ประกาศโรงพยาบาลตากฟ้า
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๗

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของโรงพยาบาลตากฟ้า

จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลอย่างมีประสิทธิภาพ มีความมั่นคง ปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่องสามารถป้องกันภัยคุกคามไซเบอร์ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลตากฟ้า ทางโรงพยาบาลจึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวทางนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ หน่วยงาน ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า "ประกาศโรงพยาบาลตากฟ้า เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๖

ข้อ ๒ ในประกาศ

(๑) "รพ.ตากฟ้า" หมายความว่า โรงพยาบาลตากฟ้า สำนักงานปลัดกกระทรวงสาธารณสุข

(๒) "ผู้บริหาร" หมายความว่า ผู้อานวยการ รพ.ตากฟ้า

(๓) "คณะกรรมการ" หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รพ.ตากฟ้า

(๔) "นโยบาย" หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตาม พระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๔.๑) พระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๔.๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๔.๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔.๔) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม (๔.๕) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๕) "แนวปฏิบัติ" หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ รพ.ตากฟ้า ได้ถือปฏิบัติตาม นโยบาย ข้อ ๒ (๕)

(๖) "ผู้ดูแลระบบ" (System Administrator) หมายความว่า บุคลากร รพ.ตากฟ้า ผู้ซึ่งได้รับมอบหมาย จากเจ้าของระบบ (System Owner/ หรือจากผู้อานวยการ รพ.ตากฟ้า ให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ์ และการบริหารจัดการระบบเทคโนโลยีสารสนเทศผู้อำนวยการ รพ.ตากฟ้า

(๗) "ผู้ใช้งาน " (User) หมายความว่า บุคลากร ผู้อำนวยการ รพ.ตากฟ้าทุกระดับ ซึ่งเป็นข้าราชการ พนักงาน ราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศ รพ.ตากฟ้า

(๘) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้อง กับระบบเทคโนโลยีสารสนเทศของ รพ.ตากฟ้า

(๙) "สินทรัพย์ " (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบ คอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสาหรับงานด้านเทคโนโลยี สารสนเทศของ รพ.ตากฟ้า ประกอบด้วย

(๙.๑) ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบเครื่องแม่ข่ายปกติ (Rack Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) และคอมพิวเตอร์พกพา (Laptop)
- เครื่องพิมพ์ (Pinter/Scanner) และอุปกรณ์สำรองข้อมูลของ รพ.ตากฟ้า อุปกรณ์โครงข่าย (Network หรือ อุปกรณ์รักษาความมั่นคงปลอดภัยและที่แก้ไขเพิ่มเติม
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สาหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๙.๒) โปรแกรมประยุกต์หรือแอปพลิเคชัน (Program or Application) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ฮาร์ดแวร์

(๑๐) "ศูนย์ข้อมูลและสารสนเทศ" หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะ เพื่อติดตั้ง อุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบ รักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

(๑๐.๑) "ศูนย์ข้อมูล" (Data Center) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของ รพ.ตากฟ้า

(๑๑) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือ การมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๑๒) "ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integity) และสภาพพร้อมใช้งาน (Availability) ของ สารสนเทศรวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (Reliability)

(๑๓) "เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๔) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทาให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ รพ.ตากฟ้า ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

(๑) นโยบายได้มาเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ

(๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๓) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๕ รพ.ตากฟ้า ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศพร้อมทั้งได้กำหนดให้ "ผู้ดูแลระบบ" รพ.ตากฟ้า เป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตาม นโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

(๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

(๗) การจัดหาระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

(๙) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management) โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๖ รพ.ตากฟ้า ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการ ใดวิธีการหนึ่งให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึงและปฏิบัติตามด้วยหนังสือเวียนภายในองค์กร ระบบ เครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์ภายในและภายนอก) รพ.ตากฟ้า

ข้อ ๗ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของ รพ.ตากฟ้า เกิดความเสียหายหรือ อันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือผ่าฝืนการปฏิบัติตาม นโยบายและ

แนวปฏิบัติ "ผู้ดูแลระบบ" ต้องรายงานต่อผู้อำนวยการ รพ.ตากฟ้า สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบ เทคโนโลยีสารสนเทศของ รพ.ตากฟ้า

ข้อ ๘) รพ.ตากฟ้า กำหนดให้ "ผู้ดูแลระบบ" เป็นผู้รับผิดชอบในการบริหารความเสี่ยง ควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรือ อันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตาม นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รพ.ตากฟ้า

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๔ พฤศจิกายน พ.ศ. ๒๕๖๖

(นายวสันต์ พนธารา)

นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลตากฟ้า