บันทึกข้อความ

ส่วนราชการ โรงพยาบาลยี่งอเฉลิมพระเกียรติ ๘๐ พรรษา อำเภอยี่งอ จังหวัดนราธิวาส

ที่ นธ. ๐๐๓๒.๓๐๑/๓๕๒ **วันที่** ๒๙ ธันวาคม ๒๕๖๔

เรื่อง ขออนุมัติและประกาศใช้นโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เรียน ผู้อำนวยการโรงพยาบาลยี่งอเฉลิมพระเกียรติ ๘๐ พรรษา

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องเหมาะสม

ดังนั้น โรงพยาบาลยี่งอเฉลิมพระเกียรติ ๘๐ พรรษา ได้ดำเนินการจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้การใช้งานระบบสารสนเทศของโรงพยาบาลมีความปลอดภัย และสอดคล้องตามหลักกฎหมายจึงควรประกาศใช้นโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ควบคุมการดำเนินการใดๆ ที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลยี่งอเฉลิมพระเกียรติ ๘๐ พรรษา

(นายณัฐพงศ์ อินทองคำ)
นักวิชาการสาธารณสุขชำนาญการ

(นายอดุลย์ เร็งมา)
ผู้อำนวยการโรงพยาบาลยี่งอเฉลิมพระเกียรติ ๘๐ พรรษา

ประกาศโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

เรื่อง นโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา เป็นไปอย่างเหมาะสม มีประสิทธิภาพปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดจากการใช้อย่างไม่ถูกต้อง ซึ่งอาจก่อให้เกิดความเสียหายและเป็นความผิดตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.๒๕๕๐ และกฎหมายอื่นๆ ที่เกี่ยวข้อง ดังนั้น จึงขอประกาศนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้บุคลากรถือปฏิบัติอย่างเคร่งครัด ดังรายละเอียดต่อไปนี้

หมวดที่ ๑ คำนิยาม

โรงพยาบาล หมายถึง โรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

ส่วนราชการ หมายถึง กระทรวงสาธารณสุข

ผู้บังคับบัญชา หมายถึง ผู้อำนวยการหรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

หน่วยงาน หมายถึง หน่วยงานต่างๆ ที่อยู่ในเครือข่ายของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

ศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์ หมายถึง หน่วยงานที่ทำหน้าที่ให้บริการและพัฒนาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

หัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์ หมายถึง หัวหน้าที่ทำหน้าที่ดูแล บริหารจัดการศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์ ของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

ผู้ดูแลระบบ (System Administrator) หมายถึง บุคลากรที่ได้รับมอบหมายจาก หัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์ ให้มีหน้าที่รับผิดชอบในการดูแลและเข้าถึงระบบคอมพิวเตอร์เครือข่ายของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

เครื่องคอมพิวเตอร์เครือข่าย หมายถึง ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาล ทั้งที่อยู่ภายในโรงพยาบาล และเครือข่ายโรงพยาบาลยิ่งอเฉลิมพรเกียรติ ๘๐ พรรษา รวมทั้งอุปกรณ์ต่อพ่วงต่างๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่างๆ ตลอดจนโปรแกรมและข้อมูลต่างๆ ที่มิได้จัดให้เป็นสื่อสาธารณะ

ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างเหมาบริการของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา หรือผู้ที่โรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา อนุญาตให้ใช้เครื่องคอมพิวเตอร์ และเครือข่ายได้

นโยบายด้านความมั่นคงปลอดภัย คือ แนวทางที่ผู้บริหารระดับสูงกำหนดที่ให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตามเพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย

บทลงโทษ หมายถึง บทลงโทษที่ส่วนราชการเป็นผู้กำหนด หรือบทลงโทษตามกฎหมาย

หมวดที่ ๒ นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. โรงพยาบาลจะดำเนินการจัดการเพื่อคุ้มครองข้อมูลส่วนบุคคลอันเป็นความลับและเป็นข้อมูลส่วนตัวของผู้ป่วยอย่างเคร่งครัด

๒. การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ต้องเป็นไปเพื่อดำเนินกิจกรรมตามพันธกิจเพื่อให้บรรลุวิสัยทัศน์ของโรงพยาบาล

หมวดที่ ๓ ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยทางการด้านกายภาพและสิ่งแวดล้อม

๑. กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นพื้นที่ควบคุม โดยกำหนดเฉพาะผู้ที่ใช้งานที่ได้รับอนุญาตให้เข้าปฏิบัติงานในพื้นที่ควบคุม

๒. ผู้ดูแลระบบเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ห้ามบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าใช้งาน หากมีหน่วยงานภายนอกต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายมาใช้งานในพื้นที่ควบคุมจะต้องลงบันทึกขออนุญาตใช้งานจากหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์

๓. ห้ามผู้ใช้งานทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หากจำเป็นให้ประสานศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์

หมวดที่ ๔ ระเบียบปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. ผู้ดูแลระบบต้องเป็นผู้กำหนดสิทธิในการเข้าถึงระบบข้อมูลต่างๆ ให้เหมาะสมกับการใช้งานของผู้ใช้งานโดยกำหนดลงทะเบียนการใช้งานและทำการเก็บประวัติการเข้าถึงข้อมูลและข้อมูลจราจรทางคอมพิวเตอร์

