



ประกาศโรงพยาบาลชานุมาน

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารของโรงพยาบาลชานุมาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศ และการสื่อสารในลักษณะที่ไม่ถูกต้อง และการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลชานุมาน หน่วยงาน และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ โรงพยาบาลชานุมานจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

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

๑. ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลชานุมาน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

๒. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใด ที่ได้กำหนดไว้แล้ว ซึ่งขัด หรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลชานุมานมีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่น และความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศ ของโรงพยาบาลชานุมาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล

๓.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานได้รับทราบ และถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาลชานุมาน ในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลชานุมาน กำหนดประเด็นสำคัญดังต่อไปนี้

๔.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๔.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัยในการเข้าใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงกำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้

และต้องเก็บบันทึกข้อมูลการเข้าถึง และข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูล ให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัยเสมอ

๔.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้ รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่เข้าใช้งานต้องเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อ ผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบการรักษาความปลอดภัยตามที่โรงพยาบาล จัดสรรไว้ และมีการออกแบบระบบเครือข่าย โดยแบ่งเขตโซน (Zone) การใช้งาน เพื่อให้ควบคุมและป้องกันภัย คุกคามได้อย่างเป็นระบบ และมีประสิทธิภาพ

๔.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดย ไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และ ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติ การใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อบริการสารสนเทศ ตลอดจนกำหนด มาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่างๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์ และป้องกันโปรแกรมไม่พึง ประสงค์ต่างๆ

๔.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่าง ต่อเนื่อง และเสถียรภาพ ต้องจัดทำระบบสารสนเทศ และระบบสำรองที่เหมาะสม ให้อยู่ในสภาพที่พร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบ ของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ อย่างต่อเนื่อง

๔.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของ หน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละครั้ง ๑ ครั้ง เพื่อให้หน่วยงานได้รับทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

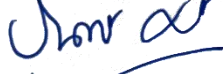
๕. กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่ง ผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของ หน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๖. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

๗. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

จึงประกาศให้ทราบโดยทั่วกัน และถือปฏิบัติโดยเคร่งครัด

ประกาศ ณ วันที่ ๑๑ เมษายน ๒๕๖๖



(นายชนกร คนเพียร)

นายแพทย์ปฏิบัติการ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลชานุมาน