คำสั่งโรงพยาบาลบ้านฉาง

ที่ ๕๔๙/๒๕๖๗

เรื่อง นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสาหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

เพื่อให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านฉางเป็นไปด้วยความมั่นคงปลอดภัยต่อเนื่องรวมถึงการเสริมสร้าง พัฒนาการบริหารจัดการป้องกันความเสียหายหรือความสูญหายของระบบเทคโนโลยีสารสนเทศตลอดจนการรักษาข้อมูลระบบเทคโนโลยีสารสนเทศและสนับสนุนการดำเนินกิจการขององค์กรได้อย่างมีประสิทธิภาพ ดังนี้

๑. นโยบายการรักษาความปลอดภัยของพื้นที่ (Physical Area Security)

๑ .๑ แบ่งเขตของพื้นที่เพื่อกำหนดความปลอดภัยของพื้นที่ดังต่อไปนี้

- พื้นที่ติดตั้ง PC Terminal
- พื้นที่สาหรับระบบเครือข่ายข้อมูลคอมพิวเตอร์
- พื้นที่ติดตั้งระบบและจัดเก็บข้อมูล (Data Center Area)

๑.๒ ต้องจัดให้มีกฎระเบียบปฏิบัติควบคุมการเข้าและการออกพื้นที่ติดตั้งระบบและจัดเก็บข้อมูล

๑.๓ การเข้าและออกพื้น ที่ปฏิบัติงาน ต้องแสดงสิทธิเข้าถึงพื้นที่ปฏิบัติงาน มีการบันทึก Log การเข้าปฏิบัติงาน สำหรับการตรวจสอบ สำหรับผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ให้ปฏิบัติตาม มาตรการรักษาความปลอดภัยของระบบ

๒. นโยบายการรักษาความปลอดภัยของระบบเครือข่าย (Network Security)

๒.๑ ระบบเครือข่ายภายใน (Local Area Network) อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายโดยติดตั้งใช้งานภายใน Local Area หรือเพื่อการทำงานภายในโรงพยาบาล ได้แก่ Router,Switching HUB กำหนดข้อปฏิบัติในการใช้งานดังนี้

๒.๑.๑ อุปกรณ์ Router, Switching HUB และอุปกรณ์อื่นๆ ที่ทำหน้าที่เป็นการขยายการเชื่อมโยงเครือข่ายต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password เป็นต้น

๒.๑.๒ การเชื่อมโยงเครือข่ายเพื่อใช้ระบบงานต่าง ๆ จะสามารถกระทำได้เมื่อได้รับอนุญาตจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ หรือผู้ดูแลเครือข่าย โดยความเห็นชอบของผู้อำนวยการโรงพยาบาล การเชื่อมโยงเครือข่ายเองโดยพลการหากทำให้เกิดความเสียหายกับระบบเครือข่ายจะได้รับการพิจารณาโทษ

๒.๑.๓ ต้องจัดให้มีแผนและดำเนินการบำรุงรักษาระบบเครือข่ายเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน

๒.๑.๔ ต้องจัดให้มีระบบจ่ายไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถทำงานได้ต่อเนื่อง

๒.๑.๕ IP address ภายในของระบบงานเครือข่ายภายในขององค์กรจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของห้องคอมพิวเตอร์แม่ข่ายได้โดยง่าย

๒.๑.๖ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๒ ระบบ Remote Access อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS) กำหนดข้อปฏิบัติในการใช้งานดังนี้

๒.๒.๑ อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

๒.๒.๒ เมื่อทำการทดสอบการใช้งานอุปกรณ์ RAS แล้ว User/Password ที่ใช้งานทดสอบเมื่อเสร็จงานแล้วให้ทำการลบทิ้งทันที

๒.๒.๓ อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่าDefault Community, Default Username และ Default Password

๓. นโยบายการรักษาความปลอดภัยของ Host (Host Security)

๓.๑ การรักษาความปลอดภัยของ Server

๓.๑.๑ ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password

๓.๑.๒ ต้อง Harden และบันทึกการ Configuration Set up ของอุปกรณ์ Server ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

๓.๑.๓ กำหนดการใช้งาน Service Port ให้เปิด Service Port ที่จำเป็นเท่านั้น ส่วนที่ไม่ใช้งานให้ปิดทั้งหมดและต้องมีบันทึกการติดตั้ง Service Patch ทุกครั้ง

๓.๑.๔ ต้องไม่เปิดเผย OS Version, Service Port และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

