ประกาศโรงพยาบาลวังเจ้า

เรื่อง นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลวังเจ้า เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลวังเจ้า และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ ดังนั้น จึงขอประกาศนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดังรายละเอียดต่อไปนี้

หมวดที่ ๑ คำนิยาม

"โรงพยาบาล" หมายถึง โรงพยาบาลวังเจ้า

"ผู้บริหาร" หมายถึง ผู้อำนวยการหรือผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลวังเจ้า

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

"ผู้ใช้งาน" หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข และลูกจ้างชั่วคราวของโรงพยาบาลวังเจ้า

"ระบบเทคโนโลยีสารสนเทศ" หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้โยชน์ ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศ เป็นต้น

"เครื่องเซิร์ฟเวอร์ (Server)" หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการ หรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย

หมวดที่ ๒ นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. โรงพยาบาลจะดำเนินการจัดการเพื่อคุ้มครองข้อมูลส่วนบุคคลอันเป็นความลับและเป็นข้อมูลส่วนตัวของผู้ป่วยอย่างเคร่งครัด

๒. การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ต้องเป็นไปเพื่อดำเนินกิจกรรมตามพันธกิจเพื่อให้บรรลุวิสัยทัศน์ของโรงพยาบาล

หมวดที่ ๓ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นพื้นที่ควบคุม โดยกำหนดเฉพาะผู้ใช้งานที่ดีรับอนุญาตให้เข้าปฏิบัติงานในพื้นที่ควบคุม

๒. ห้ามผู้ใช้งานทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายออกนอกหน่วยงาน หากจำเป็นให้ประสานกับงานเทคโนโลยีสารสนเทศ

หมวดที่ ๔ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. ผู้ดูแลระบบต้องเป็นผู้กำหนดสิทธิ์ในการเข้าถึงระบบข้อมูลต่างๆ ให้เหมาะสมกับการใช้งานของผู้ใช้งานโดยทำการลงทะเบียนการใช้งาน (User Authentication) และทำการเก็บประวัติการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์

๒. ผู้ดูแลระบบ เป็นผู้ทำหน้าที่บริหารจัดการตรวจสอบเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เครือข่ายทั้งภายในและภายนอก โดยมีการแสดงตัวตน (User Authentication) ของผู้ใช้งาน

๓. ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน และรหัสผ่าน (Password) ไว้เป็นความลับ ห้ามปิดประกาศไว้ในที่เปิดเผยให้ผู้อื่นใช้งานแทนและต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน

หมวดที่ ๕ นโยบายด้านความปลอดภัยและระบบคอมพิวเตอร์เครือข่ายและเครือข่ายไร้สาย

๑ ผู้ดูแลระบบต้องทำการควบคุมตรวจสอบ และจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ตามแนวทางปฏิบัติ เพื่อให้เกิดความปลอดภัย และสามารถระบุถึงตัวบุคคลได้

๒ ผู้ดูแลระบบเป็นผู้ติดตั้งและวาง Access point ในตำแหน่งที่เหมาะสมและกำหนดรหัสผ่านและสิทธิผู้ใช้งาน ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองโดยไม่ได้รับอนุญาต

หมวดที่ ๖ นโยบายการใช้เครื่องคอมพิวเตอร์และคอมพิวเตอร์พกพา

๑ กำหนดให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดเป็นสมบัติของโรงพยาบาลและมอบให้ผู้ใช้งานสามารถใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายได้ตามหน้าที่รับผิดชอบที่ และห้ามผู้ใช้งาน ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๒ ห้ามผู้ใช้งานหรือบุคคลภายนอก นำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายด้านคอมพิวเตอร์ทุกชนิดมาเชื่อมต่อระบบเครือข่ายของโรงพยาบาลวังเจ้า ยกเว้นทำบันทึกและได้รับอนุญาตคณะกรรมการเทคโนโลยีสารสนเทศเท่านั้น

๓ กำหนดให้ใช้ Username และ Password ก่อนใช้งานโปรแกรม HIS รวมทั้ง Log out ออกทุกครั้งเมื่อไม่ใช้งาน โดยระบบจะ Log out อัตโนมัติใน ๑๐ นาที

๔ กำหนดให้ผู้ใช้งานต้องทำการ Scan Virus ในอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy drive) ทุกครั้งก่อนใช้งานเชื่อมกับอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลวังเจ้า

