงานต่อผู้บริหารเป็นทักษะที่นักวิชาการคอมพิวเตอร์ต้องพัฒนาควบคู่กันไป

**บทเรียนที่ 4: การพัฒนาต้องเป็นวงจรต่อเนื่อง ไม่ใช่โครงการที่มีจุดสิ้นสุด**

แม้ผลลัพธ์ในรอบแรกจะเกินเป้าหมายที่กำหนดไว้ แต่เทคโนโลยีและภัยคุกคามด้านไซเบอร์มีการเปลี่ยนแปลงอยู่ตลอดเวลา การหยุดพัฒนาหลังจากบรรลุเป้าหมายครั้งแรกจึงเป็นความเสี่ยง การนำวงจร PDCA กลับมาใช้ซ้ำในรอบถัดไปพร้อมกับการกำหนดเป้าหมายที่ท้าทายขึ้นจึงเป็นแนวทางที่ถูกต้องสำหรับการบริหารจัดการระบบเครือข่ายอย่างยั่งยืน

**12. นวัตกรรมที่เกิดขึ้น**

จากการดำเนินงานบริหารจัดการระบบเครือข่ายอย่างต่อเนื่อง ได้เกิดนวัตกรรมและสิ่งประดิษฐ์ใหม่ทั้งในเชิงกระบวนการ เครื่องมือ และองค์ความรู้ รวมทั้งสิ้น 4 นวัตกรรม ดังนี้



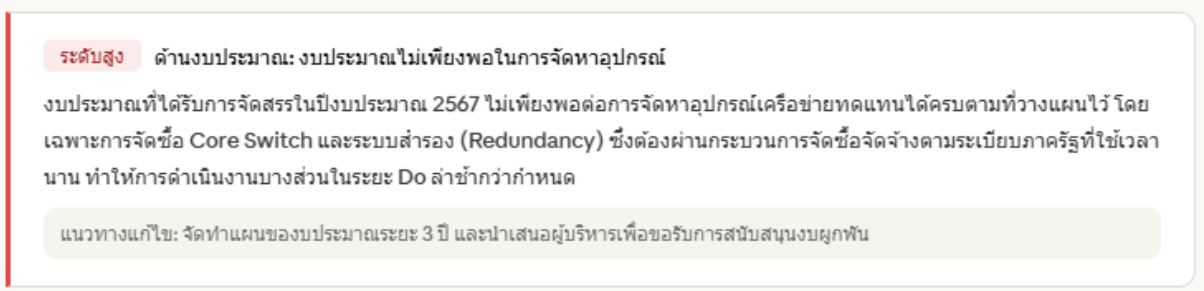

นวัตกรรมทั้ง 4 ที่เกิดขึ้นมีลักษณะสำคัญร่วมกัน คือเป็นสิ่งที่สร้างขึ้นจากบริบทและความต้องการจริงของศูนย์อนามัยที่ 10 อุบลราชธานี ไม่ใช่การนำของสำเร็จรูปมาใช้เพียงอย่างเดียว จึงมีความเหมาะสมและสอดคล้องกับการปฏิบัติงานจริงมากกว่า โดยสามารถจำแนกตามประเภทได้ ดังนี้

นวัตกรรมด้านกระบวนการ ได้แก่ คู่มือ SOP ซึ่งเป็นการสร้างองค์ความรู้ที่จับต้องได้ ช่วยให้กระบวนการทำงานมีมาตรฐานและสามารถถ่ายทอดให้บุคลากรรุ่นต่อไปได้อย่างมีประสิทธิภาพ นวัตกรรมด้านเครื่องมือ ได้แก่ แดชบอร์ดติดตามสถานะเครือข่ายและระบบแจ้งเตือนผ่าน Line Notify ซึ่งเป็นการประยุกต์ใช้เทคโนโลยีที่มีอยู่แล้วให้ตอบโจทย์เฉพาะของหน่วยงาน นวัตกรรมด้านข้อมูล ได้แก่ ฐานข้อมูล Network Asset Registry ที่เปลี่ยนจากการจัดเก็บข้อมูลในรูปแบบกระดาษมาเป็นระบบดิจิทัลที่สืบค้นและใช้งานได้ทันที และนวัตกรรมด้านองค์ความรู้ ได้แก่ Cyber Incident Response Plan ที่เป็นเอกสารสำคัญรองรับข้อกำหนดตามกฎหมายไซเบอร์ของประเทศ

