คำสั่งโรงพยาบาลบ้านด่าน
ที่ ๕ /๒๕๖๗
เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์
(CIRT: Cyber Incident Response Team) ประจำโรงพยาบาลบ้านด่าน

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายความควบคุมและกำกับดูแล พ.ศ.๒๕๖๕ หมด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยาเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา บริการตรวจวิเคราะห์ทางห้องปฏิบัติการและโลหิต และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้อยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุขนั้น

โรงพยาบาลบ้านด่านซึ่งมีบริการข้อมูลสุขภาพดิจิทัลตามประกาศฯ ดังกล่าว จึงขอแต่งตั้งเจ้าหน้าที่ เป็นเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT: Cyber Incident Response Team) ดังนี้

๑. นางสาวดวงจันทร์ ชะงักรัมย์ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ งานเทคโนโลยีสารสนเทศ กลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์ หมายเลขโทรศัพท์ ๐ ๔๔๖๖ ๔๐๔๙ ต่อ ๑๐๕, ๐๘๐ ๔๘๔๕๓๙๔ อีเมล changakram_it๔๗@hotmail.com

๒. นางสาวบุษรา หงส์เรืองรัมย์ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ งานเทคโนโลยีสารสนเทศ กลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์ หมายเลขโทรศัพท์ ๐ ๔๔๖๖ ๔๐๔๙ ต่อ ๑๐๕, ๐๖๑ ๖๙๑๖๙๖๕ อีเมล gingbu_sra@outlook.com

โดยให้ปฏิบัติหน้าที่ดังนี้

๑. เฝ้าระวังตรวจสอบช่องโหว่ของระบบงานต่างๆ และเครือข่ายคอมพิวเตอร์ทั้งอินเทอร์เน็ตและอินทราเน็ตของโรงพยาบาลบ้านด่าน

๒. ประสานงานกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ทันทีเมื่อพบเหตุการณ์ทางไซเบอร์

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๗

นายศาสตรา เข็มบุบผา
ผู้อำนวยการโรงพยาบาลบ้านด่าน

แนวปฏิบัติในการการกำหนดหน้าที่ความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ 1 ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้อำนวยการ (CEO)
- ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)
- ผู้อำนวยการฝ่ายเทคนิคและวิศวกรรม หรือเทียบเท่าระดับผู้อำนวยการฝ่าย

(1) รับผิดชอบต่อความเสี่ยง ความเสี่ยงหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 2 ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้าส่วนงาน

(1) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(2) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบข้อมูล

ข้อ 3 ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้อำนวยการ เช่น นักวิชาการคอมพิวเตอร์ เจ้าพนักงานเครื่องคอมพิวเตอร์ พนักงานเทคโนโลยีสารสนเทศ

(1) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(2) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(3) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(4) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(5) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(6) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(7) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความปลอดภัยด้านสารสนเทศ