๒. ผู้ดูแลระบบ เป็นผู้ทำหน้าที่บริหารจัดการและทำการตรวจสอบเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เครือข่ายทั้งภายในและภายนอก โดยมีการแสดงตัวตน (User Authentication) ของผู้ใช้งาน

๓. ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (User Authentication) และรหัสผ่าน (Password) ไว้เป็นความลับ ห้ามปิดประกาศไว้ในที่เปิดเผยหรือมอบให้ผู้อื่นใช้งานแทนและต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน

หมวดที่ ๕ ระเบียบปฏิบัติด้านความปลอดภัยและระบบคอมพิวเตอร์เครือข่ายและเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องทำการควบคุมตรวจสอบ และจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ตามแนวทางปฏิบัติ เพื่อให้เกิดความปลอดภัย และสามารถระบุถึงตัวบุคคลได้

๒. หากมีบุคคลภายนอกต้องการสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์เครือข่าย จะต้องทำบันทึกเพื่อขออนุญาตเข้าใช้จากหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์

๓. ผู้ดูแลระบบ เป็นผู้ติดตั้งและวาง Access point ในตำแหน่งที่เหมาะสมและกำหนดรหัสผ่านและสิทธิผู้ใช้งาน ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองโดยไม่ได้รับอนุญาต

หมวดที่ ๖ ระเบียบปฏิบัติใช้เครื่องคอมพิวเตอร์และคอมพิวเตอร์พกพา

๑. กำหนดให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดเป็นสมบัติของโรงพยาบาลและมอบให้ผู้ใช้งานสามารถใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายได้ตามหน้าที่รับผิดชอบที่กำหนดจากผู้ดูแลระบบ และห้ามผู้ใช้งานติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๒. ห้ามผู้ใช้งานหรือบุคคลภายนอก นำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายด้านคอมพิวเตอร์ทุกชนิดมาเชื่อมต่อระบบเครือข่ายของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา ยกเว้นทำบันทึกและได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์

๓. กำหนดให้ผู้ใช้งาน ต้องทำการ Scan Virus ในอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy drive) ทุกครั้งก่อนใช้งานเชื่อมต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา

หมวดที่ ๗ ระเบียบปฏิบัติการใช้อินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑. ผู้ใช้งานต้องทำการลงทะเบียน บัญชีผู้ใช้งานเครือข่ายอินเตอร์เน็ต ที่ศูนย์คอมพิวเตอร์และสารสนเทศทางการแพทย์ และก่อนใช้งานต้องใส่ Username และ Password เพื่อยืนยันตัวตน (Authentication) ทุกครั้ง

๒. ผู้ใช้งานต้องรับผิดชอบบัญชีผู้ใช้งาน (User Account) ของตนเอง จะโอน จำหน่าย หรือ จ่ายแลกสิทธิ์ให้กับผู้อื่นไม่ได้ หากผู้อื่นได้ใช้บัญชีใช้งานของตน ผู้ใช้งานจึงต้องเป็นผู้รับผิดชอบผลต่างๆที่อาจจะเกิดขึ้น

๓. ผู้ดูแลระบบจะต้องทำระบบรักษาความปลอดภัยของข้อมูล และสามารถเก็บประวัติการใช้งานของผู้ใช้งานเพื่อตรวจสอบและป้องกันภัยคุกภาม

๔. กรณีบุคคลภายนอก เช่น วิทยากร ผู้เข้าร่วมประชุม จำเป็นต้องใช้อินเตอร์เน็ตต้องให้หน่วยงานผู้รับผิดชอบติดต่อผู้ดูแลระบบเพื่อดำเนินการกำหนดบัญชีผู้ใช้งานและรหัสผ่านทุกครั้ง

หมวดที่ ๘ ระเบียบปฏิบัติในการรักษาความลับของผู้ป่วย

๑. ผู้ใช้งานทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูลในระบบคอมพิวเตอร์และเอกสารเวชระเบียนของผู้ป่วย

๒. ผู้ใช้งานห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ

๓. การส่งข้อมูลผู้ป่วยผ่านช่องทาง Social Media ต้องปฏิบัติตามระเบียบปฏิบัติด้านการส่งข้อมูลผู้ป่วยผ่าน Social Media

๔. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเตอร์เน็ตทุกรณี ยกเว้นเครื่องคอมพิวเตอร์มีภารกิจเฉพาะที่ต้องเชื่อมต่อระบบข้อมูลผู้ป่วยซึ่งได้รับอนุญาตจากผู้อำนวยการ

๕. ห้ามมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใด เข้าถึงข้อมูลผู้ป่วยรายนั้น

หมวดที่ ๙ ระเบียบปฏิบัติด้านการส่งข้อมูลผู้ป่วย Social Media

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

๒. ผู้ใช้งานต้องหลีกเลี่ยงการส่งข้อมูลผู้ป่วยผ่าน Social Media แบบกลุ่ม

๓. เมื่อส่งข้อมูลผ่าน Social Media แล้ว หากใช้ข้อมูลนั้นแล้ว ให้ทำการลบออกจาก Social Media ที่ทำการส่งทันที

ประกาศ ณ วันที่ ๒๕ ธันวาคม ๒๕๖๔

(นายอดุลย์ เร็งมา)
ผู้อำนวยการโรงพยาบาลยิ่งอเฉลิมพระเกียรติ ๘๐ พรรษา