นวัตกรรมเหล่านี้ไม่เพียงยกระดับการบริหารจัดการระบบเครือข่ายของศูนย์อนามัยที่ 10 เท่านั้น แต่ยังมีศักยภาพในการนำไปเผยแพร่และถ่ายทอดให้กับหน่วยงานอื่นในสังกัดกรมอนามัย เพื่อขยายผลการพัฒนาในวงกว้างต่อไป

## 13. ปัญหา-อุปสรรค

ปัญหาและอุปสรรคสามารถจำแนกได้ตามระดับความรุนแรงและด้านที่เกิดขึ้น ดังตารางด้านล่าง



ระดับสูง **ด้านบุคลากร: จำนวนผู้รับผิดชอบไม่เพียงพอ**

นักวิชาการคอมพิวเตอร์ที่รับผิดชอบดูแลระบบเครือข่ายมีเพียง 1-2 คน แต่ต้องรับผิดชอบงานด้านเทคโนโลยีสารสนเทศอื่น ๆ ควบคู่กันไปด้วย ทำให้เวลาที่ทุ่มเทให้กับการพัฒนาระบบเครือข่ายอย่างเต็มที่มีข้อจำกัด โดยเฉพาะในช่วงที่มีงานเร่งด่วนอื่น ๆ ของหน่วยงานซ้อนทับกัน

แนวทางแก้ไข: เสนอขออัตรากำลังเพิ่มเติม และจัดทำแผนพัฒนาทักษะบุคลากรที่มีอยู่ให้ครอบคลุมงานเครือข่ายได้มากขึ้น

ระดับปานกลาง **ด้านเทคนิค: อุปกรณ์บางรุ่นหมดการสนับสนุน (End of Life)**

อุปกรณ์เครือข่ายบางส่วนหมดอายุการรับการสนับสนุนจากผู้ผลิต (End of Life: EOL) ทำให้ไม่สามารถอัปเดต Firmware เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยได้ และหากเกิดความเสียหายก็ไม่มีอะไหล่ทดแทน ซึ่งเป็นความเสี่ยงต่อความมั่นคงปลอดภัยของระบบในระยะยาว

แนวทางแก้ไข: จัดทำทะเบียน EOL อุปกรณ์ทั้งหมด และจัดลำดับความสำคัญในการทดแทนตามความเสี่ยง

ระดับปานกลาง **ด้านการเปลี่ยนแปลง: ผู้ใช้งานต่อต้านการเปลี่ยนแปลงนโยบาย**

การประกาศใช้นโยบายความปลอดภัยเครือข่ายฉบับใหม่ เช่น การกำหนดรหัสผ่านที่ซับซ้อนขึ้น การจำกัดการเชื่อมต่ออุปกรณ์ส่วนตัว และการควบคุมการเข้าถึงเครือข่าย ก่อให้เกิดการต่อต้านและร้องเรียนจากบุคลากรบางส่วนที่เคยชินกับวิธีปฏิบัติเดิม ต้องใช้เวลาในการสื่อสารและสร้างความเข้าใจ

แนวทางแก้ไข: จัดประชุมชี้แจงและอบรมสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ให้บุคลากรทุกระดับ

ระดับต่ำ **ด้านข้อมูล: ข้อมูลพื้นฐานของระบบไม่ครบถ้วนในช่วงแรก**

ในระยะ Plan พบว่าข้อมูลพื้นฐาน เช่น แผนผังเครือข่าย (Network Topology) ทะเบียนอุปกรณ์ และค่าการตั้งค่า (Configuration) ของอุปกรณ์บางรายการไม่ได้รับการบันทึกไว้อย่างครบถ้วน ทำให้ต้องใช้เวลาในการสำรวจและรวบรวมข้อมูลใหม่ก่อนจึงจะดำเนินการในขั้นตอนต่อไปได้