๓.๑.๕ การ Login ใช้งานที่ Console นั้นเมื่อจบการทำงานแล้วต้อง Log off User นั้นโดยทันที

๓.๑.๖ ผู้ดูแลระบบจะต้องทำการสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยทุกเดือน และทดสอบ การสำรอง ข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบ

๓.๒ การรักษาความปลอดภัยของ PC Terminal

๓.๒.๑ เครื่อง PC Terminal ต้องตั้งชื่อเครื่องทุกเครื่องที่ติดต่อกับเครือข่าย

๓.๒.๒ กำหนดการใช้งาน Protocol บน เครื่อง PC Terminal ต้องใช้ติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น

๓.๒.๓ การเชื่อมโยง PC Terminal กับเครือข่ายจะต้องอยู่ภายใต้มาตรฐานการเชื่อมโยงเครือข่าย ที่ใช้งานร่วมกัน

๓.๒.๔ การใช้งาน Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

๓.๓ การรักษาความปลอดภัย Software

๓.๓.๑ เจ้าหน้าที่ต้องใช้คอมพิวเตอร์ซอฟต์แวร์ตามมาตรฐานที่โรงพยาบาลบ้านฉางกำหนด กรณีที่นำซอฟต์แวร์นอกเหนือจากมาตรฐานมาใช้ เจ้าหน้าที่ต้องรับผิดชอบในผลเสียที่เกิดขึ้นกับโรงพยาบาลบ้านฉาง

๓.๓.๒ เจ้าหน้าที่ไม่มีสิทธิ์ในการติดตั้งหรือรื้อถอนซอฟต์แวร์ที่ติดตั้งให้เป็นอันขาด หากกระทำโดย พลการและเกิดความเสียหายกับโรงพยาบาลบ้านฉางต้องได้รับโทษ

๔. นโยบายการรักษาความปลอดภัยของข้อมูล

๔.๑ การเข้าถึงข้อมูลต้องได้รับการอนุญาตจากเจ้าของข้อมูลเท่านั้น

๔.๒ ข้อมูลที่เป็นความลับต้องรักษาระดับความลับของข้อมูล ตรวจสอบระบบรักษาความลับของข้อมูลที่มีความสำคัญต่อการบริหารและการดำเนินการขององค์กร

๔.๓ ห้ามทำการสำเนาพิมพ์ข้อมูลที่เป็นความลับ ไม่ว่ากรณีใด เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้อำนวยการโรงพยาบาล เท่านั้น ข้อมูลที่เป็นความลับ หมายความว่า ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล ข้อมูลผู้รับบริการ

๔.๔ ต้องจัดให้มีแผนการสำรองข้อมูลเมื่อระบบถูกบุกรุกและแก้ไขข้อมูล

๔.๕ โรงพยาบาลบ้านฉาง มีสิทธิที่จะตรวจสอบข้อมูลโปรแกรม หรือ เอกสารอิเล็กทรอนิกส์อื่นๆ ที่เจ้าหน้าที่หรือผู้ปฏิบัติงานนำมาจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อให้ สอดคล้องกับกฎหมาย ศีลธรรม และระเบียบปฏิบัติของโรงพยาบาลหรือเพื่อการดำเนินการทางวินัยและกฎหมาย

๕. นโยบายการใช้รหัสผ่าน (Password)

๕.๑ เจ้าหน้าที่ต้องใช้ Password ที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิที่ได้รับเท่านั้น

๕.๒ เจ้าหน้าที่ที่ได้รับ Password ในครั้งแรก ต้องเปลี่ยน Password ใหม่ให้เป็นความลับเฉพาะตัวและต้องทำการเปลี่ยน Password ใหม่ทันที หาก Password ถูกเปิดเผย

๕.๓ เจ้าหน้าที่ต้องเปลี่ยน Password ทุก ๆ ๓๐ วัน หรือตามระยะเวลาที่กำหนด และในการเปลี่ยนPassword ใหม่ในแต่ละครั้งจะต้องไม่นำ Password ที่หมดอายุแล้วมาใช้ซ้ำอีก

๕.๔ เจ้าหน้าที่ต้องทำการ Log out ออกจากระบบคอมพิวเตอร์ทันทีเมื่อเลิกใช้งาน หรือ เมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน ๑๐ นาที ให้ Screen Saver ควบคุมหน้าจอคอมพิวเตอร์ด้วย Password

๕.๕ หากเจ้าหน้าที่พบเหตุที่ก่อให้เกิดความสงสัยว่าถูกผู้อื่นนำ Password ไปใช้ให้แจ้งคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์

