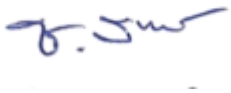
	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	**รหัสเอกสาร**	**YCN MOPH Policy-03**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	**23 มีนาคม 2569 ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย กำชัย เสาเวียง	นางสาว ลักขณา เสาเวียง	นพ ชำนาญ สมรมิตร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	นักวิชาการสาธารณสุขำนาญการ (Lead Implementer)	ผอ.โรงพยาบาลยางชุมน้อย (CISO)
วันเดือนปี	16 มีนาคม 2569	20 มีนาคม 2569	23 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**23 มีนาคม 2569**	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	**รหัสเอกสาร**	**YCN MOPH Policy-03**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**23 มีนาคม 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ 22.2.4]

1. วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับการกำหนดค่าระบบสารสนเทศ เพื่อป้องกันความเสี่ยงและลดช่องโหว่ที่อาจเกิดขึ้นจากการกำหนดค่าระบบที่ไม่ปลอดภัย

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการกำหนดค่าระบบทั้งหมดในองค์กร รวมถึงเซิร์ฟเวอร์, คอมพิวเตอร์, อุปกรณ์เครือข่าย และแอปพลิเคชันที่ใช้งานภายในองค์กร

3. หลักการรักษาความมั่นคงปลอดภัย (Security Principles)

องค์กรต้องปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

1. **สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)**

- ระบบฐานข้อมูลขององค์กรจะต้องถูกกำหนดให้พนักงานแต่ละคนเข้าถึงข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับหน้าที่ของตนเท่านั้น เช่น เจ้าหน้าที่ฝ่ายการเงินจะสามารถเข้าถึงข้อมูลการเงิน แต่ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลของพนักงานได้

2. **การแบ่งแยกหน้าที่ (Separation of Duties)**
   - ในองค์กรนั้นจะต้องมีการแบ่งแยกหน้าที่กันอย่างชัดเจน
3. **การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน**
   - องค์กรกำหนดให้ผู้ใช้ทุกคนต้องตั้งรหัสผ่านที่ประกอบด้วยอักษรพิมพ์ใหญ่, อักษรพิมพ์เล็ก, ตัวเลข และอักขระพิเศษ และต้องมีความยาวอย่างน้อย 8 ตัวอักษร
4. **การลบบัญชีที่ไม่ได้ใช้**
   - บัญชีของพนักงานที่ลาออกจะถูกลบออกจากระบบภายใน 7 วันหลังจากที่พนักงานคนนั้นออกจากองค์กร เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
5. **การลบบริการและแอปพลิเคชันที่ไม่จำเป็น**
   - เซิร์ฟเวอร์ขององค์กรจะถูกกำหนดค่าให้ลบคอมไพเลอร์ (Compiler) และแอปพลิเคชันที่ไม่จำเป็น เช่น แอปพลิเคชันที่ใช้สำหรับการทดสอบหรือสนับสนุนจากผู้ให้บริการภายนอก เพื่อ
   - ป้องกันการโจมตีที่อาจเกิดขึ้นจากช่องโหว่ในแอปพลิเคชันเหล่านั้น
6. **การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน**
   - ในการตั้งค่าเครือข่ายขององค์กร พอร์ตที่ไม่ได้ใช้งาน เช่น พอร์ต FTP จะถูกปิดเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากการเข้าถึงผ่านพอร์ตเหล่านั้น

7. **การป้องกันมัลแวร์ (Malware Protection)**
    - คอมพิวเตอร์ทุกเครื่องในองค์กรจะต้องติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์เป็นประจำ รวมถึงมีการสแกนระบบแบบอัตโนมัติทุกสัปดาห์
8. **การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบ**
    - เซิร์ฟเวอร์ขององค์กรจะได้รับการอัปเดตซอฟต์แวร์และติดตั้งแพตช์ความมั่นคงปลอดภัยที่ปล่อยออกมาโดยผู้ผลิตซอฟต์แวร์ภายใน 48 ชั่วโมงหลังจากที่แพตช์เหล่านั้นถูกปล่อยออกมา เพื่อป้องกันการโจมตีจากช่องโหว่ที่เป็นที่รู้จัก

