บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ โรงพยาบาลมหาสารคาม โทร ๙๒๗๐ ,๙๒๗๑

ที่ มค ๐๐๓๒.๒๐๒/๔๕ **วันที่** ๑๐ กันยายน ๒๕๖๓

เรื่อง ขอความร่วมมือบุคลากรให้ปฏิบัติตามแนวทางด้านความปลอดภัยของระบบไอที

เรียน หัวหน้ากลุ่มงาน/หัวหน้างาน/หัวหน้าหอผู้ป่วยทุกท่าน

จากสถานการณ์ระบบคอมพิวเตอร์ของโรงพยาบาลสระบุรีขัดข้องทั้งระบบ เนื่องจากระบบถูก Ransomware (มัลแวร์เรียกค่าไถ่) ทำให้ไม่สามารถใช้ระบบคอมพิวเตอร์ในการให้บริการได้ ส่งผลให้การบริการล่าช้า ดังนั้นศูนย์เทคโนโลยีสารสนเทศทางการแพทย์จึงได้ทบทวนระบบไอทีของโรงพยาบาลมหาสารคาม เพื่อวิเคราะห์หาแนวทางการป้องกันโดยแนวทางการป้องกันจะแบ่งเป็น ๒ ส่วน คือ

๑. ระบบคอมพิวเตอร์เครือข่ายกลางและระบบ Back up ผู้รับผิดชอบ คือ ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

๒. เครื่องคอมพิวเตอร์ทั่วไป (Client) ผู้รับผิดชอบ คือ ผู้ใช้งานทุกท่าน โดยต้องขอความร่วมมือจากผู้ใช้งานทุกท่านให้ปฏิบัติ ดังนี้

๒.๑ การใช้ Internet ห้ามโหลดไฟล์จาก Mail, Application หรือโปรแกรมที่ผิดปกติ ไม่รู้จักหรือไม่ปลอดภัยโดยเด็ดขาด

๒.๒ ห้ามผู้ใช้งานโหลดโปรแกรม Application นอกเหนือจากที่ศูนย์เทคโนโลยีสารสนเทศทางการแพทย์จัดไว้ให้ หากจำเป็นต้องใช้งานกรุณาแจ้งบุคลากรของศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ ช่วยดำเนินการให้ทุกครั้ง

๒.๓ ห้ามใช้ Handy drive Copy file หรือโหลดไฟล์มาลงในเครื่องที่ใช้ระบบคอมพิวเตอร์หรือ HIS ของโรงพยาบาลโดยเด็ดขาด หากจำเป็นต้องใช้จะต้อง Scan virus จากโปรแกรม Antivirus ทุกครั้ง หากพบข้อความแจ้งเตือน ห้ามกด Allow กรุณาติดต่อศูนย์เทคโนโลยีสารสนเทศทางการแพทย์ โทร. ๙๒๗๐, ๙๒๗๑ ทันที

๒.๔ ขอให้ทุกท่านที่ใช้ระบบคอมพิวเตอร์ ปฏิบัติตามนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ตามเอกสารที่แนบมาพร้อมหนังสือนี้) อย่างเคร่งครัด

จึงเรียนมาเพื่อทราบและชี้แจงให้บุคลากรในหน่วยงานของท่านทราบด้วย

๙ —

(นายภาคภูมิ มโนสิทธิศักดิ์)
ผู้อำนวยการโรงพยาบาลมหาสารคาม

ประกาศโรงพยาบาลมหาสารคาม

เรื่อง นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลมหาสารคามเป็นไปอย่างเหมาะสม มีประสิทธิภาพปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดจากการใช้อย่างไม่ถูกต้อง ซึ่งอาจก่อให้เกิดความเสียหายและเป็นความผิดตามพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นๆที่เกี่ยวข้อง ดังนั้น จึงขอประกาศนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้บุคลากรถือปฏิบัติอย่างเคร่งครัด ดังรายละเอียดต่อไปนี้

หมวดที่ ๑ คำนิยาม

โรงพยาบาล หมายถึง โรงพยาบาลมหาสารคาม

ส่วนราชการ หมายถึง กระทรวงสาธารณสุข

ผู้บังคับบัญชา หมายถึง ผู้อำนวยการหรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลมหาสารคาม

ผู้บริหารระบบเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายถึง ผู้บริหารระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม โดยมีบทบาทหน้าที่ในการกำหนดนโยบายและแนวทางปฏิบัติการใช้งานระบบเทคโนโลยีสนเทศ

หน่วยงาน หมายถึง หน่วยงานต่างๆที่อยู่ในเครือข่ายของโรงพยาบาลมหาสารคาม

ศูนย์เทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ทำหน้าที่ให้บริการและพัฒนาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม

หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หมายถึง หัวหน้าที่ทำหน้าที่ดูแล บริหาร จัดการศูนย์เทคโนโลยีสารสนเทศของโรงพยาบาลมหาสารคาม

ผู้ดูแลระบบ (System Administrator) หมายถึง บุคลากรที่ได้รับมอบหมายจาก CIO หรือหัวหน้าศูนย์เทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบในการดูแลและเข้าถึงระบบคอมพิวเตอร์เครือข่ายของโรงพยาบาลมหาสารคาม

เครื่องคอมพิวเตอร์เครือข่าย หมายถึง ระบบเครือข่ายและเครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาล ทั้งที่อยู่ภายในโรงพยาบาล และเครือข่ายโรงพยาบาลมหาสารคาม รวมทั้งอุปกรณ์ต่อพ่วงต่างๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่างๆ ตลอดจนโปรแกรมและข้อมูลต่างๆที่มิได้จัดให้เป็นสื่อสาธารณะ

ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานกระทรวงสาธารณสุข ลูกจ้างชั่วคราวของโรงพยาบาลมหาสารคาม หรือผู้ที่โรงพยาบาลมหาสารคามอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และเครือข่ายได้

บทลงโทษ หมายถึง บทลงโทษที่ส่วนราชการเป็นผู้กำหนด หรือบทลงโทษตามกฎหมาย

หมวดที่ ๒ นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นพื้นที่ควบคุม โดยกำหนดเฉพาะผู้ที่ใช้งานที่ได้รับอนุญาตให้เข้าปฏิบัติให้เข้าปฏิบัติงานในพื้นที่ควบคุม

๒. ผู้ดูแลระบบเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ห้ามบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าใช้งาน หากมีหน่วยงานภายนอกต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายมาใช้งานในพื้นที่ควบคุมจะต้องลงบันทึกขออนุญาตใช้งานจาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ

๓. ห้ามผู้ใช้งานทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หากจำเป็นให้ประสานศูนย์เทคโนโลยีสารสนเทศ

หมวดที่ ๓ นโยบายและแนวทางปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. ผู้ดูแลระบบต้องเป็นผู้กำหนดสิทธิในการเข้าถึงระบบข้อมูลต่างๆให้เหมาะสมกับการใช้งานของผู้ใช้งานโดยทำการลงทะเบียนการใช้งานและทำการเก็บประวัติการเข้าถึงข้อมูลและข้อมูลจราจรทางคอมพิวเตอร์

๒. ผู้ดูแลระบบ เป็นผู้ทำหน้าที่บริหารจัดการและทำการตรวจสอบเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เครือข่ายทั้งภายในและภายนอก โดยมีการแสดงตัวตน (User Authentication) ของผู้ใช้งาน

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

หมวดที่ ๔ นโยบายและแนวทางปฏิบัติด้านความปลอดภัยและระบบคอมพิวเตอร์เครือข่ายและเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องทำการควบคุมตรวจสอบ และจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ตามแนวทางปฏิบัติ เพื่อให้เกิดความปลอดภัย และสามารถระบุถึงตัวบุคคลได้

๒. หากมีบุคคลภายนอกต้องการสิทธิในการเข้าถึงระบบคอมพิวเตอร์เครือข่าย จะต้องทำบันทึกเพื่อขออนุญาตเข้าใช้จาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์

๓. ผู้ดูแลระบบ เป็นผู้ติดตั้งและวาง Access point ในตำแหน่งที่เหมาะสมและกำหนดรหัสผ่านและสิทธิผู้ใช้งาน ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองโดยไม่ได้รับอนุญาต

หมวดที่ ๕ นโยบายและแนวทางปฏิบัติใช้เครื่องคอมพิวเตอร์และคอมพิวเตอร์พกพา

๑. กำหนดให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดเป็นสมบัติของโรงพยาบาลและมอบให้ผู้ใช้งานสามารถใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายได้ตามหน้าที่รับผิดชอบที่กำหนดจากผู้ดูแลระบบ และห้ามผู้ใช้งานติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๒. ห้ามผู้ใช้งานหรือบุคคลภายนอก นำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายด้านคอมพิวเตอร์ทุกชนิดมาเชื่อมต่อระบบเครือข่ายของโรงพยาบาลมหาสารคาม ยกเว้นทำบันทึกและได้รับอนุญาตจาก CIO หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทางการแพทย์เท่านั้น

๓. กำหนดให้ผู้ใช้งาน ต้องทำการ Scan Virus ในอุปกรณ์เก็บข้อมูลแบบเคลื่อนที่ (Handy drive) ทุกครั้งก่อนใช้งานเชื่อมต่อกับอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลมหาสารคาม

หมวดที่ ๖ นโยบายและแนวทางปฏิบัติการใช้อินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

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

๒. ผู้ใช้งานต้องรับผิดชอบบัญชีผู้ใช้งาน (User Account) ของตนเอง จะโอน จำหน่าย หรือจ่ายแลกสิทธิให้กับผู้อื่นไม่ได้ หากผู้อื่นได้ใช้บัญชีผู้ใช้งานของตน ผู้ใช้งานจึงต้องเป็นผู้รับผิดชอบผลต่างๆที่อาจจะเกิดขึ้น

๓. ผู้ดูแลระบบจะต้องทำระบบรักษาความปลอดภัย และสามารถเก็บประวัติการใช้งานของผู้ใช้งานเพื่อตรวจสอบและป้องกันภัยคุกคาม

๔. กรณีบุคคลภายนอก เช่น วิทยากร ผู้เข้าร่วมประชุม จำเป็นต้องใช้อินเตอร์เน็ตต้องให้หน่วยงานผู้รับผิดชอบติดต่อผู้ดูแลระบบเพื่อดำเนินการกำหนดบัญชีผู้ใช้งานและรหัสผ่านทุกครั้ง

หมวดที่ ๗ นโยบายและแนวทางปฏิบัติในการรักษาความลับของผู้ป่วย

๑. ผู้ใช้งานทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูลในระบบคอมพิวเตอร์และเอกสารเวชระเบียนของผู้ป่วย

๒. ผู้ใช้งานห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ หรือ CIO

๓. ผู้ใช้งานห้ามส่งข้อมูลผู้ป่วยโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ส่งทาง LINE หรือ Social Media หากจำเป็นต้องส่งควรใช้ช่องทางส่วนตัวและต้องให้ผู้ป่วยยินยอม

๔. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเทอร์เน็ตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเทอร์เน็ตพร้อมกันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ หรือ CIO

ประกาศ ณ วันที่ ๑๔ สิงหาคม พ.ศ. ๒๕๖๑

ลงชื่อ

นายสุนทร ยนต์ตระกูล
ผู้อำนวยการโรงพยาบาลมหาสารคาม