วิธีปฏิบัติงาน	เรื่อง ๑ :แนวปฏิบัติด้านการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control Policy)			
รหัสเอกสาร : W-MIS-๐๑	เริ่มใช้ : ๑/๑๐/๒๕๖๘	พิมพ์ครั้งที่ : ๑	แก้ไขครั้งที่ :	หน้า :๑

ผู้รับผิดชอบ		ลงชื่อ	วัน เดือน ปี
จัดทำโดย	นายวิจิต สุขศรี		๑/๑๐/๒๕๖๘
ทบทวนโดย	นางปัทมาพร ชนะมาร		๙/๑๐/๒๕๖๘
อนุมัติโดย	พญ.เบญจพร อินทกรอุดม		๙/๑๐/๒๕๖๘

โรงพยาบาลวาปีปทุม :	**หน้าที่ :** ๑/๑
วิธีปฏิบัติเลขที่ : WT-๐๑	**ฉบับที่ :** ๑
เรื่อง : การสำรองข้อมูล	**วันที่ : ๑/๑๐/๒๕๖๙**
แผนก : ศูนย์ข้อมูล	**แผนกที่เกี่ยวข้อง :** ศูนย์ข้อมูล
ผู้จัดทำ : นายวิจิต สุขศรี	**ผู้อนุมัติ :** พญ.เบญจพร อินทกรอุดม

๑. แนวปฏิบัติด้านการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control Policy)

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลสุขภาพส่วนบุคคล

๑. การบริหารจัดการบัญชีผู้ใช้งาน (User Account Management)

- **การลงทะเบียน:** การสร้างบัญชีผู้ใช้งานต้องทำเป็นลายลักษณ์อักษร โดยผ่านการอนุมัติจากหัวหน้าแผนกและฝ่าย IT
- **บัญชีรายบุคคล:** ห้ามใช้บัญชีผู้ใช้งานร่วมกัน (No Shared Accounts) เจ้าหน้าที่ทุกคนต้องมี Username และ Password เฉพาะตัว เพื่อระบุตัวตนในการทำรายการต่างๆ ได้ชัดเจน
- **การยกเลิกสิทธิ์:** เมื่อเจ้าหน้าที่ลาออก โอนย้าย หรือสิ้นสุดสัญญาจ้าง ฝ่ายบุคคล (HR) ต้องแจ้งฝ่าย IT เพื่อ **ระงับสิทธิ์ทันที** (ภายใน ๒๔ ชั่วโมง)

๒. การควบคุมสิทธิ์ตามบทบาทหน้าที่ (Role-Based Access Control - RBAC)

- **หลักการสิทธิ์เท่าที่จำเป็น (Least Privilege):** เจ้าหน้าที่จะได้รับสิทธิ์เข้าถึงข้อมูลเฉพาะที่เกี่ยวข้องกับหน้าที่การงานเท่านั้น เช่น
  - **แพทย์/พยาบาล:** เข้าถึงประวัติการรักษาและผลแล็บของผู้ป่วย
  - **ฝ่ายการเงิน:** เข้าถึงข้อมูลค่ารักษาพยาบาลและสิทธิการรักษา
  - **ฝ่าย IT:** เข้าถึงโครงสร้างระบบแต่ไม่มีสิทธิ์อ่านข้อมูลการรักษา (เว้นแต่ได้รับอนุญาต)
- **การจำกัดสิทธิ์ผู้ดูแลระบบ (Admin):** จำกัดจำนวนผู้ถือสิทธิ์ Admin ให้มีน้อยที่สุด และต้องใช้งานเพื่อการตั้งค่าระบบเท่านั้น ไม่ใช้เพื่อการทำงานทั่วไป

๓. การพิสูจน์ตัวตนและความปลอดภัยของรหัสผ่าน (Authentication)

- **มาตรฐานรหัสผ่าน:** ต้องมีความยาวอย่างน้อย ๘ ตัวอักษร ประกอบด้วยอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และสัญลักษณ์
- **การเปลี่ยนรหัสผ่าน:** บังคับเปลี่ยนรหัสผ่านอย่างน้อยทุก ๙๐ วัน และห้ามใช้รหัสซ้ำกับ ๓ ครั้งล่าสุด
- **การยืนยันตัวตนหลายชั้น (MFA):** สำหรับการเข้าถึงระบบจากภายนอกโรงพยาบาล (Remote Access) หรือการเข้าถึงฐานข้อมูลวิกฤต **ต้อง** มีการยืนยันตัวตนชั้นที่ ๒ (เช่น OTP หรือแอปยืนยันตัวตน)

๔. การใช้งานนอกสถานที่และการเชื่อมต่อจากระยะไกล (Remote Access)

