ที่ ชร ๐๐๓๓.๓/๗๑

โรงพยาบาลแม่ลาว
๓๐๙ หมู่ที่ ๓ ตำบลจอมหมอกแก้ว
อำเภอแม่ลาว จังหวัดเชียงราย ๕๗๒๕๐

๑๒ มกราคม ๒๕๖๙

เรื่อง ขอส่งคำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศประจำโรงพยาบาลแม่ลาว

เรียน นายแพทย์สาธารณสุขจังหวัดเชียงราย

สิ่งที่ส่งมาด้วย คำสั่งแต่งตั้งผู้บริหารความมันคงปลอดภัยไซเบอร์ฯ จำนวน ๑ ชุด

พร้อมหนังสือฉบับนี้ โรงพยาบาลแม่ลาว ขอส่งคำสั่งแต่งตั้งผู้บริหารความมั่นคงปลอดภัยผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศประจำโรงพยาบาลแม่ลาว เพื่อเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไปด้วย

ขอแสดงความนับถือ

(นายสุขชัย เธียรเศวตตระกูล)
นายแพทย์เชี่ยวชาญ
ผู้อำนวยการโรงพยาบาลแม่ลาว (CISO)

กลุ่มงานสุขภาพดิจิทัล
โทร.๐ ๕๓๖๐ ๓๑๐๐ ต่อ ๓๑๖๓
โทรสาร.๐ ๕๓๖๐ ๓๑๑๑
ไปรษณีย์อิเล็กทรอนิกส์กลาง saraban-maelaohospital@moph.go.th

คำสั่งโรงพยาบาลแม่ลาว

ที่ ๑๑๓/๒๕๖๙

เรื่อง แต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศประจำโรงพยาบาลแม่ลาว

ด้วยโรงพยาบาลแม่ลาว มีการดำเนินงานด้านเทคโนโลยีสารสนเทศและระบบดิจิทัล เพื่อสนับสนุนการให้บริการด้านสาธารณสุขแก่ประชาชน และเพื่อให้สอดคล้องกับ กฎหมาย มาตรฐาน และแนวทางปฏิบัติที่เกี่ยวข้อง อันได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อันจะก่อให้เกิดการคุ้มครองข้อมูล การป้องกันความเสี่ยง และการบริหารจัดการเหตุการณ์ด้านไซเบอร์อย่างมีประสิทธิภาพ โรงพยาบาลแม่ลาว จึงเห็นสมควรแต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ

๑. ผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ
(Chief Information Security Officer : CISO)

๑. นพ.สุขชัย เธียรเศวตตระกูล ตำแหน่งผู้อำนวยการโรงพยาบาลแม่ลาว

หน้าที่ความรับผิดชอบ

๑. กำหนดและอนุมัติ รวมถึงการทบทวน นโยบาย กลยุทธ์ และแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศให้สอดคล้องกับเป้าหมายองค์กร

๒. ประเมิน วิเคราะห์ และกำกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศขององค์กร

๓. กำกับดูแลการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ (Cybersecurity Incident Response) และการกู้คืนระบบ (Disaster Recovery)

๔. ประสานงานและรายงานสถานะความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ต่อคณะผู้บริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง

๕. ส่งเสริมและสนับสนุนการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ในองค์กร

๖. ให้ความคิดเห็นด้านภัยคุกคามไซเบอร์, การบริหารจัดการความเสี่ยง ต่อคณะผู้บริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง

๒. ผู้ทีมผู้รับผิดชอบการดำเนินงานตามมาตรฐาน (Implementer Team)

๑. นายพรศักดิ์ ตามวงค์ ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ (Lead Implementer)
๒. นายสุทธิชัย เสาว์สิงห์ ตำแหน่งนักวิชาการคอมพิวเตอร์ (Implementer)

หน้าที่ความรับผิดชอบ...

หน้าที่ความรับผิดชอบ

๑. วางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามกฎหมาย พรบ ไซเบอร์

๒. จัดทำและดูแลให้มีการปฏิบัติ นโยบาย ระเบียบปฏิบัติ ขั้นตอนการทำงาน และบันทึกต่าง ๆ พร้อมประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้มาตรการความมั่นคงปลอดภัยไซเบอร์ถูกนำไปปฏิบัติได้จริง

๓. บริหารจัดการความเสี่ยงสารสนเทศทางด้านไซเบอร์และข้อมูลสารสนเทศ

๔. จัดทำรายงานผลการดำเนินงานและข้อเสนอแนะในการปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์

๕. ติดตามและสนับสนุนการปรับปรุงกระบวนการอย่างต่อเนื่อง (Continuous Improvement)

๓. ทีมผู้ตรวจสอบระบบการจัดการ (Auditor Team)

๑. นางสินีนาฏ ตามวงค์ ตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ (Lead Auditor)

๒. นางสายสมร ภัทรจิตรานนท์ ตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ (Auditor)

หน้าที่ความรับผิดชอบ

๑. วางแผนและดำเนินการตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศขององค์กร

๒. ประเมินความสอดคล้องของระบบบริหารจัดการกับมาตรฐาน พรบ ไซเบอร์, ISO/IEC ๒๗๐๐๑, PDPA และกฎหมาย/ข้อบังคับที่เกี่ยวข้อง

๓. ตรวจสอบการปฏิบัติตามนโยบายและมาตรการความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศของทุกหน่วยงาน