๖. นโยบายการใช้อินเตอร์เน็ต

๖.๑ เจ้าหน้าที่ต้องไม่ใช้อินเตอร์เน็ตในเครือข่ายของโรงพยาบาลบ้านฉาง เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่ Web Site ที่ไม่เหมาะสม เช่น Web Site ที่ขัดต่อศีลธรรมอันดี Web Site ที่มีเนื้อหาต่อต้านชาติ ศาสนา พระมหากษัตริย์หรือ Web Siteที่เป็นภัยต่อสังคม รวมถึงลามกอนาจาร เป็นต้น

๖.๒ เจ้าหน้าที่ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับโรงพยาบาลบ้านฉาง

๖.๓ เจ้าหน้าที่มีหน้าที่ต้องรายงานต่อคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ ทันที หากพบเห็นการใช้อินเตอร์เน็ตในเครือข่ายของโรงพยาบาลบ้านฉางไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิของโรงพยาบาลบ้านฉาง เช่น ส่งข้อมูลที่เป็นความลับให้บุคคลภายนอก เป็นต้น

๖.๔ การเชื่อมต่อ เครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเตอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลบ้านฉาง จัดสรรไว้เท่านั้น ห้ามเจ้าหน้าที่ทำการเชื่อมต่อ เข้าสู่เครือข่ายอินเตอร์เน็ตโดยตรงโดยผ่านช่องทางอื่น เช่น Dial up Modem เว้นแต่ว่าจะได้รับอนุญาตเป็นกรณีพิเศษ

๖.๕ ให้ใช้เฉพาะเครื่อง PC Terminal ที่กำหนดให้ใช้อินเตอร์เน็ตเท่านั้น ห้ามใช้เครื่องส่วนบุคคลเข้าสู่ระบบงานเข้าอินเตอร์เน็ตของโรงพยาบาลบ้านฉาง เป็นอันขาด

๖.๖ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีขออนุญาตจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ก่อน และ ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ทุกครั้ง

๗. นโยบายการรับ – ส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) (*หมายเหตุ เจ้าหน้าที่ = User)

๗.๑ เจ้าหน้าที่ควรระมัดระวังในการใช้ E-Mail เพื่อไม่ให้เกิดความเสียหาย หรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น หรือ ผิด กฎหมาย หรือ ละเมิด ศีลธรรม และไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ E-Mail ในระบบของโรงพยาบาลบ้านฉาง

๗.๒ เจ้าหน้าที่ต้องรับผิดชอบในข้อความ รูปภาพ เสียง หรือ แฟ้มข้อมูลที่ส่งออกจากเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ทั้งหมด

๗.๔ ก่อนที่จะ Download ไฟล์จาก E-Mail ต้องทำการ Scan Virus ก่อนทุกครั้ง

๘. นโยบายการป้องกันไวรัสคอมพิวเตอร์

๘.๑ ห้ามเจ้าหน้าที่นำคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์ มาติดตั้งหรือใช้งานในโรงพยาบาลบ้านฉาง เว้นแต่คอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์นั้นได้ผ่านการตรวจสอบจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ โรงพยาบาลบ้านฉาง แล้วเท่านั้น

๘.๒ เจ้าหน้าที่ควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ประจำหน่วยงานไว้ เช่น CD-RWหรือ Flash Drive เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

๘.๓ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิกการทำงานของคอมพิวเตอร์ซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่โรงพยาบาลบ้านฉาง จัดหาให้

๘.๔ เจ้าหน้าที่ควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้โดยตรวจสอบว่ามีการUpdate ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่าง สม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๘.๕ เจ้าหน้าที่ควรแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟท์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อมีสงสัยว่ามีการติดไวรัสคอมพิวเตอร์

๙. นโยบายการปฏิบัติตามข้อกำหนด (Compliance)

๙.๑ โรงพยาบาลบ้านฉาง ต้องเก็บ Log file การเข้าสู่ระบบคอมพิวเตอร์ของเจ้าหน้าที่ ไว้ไม่ต่ำกว่า ๙๐ วัน

๙.๒ ห้ามตัดต่อภาพ ปรับเปลี่ยน แก้ไขข้อมูล บางส่วน หรือทั้งหมด ก่อนได้รับอนุญาตจากเจ้าของข้อมูล หรือ กระทำกับข้อมูลอันเป็นการสร้างความเสียหายแก่ผู้อื่น โดยเด็ดขาด และคำสั่งนี้โรงพยาบาลบ้านฉางได้แต่งตั้งบุคคลต่อไปนี้ ประกอบด้วย

๑. คณะทำงานสารสนเทศทางการแพทย์และคอมพิวเตอร์โรงพยาบาลบ้านฉาง

๑. นายธเนษฐ์ กมลอดิศัย	ตำแหน่งทันตแพทย์ชำนาญการ	ประธานกรรมการ
๒. นางสมลักษณ์ ทองสุข	ตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ	รองประธานกรรมการ
๓. นางปาริชาติ จันทะเกิด	ตำแหน่งพยาบาลวิชาชีพชำนาญการ	กรรมการ
๔. นางสาวจารุภา ตั้งก่อพันธุ์	ตำแหน่งเภสัชกรชำนาญการ	กรรมการ
๕. นายศิวกร เสือคำรณ	ตำแหน่งนักเทคนิคการแพทย์ปฏิบัติการ	กรรมการ
๖. นางสาววารีย์ ศรีบุษย์	ตำแหน่งพยาบาลวิชาชีพชำนาญการ	กรรมการและเลขานุการ

ให้คณะทำงานมีอำนาจและหน้าที่ดังนี้

๑. ให้คำปรึกษาเชิงนโยบายและแนวทางการดำเนินการด้านการพัฒนาระบบสารสนเทศ ความมั่นคงปลอดภัยของระบบสารสนเทศของโรงพยาบาล ตลอดจน แนวทางแก้ไขปัญหาและอุปสรรคที่เกิดขึ้นจากการปฏิบัติงาน

๒. พิจารณาให้ความเห็นต่อแผนปฏิบัติงานสารสนเทศ และติดตามการดำเนินการด้านการพัฒนาระบบสารสนเทศตามแผนปฏิบัติที่กำหนดไว้

๓. ให้ข้อเสนอแนะอื่นๆ ที่เกี่ยวกับการบริหารระบบสารสนเทศของโรงพยาบาล

๔. กำกับ ดูแล และติดตามการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

๒. คณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ โรงพยาบาลบ้านฉาง

๑. นายอภิชาติ อรรคบุตร	ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ประธานคณะทำงาน
๒. นายยุทธนา เวชเวโรจน์	ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๓. นายพงศกร ต่อพล	ตำแหน่ง นักวิชาการคอมพิวเตอร์	คณะทำงาน
๔. น.ส.ธัศม์มสา อธิวัฒน์ธนะภัค	ตำแหน่ง พนักงานธุรการงานโสต	คณะทำงาน
๕. น.ส.จิรภัทร สาขามุละ	ตำแหน่ง โสตทัศศึกษา	เลขานุการ

ให้คณะเจ้าหน้าที่ผู้ดูแลระบบมีอำนาจและหน้าที่ดังนี้

๑. วางแนวทางพัฒนาระบบเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยของระบบสารสนเทศตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยี สารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

๒. ดูแลระบบคอมพิวเตอร์ของโรงพยาบาล ทั้งด้าน Hardware, Software และ Network ให้มีความพร้อมใช้งาน ตลอดเวลา

๓. มีภารกิจด้านการดูแลระบบการบันทึกข้อมูลการให้บริการผู้ป่วยผ่านระบบ Hospital Information System ให้มีคุณภาพ

๔. ดูแลการสื่อสารในรูปแบบอิเลคทรอนิกส์ไฟล์ผ่านเครือข่ายภายในระบบคอมพิวเตอร์ของโรงพยาบาลให้มีความพร้อมใช้งาน ตลอดเวลา

๕. ดูแลและรักษาความปลอดภัยของระบบเครือข่ายให้สามารถรองรับการใช้งานได้ตลอดเวลา โดยจัดให้มีเจ้าหน้าที่รับผิดชอบทั้งในและนอกเวลาราชการ

๖. ดูแล และรักษาการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ของ โรงพยาบาลบ้านฉาง โดยเคร่งครัด

๗. งานอื่นๆ ที่เกี่ยวกับการบริหารระบบสารสนเทศของโรงพยาบาล และที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗

(นายสุรชัย คำภักดี)
ผู้อำนวยการโรงพยาบาลบ้านฉาง
Sign: 39962B3EB75DACEC6489B08A7356815B
RefNo: 25670304161149844

สำเนาคู่ฉบับ

คำสั่งโรงพยาบาลบ้านฉาง

ที่ ๕๔๙/๒๕๖๗

เรื่อง นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสาหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

