



ประกาศโรงพยาบาลหนองขาหย่าง

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลหนองขาหย่างเป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและภัยคุกคามต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้อง โรงพยาบาลหนองขาหย่างจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

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

๑. ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลหนองขาหย่างเรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”
๒. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ใดกำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน
๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลหนองขาหย่างมีวัตถุประสงค์ดังต่อไปนี้
 - ๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลหนองขาหย่าง ดำเนินงานได้อย่างมีประสิทธิภาพประสิทธิผล
 - ๓.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานในสังกัดโรงพยาบาลหนองขาหย่างได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด
 - ๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานสาธารณสุขจังหวัดอุทัยธานี ตระหนักถึงความสำคัญในการรักษาความมั่นคงด้านสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยให้ทบทวนนโยบายปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลหนองขาหย่างกำหนดประเด็นสำคัญ ดังต่อไปนี้

๔.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

- ๔.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- ๔.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน การตรวจสอบบัญชีผู้ใช้งาน การอนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นสามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามลำดับชั้น ความลับของผู้ใช้งาน คือต้องทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ
- ๔.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยที่สำนักงานสาธารณสุขจังหวัดอุทัยธานี จัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบมีประสิทธิภาพ
- ๔.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างวันจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรม อรรถประโยชน์ต่างๆ เพื่อไม่ให้เป็นการละเมิดสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ
- ๔.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์และแอปพลิเคชันต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาร (Wireless LAN) ระบบอินเทอร์เน็ต

(Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้อง
ได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์
ดังกล่าวอย่างสม่ำเสมอ

- ๔.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
และมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน
โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และ
ความรับผิดชอบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถ
ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้
ตามปกติอย่างต่อเนื่อง
- ๔.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน
(Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External
Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคง
ปลอดภัยสารสนเทศ
๕. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่ง
ผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการ
รักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้าน
สารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น
๖. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่แนบท้ายประกาศนี้
๗. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๕



(นายธีรสุทธิ ปิตวิบลเสถียร)

นายแพทย์ชำนาญการพิเศษ รักษาการใน
ตำแหน่งผู้อำนวยการโรงพยาบาลหนองขาหย่าง