- **การใช้งาน VPN:** การเชื่อมต่อเข้าระบบภายในจากภายนอกโรงพยาบาล ต้องผ่านระบบเครือข่ายเสมือนส่วนตัว (VPN) ของโรงพยาบาลเท่านั้น
- **อุปกรณ์ที่อนุญาต:** ห้ามใช้เครื่องคอมพิวเตอร์สาธารณะ (เช่น ร้านอินเทอร์เน็ต) เข้าถึงระบบฐานข้อมูลผู้ป่วย

๕. ความปลอดภัยของสถานีงาน (Workstation Security)

- **การล็อกหน้าจออัตโนมัติ:** กำหนดให้หน้าจอคอมพิวเตอร์ล็อกอัตโนมัติหากไม่มีการใช้งานภายใน ๕-๑๐ นาที
- **นโยบายโต๊ะสะอาด/หน้าจอสะอาด:** เจ้าหน้าที่ต้องไม่จดรหัสผ่านทิ้งไว้บนโต๊ะ หรือติดไว้ที่หน้าจอคอมพิวเตอร์

๖. การตรวจสอบและทบทวนสิทธิ์ (Access Review & Audit)

- **การสุ่มตรวจ Log:** ฝ่าย IT ต้องตรวจสอบบันทึกการเข้าใช้งาน (Event Logs) เป็นประจำเพื่อเฝ้าระวังพฤติกรรมที่ผิดปกติ
- **การทบทวนรอบปี:** คณะกรรมการฯ ต้องทำการทบทวนรายชื่อและสิทธิ์การเข้าถึงของเจ้าหน้าที่ทุกคนอย่างน้อยปีละ ๒ ครั้ง เพื่อปรับปรุงให้เป็นปัจจุบัน

ตารางสรุปสิทธิ์การเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control Matrix)
สัญลักษณ์ระดับสิทธิ์:

- **R (Read):** อ่าน/ดูข้อมูลได้อย่างเดียว
- **W (Write):** เพิ่ม/แก้ไข/บันทึกข้อมูลได้
- **D (Delete):** ลบข้อมูลได้ (จำกัดเฉพาะผู้มีอำนาจสูง)
- **N (No Access):** ไม่มีสิทธิ์เข้าถึงข้อมูล

ตำแหน่งงาน / ข้อมูล	ข้อมูลส่วนตัวผู้ป่วย (Name/ID)	ประวัติการรักษา (Clinical Data)	การสั่งยา/เวชภัณฑ์ (Prescription)	ข้อมูลการเงิน/สิทธิ (Billing)	รายงานสถิติ/บริหาร (Dashboard)
๑. แพทย์ (Physician)	R/W	R/W	R/W	R	R
๒. พยาบาล (Nurse)	R/W	R/W	R (ดูคำสั่งยา)	R	N
๓. เภสัชกร (Pharmacist)	R	R (เพื่อตรวจสอบ)	R/W (บันทึกจ่ายยา)	R	R
๔. เวชระเบียน (Medical Record)	R/W	R	N	R	R
๕. การเงิน/บัญชี (Finance)	R	N	N	R/W	R

๖. ฝ่ายไอที (IT Admin)	R (เฉพาะเพื่อซ่อมแซม)	N*	N	N	R (เชิงระบบ)
๗. ผู้บริหาร (Executive)	N	N	N	R	R

**หมายเหตุ: ฝ่ายไอทีมีสิทธิ์เข้าถึงโครงสร้างฐานข้อมูล แต่ไม่ได้รับอนุญาตให้อ่านรายละเอียดการรักษาของผู้ป่วยรายบุคคล เว้นแต่จะได้รับอนุมัติเป็นกรณีพิเศษเพื่อการตรวจสอบ (Auditing)*

คำอธิบายเพิ่มเติมประกอบตาราง:

๑. **การควบคุมการบันทึก (Data Integrity):**

๑. เฉพาะ **แพทย์** เท่านั้นที่มีสิทธิ์สั่งการรักษาและสั่งยาในระบบ

๒. **พยาบาล** มีสิทธิ์บันทึกสัญญาณชีพ (V/S) และบันทึกการพยาบาล แต่ไม่สามารถแก้ไขคำสั่งสั่งยาของแพทย์ได้

๒. **การจำกัดการมองเห็น (Confidentiality):**

๑. **ฝ่ายการเงินและเวชระเบียน** จะเห็นเฉพาะข้อมูลที่จำเป็นต้องใช้ในการเบิกจ่ายหรือลงทะเบียนเท่านั้น โดยระบบควรปิดกั้น (Masking) ข้อมูลการวินิจฉัยโรคที่ละเอียดอ่อน (Sensitive Data) หากไม่จำเป็นต่อหน้าที่