เพื่อให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านฉางเป็นไปด้วยความมั่นคงปลอดภัยต่อเนื่องรวมถึงการเสริมสร้าง พัฒนาการบริหารจัดการป้องกันความเสียหายหรือความสูญหายของระบบเทคโนโลยีสารสนเทศตลอดจนการรักษาข้อมูลระบบเทคโนโลยีสารสนเทศและสนับสนุนการดำเนินกิจการขององค์กรได้อย่างมีประสิทธิภาพ ดังนี้

๑. นโยบายการรักษาความปลอดภัยของพื้นที่ (Physical Area Security)

๑ .๑ แบ่งเขตของพื้นที่เพื่อกำหนดความปลอดภัยของพื้นที่ดังต่อไปนี้

- พื้นที่ติดตั้ง PC Terminal
- พื้นที่สาหรับระบบเครือข่ายข้อมูลคอมพิวเตอร์
- พื้นที่ติดตั้งระบบและจัดเก็บข้อมูล (Data Center Area)

๑.๒ ต้องจัดให้มีกฎระเบียบปฏิบัติควบคุมการเข้าและการออกพื้นที่ติดตั้งระบบและจัดเก็บข้อมูล

๑.๓ การเข้าและออกพื้น ที่ปฏิบัติงาน ต้องแสดงสิทธิเข้าถึงพื้นที่ปฏิบัติงาน มีการบันทึก Log การเข้าปฏิบัติงาน สำหรับการตรวจสอบ สำหรับผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ให้ปฏิบัติตาม มาตรการรักษาความปลอดภัยของระบบ

๒. นโยบายการรักษาความปลอดภัยของระบบเครือข่าย (Network Security)

๒.๑ ระบบเครือข่ายภายใน (Local Area Network) อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายโดยติดตั้งใช้งานภายใน Local Area หรือเพื่อการทำงานภายในโรงพยาบาล ได้แก่ Router,Switching HUB กำหนดข้อปฏิบัติในการใช้งานดังนี้

๒.๑.๑ อุปกรณ์ Router, Switching HUB และอุปกรณ์อื่นๆ ที่ทำหน้าที่เป็นการขยายการเชื่อมโยงเครือข่ายต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password เป็นต้น

๒.๑.๒ การเชื่อมโยงเครือข่ายเพื่อใช้ระบบงานต่าง ๆ จะสามารถกระทำได้เมื่อได้รับอนุญาตจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ หรือผู้ดูแลเครือข่าย โดยความเห็นชอบของผู้อำนวยการโรงพยาบาล การเชื่อมโยงเครือข่ายเองโดยพลการหากทำให้เกิดความเสียหายกับระบบเครือข่ายจะได้รับการพิจารณาโทษ

๒.๑.๓ ต้องจัดให้มีแผนและดำเนินการบำรุงรักษาระบบเครือข่ายเพื่อให้อยู่ในสภาพที่พร้อมใช้งาน

๒.๑.๔ ต้องจัดให้มีระบบจ่ายไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถทำงานได้ต่อเนื่อง

๒.๑.๕ IP address ภายในของระบบงานเครือข่ายภายในขององค์กรจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของห้องคอมพิวเตอร์แม่ข่ายได้โดยง่าย

๒.๑.๖ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๒ ระบบ Remote Access อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS) กำหนดข้อปฏิบัติในการใช้งานดังนี้

๒.๒.๑ อุปกรณ์ RAS จะต้องทำ Harden และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

๒.๒.๒ เมื่อทำการทดสอบการใช้งานอุปกรณ์ RAS แล้ว User/Password ที่ใช้งานทดสอบเมื่อเสร็จงานแล้วให้ทำการลบทิ้งทันที

๒.๒.๓ อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่มีค่าDefault Community, Default Username และ Default Password

๓. นโยบายการรักษาความปลอดภัยของ Host (Host Security)

๓.๑ การรักษาความปลอดภัยของ Server

๓.๑.๑ ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password

๓.๑.๒ ต้อง Harden และบันทึกการ Configuration Set up ของอุปกรณ์ Server ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง

๓.๑.๓ กำหนดการใช้งาน Service Port ให้เปิด Service Port ที่จำเป็นเท่านั้น ส่วนที่ไม่ใช้งานให้ปิดทั้งหมดและต้องมีบันทึกการติดตั้ง Service Patch ทุกครั้ง

๓.๑.๔ ต้องไม่เปิดเผย OS Version, Service Port และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

๓.๑.๕ การ Login ใช้งานที่ Console นั้นเมื่อจบการทำงานแล้ว ต้อง Log off User นั้นโดยทันที

