โรงพยาบาลเขาย้อย



คำสั่ง โรงพยาบาลเขาย้อย
ที่ ๑๒๕ / ๒๕๖๙
เรื่อง แต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศประจำโรงพยาบาลเขาย้อย

.....

ด้วยโรงพยาบาลเขาย้อย มีการดำเนินงานด้านเทคโนโลยีสารสนเทศและระบบดิจิทัล เพื่อสนับสนุนการให้บริการด้านสาธารณสุขแก่ประชาชน และเพื่อให้สอดคล้องกับ กฎหมาย มาตรฐาน และแนวทางปฏิบัติที่เกี่ยวข้อง อันได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อันจะก่อให้เกิดการคุ้มครองข้อมูล การป้องกันความเสี่ยง และการบริหารจัดการเหตุการณ์ด้านไซเบอร์อย่างมีประสิทธิภาพ โรงพยาบาลเขาย้อย จึงเห็นสมควรแต่งตั้งผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและคณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ

๑. ผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ (Chief Information Security Officer : CISO)

แพทย์หญิงอรวรรณ ตะเวทิพงศ์ ตำแหน่ง ผู้อำนวยการโรงพยาบาลเขาย้อย

หน้าที่ความรับผิดชอบ

๑) กำหนดและอนุมัติ รวมถึงการทบทวน นโยบาย กลยุทธ์ และแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศให้สอดคล้องกับเป้าหมายองค์กร
๒) ประเมิน วิเคราะห์ และกำกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศขององค์กร
๓) กำกับดูแลการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ (Cybersecurity Incident Response) และการกู้คืนระบบ (Disaster Recovery)
๔) ประสานงานและรายงานสถานะความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ต่อคณะผู้บริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง
๕) ส่งเสริมและสนับสนุนการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศในองค์กร
๖) ให้ความคิดเห็นด้านภัยคุกคามไซเบอร์, การบริหารจัดการความเสี่ยง ต่อคณะผู้บริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง

๒. ผู้รับผิดชอบระบบสารสนเทศโรงพยาบาล (Head of Information Security : HIS)

แพทย์หญิงอัซฮานี รักชุมคง ตำแหน่ง นายแพทย์ชำนาญการ

หน้าที่ความรับผิดชอบ

๑) กำกับดูแลและประสานงานด้านการใช้งานระบบแอพพลิเคชั่นหลัก เช่น ระบบบริหารจัดการโรงพยาบาล (HIS- Hospital Information System) ของโรงพยาบาล

๒) ตรวจสอบความถูกต้อง ครบถ้วน และปลอดภัยของข้อมูลผู้ป่วยและข้อมูลทางคลินิก

๓) ประสานงานกับทีมเทคนิคและผู้ใช้งานเพื่อแก้ไขปัญหาและพัฒนาระบบบริหารจัดการโรงพยาบาล (HIS- Hospital Information System)

๔) จัดทำรายงานและวิเคราะห์ข้อมูลจากระบบบริหารจัดการโรงพยาบาล (HIS- Hospital Information System) เพื่อสนับสนุนการตัดสินใจเชิงบริหาร

5) สนับสนุนและอบรมบุคลากรในการใช้งานระบบบริหารจัดการโรงพยาบาล (HIS- Hospital Information System) อย่างถูกต้องและปลอดภัย

6) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามไซเบอร์

7) ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และตระหนักรู้ทางด้านไซเบอร์

๓. ทีมผู้รับผิดชอบการดำเนินงานตามมาตรฐาน (Implementer Team)

นางสาวอารีพร บุญชูยิ่ง ตำแหน่ง เจ้าพนักงานเวชสถิติชำนาญงาน (Lead Implementer)

นางสาวบุญญาภรณ์ ระวังแค้ม ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ(Implementer)

นายพัฒนา บุญมามาก ตำแหน่ง นักวิชาการคอมพิวเตอร์ (Implementer)

นางสาวนารีนาถ นาคประดับ ตำแหน่ง นักวิชาการคอมพิวเตอร์(Implementer)

