นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาล และบริษัทในเครือ ธนบุรี เฮลท์แคร์ กรุ๊ป

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล และบริษัทในเครือ ธนบุรี เฮลท์แคร์ กรุ๊ป เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้อง จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น ดังต่อไปนี้

ข้อ 1. ประกาศนี้เรียกว่า "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาล และบริษัทในเครือ "ธนบุรี เฮลท์แคร์ กรุ๊ป"

ข้อ 2. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาล และบริษัทในเครือ ธนบุรี เฮลท์แคร์ กรุ๊ป มีวัตถุประสงค์ ดังต่อไปนี้

2.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศ ของโรงพยาบาล และบริษัทในเครือฯ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2 เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในโรงพยาบาล และบริษัทในเครือฯ และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติ อย่างเคร่งครัด

2.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและ บุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล และบริษัทในเครือฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาล และบริษัทในเครือฯ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ 3. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล และบริษัทในเครือฯ กำหนดประเด็นสำคัญดังต่อไปนี้

3.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

3.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ มีการกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับ ได้รับรู้ เข้าใจ และ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และ ตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศ

3.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึง ระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติ และกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และจะต้องเก็บบันทึกข้อมูลการเข้าถึง และ ข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสม ตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดปลอดภัยเสมอ

3.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทาง เครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินนเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัย และมีการออกแบบระบบเครือข่าย โดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

3.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดง ตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบ สารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธ และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

3.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์ การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงาน เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3.2 การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถ ให้บริการได้อย่างต่อเนื่อต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณี ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศ ได้ตามปกติอย่างต่อเนื่อง

3.3 ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบ จากผู้ตรวจสอบภายในของหน่วยงาน (Internal Audit) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย จากภายนอก (External Audit) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ 4. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

THONBURI HEALTHCARE GROUP PUBLIC COMPANY LIMITED 34/1 Soi Itsaraphap 44, Ban Chang Lo, Bangkok Noi, Bangkok 10700

ข้อ 5. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของบริษัท ธนบุรี แฮลท์แคร์ กรุ๊ป จำกัด (มหาชน) ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ 17 กรกฎาคม พ.ศ. 2566

(นายแพทย์ธนาธิป ศุภประดิษฐ์)
ประธานเจ้าหน้าที่บริหาร
บริษัท ธนบุรี แฮลท์แคร์ กรุ๊ป จำกัด (มหาชน)

ฝ่ายเทคโนโลยีสารสนเทศ
บริษัท ธนบุรี แฮลท์แคร์ กรุ๊ป จำกัด (มหาชน)
Email: IT@thg.co.th