4. การตรวจสอบและการปฏิบัติตามนโยบาย (Audit and Compliance)

องค์กรต้องดำเนินการตรวจสอบการปฏิบัติตามนโยบายนี้อย่างสม่ำเสมอ โดยการตรวจสอบการตั้งค่าระบบและการใช้งานสิทธิ์ต่าง ๆ และรายงานผลการตรวจสอบต่อผู้บริหารที่เกี่ยวข้อง นโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป

5. การฝ่าฝืนนโยบาย (Policy Violations)

ผู้ใช้งานใดที่ฝ่าฝืนนโยบายนี้จะต้องได้รับการพิจารณาและอาจต้องรับโทษตามมาตรการที่กำหนดไว้ในกฎระเบียบขององค์กร

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

รายงานผลการดำเนินการตั้งค่าอุปกรณ์ Firewall

(Firewall Configuration Implementation Report)

1. ข้อมูลทั่วไป

หน่วยงาน	โรงพยาบาลยางชุมน้อย
สถานที่ติดตั้ง	ห้อง Network / Data Center
อุปกรณ์ Firewall	Fortigate 80f
รุ่น / Serial No.	FG-80F-BDL-950-12
ระบบที่เกี่ยวข้อง	Himpro , LIS, PACS, Server/Application ภายใน

รอบระยะเวลารายงาน เดือน กันยายน พ.ศ. 2569

ผู้รับผิดชอบ	นาย กำชัย เสาเวียง
วันที่จัดทำรายงาน	19 มี.ค. 2569

2. วัตถุประสงค์

2.1 เพื่อแสดงผลการดำเนินการตั้งค่าอุปกรณ์ Firewall ให้เป็นไปตามเงื่อนไขการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ทั้ง 12 ข้อ

2.2 เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต และลดความเสี่ยงต่อระบบสารสนเทศที่สำคัญขององค์กร

3. **รายละเอียดผลการดำเนินการตามเงื่อนไขการควบคุม 12 ข้อ**

ข้อ 1: Open Port Access จากภายนอกเท่าที่จำเป็น

รายละเอียดการดำเนินการ

- เปิดการเข้าถึงจากภายนอกเฉพาะพอร์ตที่จำเป็นต่อการให้บริการ
- ตัวอย่าง: HTTPS (TCP Port 443)
- พอร์ตอื่นที่ไม่จำเป็นถูกปิดทั้งหมด

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: Firewall Rule Configuration / Dump Screen

ข้อ 2: IP Address Filter

รายละเอียดการดำเนินการ

- กำหนดขอบเขต IP Address ที่อนุญาตให้เข้าใช้งานระบบ
- ใช้การควบคุมตาม IP Location / Geographic Policy
- ปฏิเสธการเชื่อมต่อจาก IP ที่ไม่อยู่ในรายการที่กำหนด

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: System Hardening Procedure / มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

ข้อ 3: Enable IDS/IPS

รายละเอียดการดำเนินการ

- เปิดใช้งานระบบ Intrusion Detection / Prevention System
- ตรวจจับและป้องกันพฤติกรรมที่เข้าข่ายการโจมตี

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: IDS/IPS Status Log

ข้อ 4: ใช้ระบบ VPN (IPsec / SSL)

รายละเอียดการดำเนินการ

- ใช้ระบบ VPN สำหรับการเข้าถึง Server/Application ภายใน
- ใช้โปรโตคอล IPsec หรือ SSL
- ห้ามเข้าถึงระบบภายในโดยตรงจาก Internet

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: VPN Configuration

ข้อ 5: การแบ่งโซน Network ภายใน

รายละเอียดการดำเนินการ

- แบ่งโซนเครือข่ายภายใน เช่น User Zone, Server Zone, Medical System Zone
- ติดตั้ง Firewall คั่นระหว่างโซนที่มีความสำคัญ

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: Network Diagram / Firewall Zone Policy

ข้อ 6: User Access Accounts

รายละเอียดการดำเนินการ

- กำหนดสิทธิ์ผู้ใช้งานตามหน้าที่ (Role-Based / Group-Based)
- จำกัดการเข้าถึงเฉพาะระบบที่จำเป็น

