มาตรการความปลอดภัยศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต

๑. โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ให้ความสำคัญอย่างยิ่งต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะข้อมูลด้านสาธารณสุขที่มีความสำคัญและต้องรักษาไว้ด้วยความมั่นคงปลอดภัยสูงสุด เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่มีสิทธิ์ จึงได้กำหนดมาตรการควบคุมการเข้า–ออกห้อง Data Center อย่างเข้มงวด โดยใช้ระบบกุญแจล็อกประตู ซึ่งกุญแจดังกล่าวจะถูกจัดเก็บและดูแลโดยเจ้าหน้าที่ผู้ดูแลระบบที่ปฏิบัติหน้าที่เวร (On Call) เท่านั้น มาตรการดังกล่าวประกอบกับการลงบันทึกประวัติการเข้า–ออกอย่างเคร่งครัด ช่วยให้สามารถควบคุมการเข้าใช้พื้นที่ ตรวจสอบประวัติการเข้าออกได้ ลดความเสี่ยงต่อการสูญหายหรือรั่วไหลของข้อมูล และยังเป็นไปตามมาตรฐานด้านความปลอดภัยของระบบสารสนเทศ (Information Security)

๒. โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ตระหนักถึงความสำคัญของ ห้อง Data Center ซึ่งเป็นศูนย์กลางในการจัดเก็บและประมวลผลข้อมูลด้านสาธารณสุขและข้อมูลสำคัญของหน่วยงาน การบริหารจัดการพื้นที่ดังกล่าวจึงต้องมีมาตรการดูแลที่รัดกุม เพื่อให้ระบบปฏิบัติการ และบริการด้านเทคโนโลยีสารสนเทศทำงานได้อย่างต่อเนื่อง ปลอดภัย และมีประสิทธิภาพสูงสุด เพื่อให้การดูแลรักษาความปลอดภัยและความพร้อมใช้งานของระบบเป็นไปอย่างมีมาตรฐาน โรงพยาบาลพระอาจารย์มั่น ภูริทัตโตได้ กำหนดหน้าที่และความรับผิดชอบในการดูแลห้อง Data Center โดยจัดตารางการปฏิบัติงานในรูปแบบ “On Call” ให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ฉุกเฉินได้ทุกเวลา ทั้งในและนอกเวลาราชการ การดำเนินการในรูปแบบ On Call นี้ ช่วยให้สามารถเฝ้าระวัง ตรวจสอบ และแก้ไขปัญหาที่อาจเกิดขึ้นกับระบบเซิร์ฟเวอร์ เครือข่าย และอุปกรณ์สำคัญอื่น ๆ ได้อย่างทันท่วงที ลดความเสี่ยงจากการหยุดชะงักของบริการ และสร้างความเชื่อมั่นให้กับผู้ใช้บริการและหน่วยงานที่เกี่ยวข้อง

๓. การควบคุมการเข้า–ออกสำหรับบุคคลภายนอก (Visitor & Vendor Access Control) ในกรณีที่มีความจำเป็นต้องให้บุคคลภายนอก เช่น ผู้รับเหมา วิศวกร หรือตัวแทนจำหน่าย เข้ามาปฏิบัติงานบำรุงรักษาอุปกรณ์เครือข่ายหรือเครื่องแม่ข่ายภายในห้อง Data Center จะต้องปฏิบัติตามมาตรการดังต่อไปนี้อย่างเคร่งครัด

๓.๑. ต้องขออนุญาตและลงนามในแบบฟอร์มบันทึกการเข้า–ออกห้อง Data Center (Logbook) ทุกครั้ง พร้อมระบุวัตถุประสงค์ วันเวลาที่เข้าและออกอย่างชัดเจน

๓.๒. ต้องมีเจ้าหน้าที่ผู้ดูแลระบบ (IT Administrator) ของโรงพยาบาลที่เข้าเวรปฏิบัติหน้าที่เป็นผู้ไขกุญแจเปิดประตูให้ และต้องอยู่ควบคุมดูแล (Escort) ตลอดระยะเวลาที่บุคคลภายนอกปฏิบัติงานอยู่ภายในห้อง ห้ามปล่อยให้บุคคลภายนอกอยู่ตามลำพังโดยเด็ดขาด

๔. การทบทวนและยกเลิกสิทธิ์การเข้าถึง (Access Review & Revocation) เพื่อให้การควบคุมการเข้าออกมีความรัดกุมและเป็นปัจจุบันอยู่เสมอ โรงพยาบาลกำหนดให้มีการทบทวนสิทธิ์การเข้าถึงและการถือครองกุญแจห้อง Data Center ดังนี้

๔.๑. การทบทวนสิทธิ์ตามวงรอบ ให้ผู้ดูแลระบบทำการตรวจสอบรายชื่อผู้ที่มีสิทธิ์ถือกุญแจและเข้าห้อง Data Center อย่างน้อยทุกๆ ๖ เดือน เพื่อยืนยันว่ามีเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องในปัจจุบันเท่านั้น

๔.๒. การยกเลิกสิทธิ์ทันที กรณีที่เจ้าหน้าที่มีการโยกย้าย เปลี่ยนแปลงหน้าที่ หรือพ้นสภาพการเป็นบุคลากรของโรงพยาบาล ให้ส่งมอบกุญแจคืนทันที และให้ผู้ดูแลระบบดำเนินการยกเลิกสิทธิ์การเข้าห้อง Data Center ในทะเบียนรายชื่อภายใน ๑ วันทำการ (กรณีที่กุญแจสูญหาย ต้องพิจารณาดำเนินการเปลี่ยนชุดกุญแจห้อง Data Center ใหม่ทันที) เพื่อป้องกันการลักลอบเข้าถึงระบบข้อมูลสำคัญ

๕. มาตรการควบคุมสภาพแวดล้อมทางกายภาพ (Physical Environment & Facilities Control) นอกจากมาตรการด้านบุคคลแล้ว ผู้รับผิดชอบดูแลห้อง Data Center ต้องควบคุมสภาพแวดล้อมทางกายภาพให้มีความปลอดภัยและพร้อมใช้งานตลอดเวลา ได้แก่

๕.๑. ระบบกล้องวงจรปิด (CCTV) ติดตั้งกล้องวงจรปิดเพื่อบันทึกภาพบริเวณประตูทางเข้าและภายในห้อง Data Center ตลอด ๒๔ ชั่วโมง โดยให้เก็บรักษาข้อมูลภาพบันทึกไว้อย่างน้อย ๙๐ วัน

๕.๒. ระบบควบคุมอุณหภูมิและความชื้น ต้องเปิดเครื่องปรับอากาศทำงานสลับกันตลอด ๒๔ ชั่วโมง เพื่อรักษาระดับอุณหภูมิให้เหมาะสมกับการทำงานของระบบคลัสเตอร์เครื่องแม่ข่ายและอุปกรณ์เครือข่าย ป้องกันความเสียหายจากความร้อนสะสม

๕.๓. ระบบไฟฟ้าสำรองและป้องกันอัคคีภัย ตรวจสอบสถานะของเครื่องสำรองไฟฟ้า (UPS) ให้พร้อมทำงานทันทีเมื่อเกิดกระแสไฟฟ้าขัดข้อง และต้องมีถังดับเพลิงชนิดที่เหมาะสมสำหรับอุปกรณ์อิเล็กทรอนิกส์ติดตั้งไว้ในบริเวณที่เข้าถึงได้ง่าย