๓.๑.๖ ผู้ดูแลระบบจะต้องทำการสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยทุกเดือน และทดสอบ การสำรอง ข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบ

๓.๒ การรักษาความปลอดภัยของ PC Terminal

๓.๒.๑ เครื่อง PC Terminal ต้องตั้งชื่อเครื่องทุกเครื่องที่ติดต่อกับเครือข่าย

๓.๒.๒ กำหนดการใช้งาน Protocol บน เครื่อง PC Terminal ต้องใช้ติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น

๓.๒.๓ การเชื่อมโยง PC Terminal กับเครือข่ายจะต้องอยู่ภายใต้มาตรฐานการเชื่อมโยงเครือข่าย ที่ใช้งานร่วมกัน

๓.๒.๔ การใช้งาน Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

๓.๓ การรักษาความปลอดภัย Software

๓.๓.๑ เจ้าหน้าที่ต้องใช้คอมพิวเตอร์ซอฟต์แวร์ตามมาตรฐานที่โรงพยาบาลบ้านฉางกำหนด กรณีที่นำซอฟต์แวร์นอกเหนือจากมาตรฐานมาใช้ เจ้าหน้าที่ต้องรับผิดชอบในผลเสียที่เกิดขึ้นกับโรงพยาบาลบ้านฉาง

๓.๓.๒ เจ้าหน้าที่ไม่มีสิทธิ์ในการติดตั้งหรือรื้อถอนซอฟต์แวร์ที่ติดตั้งให้เป็นอันขาด หากกระทำโดย พลการและเกิดความเสียหายกับโรงพยาบาลบ้านฉางต้องได้รับโทษ

๔. นโยบายการรักษาความปลอดภัยของข้อมูล

๔.๑ การเข้าถึงข้อมูลต้องได้รับการอนุญาตจากเจ้าของข้อมูลเท่านั้น

๔.๒ ข้อมูลที่เป็นความลับต้องรักษาระดับความลับของข้อมูล ตรวจสอบระบบรักษาความลับของข้อมูลที่มีความสำคัญต่อการบริหารและการดำเนินการขององค์กร

๔.๓ ห้ามทำการสำเนาพิมพ์ข้อมูลที่เป็นความลับ ไม่ว่ากรณีใด เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้อำนวยการโรงพยาบาล เท่านั้น ข้อมูลที่เป็นความลับ หมายความว่า ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล ข้อมูลผู้รับบริการ

๔.๔ ต้องจัดให้มีแผนการสำรองข้อมูลเมื่อระบบถูกบุกรุกและแก้ไขข้อมูล

๔.๕ โรงพยาบาลบ้านฉาง มีสิทธิที่จะตรวจสอบข้อมูลโปรแกรม หรือ เอกสารอิเล็กทรอนิกส์อื่นๆ ที่เจ้าหน้าที่หรือผู้ปฏิบัติงานนำมาจัดเก็บไว้ในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อให้ สอดคล้องกับกฎหมาย ศีลธรรม และระเบียบปฏิบัติของโรงพยาบาลหรือเพื่อการดำเนินการทางวินัยและกฎหมาย

๕. นโยบายการใช้รหัสผ่าน (Password)

๕.๑ เจ้าหน้าที่ต้องใช้ Password ที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิที่ได้รับเท่านั้น

๕.๒ เจ้าหน้าที่ที่ได้รับ Password ในครั้งแรก ต้องเปลี่ยน Password ใหม่ให้เป็นความลับเฉพาะตัวและต้องทำการเปลี่ยน Password ใหม่ทันที หาก Password ถูกเปิดเผย

๕.๓ เจ้าหน้าที่ต้องเปลี่ยน Password ทุก ๆ ๓๐ วัน หรือตามระยะเวลาที่กำหนด และในการเปลี่ยนPassword ใหม่ในแต่ละครั้งจะต้องไม่นำ Password ที่หมดอายุแล้วมาใช้ซ้ำอีก

๕.๔ เจ้าหน้าที่ต้องทำการ Log out ออกจากระบบคอมพิวเตอร์ทันทีเมื่อเลิกใช้งาน หรือ เมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน ๑๐ นาที ให้ Screen Saver ควบคุมหน้าจอคอมพิวเตอร์ด้วย Password

๕.๕ หากเจ้าหน้าที่พบเหตุที่ก่อให้เกิดความสงสัยว่าถูกผู้อื่นนำ Password ไปใช้ให้แจ้งคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์