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: User & Role Configuration

ข้อ 7: User Password Policy

รายละเอียดการดำเนินการ

- กำหนดความยาวรหัสผ่านไม่น้อยกว่า 12 ตัวอักษร
- ใช้การจัดเก็บรหัสผ่านแบบ Hash เช่น MD5, SHA-256

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: Password Policy Setting / **มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย** (Security Baseline Configuration Standards)

ข้อ 8: Time Sync

รายละเอียดการดำเนินการ

- ตั้งค่าอุปกรณ์ Firewall ให้ซิงโครไนซ์เวลา (NTP)
- เพื่อความถูกต้องของ Log และการตรวจสอบย้อนหลัง

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: NTP Configuration / Dump Screem Time syn ของ PC สัก 5 เครื่อง

ข้อ 9: Change Default Accounts

รายละเอียดการดำเนินการ

- เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นของอุปกรณ์
- ปิดหรือยกเลิกบัญชี Default ที่ไม่จำเป็น

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

ข้อ 10: Review Privilege Accounts

รายละเอียดการดำเนินการ

- ทบทวนบัญชีผู้มีสิทธิ์ระดับสูง (Admin / Privileged Account)
- ดำเนินการอย่างน้อยปีละ 1 ครั้ง

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: Privilege Review Record

ข้อ 11: Review Logs Access

รายละเอียดการดำเนินการ

- ตรวจสอบ Log การใช้งานและเหตุการณ์ด้านความมั่นคงปลอดภัย
- จำกัดสิทธิ์การเข้าถึง Log เฉพาะผู้ได้รับมอบหมาย

สถานะ: ✓ ดำเนินการแล้ว

หลักฐาน: Log Review Report

ข้อ 12: Feeds IOC (Option)

รายละเอียดการดำเนินการ

- เชื่อมต่อข้อมูล Indicator of Compromise (IOC) จากแหล่งภายนอก (ถ้ามี)
- ใช้ข้อมูล IOC เพื่อเพิ่มประสิทธิภาพการป้องกันภัยคุกคาม

สถานะ: ☐ ดำเนินการแล้ว / ☐ อยู่ระหว่างดำเนินการ

หลักฐาน: Threat Intelligence Configuration

4. สรุปผลการดำเนินการ

จากการตรวจสอบและตั้งค่าอุปกรณ์ Firewall ตามเงื่อนไขการควบคุมทั้ง 12 ข้อ พบว่าระบบมีการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสม สามารถลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต และมีความพร้อมสำหรับการตรวจประเมินจากหน่วยงานที่เกี่ยวข้อง

5. การรับรองรายงาน

ผู้ดำเนินการ : นาย เสฏฐวุฒิ บุญสนิท นักวิชาการคอมพิวเตอร์ / 31 มี.ค 2569

ผู้ตรวจสอบ : นายแพทย์ ปฏิเวธ ปะมา นายแพทย์ชำนาญการ / 31 มี.ค 2569

ผู้อนุมัติ : นายแพทย์ ชำนาญ สมรมิตร ผู้อำนวยการโรงพยาบาลยางชุมน้อย / 31 มี.ค 2569

รายงานการตรวจสอบการใช้ซอฟต์แวร์

(Software Usage Audit Report)

1. ข้อมูลทั่วไป

หน่วยงาน	โรงพยาบาลยางชุมน้อย
ฝ่าย/กลุ่มงาน	กลุ่มงานสุขภาพดิจิตัล
สถานที่ตรวจสอบ	โรงพยาบาลยางชุมน้อย
รอบระยะเวลาการตรวจสอบ	เดือน มีนาคม พ.ศ. 2569
ผู้ตรวจสอบ	นาย กำชัย เสาเวียง
วันที่จัดทำรายงาน	19 / มีนาคม / 2569

2. วัตถุประสงค์ของการตรวจสอบ

1. เพื่อตรวจสอบการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์และเงื่อนไขการใช้งาน
2. เพื่อป้องกันความเสี่ยงด้านกฎหมาย ความมั่นคงปลอดภัย และการละเมิดลิขสิทธิ์
3. เพื่อให้สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศ และมาตรฐานที่เกี่ยวข้อง

