



ประกาศโรงพยาบาลบ้านนา

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารของโรงพยาบาลบ้านนา เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศ และการสื่อสารในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลบ้านนา และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ โรงพยาบาลบ้านนาจึงเห็นสมควร กำหนดนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

ข้อ ๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลบ้านนามีวัตถุประสงค์ ดังต่อไปนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลบ้านนา ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล

๑.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดโรงพยาบาลบ้านนา และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าใจ เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งานผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลบ้านนา ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาลบ้านนา ในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัดโดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลบ้านนา กำหนดประเด็นสำคัญดังต่อไปนี้

๒.๑ การควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ

๒.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติ และกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งาน และ ตรวจสอบการละเมิดความปลอดภัยเสมอ

๒.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่ใช้งานต้องลงบันทึกเข้าใช้งาน(Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยตามที่โรงพยาบาลบ้านนา และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุม และป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๒.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่ใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่างๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๒.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่างๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศ และระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๒.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๓. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเอียด หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๔. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลบ้านนา พ.ศ. ๒๕๖๙ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๖ มีนาคม พ.ศ. ๒๕๖๙

(นายฐาปกรณ์ พรประภาคคีติ)

นายแพทย์ชำนาญการ

รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลบ้านนา