๖. นโยบายการใช้อินเตอร์เน็ต

๖.๑ เจ้าหน้าที่ต้องไม่ใช้อินเตอร์เน็ตในเครือข่ายของโรงพยาบาลบ้านฉาง เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่ Web Site ที่ไม่เหมาะสม เช่น Web Site ที่ขัดต่อศีลธรรมอันดี Web Site ที่มีเนื้อหาต่อต้านชาติ ศาสนา พระมหากษัตริย์หรือ Web Siteที่เป็นภัยต่อสังคม รวมถึงลามกอนาจาร เป็นต้น

๖.๒ เจ้าหน้าที่ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับโรงพยาบาลบ้านฉาง

๖.๓ เจ้าหน้าที่มีหน้าที่ต้องรายงานต่อคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ ทันที หากพบเห็นการใช้อินเตอร์เน็ตในเครือข่ายของโรงพยาบาลบ้านฉางไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิของโรงพยาบาลบ้านฉาง เช่น ส่งข้อมูลที่เป็นความลับให้บุคคลภายนอก เป็นต้น

๖.๔ การเชื่อมต่อ เครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเตอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลบ้านฉาง จัดสรรไว้เท่านั้น ห้ามเจ้าหน้าที่ทำการเชื่อมต่อ เข้าสู่เครือข่ายอินเตอร์เน็ตโดยตรงโดยผ่านช่องทางอื่น เช่น Dial up Modem เว้นแต่ว่าจะได้รับอนุญาตเป็นกรณีพิเศษ

๖.๕ ให้ใช้เฉพาะเครื่อง PC Terminal ที่กำหนดให้ใช้อินเตอร์เน็ตเท่านั้น ห้ามใช้เครื่องส่วนบุคคลเข้าสู่ระบบงานเข้าอินเตอร์เน็ตของโรงพยาบาลบ้านฉาง เป็นอันขาด

๖.๖ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีขออนุญาตจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ก่อน และ ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ทุกครั้ง

๗. นโยบายการรับ – ส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) (*หมายเหตุ เจ้าหน้าที่ = User)

๗.๑ เจ้าหน้าที่ควรระมัดระวังในการใช้ E-Mail เพื่อไม่ให้เกิดความเสียหาย หรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น หรือ ผิด กฎหมาย หรือ ละเมิด ศีลธรรม และไม่แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้ E-Mail ในระบบของโรงพยาบาลบ้านฉาง

๗.๒ เจ้าหน้าที่ต้องรับผิดชอบในข้อความ รูปภาพ เสียง หรือ แฟ้มข้อมูลที่ส่งออกจากเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ทั้งหมด

๗.๔ ก่อนที่จะ Download ไฟล์จาก E-Mail ต้องทำการ Scan Virus ก่อนทุกครั้ง

๘. นโยบายการป้องกันไวรัสคอมพิวเตอร์

๘.๑ ห้ามเจ้าหน้าที่นำคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ หรือข้อมูลที่ไม่มั่นใจว่าติดไวรัสคอมพิวเตอร์ มาติดตั้งหรือใช้งานในโรงพยาบาลบ้านฉาง เว้นแต่คอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์นั้นได้ผ่านการตรวจสอบจากคณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ โรงพยาบาลบ้านฉาง แล้วเท่านั้น

๘.๒ เจ้าหน้าที่ควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ประจำหน่วยงานไว้ เช่น CD-RWหรือ Flash Drive เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

๘.๓ ห้ามเจ้าหน้าที่ปรับแต่ง หรือยกเลิกการทำงานของคอมพิวเตอร์ซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่โรงพยาบาลบ้านฉาง จัดหาให้

๘.๔ เจ้าหน้าที่ควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการUpdate ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่าง สม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๘.๕ เจ้าหน้าที่ควรแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟท์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อมีสงสัยว่ามีการติดไวรัสคอมพิวเตอร์

๙. นโยบายการปฏิบัติตามข้อกำหนด (Compliance)

๙.๑ โรงพยาบาลบ้านฉาง ต้องเก็บ Log file การเข้าสู่ระบบคอมพิวเตอร์ของเจ้าหน้าที่ ไว้ไม่ต่ำกว่า ๙๐ วัน

๙.๒ ห้ามตัดต่อภาพ ปรับเปลี่ยน แก้ไขข้อมูล บางส่วน หรือทั้งหมด ก่อนได้รับอนุญาตจากเจ้าของข้อมูล หรือ กระทำกับข้อมูลอันเป็นการสร้างความเสียหายแก่ผู้อื่น โดยเด็ดขาด และคำสั่งนี้โรงพยาบาลบ้านฉางได้แต่งตั้งบุคคลต่อไปนี้ ประกอบด้วย

