ประกาศโรงพยาบาลทัพทัน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทัพทัน เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและภัยคุกคามต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง โรงพยาบาลทัพทัน จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลทัพทัน เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

๒. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลทัพทันมีวัตถุประสงค์ ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาบาลทัพทัน ดำเนินงานได้อย่างมีประสิทธิภาพประสิทธิผล

๓.๒ เพื่อเผยแพรให้เจ้าหน้าที่ทุกระดับในหน่วยงาน ในสังกัดโรงพยาบาลทัพทันได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลทัพทัน ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาลทัพทัน ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลทัพทัน กำหนดประเด็นสำคัญและผู้รับผิดชอบ ดังต่อไปนี้

๔.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ผู้รับผิดชอบ : ๑. นายวีรยุทธ เอี่ยมมี นายช่างเทคนิค
๒. นายศุภวัฒน์ ขยันการนาวี เจ้าพนักงานเครื่องคอมพิวเตอร์
๓. นายวัชรพงษ์ ตันติพงษ์ นักวิชาการคอมพิวเตอร์

๔.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔.๑.๒ การบริหารจัดการ การเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานการตรวจสอบบัญชีผู้ใช้งาน การอนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้น สามารถเข้าใช้งานระบบสารสนเทศได้ ตลอดจนบริหารจัดการสิทธิ์ ทบทวนสิทธิ์ การเข้าถึงข้อมูลให้เหมาะสมตามลำดับชั้นความลับ

๔.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงทางเครือข่ายโดยไม่ได้รับอนุญาตต้องกำหนดสิทธิ์การเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งาน ต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน โดยกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลทัพทันจัดสรรไว้และมีการออกแบบ ระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งานเพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบมีประสิทธิภาพ

๔.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งาน ต้องลงบันทึกเข้าใช้งาน (Login) แสดงตัวตนด้วยชื่อผู้ใช้และมีการพิสูจน์ยืนยันตัวตน(Authentication) ด้วยการใช้รหัสก่อนเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อ

ว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ให้เป็นการละเมิดสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ

๔.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่น ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์และแอพพลิเคชั่นต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบ รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๒ การจัดทำระบบสำรองข้อมูล

ผู้รับผิดชอบ : ๑. นายวีรยุทธ เอี่ยมมี นายช่างเทคนิค

๒. นายศุภวัฒน์ ขยันการนาวี เจ้าพนักงานเครื่องคอมพิวเตอร์

เพื่อให้ระบบสารสนเทศหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ มีความเหมาะสมพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ อย่างน้อยปีละ ๑ ครั้ง ให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๔.๓ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ผู้รับผิดชอบ : ๑. นายพีรพล พูลสุขเสริม นักวิเคราะห์นโยบายและแผน

โดยจัดให้มีผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย

๕. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อ ความสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น

๖. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

๗. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๖ เดือน พฤษภาคม พ.ศ. ๒๕๖๕

(นายวศิน โพธิพฤกษ์)
นายแพทย์เชี่ยวชาญ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลทัพทัน