<table>
<tr><td rowspan="3"></td><td colspan="2">มาตรฐานความปลอดภัยศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)</td></tr>
<tr><td>กลุ่มงาน / หน่วยงาน สุขภาพดิจิทัล</td><td>หน้าที่ หน้า 1 จาก 11</td></tr>
<tr><td>SOP – มาตรฐานจำเป็นต่อความปลอดภัย<br>เรื่อง มาตรฐานความมั่นคงปลอดภัยทางกายภาพ Data Center</td><td>วันที่เริ่มใช้ 1 ตุลาคม 2568<br>แก้ไขครั้งที่ 00</td></tr>
<tr><td>ผู้จัดทำ นายสุทธิชัย เสาว์สิงห์<br>ตำแหน่ง นวก.คอมพิวเตอร์</td><td>ผู้ทบทวน นายพรศักดิ์ ตามวงค์<br>ตำแหน่ง นวก.คอมพิวเตอร์ปฏิบัติการ</td><td>ผู้อนุมัติ นพ.สุขชัย เธียรเศวตตระกูล<br>ตำแหน่ง ผู้อำนวยการ รพ.แม่ลาว</td></tr>
</table>

**๑.วัตถุประสงค์**

เพื่อใช้เป็นแนวนโยบาย การควบคุมการเข้าถึงทางกายภาพ โดยไม่ได้รับอนุญาต อีกทั้งเพื่อป้องกันทรัพย์สินขององค์กร จากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต โดยจัดทำขึ้นตามข้อกาหนดของมาตรฐานระบบจัดการ ISO ๒๗๐๐๑:๒๐๑๓ โรงพยาบาลแม่ลาว

ข้อกำหนดจัดการ ISO ๒๗๐๐๑:๒๐๑๓ ที่เกี่ยวข้อง ประกอบด้วย

- A.๑๑ นโยบายความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security Policy)

**๒. ขอบเขต**

ใช้เป็นแนวทางการปฏิบัติเพื่อเฝ้าระวัง และรักษาความมั่นคงปลอดภัยทางกายภาพเฉพาะภายในโรงพยาบาลแม่ลาว

**๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area) (Annex A: A.๑๑.๑)**

เพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต การก่อให้ เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินขององค์กร อีกทั้งเพื่อป้องกันทรัพย์สินขององค์กร จากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต และป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมการดาเนินงาน

**๓.๑ การจัดทำขอบเขตหรือบริเวณโดยรอบพื้นที่ควบคุม (Physical Security Perimeter)**

หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้ มีการควบคุมห้อง Data Center ดังต่อไปนี้

๑. ห้อง Data Center ต้องอยู่ในอาคารซึ่งอยู่ในพื้นที่ที่มีรั้วล้อมรอบ

๒. ผนังของอาคาร ต้องมีโครงสร้างที่แข็งแรง ประตูชั้นนอกทั้งหมดต้องมีการป้องกันการเข้าถึงโดยมิได้รับอนุญาตอย่างแน่นหนา ด้วยกลไกควบคุมและมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

๓. ภายในห้อง Data Center อาคารที่มีห้อง Data Center ตั้งอยู่ และบริเวณล้อมรอบ ต้องมีการติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่ที่สำคัญทั้งหมด โดยต้องเก็บข้อมูลบันทึกภาพไว้ อย่างน้อยเป็นเวลา ๙๐ วัน

**๓.๒ การควบคุมการเข้า-ออกทางกายภาพ (Physical Entry Controls)การเข้า-ออกของห้อง Data Center ต้องมีการควบคุม** ดังต่อไปนี้

๑. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการรักษาความปลอดภัยบริเวณทางเข้า – ออกของห้อง Data Center (ผ่านทาง Access card หรือเจ้าหน้าที่รักษาความปลอดภัย) เพื่อเฝ้าระวังและรักษาความปลอดภัย

๒. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องกำหนดสิทธิ์พนักงานและลูกจ้างหน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กรตามสิทธิ์การเข้าถึงที่ระบุโดยส่วนงานที่เป็นเจ้าของทรัพย์สิน และตามช่วงเวลาที่มีสิทธิ์ผ่านเข้า – ออกห้อง Data Center อย่างเป็นลายลักษณ์อักษร

๓. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องทบทวนสิทธิ์ผ่านเข้า – ออกห้อง Data Center เป็นประจำอย่างน้อยทุก ๖ เดือน หรือเมื่อมีการเปลี่ยนแปลง

๔. ในการเข้า – ออกห้อง Data Center ทุกคนที่เข้า – ออกห้อง Data Center ต้องทำการลงบันทึกข้อมูลในแบบฟอร์มเข้า-ออกพื้นที่ (Physical Entry Control)

๕. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องตรวจสอบความถูกต้องครบถ้วนของแบบฟอร์มเข้า-ออกพื้นที่ (Physical Entry Control) เป็นประจำทุกสัปดาห์และจัดเก็บบันทึกผู้มาติดต่อไว้อย่างน้อย ๑ ปี

๖. ประตูบริเวณทางเข้า-ออกของห้อง Data Center ควรมีระบบควบคุมการเข้าออก ที่มีการรักษาความมั่นคงปลอดภัยเช่น การใช้บัตรผ่านเฉพาะบุคคล (Access Card) การใช้รหัสผ่านเฉพาะบุคคล (PIN) หรือระบบตรวจสอบลายนิ้วมือเป็นต้น โดยหัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ควรตรวจสอบประวัติการเข้า-ออกของห้อง Data Center เป็นประจาอย่างน้อยทุก ๓ เดือน เพื่อหาพฤติกรรมการเข้าออกที่ผิดไปจากปกติพร้อมทั้งควรมีการจัดเก็บประวัติ การเข้าออกห้อง Data Center ไว้ อย่างน้อย ๑ ปี

**๓.๓ การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices ,Rooms, and Facilities)**

๑. ส่วนงานที่รับผิดชอบด้านความปลอดภัยอาคารและสถานที่ หรือ หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีเจ้าหน้าที่หรือวิธีการรักษาความปลอดภัย เพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น

๒. พนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร และนักศึกษาฝึกงาน ควรมีวิธีการป้องกันการเข้าถึงสารสนเทศ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม ขององค์กร เมื่อไม่อยู่ภายในห้อง

**๓.๔ การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against External and Environmental Threats)**

๑. มีระบบป้องกันไฟไหม้ เช่น ระบบตรวจจับความร้อน ระบบตรวจจับควัน เป็นต้น

๒. มีอุปกรณ์ดับเพลิงอย่างพอเพียงและติดตั้งอยู่ในจุดที่สะดวกแก่การใช้งาน ทั้งบริเวณอาคารที่ตั้งห้อง Data Center และภายในห้อง Data Center

๓. มีระบบควบคุมอุณหภูมิและความชื้น โดยอุณหภูมิและความชื้นต้องอยู่ในระดับที่เหมาะสมกับอุปกรณ์ประมวลผลสารสนเทศที่จัดอยู่ในห้อง Data Center

๔. มีการควบคุมมิให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้ หรือวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในห้อง Data Center

**๓.๕ การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas) ทุกคนที่ปฏิบัติงานภายในห้อง Data Center** ต้องปฏิบัติตามข้อปฏิบัติ ดังต่อไปนี้

๑. เมื่อพบเห็นผู้ที่มีพฤติกรรมน่าสงสัยอยู่ภายในห้อง Data Center ต้องแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้อง โดยทันที

๒. ห้ามสูบบุหรี่ ภายในห้อง Data Center

๓. ห้ามนำอาหารและเครื่องดื่ม เข้าไปในห้อง Data Center

๔. ห้ามนำอุปกรณ์ที่บันทึกรูปภาพ วิดีทัศน์หรือเสียง และสื่อบันทึกชนิดเคลื่อนที่ เข้าไปภายในห้อง Data Centerเว้นแต่ได้รับอนุมัติจากหัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่เท่านั้น

**๓.๖ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access,Delivery, and Loading Areas)**

หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการควบคุมสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกสำหรับห้อง Data Center ดังต่อไปนี้

๑. มีบริเวณพักรอสำหรับบุคคลภายนอกที่ไม่สามารถเข้าถึงบริเวณอื่นๆ ของห้อง Data Center

๒. มีบริเวณสำหรับการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อให้สามารถส่งมอบผลิตภัณฑ์โดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่นๆ ของห้อง Data Center

๓. มีการตรวจสอบว่าผลิตภัณฑ์ดังกล่าวอาจจะก่อให้เกิดความเสียหายต่อห้อง Data Center หรือไม่ เช่น วัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้ หรือวัสดุที่ติดไฟได้ง่าย ก่อนจะเคลื่อนย้ายผลิตภัณฑ์จากบริเวณสำหรับการเข้าถึงหรือการ ส่งมอบไปยังจุดที่ติดตั้งใช้งานจริง