นายสุทธิพงษ์ อุ่นเป็นนิจ ตำแหน่ง เจ้าพนักงานเวชสถิติปฏิบัติงาน(Implementer)

ความรับผิดชอบหน้าที่

๑) วางแผนและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามกฎหมาย พรบ ไซเบอร์

๒) จัดทำและดูแลให้มีการปฏิบัติ นโยบาย ระเบียบปฏิบัติ ขั้นตอนการทำงาน และบันทึกต่าง ๆ พร้อมประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้มาตรการความมั่นคงปลอดภัยไซเบอร์ถูกนำไปปฏิบัติได้จริง

3) บริหารจัดการความเสี่ยงสารสนเทศทางด้านไซเบอร์และข้อมูลสารสนเทศ

๔) จัดทำรายงานผลการดำเนินงานและข้อเสนอแนะในการปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์

๕) ติดตามและสนับสนุนการปรับปรุงกระบวนการอย่างต่อเนื่อง (Continuous Improvement)

๔. ทีมผู้ตรวจสอบระบบการจัดการ (Auditor Team)

นางตติยา เต็มเปี่ยม ตำแหน่ง พยาบาลวิชาชีพชำนาญการ (Lead Auditor)

นางสาวบงกช อังกินันทน์ ตำแหน่ง พยาบาลวิชาชีพชำนาญการพิเศษ (Auditor)

นางสาววาศิณี จันทร์กระจ่าง ตำแหน่ง พยาบาลวิชาชีพชำนาญการ (Auditor)

นางสาวธัญลักษณ์ ป้านสะอาด ตำแหน่ง นักวิชาการสาธารณสุขปฏิบัติการ (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

๕. ทีมบริหารความเสี่ยง (Risk Team)

นางสาวบงกช อังกินันทน์ ตำแหน่ง พยาบาลวิชาชีพชำนาญการพิเศษ
นางชมัยพร เสียงสนั่น ตำแหน่ง พยาบาลวิชาชีพชำนาญการพิเศษ
นางสาววาสนา สกุณี ตำแหน่ง พยาบาลวิชาชีพชำนาญการ
นางสาววชิรา ประเทืองทิน ตำแหน่ง พยาบาลวิชาชีพชำนาญการ
ทพญ.ทักษรพร เทียนสุวรรณ ตำแหน่ง ทันตแพทย์ชำนาญการ
นางสาวศรัณยา ภู่จีบ ตำแหน่ง นักวิทยาศาสตร์การแพทย์ปฏิบัติการ
นางสาวสุดาพร เนตรลือชา ตำแหน่ง นักกายภาพบำบัดชำนาญการ
นางสาวรุจิรา เทพลำลึก ตำแหน่ง นักจัดการงานทั่วไปปฏิบัติการ
นางสาวมัณฑนา มังสมบัติ ตำแหน่ง นักวิชาการสาธารณสุขชำนาญการ
นางรมณี บุตรเคียง ตำแหน่ง พยาบาลวิชาชีพชำนาญการ
นางสิตา อิ่มโอษฐ ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

หน้าที่ความรับผิดชอบ

๑) วางแผนและดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศขององค์กร

๒) ติดตามและประเมินความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นจากกระบวนการทำงานและการใช้เทคโนโลยี

๓) เสนอแนะแนวทางการป้องกัน แก้ไข และลดผลกระทบจากความเสี่ยงที่พบ

๔) จัดทำรายงานความเสี่ยงและเสนอผู้บริหารเพื่อการตัดสินใจ

๕) สนับสนุนการสร้างวัฒนธรรมองค์กรที่ตระหนักถึงการบริหารความเสี่ยง

๖. ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ในองค์กร (KYH - Cybersecurity Incident Response Team, KYH - CSIRT)

