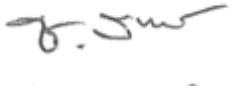
	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	**รหัสเอกสาร**	**YCN MOPH Protect -01**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	**23 มี.ค. 2569 ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

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

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**23 มี.ค. 2569**	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

	การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)	**รหัสเอกสาร**	**YCN MOPH Protect -01**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**23 มี.ค. 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

สารบัญ

การจัดการตัวตนและการควบคุมการเข้าถึง (Identity and Access Management Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43), ประมวลและกรอบ [ข้อ 22.1.1, ข้อ 22.1.2, ข้อ 22.1.3, ข้อ 22.1.4]

1. วัตถุประสงค์

กระบวนการนี้จัดทำขึ้นเพื่อควบคุมและกำกับดูแลการเข้าถึงบริการที่สำคัญของหน่วยงาน สำหรับป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและเป็นการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

2. ขอบเขต

กระบวนการนี้ครอบคลุมถึงการควบคุมการเข้าถึงสำหรับบุคลากร อุปกรณ์ และอินเทอร์เฟซ รวมถึงการตรวจสอบและจัดเก็บบันทึกการเข้าถึงบริการที่สำคัญของหน่วยงาน เพื่อให้แน่ใจว่าการเข้าถึงเหล่านี้เป็นไปตามข้อกำหนดที่ได้กำหนดไว้

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	เจ้าหน้าที่ของหน่วยงาน	เจ้าหน้าที่ของหน่วยงานต่าง ๆ ของ โรงพยาบาลยางชุมน้อย
2	ผู้ดูแลระบบ	เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลระบบสารสนเทศ หรือ ระบบคอมพิวเตอร์และเครือข่าย
3	ISM	หัวหน้าคณะทำงานระบบบริหารการรักษาความมั่นปลอดภัยสารสนเทศขององค์กร

4. หน้าที่และความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	Top Management / ISM	รับผิดชอบในการกำกับดูแลการดำเนินการตามกระบวนการควบคุมการเข้าถึง และตรวจสอบให้แน่ใจว่ามีการปฏิบัติตามข้อกำหนดอย่างครบถ้วน
2	ผู้ดูแลระบบ	รับผิดชอบในการกำหนดและจัดการสิทธิ์การเข้าถึง รวมถึงการตรวจสอบบันทึกการเข้าถึงอย่างสม่ำเสมอ
3	เจ้าหน้าที่ของหน่วยงาน	มีหน้าที่ปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการเข้าถึงบริการที่สำคัญของหน่วยงาน

5. ขั้นตอนปฏิบัติ

5.1 การจำกัดการเข้าถึง (Access Restrictions)

1) การจำกัดการเข้าถึงบริการที่สำคัญ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญถูกจำกัดเฉพาะบุคลากรที่ได้รับอนุญาต (กิจกรรมที่ได้รับอนุญาต อุปกรณ์ และอินเทอร์เฟซที่ได้รับอนุญาตเท่านั้น) โดยการกำหนดสิทธิ์การเข้าถึงระบบให้กับผู้ดูแลระบบและบุคลากรที่มีหน้าที่เกี่ยวข้องโดยตรงเท่านั้น

2) การใช้เทคนิคการตรวจสอบสิทธิ์

ขั้นตอน: กำหนดให้บุคลากรและกิจกรรมที่ได้รับอนุญาตใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับแต่ละโหมดการเข้าถึง โดยการใช้การยืนยันตัวตนสองปัจจัย (Two-Factor Authentication) สำหรับการเข้าถึงระบบที่มีข้อมูลสำคัญ

5.2 การบันทึกและตรวจสอบการเข้าถึง (Access Logging and Monitoring)

1) การเก็บรักษาบันทึกการเข้าถึง

ขั้นตอน: เก็บรักษาบันทึกของการเข้าถึงทั้งหมดและความพยายามในการเข้าถึงบริการที่สำคัญ รวมถึงตรวจสอบบันทึกเหล่านี้เป็นประจำเพื่อหากิจกรรมที่ผิดปกติ โดยการจัดทำระบบบันทึกการเข้าถึงเซิร์ฟเวอร์และตรวจสอบบันทึกเหล่านี้รายสัปดาห์เพื่อหากิจกรรมที่น่าสงสัย

2) ความสม่ำเสมอในการตรวจสอบบันทึก

ขั้นตอน: กำหนดความสม่ำเสมอในการตรวจสอบบันทึกการเข้าถึงตามความถี่ของกิจกรรมการเข้าถึงและระดับความเสี่ยงที่เกี่ยวข้อง โดยการตรวจสอบบันทึกการเข้าถึงของระบบเครือข่าย ภายในทุกวันและการตรวจสอบบันทึกการเข้าถึงข้อมูลสำคัญอย่างน้อยรายสัปดาห์

5.3 การควบคุมการเข้าถึงอินเทอร์เฟซและการเข้าถึงทางลอจิคอล (Interface and Logical Access Control)

1) การควบคุมการเข้าถึงอินเทอร์เฟซ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ เช่น USB และพอร์ตอนุกรม ต้องถูกควบคุมและดำเนินการภายใต้การดูแลของหน่วยงานที่เกี่ยวข้องเท่านั้น โดยได้รับการตั้งค่าข้อจำกัดในการใช้งานพอร์ต USB บนอุปกรณ์คอมพิวเตอร์ที่ใช้ในหน่วยงาน

2) การเข้าถึงทางลอจิกคอล

ขั้นตอน: กำกับดูแลการเข้าถึงทางลอจิกคอลของบริการที่สำคัญ โดยให้ดำเนินการในสถานที่ที่ได้รับอนุญาตและอยู่ภายใต้การควบคุมของหน่วยงาน โดยการกำหนดให้การเข้าถึงระบบจัดการ ข้อมูลต้องทำจากภายในหน่วยงานเท่านั้น และห้ามเข้าถึงจากภายนอกหน่วยงาน

5.4 การควบคุมกำกับดูแลให้มีการลงนามในเอกสารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ขั้นตอน: ในกรณีที่ผู้ให้บริการภายนอกมีการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของหน่วยงาน หน่วยงานจะต้องดำเนินการให้ผู้ให้บริการภายนอกลงในนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และต้องปฏิบัติตามนโยบายกฎระเบียบ ขั้นตอนการปฏิบัติงานและวิธีปฏิบัติงานของหน่วยงานอย่างเคร่งครัด

5.5 การควบคุมกำกับดูแลผู้ให้บริการภายนอกที่ต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

ขั้นตอน: 1. ในกรณีที่ผู้ให้บริการภายนอกต้องการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติจาก Top Management / ISM

2. ผู้ดูแลระบบ ดำเนินการกำหนดระยะเวลาของสิทธิ์ในการใช้งาน/เข้าใช้งาน ทำการบันทึกสิทธิ์ในการเข้าถึงระบบต่าง ๆ และตรวจสอบการใช้งานของผู้ให้บริการภายนอก

3. ผู้ดูแลระบบ ดำเนินการเพิกถอนสิทธิ์ในการเข้าระบบต่าง ๆ ของผู้ให้บริการภายนอก เมื่อหมดความจำเป็นตามวัตถุประสงค์ที่ได้ขออนุมัติไว้

6. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

7. เอกสารที่เกี่ยวข้อง

ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร
1		

8. เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) - การควบคุมการเข้าถึง (Access Control)
2	-หลักฐาน Logs of Access
3	-หลักฐานสิทธิ์การเข้าถึงระบบ (User Permission Matrix)
4	-หลักฐานการจัดการตัวตน (Identity Users)

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

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