**๔ การสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์ (Equipment) (Annex A: A.๑๑.๒)**

**๔.๑ การจัดวางและป้องกันอุปกรณ์ (Equipment Siting and Protection)**

มีการจัดวางและป้องกันอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม และอุปกรณ์สานักงานขององค์กร เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยมิได้รับอนุญาต

ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคมหรืออุปกรณ์โทรคมนาคม และอุปกรณ์สานักงานขององค์กร ดังต่อไปนี้

๑. ต้องจัดวาง อยู่ในพื้นที่ที่ได้รับการจัดสรรไว้ เพื่อให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๒. ต้องจัดวางอยู่ในพื้นที่และสภาพแวดล้อมที่เหมาะสมตามคู่มือการใช้งานของเจ้าของผลิตภัณฑ์

๓. ต้องจัดวางอยู่ในพื้นที่และสภาพแวดล้อมที่เหมาะสม เพื่อลดความเสี่ยงอันเกิดจากความเสียหายจากภัยธรรมชาติ เช่นอุทกภัย วาตภัย เป็นต้น

๔. ต้องได้รับการป้องกันการสูญหายอย่างเหมาะสม เช่น การใช้สายล็อคอุปกรณ์ เป็นต้น

๕. ต้องได้รับการป้องกันความเสียหายอันเกิดจากระบบไฟฟ้าอย่างเหมาะสม เช่น มีระบบกรองกระแส ไฟฟ้า (StabilizerSystem) เป็นต้น

๖. ต้องมีการประกันภัยเพียงพอตามความเหมาะสม

**๔.๒ การบริหารจัดการอุปกรณ์สนับสนุนการประมวลผลสารสนเทศ (Supporting Utilities)**

อุปกรณ์สนับสนุนการประมวลผลสารสนเทศสำหรับห้อง Data Center ต้องมีการควบคุม ดังต่อไปนี้

๑. ผู้บริหารสารสนเทศระดับสูง ต้องจัดให้มีอุปกรณ์สนับสนุนการประมวลผลสารสนเทศอย่างเพียงพอ เพื่อสนับสนุนการทำงานของอุปกรณ์ประมวลผลสารสนเทศ

๒. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการตรวจสอบการทำงานของอุปกรณ์สนับสนุนการประมวลผลสารสนเทศอย่างสม่ำเสมอ

๓. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีระบบหรือกระบวนการในการปิดการทำงานฉุกเฉินสำหรับอุปกรณ์ประมวลผลสารสนเทศเมื่อเกิดเหตุฉุกเฉินหรือระบบไฟฟ้าสำรองมีกระแสไฟฟ้า

เหลืออยู่ในจำนวนจำกัดเพื่อป้องกันความเสียหายอันเกิดจากอุปกรณ์ประมวลผลสารสนเทศไม่ได้รับการปิดการทำงานได้ทันท่วงที

**๔.๓ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)**

กรณีภายในห้อง Data Center ภายในห้องคอมพิวเตอร์ส่วนงานที่รับผิดชอบระบบสารสนเทศ และหัวหน้าส่วนงานที่รับผิดชอบ

พื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการควบคุมการ เดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ ดังต่อไปนี้

๑. สายไฟฟ้า สายสื่อสารและสายเคเบิ้ลอื่นๆ ต้องวางสายภายในท่อหรือรางร้อยสาย หรือได้รับการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อหลีกเลี่ยงจากการเกิดความเสียหาย หรือการดักรับข้อมูลโดยผู้ที่มิได้รับอนุญาต

๒. ระงับสัญญาณหรือการให้บริการสำหรับ สายสื่อสารและสายเคเบิ้ลอื่นๆ ที่ไม่มีความจำเป็นต้องใช้งาน

๓. สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสมเพื่อป้องกันการรบกวนของสัญญาณ

๔. สายสื่อสาร และสายเคเบิ้ลอื่นๆ ต้องได้รับการทำสัญลักษณ์อย่างชัดเจน

๕. สำหรับสายสื่อสาร และสายเคเบิ้ลอื่นๆ ที่ใช้สำหรับส่งผ่านสารสนเทศ ควรพิจารณาให้มีการควบคุม ดังต่อไปนี้