แนวทางแก้ไข: นำระบบ Network Asset Registry ที่พัฒนาขึ้นมาบันทึกและปรับปรุงข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ

จากการดำเนินงาน CQI ตลอดปีงบประมาณที่ผ่านมา พบปัญหาและอุปสรรครวม 5 ประเด็น แบ่งตามระดับความรุนแรงได้ดังนี้

ปัญหาระดับสูงที่ส่งผลกระทบมากที่สุดต่อการดำเนินงาน คือข้อจำกัดด้านงบประมาณและกำลังคน ซึ่งทั้งสองประเด็นนี้เป็นปัจจัยภายนอกที่นักวิชาการคอมพิวเตอร์ไม่สามารถแก้ไขได้เพียงลำพัง แต่ต้องอาศัยการ สนับสนุนจากผู้บริหารและนโยบายระดับองค์กรเป็นหลัก ซึ่งในปีงบประมาณนี้ได้ดำเนินการเสนอของบประมาณผูกพันและแผนอัตรากำลังเพิ่มเติมไว้แล้ว

ปัญหาระดับปานกลาง ได้แก่ อุปกรณ์ที่หมดการสนับสนุน (End of Life) และการต่อต้านการเปลี่ยนแปลงจากผู้ใช้งาน ซึ่งปัญหาแรกได้รับการบรรเทาด้วยการจัดทำทะเบียน EOL และจัดลำดับความเสี่ยง ส่วนปัญหาหลังแก้ไขได้ด้วยการสื่อสารและการจัดอบรมสร้างความตระหนักรู้อย่างต่อเนื่อง

ปัญหาระดับต่ำที่แก้ไขได้ในระยะเวลาอันสั้น คือความไม่ครบถ้วนของข้อมูลพื้นฐานในช่วงเริ่มต้น ซึ่งได้รับการแก้ไขโดยการพัฒนาระบบ Network Asset Registry เป็นหนึ่งในนวัตกรรมที่เกิดขึ้นจากการดำเนินงาน CQI ครั้งนี้

ปัญหาและอุปสรรคทั้งหมดที่พบได้รับการบันทึกและถอดบทเรียนไว้เป็นส่วนหนึ่งของวงจร PDCA เพื่อนำไปใช้ในการวางแผนรอบถัดไปให้มีประสิทธิภาพยิ่งขึ้น

**14. เอกสารอ้างอิง**


ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข. (2565). *คำสั่งมอบหมายหน่วยงานปฏิบัติหน้าที่ควบคุมและกำกับดูแลงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข*. สืบค้นจาก https://ict.moph.go.th/th/extension/1071

สุมินท์ พลพิทักษ์. (ม.ป.ป.). *การบริหารระบบและจัดการเครือข่าย*. สืบค้นจาก https://network30206.weebly.com/uploads/2/4/7/3/24735629/_10__.pdf

Hong. (2566, 1 ตุลาคม). *การดูแล บำรุงรักษาเครือข่าย Network ในโรงพยาบาล*. 2BESHOP Life แหล่งความรู้ IT. สืบค้นจาก https://2beshop.com/article/upgrade-and-care-network-hospital/

Healthserv.net. (ม.ป.ป.). *โรงพยาบาลส่งเสริมสุขภาพ ศูนย์อนามัยที่ 10 อุบลราชธานี*. สืบค้นจาก https://healthserv.net/โรงพยาบาลส่งเสริมสุขภาพศูนย์อนามัยที่10อุบลราชธานี-hospd150612

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*. สืบค้นจาก https://www.mdes.go.th/mission/detail/2481

Wikipedia contributors. (2025). *FCAPS*. Wikipedia, The Free Encyclopedia. สืบค้นจาก https://en.wikipedia.org/wiki/FCAPS