3. ขอบเขตการตรวจสอบ

การตรวจสอบครอบคลุม:

- เครื่องคอมพิวเตอร์แม่ข่าย (Server)
- เครื่องคอมพิวเตอร์ผู้ใช้งาน (Workstation / Notebook)
- ซอฟต์แวร์ระบบ (Operating System)
- ซอฟต์แวร์ประยุกต์ (Application Software)
- ซอฟต์แวร์เฉพาะทาง (เช่น Himpro, LIS, PACS)

4. เกณฑ์และมาตรฐานที่ใช้อ้างอิง

- นโยบายการรักษาความมมั่นคงปลอดภัยไซเบอร์
- เงื่อนไขสัญญาอนุญาตใช้ซอฟต์แวร์ (Software License Agreement)
- พ.ร.บ.ลิขสิทธิ์ และกฎหมายที่เกี่ยวข้อง เช่น PDPA

5. วิธีการตรวจสอบ

- ตรวจสอบรายการซอฟต์แวร์ที่ติดตั้งจริงในระบบ
- ตรวจสอบเอกสารสิทธิ์การใช้งาน (License / Subscription)
- เปรียบเทียบจำนวน License กับจำนวนการใช้งานจริง
- สัมภาษณ์ผู้ดูแลระบบและผู้ใช้งานที่เกี่ยวข้อง

6. ผลการตรวจสอบการใช้ซอฟต์แวร์

6.1 ภาพรวมผลการตรวจสอบ

รายการ	ผลการตรวจสอบ
ซอฟต์แวร์มีลิขสิทธิ์ถูกต้อง	✓
ซอฟต์แวร์ไม่มีลิขสิทธิ์	☐
ซอฟต์แวร์เกินจำนวน License	☐
ซอฟต์แวร์หมดอายุ License	☐

6.2 รายละเอียดซอฟต์แวร์ที่ตรวจสอบ

ลำดับ	ชื่อซอฟต์แวร์	ประเภท	จำนวนใช้งาน	จำนวน License	สถานะ
1	Windows Server	OS	5	5	ถูกต้อง
2	Microsoft Office	Software	50	50	ถูกต้อง
3	Himpro	Application	1	1	ถูกต้อง
4	LIS	Application	1	1	ถูกต้อง

7. ประเด็นที่ตรวจพบ (Findings)

- ไม่พบการติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์
- ไม่พบการใช้งานเกินจำนวน License ที่ได้รับอนุญาต
- เอกสารการจัดการ License มีการจัดเก็บครบถ้วน

8. **ข้อเสนอแนะ**

1. จัดทำทะเบียนซอฟต์แวร์ (Software Asset Register) ให้เป็นปัจจุบัน
2. ตรวจสอบ License อย่างน้อยปีละ 1 ครั้ง
3. จำกัดสิทธิ์การติดตั้งซอฟต์แวร์เฉพาะผู้ดูแลระบบ

9. **สรุปผลการตรวจสอบ**

จากการตรวจสอบการใช้ซอฟต์แวร์ในรอบระยะเวลาที่รายงาน
พบว่าการใช้งานซอฟต์แวร์ของหน่วยงานเป็นไปตามนโยบายและเงื่อนไขการใช้งาน
ไม่มีการละเมิดลิขสิทธิ์ และมีความพร้อมสำหรับการตรวจประเมินจากหน่วยงานที่เกี่ยวข้อง

10. **การรับรองรายงาน**

ผู้ดำเนินการ : นาย เสฏฐวุฒิ บุญสนิท นักวิชาการคอมพิวเตอร์ / 31 มี.ค 2569

ผู้ตรวจสอบ : นายแพทย์ ปฏิเวธ ปะมา นายแพทย์ชำนาญการ / 31 มี.ค 2569

ผู้อนุมัติ : นายแพทย์ ชำนาญ สมรมิตร ผู้อำนวยการโรงพยาบาลยางชุมน้อย / 31 มี.ค 2569

รายงานผลการดำเนินการสำรองข้อมูล (Backup Operation Report)

