ประกาศโรงพยาบาลค่ายสุรศักดิ์มนตรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙

ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ระเบียบ ทบ. ว่าด้วยการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของ ทบ. (ฉบับที่ ๒) ปี ๒๕๖๐ รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของโรงพยาบาลค่ายสุรศักดิ์มนตรี ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) มีผลกระทบต่อประชาชนโดยตรง จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัล อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถ ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลค่ายสุรศักดิ์มนตรี รวมทั้งประชาชนผู้มารับบริการ ประกอบกับโรงพยาบาลค่ายสุรศักดิ์มนตรี ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ ๒๕๖๗ ตามประกาศ ระเบียบ ทบ. ว่าด้วยการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของ ทบ. (ฉบับที่ ๒) ปี ๒๕๖๐ และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ.๒๕๕๖ ข้อ ๓ ได้กำหนดให้หน่วยงานรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศโรงพยาบาลค่ายสุรศักดิ์มนตรี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙”

ข้อ ๒ ในประกาศนี้

(๑) “รพ.ค่ายสุรศักดิ์มนตรี” หมายความว่า โรงพยาบาลค่ายสุรศักดิ์มนตรี

(๒) “ผู้บริหารระดับสูง” หมายความว่า ผู้อำนวยการโรงพยาบาล

(๓) “ผู้บริหารเทคโนโลยีสารสนเทศ”หมายความว่า ประธานงานสารสนเทศ

(๔) “คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๕) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๓.๑) ระเบียบ ทบ. ว่าด้วยการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของ ทบ. (ฉบับที่ ๒) ปี ๒๕๖๐

(๓.๒) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐

(๓.๓) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๓.๔) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๓.๕) พระราชบัญญัติว่า ด้วยธรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และ พ.ศ. ๒๕๖๕

(๓.๖) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๓.๗) กฎหมายอื่นๆ ทั้งในและต่างประเทศที่เกี่ยวข้อง

(๖) “แนวปฏิบัติ” หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ รพ.ค่ายสุรศักดิ์มนตรี ได้ถือปฏิบัติตามนโยบาย ข้อ ๒ (๕)

(๗) “ผู้ดูแลระบบ” (System Administrator) หมายความว่า บุคลากร รพ.ค่ายสุรศักดิ์มนตรี ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากประธานสารสนเทศ ให้มีหน้าที่รับผิดชอบในการ กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ ของ รพ.ค่ายสุรศักดิ์มนตรี

(๘) “เจ้าของระบบ” (System Owner) หมายความว่า ศูนย์บริการคอมพิวเตอร์ เป็นผู้รับผิดชอบในการพัฒนาระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพต่อ รพ.ค่ายสุรศักดิ์มนตรีในภาพรวม หรือตามที่ผู้บริหารให้ดำเนินงาน หรือมีหน้าที่อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

(๙) “ผู้ใช้งาน” (User) หมายความว่า บุคลากร รพ.ค่ายสุรศักดิ์มนตรี ทุกระดับ ซึ่งเป็น ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมประยุกต์หรือแอพพลิเคชั่นของ รพ.ค่ายสุรศักดิ์มนตรี

(๑๐) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของ รพ.ค่ายสุรศักดิ์มนตรี

(๑๑) “สินทรัพย์” (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ รพ.ค่ายสุรศักดิ์มนตรี ประกอบด้วย

(๑๑.๑) ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่ายแบบชุด (Blade Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุน เครื่องพิมพ์ (printer/Scanner) และอุปกรณ์สำรองข้อมูลของ รพ.ค่ายสุรศักดิ์มนตรี
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point)หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๑๑.๒) โปรแกรมประยุกต์หรือแอพพลิเคชั่น(Program or Application) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

(๑๑.๓) เครือข่าย (Network and Communication) หมายความว่าระบบเทคโนโลยีด้านการสื่อสารโทรคมนาคม ของ รพ.ค่ายสุรศักดิ์มนตรี

(๑๑.๔) “ระบบสารสนเทศ” หมายความว่า ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ (Website) เว็บพอร์ทัล (Portal Web) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนาหรือการนำมาประยุกต์ใช้เพื่อสนับสนุนการปฏิบัติงานของ รพ.ค่ายสุรศักดิ์มนตรี

(๑๑.๕) “ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล (Data) หรือสารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (Files) ฐานข้อมูล(Database) หรือเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (e-Document) เป็นต้น

(๑๒) “พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายใน รพ.ค่ายสุรศักดิ์มนตรี ซึ่งได้มีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วง และเครือข่ายแบบมีสาย (LAN) และไร้สาย (Wireless)

(๑๓) “ศูนย์ข้อมูลและสารสนเทศ” หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่าย คอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษา ความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