๑) Executive Sponsor

แพทย์หญิงอรวรรณ ตะเวทิพงศ์ ตำแหน่ง ผู้อำนวยการโรงพยาบาลเขาย้อย

หน้าที่ความรับผิดชอบ : ให้การสนับสนุนเชิงนโยบายและทรัพยากร

๒) CSIRT Manager

นางสาวรุจิรา เทพลำลึก ตำแหน่ง นักจัดการงานทั่วไปปฏิบัติการ

หน้าที่ความรับผิดชอบ : กำกับดูแลการดำเนินงาน, ประสานงานกับผู้บริหารและหน่วยงานภายนอก

๓) CSIRT Member (Incident Handler)

นางสาวบุญญาภรณ์ ระวังแค้ม ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายพัฒนา บุญมามาก ตำแหน่ง นักวิชาการคอมพิวเตอร์

นางสาวนารีนาถ นาคประดับ ตำแหน่ง นักวิชาการคอมพิวเตอร์

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

๗. ทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต (Crisis Communication Team)

นางสาวธัญลักษณ์ ป้านสะอาด ตำแหน่ง นักวิชาการสาธารณสุขปฏิบัติการ

นางสาวรุจิรา เทพลำลึก ตำแหน่ง นักจัดการงานทั่วไปปฏิบัติการ

นางสาวกาญจนา นวมนิ่ม ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน

หน้าที่ความรับผิดชอบ

๑) จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒) ตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๓) ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔) ประสานงานกับบุคลากรในองค์กรและภายนอก รวมถึงตรวจสอบประเด็นทางกฎหมายและ PDPA

๘. ทีมการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (BCP – Business Continuity Plan Team)

นางสิตา อิ่มโอษฐ ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

นางสาวกนกรัตน เมฆนาคา ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

นางประทุมพร จันทร์กระจ่าง ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

นางสาวสกลวรรณ ผ่องอารมณ์ ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

นางสาวรุจิรา เทพลำลึก ตำแหน่ง นักจัดการงานทั่วไปปฏิบัติการ

นางสาวศรัญญา มั่งเจริญ ตำแหน่งนักกายภาพบำบัดชำนาญการ

นางสาวพิชชาภัสส์ รุ่งเรืองสุรกิจ นักเทคนิคการแพทย์ชำนาญการ

นางสาวสุพัตรา ย้อมสี ตำแหน่ง พยาบาลวิชาชีพปฏิบัติการ

นางสาวนาตยา อยู่สำราญ ตำแหน่ง แพทย์แผนไทยปฏิบัติการ

นางปนัดดา จันทร์เปล่ง ตำแหน่ง พยาบาลวิชาชีพปฏิบัติการ

นางสาวสายทอง อาศัยจ้าว ตำแหน่ง พยาบาลวิชาชีพชำนาญการ

หน้าที่ความรับผิดชอบ

๑) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญขององค์กรสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก

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

๓) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

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

๙. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO - Data Protection Officer)

นางสาวอารีพร บุญชูยิ่ง ตำแหน่ง เจ้าพนักงานเวชสถิติชำนาญงาน

หน้าที่ความรับผิดชอบ

๕) ให้คำแนะนำทั้งกับผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล รวมถึงลูกจ้างหรือผู้รับจ้างที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

๖) ตรวจสอบการดำเนินการขององค์กร เพื่อให้แน่ใจว่า การเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนดของกฎหมาย PDPA

๗) เมื่อเกิดปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลรั่วไหล , DPO จะต้องทำหน้าที่ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส)

๘) ต้องรักษาข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาในระหว่างการปฏิบัติหน้าที่ให้เป็นไปความลับ

๙) ต้องมีบทบาทในการสร้างความเข้าใจและการตระหนักรู้เรื่อง PDPA ให้แก่พนักงานในองค์กร เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง

จึงเรียนมาเพื่อโปรดทราบและให้ถือปฏิบัติ โดยเคร่งครัด

สั่ง ณ วันที่ ๑๕ เดือน ตุลาคม พ.ศ. ๒๕๖๙

(นางสาวอรวรรณ ตะเวทิพงศ์)

ผู้อำนวยการโรงพยาบาลชะอำ

รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลเขาย้อย (CISO)