1. ข้อมูลทั่วไป

ชื่อหน่วยงาน โรงพยาบาลยางชุมน้อย

ฝ่าย/กลุ่มงาน กลุ่มงานสุขภาพดิจิตัล

รอบระยะเวลารายงาน เดือน มีนาคม พ.ศ. 2569

ผู้จัดทำรายงาน นาย เสฏฐวุฒิ บุญสนิท

วันที่จัดทำรายงาน 19 / มีนาคม / 2569

2. วัตถุประสงค์ของการสำรองข้อมูล

1. เพื่อป้องกันการสูญหายของข้อมูลทางการแพทย์และข้อมูลสำคัญของโรงพยาบาล
2. เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีเกิดเหตุฉุกเฉิน เช่น ระบบขัดข้อง การโจมตีทางไซเบอร์ หรือภัยพิบัติ
3. เพื่อให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และกฎหมายที่เกี่ยวข้อง

3. ขอบเขตของระบบที่ทำการสำรองข้อมูล

ลำดับ	ชื่อระบบ	ประเภทข้อมูล	ความสำคัญ
1	Himpro	ข้อมูลผู้ป่วย, เวชระเบียน, การรักษา	สูงมาก
2	LIS (Laboratory Information System)	ผลตรวจทางห้องปฏิบัติการ	สูงมาก
3	PACS (ถ้ามี)	ภาพทางการแพทย์	สูง
4	ระบบสนับสนุนอื่น ๆ	ข้อมูลบริหาร, รายงาน	ปานกลาง

4. รูปแบบและวิธีการสำรองข้อมูล

รายการ	รายละเอียด
วิธีการสำรองข้อมูล	Full Backup / Incremental Backup
ความถี่	รายวัน (Daily)
เวลาที่ดำเนินการ	00:00 – 02:00 น.
สื่อที่ใช้จัดเก็บ	NAS / External HDD / Cloud (ถ้ามี)
สถานที่จัดเก็บ	ห้อง Server / Offsite

5. ผลการดำเนินการสำรองข้อมูล (ประจำรอบเดือน มีนาคม)

วันที่	ระบบ	สถานะ	หมายเหตุ
10/12/68	Himpro	สำเร็จ	ไม่มีข้อผิดพลาด
11/12/68	LIS	สำเร็จ	ใช้เวลา 45 นาที
12/12/68	Himpro	สำเร็จ	-
13/12/68	PACS	สำเร็จ	-

6. ปัญหาที่พบ (ถ้ามี ให้ระบุรายละเอียด)

7. ปัญหา อุปสรรค และการแก้ไข

- พื้นที่จัดเก็บข้อมูลสำรองไม่เพียงพอ → ดำเนินการเพิ่ม Storage
- ระยะเวลา Backup ยาวนานในบางวัน → ปรับแผนเป็น Incremental Backup

8. ข้อเสนอแนะเพื่อการปรับปรุง

1. จัดให้มีการสำรองข้อมูลแบบ Offsite หรือ Cloud เพิ่มเติม
2. ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1–2 ครั้ง
3. จัดทำ Log การ Backup และ Restore อย่างเป็นทางการ

9. สรุปผล

จากการดำเนินการสำรองข้อมูลในรอบระยะเวลาที่รายงาน พบว่าส่วนใหญ่สามารถดำเนินการได้ตามแผนที่กำหนด ระบบสำคัญของโรงพยาบาลยังคงมีความพร้อมในการกู้คืนข้อมูลในกรณีเกิดเหตุฉุกเฉิน
ทั้งนี้ควรมีการปรับปรุงด้านโครงสร้างพื้นฐานและการเฝ้าระวังอย่างต่อเนื่อง

10. การรับรองรายงาน

ผู้ดำเนินการ : นาย เสฏฐวุฒิ บุญสนิท นักวิชาการคอมพิวเตอร์ / 31 มี.ค 2569

ผู้ตรวจสอบ : นายแพทย์ ปฏิเวธ ปะมา นายแพทย์ชำนาญการ / 31 มี.ค 2569

ผู้อนุมัติ : นายแพทย์ ชำนาญ สมรมิตร ผู้อำนวยการโรงพยาบาลยางชุมน้อย / 31 มี.ค 2569