๓. **การลบข้อมูล (Data Deletion):**

๑. สิทธิ์ในการ **ลบ (Delete)** ข้อมูลสำคัญ จะต้องจำกัดไว้ที่ระดับหัวหน้าแผนกหรือผู้ดูแลระบบสูงสุด และต้องมีการบันทึกเหตุผล (Reason) ทุกครั้งที่มีการลบข้อมูล

๔. **การตรวจสอบภายหลัง (Audit Trail):**

๑. ทุกการเข้าถึง (Read) และการแก้ไข (Write) จะต้องถูกบันทึกไว้ใน **Log File** ของระบบ เพื่อสามารถตรวจสอบย้อนหลังได้ว่าใครเข้าถึงข้อมูลใคร เมื่อเวลาใด

ผู้รับผิดชอบ		ลงชื่อ	วัน เดือน ปี
จัดทำโดย	นายวิจิต สุขศรี		๑/๑๐/๒๕๖๘
ทบทวนโดย	นางปัทมาพร ชนะมาร		๙/๑๐/๒๕๖๘
อนุมัติโดย	พญ.เบญจพร อินทกรอุดม		๙/๑๐/๒๕๖๘

โรงพยาบาลวาปีปทุม :	**หน้าที่ :** ๑/๑
วิธีปฏิบัติเลขที่ : WT-๐๒	**ฉบับที่ :** ๑
เรื่อง : การสำรองข้อมูล	**วันที่ : ๑/๑๐/๒๕๖๙**
แผนก : ศูนย์ข้อมูล	**แผนกที่เกี่ยวข้อง :** ศูนย์ข้อมูล
ผู้จัดทำ : นายวิจิต สุขศรี	**ผู้อนุมัติ :** พญ.เบญจพร อินทกรอุดม

การสำรองข้อมูล

นโยบาย

เพื่อใช้เป็นคู่มือในการสำรองข้อมูลสารสนเทศของโรงพยาบาลของโรงพยาบาล

วิธีปฏิบัติ

1. ผู้ดูแลระบบสร้าง Folder สำหรับสำรองข้อมูลในเครื่อง SRVER สำรองข้อมูล
2. ผู้ดูแลระบบกำหนดสร้างชุดคำสั่งให้ระบบทำการสำรองข้อมูลในช่วงเวลา ๑๒.๔๐ น. และ ๒๓.๔๐ น. ของทุกวันไว้ในเครื่องสำรอง
3. ระบบจะทำการสำรองข้อมูลอัตโนมัติทุกวันตามเวลาดังกล่าว
4. ผู้ดูแลระบบจะทำการ Copy File ข้อมูลสำรองอีกครั้งจากเครื่องสำรองเก็บไว้ใน Harddisk External ทุกวัน เก็บในตู้เก็บอุปกรณ์และใส่กุญแจเพื่อเป็นการป้องกันการนำข้อมูลไปใช้โดยมิชอบ
5. ผู้ดูแลระบบจะทำการสำรองข้อมูลจาก Harddisk External เก็บไว้ยัง DVD และเก็บไว้ในตู้นิรภัยอีกครั้งหนึ่ง ทุก๑๕ วัน
6. การขอข้อมูลสำรองมาใช้งาน ให้ผู้ขอข้อมูลสำรองยื่นเรื่องที่ผู้ดูแลระบบโดยการกรอกแบบฟอร์มหรือทำหนังสือขอยืมอุปกรณ์ ซึ่งผู้ดูแลระบบจะต้องแจ้งเรื่องต่อหัวหน้างานและประธานสารสนเทศหรือผู้เกี่ยวข้องทราบ จึงจะสามารถอนุญาตให้ผู้ขอข้อมูลสำรองนำข้อมูลไปใช้งานได้

รหัสเอกสาร : W-MIS-๐๐๓	เริ่มใช้ : ๑/๑๐/๒๕๖๘	พิมพ์ครั้งที่ : ๑	แก้ไขครั้งที่ :	หน้า :๑

ผู้รับผิดชอบ		ลงชื่อ	วัน เดือน ปี
จัดทำโดย	นายวิจิต สุขศรี		๑/๑๐/๒๕๖๘
ทบทวนโดย	นางปัทมาพร ชนะมาร		๙/๑๐/๒๕๖๘
อนุมัติโดย	พญ.เบญจพร อินทกรอุดม		๙/๑๐/๒๕๖๘