๔. จัดทำรายงานผลการตรวจสอบ พร้อมข้อเสนอแนะเพื่อการแก้ไขปรับปรุง

๕. ติดตามผลการแก้ไขข้อบกพร่อง (Follow-up Audit) เพื่อให้มั่นใจว่ามีการปรับปรุงอย่างแท้จริง

๔. ทีมบริหารความเสี่ยง (Risk Team)

๑. นายปชนน อนุพงศานุกูล ตำแหน่งเภสัชกรชำนาญการพิเศษ

๒. ทพญ.บงกช บัณฑิตศศิกุล ตำแหน่งทันตแพทย์หญิงชำนาญการพิเศษ

๓. นายพรศักดิ์ ตามวงค์ ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ

หน้าที่ความรับผิดชอบ

๑. วางแผนและดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ขององค์กร

๒. ติดตามและประเมินความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นจากกระบวนการทำงานและการใช้เทคโนโลยี

๓. เสนอแนะแนวทางการป้องกัน แก้ไข และลดผลกระทบจากความเสี่ยงที่พบ

๔. จัดทำรายงานความเสี่ยงและเสนอผู้บริหารเพื่อการตัดสินใจ

๕. สนับสนุนการสร้างวัฒนธรรมองค์กรที่ตระหนักถึงการบริหารความเสี่ยง

๕. ทีมบริการความเสี่ยง....

๕. ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ในองค์กร (โรงพยาบาลแม่ลาว - Cybersecurity Incident Response Team, MLH - CSIRT)

๑. Executive Sponsor

นพ.สุขชัย เธียรเศวตตระกูล ตำแหน่งผู้อำนวยการโรงพยาบาลแม่ลาว

หน้าที่ความรับผิดชอบ : ให้การสนับสนุนเชิงนโยบายและทรัพยากร

๒. CSIRT Manager

ทพ.เสรสรร คูดิษฐาเลิศ ตำแหน่งรองอำนวยการโรงพยาบาลแม่ลาว

หน้าที่ความรับผิดชอบ : กำกับดูแลการดำเนินงาน, ประสานงานกับผู้บริหารและหน่วยงานภายนอก

๓. CSIRT Member (Incident Handler)

พันจ่าเอกพรชัย บุญเพียร ตำแหน่งนักจัดการทั่วไปชำนาญการ

นายพรศักดิ์ ตามวงค์ ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ

หน้าที่ความรับผิดชอบ : เฝ้าระวังระบบไซเบอร์และสารสนเทศ เครือข่ายและระบบบริหารจัดการโรงพยาบาล (HIS- Hospital Information System), ประเมินระดับความร้ายแรงและผลกระทบของเหตุการณ์, รายงานความคืบหน้าให้ CSIRT Manager และประสานงานกับ ทีมงานที่เกี่ยวข้อง เพื่อแก้ไขปัญหาที่เกิดขึ้น

๖. ทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต (Crisis Communication Team)

๑. นางสาวมัณฑนา บุศเมือง ตำแหน่งนักเทคนิคการแพทย์ชำนาญการ

๒. นายศราวุธ ชัยรัตน์ ตำแหน่งนักสาธารณสุขปฏิบัติการ

๓. นายสุทธิชัย เสาว์สิงห์ ตำแหน่งนักวิชาการคอมพิวเตอร์

หน้าที่ความรับผิดชอบ

๑. จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒. ตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๓. ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔. ประสานงานกับบุคลากรในองค์กรและภายนอก รวมถึงตรวจสอบประเด็นทางกฎหมายและ PDPA

๗. ทีมการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (BCP – Business Continuity Plan Team)

๑. นายพรศักดิ์ ตามวงค์ ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ (Lead Implementer)

๒. พันจ่าเอกพรชัย บุญเพียร ตำแหน่งนักจัดการทั่วไปชำนาญการ (Implementer)

๓. นายสุทธิชัย เสาว์สิงห์ ตำแหน่งนักวิชาการคอมพิวเตอร์ (Implementer)

หน้าที่ความรับผิดชอบ...

หน้าที่ความรับผิดชอบ

๑. จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญขององค์กรสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก

๒. ต้องมีการสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานขององค์กร เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๓. จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๔. มีการตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๘. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO - Data Protection Officer)

๑. นางอรุณี ไชยเมือง	ตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ
๒. นายพรศักดิ์ ตามวงค์	ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ
๓. นางสารรำไพ ยารวง	ตำแหน่งเจ้าพนักงานเวชสถิติชำนาญงาน

หน้าที่ความรับผิดชอบ

๑. ให้คำแนะนำทั้งกับผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล รวมถึงลูกจ้างหรือผู้รับจ้างที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

๒. ตรวจสอบการดำเนินการขององค์กร เพื่อให้แน่ใจว่า การเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนดของกฎหมาย PDPA

๓. เมื่อเกิดปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลรั่วไหล , DPO จะต้องทำหน้าที่ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)

๔. ต้องรักษาข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาในระหว่างการปฏิบัติหน้าที่ให้เป็นไปความลับ

๕. ต้องมีบทบาทในการสร้างความเข้าใจและการตระหนักรู้เรื่อง PDPA ให้แก่พนักงานในองค์กร เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง

จึงเรียนมาเพื่อโปรดทราบและให้ถือปฏิบัติ โดยเคร่งครัด

(นายสุขชัย เธียรเศวตตระกูล)
นายแพทย์เชี่ยวชาญ
ผู้อำนวยการโรงพยาบาลแม่ลาว (CISO)