๒. คณะทำงานสารสนเทศทางการแพทย์และคอมพิวเตอร์โรงพยาบาลบ้านฉาง

๑. นายธเนษฐ์ กมลอดิศัย	ตำแหน่งทันตแพทย์ชำนาญการ	ประธานกรรมการ
๒. นางสมลักษณ์ ทองสุข	ตำแหน่งพยาบาลวิชาชีพชำนาญการพิเศษ	รองประธานกรรมการ
๓. นางปาริชาติ จันทะเกิด	ตำแหน่งพยาบาลวิชาชีพชำนาญการ	กรรมการ
๔. นางสาวจารุภา ตั้งก่อพันธุ์	ตำแหน่งเภสัชกรชำนาญการ	กรรมการ
๕. นายศิวกร เสือคำรณ	ตำแหน่งนักเทคนิคการแพทย์ปฏิบัติการ	กรรมการ
๖. นางสาววารีย์ ศรีบุษย์	ตำแหน่งพยาบาลวิชาชีพชำนาญการ	กรรมการและเลขานุการ

ให้คณะทำงานมีอำนาจและหน้าที่ดังนี้

๑. ให้คำปรึกษาเชิงนโยบายและแนวทางการดำเนินการด้านการพัฒนาระบบสารสนเทศ ความมั่นคงปลอดภัยของระบบสารสนเทศของโรงพยาบาล ตลอดจน แนวทางแก้ไขปัญหาและอุปสรรคที่เกิดขึ้นจากการปฏิบัติงาน

๒. พิจารณาให้ความเห็นต่อแผนปฏิบัติงานสารสนเทศ และติดตามการดำเนินการด้านการพัฒนาระบบสารสนเทศตามแผนปฏิบัติที่กำหนดไว้

๓. ให้ข้อเสนอแนะอื่นๆ ที่เกี่ยวกับการบริหารระบบสารสนเทศของโรงพยาบาล

๔. กำกับ ดูแล และติดตามการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

๒. คณะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยี สารสนเทศ และคอมพิวเตอร์ โรงพยาบาลบ้านฉาง

๑. นายอภิชาต อรรคบุตร	ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ประธานคณะทำงาน
๒. นายยุทธนา เวชเวโรจน์	ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๓. นายพงศกร ต่อพล	ตำแหน่ง นักวิชาการคอมพิวเตอร์	คณะทำงาน
๔. น.ส.ธัศม์มสา อธิวัฒน์ธนะภัค	ตำแหน่ง พนักงานธุรการงานโสต	คณะทำงาน
๕. น.ส.จิรภัทร สาขามุละ	ตำแหน่ง โสตทัศศึกษา	เลขานุการ

ให้คณะเจ้าหน้าที่ผู้ดูแลระบบมีอำนาจและหน้าที่ดังนี้

๑. วางแนวทางพัฒนาระบบเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยของระบบสารสนเทศตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยี สารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านฉาง

๒. ดูแลระบบคอมพิวเตอร์ของโรงพยาบาล ทั้งด้าน Hardware, Software และ Network ให้มีความพร้อมใช้งาน ตลอดเวลา

๓. มีภารกิจด้านการดูแลระบบการบันทึกข้อมูลการให้บริการผู้ป่วยผ่านระบบ Hospital Information System ให้มีคุณภาพ

๗. ดูแลการสื่อสารในรูปแบบอิเล็คทรอนิกส์ไฟล์ผ่านเครือข่ายภายในระบบคอมพิวเตอร์ของโรงพยาบาลให้มีความพร้อมใช้งาน ตลอดเวลา

๘. ดูแลและรักษาความปลอดภัยของระบบเครือข่ายให้สามารถรองรับการใช้งานได้ตลอดเวลา โดยจัดให้มีเจ้าหน้าที่รับผิดชอบทั้งในและนอกเวลาราชการ

๙. ดูแล และรักษาการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ของ โรงพยาบาลบ้านฉาง โดยเคร่งครัด

๗. งานอื่นๆ ที่เกี่ยวกับการบริหารระบบสารสนเทศของโรงพยาบาล และที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗

๑๗

(นายสุรชัย คำภักดี)
ผู้อำนวยการโรงพยาบาลบ้านฉาง
Sign: 39962B3EB75DACEC6489B08A7356815B
RefNo: 25670304161149844

ร่าง/ตรวจ.....

พิมพ์/ทาน.....