(๑๓.๑) “ศูนย์กลางข้อมูล” (DC : Data Center) หมายความว่า ศูนย์กลางข้อมูลและสารสนเทศ ของ รพ.ค่ายสุรศักดิ์มนตรี ตั้งอยู่ที่ชั้น ๒ อาคารกองบังคับการ

(๑๓.๒) “ศูนย์สำรองข้อมูล” (DR Site : Disaster Recovery Site) หมายความว่า ศูนย์กลางสำรองข้อมูลและสารสนเทศ ของ รพ.ค่ายสุรศักดิ์มนตรี ตั้งอยู่ที่ชั้น ๑ อาคารอุบัติเหตุ

(๑๓.๓) “ศูนย์บริการสุขภาพ” (OSS” One Stop Service) หมายความว่า หน่วยให้บริการข้อมูลด้านระบบบริการสุขภาพแบบเบ็ดเสร็จครบวงจร ณ จุดเดียวตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ตั้งอยู่ที่ชั้น ๑ อาคารอุบัติเหตุ

(๑๓.๔) “ห้องเซิร์ฟเวอร์” (Server Room) หมายความว่า ศูนย์ข้อมูลและสารสนเทศ ของ รพ.ค่ายสุรศักดิ์มนตรี ตั้งอยู่ที่ชั้น ๒ อาคารกองบังคับการ

(๑๔) “เครือข่าย” (Network System) หมายความว่า ระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ในหัวข้อ Hardware, Software และระบบเทคโนโลยีสารสนเทศของ รพ.ค่ายสุรศักดิ์มนตรีทั้งแบบใช้สายและไร้สาย

(๑๕) “ระบบงาน” หมายความว่า ระบบฐานข้อมูลที่สนับสนุนการดำเนินงาน ของ รพ.ค่ายสุรศักดิ์มนตรี

(๑๓.๑) งานคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ
(๑๓.๒) งานสนับสนุนการบริหารจัดการและกำกับมาตรฐานระบบบริการสุขภาพ
(๑๓.๓) งานวิศวกรรมการแพทย์และเครื่องมือแพทย์
(๑๓.๔) งานแบบมาตรฐานอาคารด้านระบบบริการสุขภาพ
(๑๓.๕) งานการมีส่วนร่วมภาคประชาชน
(๑๓.๖) งานสุขศึกษา
(๑๓.๗) งานสนับสนุนสุขภาพภาคประชาชน

(๑๖) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๑๗) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า การธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non- repudiation) และความน่าเชื่อถือ (Reliability)

(๑๘) “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า กรณีที่ ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความ มั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๙) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ รพ.ค่ายสุรศักดิ์มนตรี ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษรตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔ ถึง ข้อ ๙

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของ รพ.ค่ายสุรศักดิ์มนตรี

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๔) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (Access Control) มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้ อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่เปิดเผย (Business Requirements for Access Control)

(๑.๑) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๑.๒) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๑.๓) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒) ศูนย์ข้อมูลและสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐานโดยแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ควบคุมคุณภาพและดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น

(๕) การสร้างความรู้ ความเข้าใจการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ ความเข้าใจ โดยการจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ผู้ใช้งาน

ข้อ ๕ รพ.ค่ายสุรศักดิ์มนตรี ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งได้กำหนดให้ ประธานสารสนเทศเป็นผู้กำกับดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน 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) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

ข้อ ๖ รพ.ค่ายสุรศักดิ์มนตรี ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึงเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่งให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบเพื่อให้สามารถเข้าใจเข้าถึงและปฏิบัติตามด้วยหนังสือเวียนภายในองค์กร ระบบเครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์ภายในและภายนอก รพ.ค่ายสุรศักดิ์มนตรี

ข้อ ๗ หน่วยงานภายใน รพ.ค่ายสุรศักดิ์มนตรี ที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานได้เอง ทั้งนี้ต้องให้สอดคล้องกับ “ประกาศโรงพยาบาลค่ายสุรศักดิ์มนตรี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙”

ข้อ ๘ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ ของ รพ.ค่ายสุรศักดิ์มนตรี เกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ประธานสารสนเทศ ต้องรายงานต่อผู้บริหารระดับสูงสุด สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ รพ.ค่ายสุรศักดิ์มนตรี

ข้อ ๙ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ เมษายน พ.ศ. ๒๕๖๙

พ.อ.
(จรัญวิชญ์ สุขชัย)
ผู้อำนวยการโรงพยาบาลค่ายสุรศักดิ์มนตรี

ศูนย์บริการคอมพิวเตอร์
โทรศัพท์ ๐๕๔-๘๓๙๓๐๕ ต่อ ๖๒๐๓
โทรสาร ๐๕๔-๘๓๙๓๑๐