บันทึกข้อความ

ส่วนราชการ โรงพยาบาลกำแพงแสน กลุ่มงานประกันฯ โทร ๐-๓๔๓๑-๐๓๓๔ ต่อ ๑๘๘

ที่ นฐ ๐๐๓๓.๕/๔/บ.๖๖๔ **วันที่** ๗ มิถุนายน ๒๕๖๖

เรื่อง ขออนุมัติแต่งตั้งเจ้าหน้าที่ประสานงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกาศนโยบาย และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เรียน ผู้อำนวยการโรงพยาบาลกำแพงแสน

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและมอบหมายการควบคุมและกำกับดูแล พ.ศ.๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุขนั้น

ในการนี้ งานสารสนเทศทางการแพทย์ โรงพยาบาลกำแพงแสน ขออนุมัติแต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT:Cyber Incident Response Team) ประกาศนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รายละเอียดตามคำสั่งที่แนบเรียนมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาลงนามในคำสั่ง

(นายสมชาย เจนลาภวัฒนกุล)
ผู้อำนวยการโรงพยาบาลกำแพงแสน

คำสั่งโรงพยาบาลกำแพงแสน
ที่ /๒๕๖๖
เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข โรงพยาบาลกำแพงแสน ภายใต้การกำกับสำนักงานปลัดกระทรวงสาธารณสุข เป็นหน่วยงานที่ได้รับมอบหมายให้ดำเนินการควบคุมและกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที จึงเห็นควรมีการแต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT: Cyber Incident Response Team) ต่อไป

อาศัยอำนาจตาม มาตรา ๕๕ และมาตรา ๖๐ (๒) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ.๒๕๓๔ และแก้ไขเพิ่มเติม สำนักงานสาธารณสุขจังหวัดนครปฐม จึงมีคำสั่งแต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

(๑) นางสาวอารีย์ สุขเกษม ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(๒) นายวรพันธุ์ พิสิฐธนโชติ ตำแหน่ง เจ้าพนักงานเภสัชกรรมชำนาญงาน

โดยมีหน้าที่ ดังต่อไปนี้

(๑) เฝ้าระวังตรวจสอบช่องโหว่ของระบบต่างๆ และเครือข่ายคอมพิวเตอร์ทั้งอินเทอร์เน็ตและอินทราเน็ตของสำนักงานสาธารณสุขจังหวัดนครปฐม

(๒) ประสานงานกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CRET) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ทันทีเมื่อพบเหตุการณ์ทางไซเบอร์

(๓) ติดตามการแจ้งข่าวสารเหตุการณ์จากศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข และข่าวสารเหตุการณ์ในปัจจุบัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ พฤษภาคม พ.ศ. ๒๕๖๖

(นายสมชาย เจนลาภวัฒนกุล)
ผู้อำนวยการโรงพยาบาลกำแพงแสน

ประกาศโรงพยาบาลกำแพงแสน
เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลกำแพงแสน เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและถูกคุกคามจาภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหาย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่๒) พ.ศ.๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง จึงเห็นสมควรกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นดังต่อไปนี้

๑. ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลกำแพงแสน เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลมีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศทำให้ดำเนินงาน ได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบ และถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๓. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลกำหนดประเด็นสำคัญดังต่อไปนี้

๓.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๓.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้น ที่สามารถใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์และเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัยเสมอ

๓.๑.๓ การควบคุมการเข้าถึงโปรแกรมและแอพพลิเคชั่น ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่างๆรวมถึง

จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบอินเตอร์เน็ต(Internet)ระบบงานต่างๆโดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานผู้รับผิดชอบ และได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของโรงพยาบาลสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความสำคัญจากมากไปน้อย พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถใช้งานสารสนเทศได้ตามปกติ

๓.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในโรงพยาบาล(Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)อย่างน้อยปีละ ๑ ครั้ง เพื่อให้โรงพยาบาลได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๔. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆแก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาล เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๕. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

๖. ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ พฤษภาคม พ.ศ. ๒๕๖๖

(นายสมชาย เจนลาภวัฒนกุล)
ผู้อำนวยการโรงพยาบาลกำแพงแสน