๕.๑ ติดตั้งท่อหุ้มสายชนิดพิเศษ (Armored Conduit)

๕.๒ มีเส้นทางสำรอง

๕.๓ ใช้สายใยแก้วนำแสง (Fiber Optic)

๕.๔ ใช้อุปกรณ์ห่อหุ้มสายเพื่อป้องกันคลื่นแม่เหล็กไฟฟ้า

๕.๕ ตรวจสอบระบบสายเพื่อตรวจจับอุปกรณ์แปลกปลอม

๕.๖ ควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel)

**๔.๔ การบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance)**

๑. มีการบารุงรักษาอุปกรณ์อย่างสม่าเสมอ อย่างน้อยตามที่ได้ระบุในคู่มือการใช้งานของอุปกรณ์ และจัดให้มีการซ่อมบำรุงอย่างทันท่วงทีตามความสำคัญของระบบ

๒. มีการบันทึกประวัติการบำรุงรักษาและ ซ่อมบำรุงอุปกรณ์ ทั้งนี้บันทึกดังกล่าวต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

๒.๑ วันที่ในการบำรุงรักษาและซ่อมบำรุง

๒.๒ ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุง

๒.๓ รายละเอียดการบำรุงรักษาและซ่อมบำรุง

๒.๔ สถานะของอุปกรณ์

๒.๕ ปัญหาที่พบและการแก้ไข

๒.๖ ลายมือชื่อผู้บำรุงรักษาและซ่อมบำรุง

๓. ถ้ามีการว่าจ้างหน่วยงานภายนอกเพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ ส่วนงานที่ว่าจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการว่าจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

**๔.๕ การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Assets)**

๑. บุคคลผู้นำอุปกรณ์ออกนอกอาคารหรือองค์กร ต้องได้รับการอนุมัติจากหัวหน้าส่วนงานที่เป็นเจ้าของทรัพย์สินก่อนเท่านั้น

๒. เจ้าหน้าที่รักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมาย ต้องตรวจสอบลักษณะของทรัพย์สินที่นำออก โดยเปรียบเทียบกับเอกสารการนำของออกอย่างละเอียดรอบคอบ

๓. เจ้าหน้าที่รักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมาย ต้องเก็บเอกสารการนำของออก จัดทำบันทึกการอนุญาตการนำของออกนอกอาคารหรือนอกองค์กร และรายงานการนำทรัพย์สินออกไปยังส่วนงานที่เป็นเจ้าของทรัพย์สิน เพื่อตรวจสอบและยืนยันความถูกต้องตามระยะเวลาที่กาหนด อ้างอิง Asset management Policy

**๔.๖ การควบคุมการกำจัดอุปกรณ์และการนำกลับมาใช้งาน (Secure Disposal or Re-use of Equipment)** ในการจำหน่ายอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม ขององค์กรออกนอกองค์กร ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ก่อนการจำหน่าย เพื่อให้ มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนากลับมาได้ (Non-Retrievable) โดยอ้างอิงจากเอกสาร AssetManagement Policy

**๔.๗ การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งาน (Unattended User Equipment)**

๑. ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการจัดวางอุปกรณ์อย่างเหมาะสม เพื่อป้องกันการเข้าถึงขณะที่ไม่มีผู้ใช้งาน

๒. ส่วนงานที่รับผิดชอบระบบสารสนเทศ ต้องจัดให้มีการ Lock off จากระบบ หรือยกเลิกการเชื่อมต่อกับแอปพลิเคชันหรือเครือข่าย (Session Time-Out) อย่างอัตโนมัติ เมื่อไม่มีการใช้งาน โดยกาหนดระยะเวลาอย่างเหมาะสม ตามระดับความมั่นคงปลอดภัยของสารสนเทศ โดยให้ปฏิบัติตาม Asset Management Policy

**๔.๘ นโยบายควบคุมการละทิ้งทรัพย์สิน (Clear Desk and Clear Screen Policy)** พนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร และนักศึกษาฝึกงาน ต้องมีการจัดเก็บเอกสารและสื่อบันทึกข้อมูลที่บันทึกสารสนเทศ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ โดยให้ปฏิบัติตาม Asset ManagementPolicy เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต เช่น ไม่วางเอกสารสำคัญทิ้งไว้บนโต๊ะทำงาน เก็บเอกสารไว้ในตู้หรือลิ้นชักที่มีกุญแจล็อคเป็นต้น