หมวดที่ ๗ นโยบายการใช้งานอินเตอร์เน็ตและจดหมายอิเลคทรอนิกส์

๑. ผู้ใช้งานต้องรับผิดชอบบัญชีผู้ใช้งาน (User Account) ของตนเองจะโอน จำหน่าย หรือจ่ายแลกสิทธิให้กับผู้อื่นไม่ได้ หากผู้อื่นได้ใช้บัญชีผู้ใช้งานของตน ผู้ใช้งานจึงต้องเป็นผู้รับผิดชอบผลต่างๆที่อาจเกิดขึ้น

๒. ผู้ดูแลระบบจะต้องทำระบบรักษาความปลอดภัยของข้อมูล และสามารถเก็บประวัติการใช้งานของผู้ใช้งานเพื่อตรวจสอบและป้องกันภัยคุกคาม

๓. กรณีบุคคลภายนอก เช่น วิทยากร ผู้เข้าร่วมประชุม จำเป็นต้องใช้อินเตอร์เน็ตต้องให้หน่วยงานผู้รับผิดชอบติดต่อผู้ดูแลระบบเพื่อดำเนินการกำหนดบัญชีผู้ใช้งานและรหัสผ่านทุกครั้ง

หมวดที่ ๘ นโยบายในการรักษาความลับของผู้ป่วย

๑. ผู้ใช้งานทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูลในระบบคอมพิวเตอร์และเอกสารเวชระเบียนของผู้ป่วย

๒. ผู้ใช้งานห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากคณะกรรมการเทคโนโลยีสารสนเทศ

๓. การส่งข้อมูลผู้ป่วยผ่านช่องทาง Social Media ต้องปฏิบัติตามระเบียบปฏิบัติด้านการส่งข้อมูลผู้ป่วยผ่าน Social Media

๔. ห้ามมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใด เข้าถึงข้อมูลผู้ป่วยรายนั้น

หมวดที่ ๙ นโยบายด้านการส่งข้อมูลผู้ป่วยSocial media

๑. ผู้ใช้งานต้องหลีกเลี่ยงการระบุ ชื่อ, สกุล, HN, เลข ๑๓ หลัก, ใบหน้า หรือข้อมูลที่ระบุตัวตนผู้ป่วยได้

๒. ผู้ใช้งานต้องหลีกเลี่ยงการส่งข้อมูลผู้ป่วยผ่าน Social Media แบบกลุ่ม

๓. เมื่อส่งข้อมูลผ่าน Social Media แล้ว หากใช้ข้อมูลนั้นแล้ว ให้ทำการลบออกจาก Social Media ที่ทำการส่งทันที

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๗ พฤษภาคม ๒๕๖๔

(นายพิจารณ์ สารเสวก)

ผู้อำนวยการโรงพยาบาลวังเจ้า

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

โรงพยาบาลวังเจ้า

Don't 1 — การใช้งาน โปรแกรมโรงพยาบาล

- ห้ามบุคคลภายนอกหรือผู้ไม่เกี่ยวข้อง ใช้งานระบบคอมพิวเตอร์ของโรงพยาบาล และผู้ใช้งานทำการ Log out ออกทุกครั้งเมื่อไม่ใช้งาน (Log out อัตโนมัติภายใน 10 นาที)

Don't 2 — เครือข่ายและการใช้งาน

- ห้ามผู้ใช้งานเคลื่อนย้ายคอมพิวเตอร์ และอุปกรณ์เครือข่ายออกนอกหน่วยงาน หากจำเป็นให้ประสานงานศูนย์คอมพิวเตอร์

Don't 3 — การรักษาความปลอดภัยของข้อมูล

- ห้ามผู้ใช้งาน ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

Don't 4 — การป้องกันผู้ไม่มีสิทธิใช้งาน

- ห้ามมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใดเข้าถึงข้อมูลผู้ป่วยรายนั้น

Don't 5 — การเชื่อมต่ออุปกรณ์

- ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล ก่อนได้รับอนุญาต

Don't 6 — การรักษาความลับของผู้ป่วย

- ห้ามผู้ใช้งาน ส่งข้อมูลผู้ป่วยผ่านสื่อ Social Media ต่างๆ หากมีความจำเป็นต้องได้รับการยินยอมจากผู้ป่วยหรือญาติเป็นลายลักษณ์อักษร

Do 7 — การป้องกันไวรัส

- ผู้ใช้งานต้องทำการ Scan ไวรัสจากอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy Drive) ทุกครั้งก่อนใช้งาน

Do 8 — การเก็บรักษา User & Password

- ผู้ใช้งานต้องเก็บรักษา User & Password ไว้เป็นความลับและต้องเปลี่ยนทุก 3 เดือน

(แนะนำใช้ Password มีตัวเลขสลับตัวอักษร 6 ตัวขึ้นไป)