โรงพยาบาลวาปีปทุม :	**หน้าที่ :** ๑/๑
วิธีปฏิบัติเลขที่ : WT-๐๓	**ฉบับที่ :** ๑
เรื่อง : การสำรองข้อมูล	**วันที่ : ๑/๑๐/๒๕๖๙**
แผนก : ศูนย์ข้อมูล	**แผนกที่เกี่ยวข้อง :** ศูนย์ข้อมูล
ผู้จัดทำ : นายวิจิต สุขศรี	**ผู้อนุมัติ :** พญ.เบญจพร อินทกรอุดม

๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit & Risk Assessment)

๑. วัตถุประสงค์ (Purpose)

- เพื่อค้นหา วิเคราะห์ และประเมินโอกาสที่จะเกิดภัยคุกคามต่อระบบสารสนเทศของโรงพยาบาล
- เพื่อกำหนดมาตรการจัดการความเสี่ยง (Risk Treatment) ให้สอดคล้องกับมาตรฐานความปลอดภัยและกฎหมายที่เกี่ยวข้อง

๒. ขอบข่าย (Scope)

- ครอบคลุมทรัพย์สินสารสนเทศ (Information Assets) ทั้งหมด ได้แก่ ข้อมูลผู้ป่วย (HIS), อุปกรณ์แม่ข่าย (Server), ระบบเครือข่าย และบุคลากรที่เกี่ยวข้องกับการใช้งานระบบ

๓. ความรับผิดชอบ (Responsibility)

- **คณะกรรมการสารสนเทศ (MIS):** กำหนดเกณฑ์การให้คะแนนความเสี่ยง (Likelihood & Impact)
- **งานสารสนเทศ (IT):** ดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment) และรวบรวมผลประเมิน
- **ทุกหน่วยงาน:** ร่วมระบุความเสี่ยงที่พบจากการใช้งานจริงในหน้างานของตนเอง

๔. วิธีปฏิบัติ (Procedure)

- **๔.๑ การระบุทรัพย์สินและความเสี่ยง:** ทุกแผนกจัดทำบัญชีทรัพย์สินสารสนเทศ และระบุภัยคุกคามที่อาจเกิดขึ้น (เช่น ข้อมูลรั่วไหล, ระบบล่ม, อุปกรณ์ชำรุด)
- **๔.๒ การวิเคราะห์ความเสี่ยง:** ประเมินความเสี่ยงตามเกณฑ์ **โอกาส (๑-๕) x ผลกระทบ (๑-๕)** เพื่อจัดระดับความเสี่ยง (Low, Medium, High, Extreme)
- **๔.๓ การจัดทำแผนจัดการความเสี่ยง:** สำหรับความเสี่ยงที่อยู่ในระดับสูงขึ้นไป ต้องกำหนดมาตรการแก้ไข ระยะเวลา และผู้รับผิดชอบที่ชัดเจน

- **๔.๔ การตรวจสอบความปลอดภัย (Audit):**
    - **Internal Audit:** ทีม IT ตรวจสอบความปลอดภัยเชิงเทคนิค (เช่น การสแกนไวรัส, การอัปเดต Patch) อย่างน้อยทุกไตรมาส
    - **Access Audit:** ตรวจสอบประวัติการเข้าถึงข้อมูล (Log) ของผู้ใช้งานเพื่อค้นหาพฤติกรรมผิดปกติ

๕. การติดตามและรายงานผล (Monitoring & Reporting)

- คณะทำงานสารสนเทศสรุปผลการประเมินและความเสี่ยงที่ยังคงเหลือ (Residual Risk) เพื่อเสนอต่อ **คณะกรรมการบริหารความเสี่ยง** และ **ผู้อำนวยการโรงพยาบาล** อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบงานที่สำคัญ

แบบฟอร์มบันทึกความเสี่ยง (แนบท้ายระเบียบปฏิบัติ)

(คุณสามารถนำตารางนี้ไปใช้เก็บข้อมูลจริงในโรงพยาบาลได้เลยครับ)

รายการทรัพย์สิน	**ภัยคุกคามที่อาจเกิด**	**คะแนนความเสี่ยง (L x I)**	**ระดับความเสี่ยง**	**มาตรการจัดการ**
ฐานข้อมูลผู้ป่วย (HIS)	การโจมตีจาก Ransomware	๔ x ๕ = ๒๐	**วิกฤต**	ทำ Offline Backup รายวัน
รหัสผ่านผู้ใช้งาน	การสุ่มรหัสผ่าน (Brute Force)	๓ x ๔ = ๑๒	**สูง**	บังคับใช้ MFA / เปลี่ยนรหัสทุก ๙๐ วัน
ระบบ Wi-Fi แผนก	บุคคลภายนอกลักลอบเข้าถึง	๓ x ๓ = ๙	**ปานกลาง**	แยกวง Guest Wi-Fi ออกจากวงภายใน