ประกาศโรงพยาบาลวังน้ำเย็น

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๗

.....

ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของโรงพยาบาลวังน้ำเย็น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลวังน้ำเย็น ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลวังน้ำเย็น รวมทั้งประชาชนผู้ใช้บริการโรงพยาบาลวังน้ำเย็นได้ ทางโรงพยาบาลวังน้ำเย็นตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ จึงประกาศนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลวังน้ำเย็น ดังต่อไปนี้

๑. แนวปฏิบัติด้านการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๒. แนวปฏิบัติการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๑. ประกาศนี้ เรียกว่า “ประกาศโรงพยาบาลวังน้ำเย็น เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๗”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. คำนิยาม

(๑) “ผู้บริหารระดับสูงสุด” หมายความว่า ผู้อำนวยการโรงพยาบาลหรือรองผู้อำนวยการโรงพยาบาลที่ได้รับมอบหมายในฐานะผู้บริหารระดับสูง

(๒) “ผู้ดูแลระบบ” (System Administrator) หมายความว่า บุคลากร หรือเจ้าหน้าที่ผู้ซึ่งได้รับมอบหมายจาก เจ้าของระบบ (System Owner) หรือจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ ของ ระบบเทคโนโลยีสารสนเทศ สบส.

(๓) “ผู้ใช้งาน” (User) หมายความว่า บุคลากร เจ้าหน้าที่โรงพยาบาลวังน้ำเย็นทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมประยุกต์ แอปพลิเคชัน หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยี สารสนเทศโรงพยาบาล โดยสิทธิของผู้ใช้งาน (Role) ตามบทบาทที่โรงพยาบาลกำหนดไว้

(๔) “สิทธิของผู้ใช้งาน” หมายความว่าสิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่ เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของที่โรงพยาบาลกำหนดไว้

(๕) “สินทรัพย์” (Asset) หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามเกี่ยวกับระบบเทคโนโลยีสารสนเทศโรงพยาบาลวังน้ำเย็น

(๖) “ฮาร์ดแวร์”...

(๖) "ฮาร์ดแวร์" (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใด อย่างหนึ่งในต่อไปนี้

(๖.๑) เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบเครื่องแม่ข่ายปกติ (Rack Server) และ เครื่องแม่ข่ายแบบชุด (Blade Server)

(๖.๒) เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุน เครื่องพิมพ์ (Printer/Scanner) และอุปกรณ์สำรองข้อมูล ของโรงพยาบาลวังน้ำเย็น

(๖.๓) อุปกรณ์โครงข่าย (Network) หรืออุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๗) "โปรแกรมประยุกต์หรือแอปพลิเคชั่น" (Program Application) หมายความว่าระบบคุณลักษณใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

(๘) "ศูนย์เทคโนโลยีสารสนเทศ" หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลวังน้ำเย็น

(๙) "การรักษาความมั่นคงปลอดภัย" หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลโคกสูง

(๑๐) "ผู้ถือครองเครื่องคอมพิวเตอร์" หมายความว่า ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำในการปฏิบัติงานและถือ ครอง รับผิดชอบ ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้อง

(๑๑) "ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๑๒) "รหัสผ่าน" (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๑๓) "ชุดคำสั่งไม่พึงประสงค์" หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๑๔) "เครือข่าย" (Network System) หมายความว่า ระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ในหัวข้อ Hardware, Software และระบบเทคโนโลยีสารสนเทศ ทั้งแบบใช้สายและไร้สาย ของโรงพยาบาลวังน้ำเย็น

(๑๕) "ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ (Website) เว็บพอร์ทัล (Portal Web) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือติดตั้ง หรือการนำมาประยุกต์ใช้เพื่อสนับสนุนการปฏิบัติงานของโรงพยาบาลวังน้ำเย็น

(๑๖) "ข้อมูลสารสนเทศ" หมายความว่า ข้อมูล(Data) หรือสารสนเทศ(Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (Files) ฐานข้อมูล (Database) หรือเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (e-Document) เป็นต้น

(๑๗) "พื้นที่ปฏิบัติงานทั่วไป"...

(๑๗) "พื้นที่ปฏิบัติงานทั่วไป" (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายในโรงพยาบาลวังน้ำเย็น ซึ่งได้มีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วงและเครือข่ายแบบมีสาย (LAN) และไร้สาย (Wireless)

(๑๘) "ศูนย์ข้อมูลและสารสนเทศ" หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษา ความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน

(๑๙) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๒๐) "ความมั่นคงปลอดภัยด้านสารสนเทศ"(Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (Reliability)

(๒๑) "เหตุการณ์ด้านความมั่นคงปลอดภัย"(Information Security Event) หมายความว่า กรณีที่ ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความ มั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๒) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด"(Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔. คำนิยาม โรงพยาบาลวังน้ำเย็น ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษรตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึง ข้อ ๙

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาลวังน้ำเย็น

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๔) ต้องทบทวนและปรับปรุงนโยบายอย่างน้อย ปีละ ๑ ครั้ง

๕.๒ ส่วนที่ว่าด้วย...

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (Access Control) มีนโยบายที่จะให้บริการ เทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่เปิดเผย (Business Requirements for Access Control)

(๑.๑) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๑.๒) การควบคุมการเข้าถึงโปรแกรมประยุกต์และ

(๑.๓) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒) ศูนย์ข้อมูลและสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อม ใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ควบคุมคุณภาพและดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคง ปลอดภัยที่เกิดขึ้น

(๕) การสร้างความรู้ ความเข้าใจการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการ สร้างความรู้ ความเข้าใจ โดยการจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ผู้ใช้งาน

ข้อ ๖. โรงพยาบาลวังน้ำเย็น ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งได้กำหนดให้ หัวหน้ากลุ่มงานสุขภาพดิจิทัลเป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติ ดังกล่าวไว้อย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (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) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

ข้อ ๗. โรงพยาบาลวังน้ำเย็น ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ให้ผู้ใช้งานและบุคคลภายนอกทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามผ่านทางเว็บไซต์ ของโรงพยาบาลวังน้ำเย็น

ข้อ ๘. หน่วยงานภายในโรงพยาบาลวังน้ำเย็น ต้องปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด ตามประกาศ“ประกาศโรงพยาบาลวังน้ำเย็น เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๗”

ข้อ ๙. หากระบบคอมพิวเตอร์...

ข้อ ๙. หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลวังน้ำเย็น เกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติหัวหน้ากลุ่มงานสุขภาพดิจิทัล ต้องรายงานต่อผู้บริหารระดับสูงสุด สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลวังน้ำเย็น เพื่อรายงานต่อผู้บริหารระดับจังหวัด

ข้อ ๑๐. โรงพยาบาลวังน้ำเย็น กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ระบบสารสนเทศและข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่โรงพยาบาลวังน้ำเย็น หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้

ข้อ ๑๑. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ทั้งนี้ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ กรกฎาคม พ.ศ. ๒๕๖๗

(นายวัฒนพล จิติลาภะ)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลวังน้ำเย็น