	การจัดการตัวตนและการควบคุมการเข้าถึง **(Identity and Access Management Procedure)**	รหัสเอกสาร	MLH-MOPH-Protect -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นายสุทธิชัย เสาว์สิงห์	นายพรศักดิ์ ตามวงค์	นพ.สุขชัย เธียรเศวตตระกูล
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	ผู้อำนวยการโรงพยาบาลแม่ลาว
วันเดือนปี	22 ธันวาคม 2568	30 ธันวาคม 2568	5 มกราคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	5 ม.ค 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

สารบัญ

1. วัตถุประสงค์ 3
2. ขอบเขต 3
3. คำจำกัดความ/นิยามศัพท์เฉพาะ 3
4. หน้าที่และความรับผิดชอบ 4
5. ขั้นตอนปฏิบัติ 4
6. เอกสารที่เกี่ยวข้อง 6
7. เอกสารอ้างอิง 7

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 โรงพยาบาลแม่ลาว
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)