



บันทึกข้อความ

ส่วนราชการ คณะกรรมการพัฒนาระบบสาธารณสุข โรงพยาบาลอ่างทอง

ที่ อท. ๐๐๓๒.๒๐๓.๙/๕

วันที่ ๓๑ มีนาคม ๒๕๕๙

เรื่อง แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลอ่างทอง

เรียน ผู้อำนวยการโรงพยาบาลอ่างทอง

ตามหนังสือ สำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๐๒.๐๕/ว๒๖ ลว.๙ มกราคม ๒๕๕๖ เรื่อง ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ นั้น

ในการนี้ คณะกรรมการพัฒนาระบบสาธารณสุข ได้จัดทำ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลอ่างทอง ขึ้น เพื่อใช้เป็นแนวทางในการควบคุม กำกับ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลอ่างทอง อย่างเป็นรูปธรรม

จึงเรียนมาเพื่อพิจารณา หากเห็นชอบ โปรดลงนามในแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลอ่างทอง จักเป็นพระคุณยิ่ง

๙ / - 1

(นายณรงค์ คั่นสกุลคุงี)

รองผู้อำนวยการกลุ่มภารกิจพัฒนาระบบบริการสุขภาพ

ประธานกรรมการพัฒนาระบบสาธารณสุข

แนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลอ่างทอง

หมวดที่ ๑ บททั่วไป

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ บุคคลภายนอก หรือ ผู้ที่ได้รับอนุมัติให้ใช้สินทรัพย์ของโรงพยาบาลอ่างทอง

“ผู้บริหาร” หมายถึง ผู้อำนวยการโรงพยาบาลอ่างทอง หรือ บุคลากรระดับบริหารของโรงพยาบาลที่ทำหน้าที่เป็นผู้นำในการบริการด้านเทคโนโลยีสารสนเทศ

“ผู้ดูแลระบบ” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้อำนวยการโรงพยาบาลอ่างทอง หรือ บุคลากรระดับบริหารของโรงพยาบาลที่ทำหน้าที่เป็นผู้นำในการบริการด้านเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบดูแลรักษา หรือ จัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาล ซึ่งได้รับอนุมัติจากผู้บริหารของโรงพยาบาลอ่างทอง

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และแบบพกพา เครื่องพิมพ์ผลลัพท์ หรืออุปกรณ์ที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์ที่มีลิขสิทธิ์

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือ การส่งข้อมูลและสารสนเทศ ระหว่างหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) ระบบเครือข่ายแบบไร้สาย (Wireless LAN)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือ การมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือ ระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้ง การอนุญาตสำหรับบุคคลภายนอก

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การรักษาความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“บทลงโทษ” หมายถึง บทลงโทษที่กำหนดขึ้นตามระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลอ่างทอง หรือ บทลงโทษตามกฎหมาย

หมวดที่ ๒ แนวทางปฏิบัติสำหรับ ผู้ดูแลระบบ

๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน

๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารโรงพยาบาลอ่างทอง

๓. ผู้ดูแลระบบ ทำหน้าที่กำหนดสิทธิ์ และระดับสิทธิ์ การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงาน และทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

หมวดที่ ๓ แนวทางปฏิบัติสำหรับ ผู้ใช้งาน

๑. ผู้ใช้งาน ต้องขออนุมัติใช้งานอย่างเป็นทางการเป็นลายลักษณ์อักษร และต้องได้รับอนุมัติสิทธิการเข้าถึงหรือควบคุมการใช้งานสารสนเทศจากผู้บริหาร ซึ่งเป็นการอนุมัติสิทธิเฉพาะบุคคลเท่านั้น จะโอน จำหน่าย หรือ แจกสิทธินี้ให้กับผู้อื่นไม่ได้ ยกเว้นจัดไว้เพื่อเป็นการสาธารณะ โดยต้องเก็บรักษา “รหัสผ่าน” ของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น

๒. การเข้าใช้งานระบบคอมพิวเตอร์ และการใช้งานอินเทอร์เน็ต (Internet) ผู้ใช้งาน ต้องทำการพิสูจน์ตัวตนทุกครั้ง โดยการลงชื่อเข้าใช้ (Log In) และลงชื่อออก (Log Out) ทุกครั้งเมื่อไม่ใช้งาน

๓. ผู้ใช้งาน ต้องเป็นผู้รับผิดชอบผลเสียหายต่างๆ ที่เกิดกับสินทรัพย์ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔. ผู้ใช้งาน ห้ามปฏิบัติการใดๆ ที่เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือ ศีลธรรมอันดีแห่งสาธารณชน ไม่ล่วงละเมิดสถาบันชาติ ศาสนา พระมหากษัตริย์ และบุคคล การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่น หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของโรงพยาบาลอ่างทอง

๕. ผู้ใช้งาน ห้ามทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้า หรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๖. ผู้ใช้งาน ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรก่อนการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ ผ่านทางเว็บไซต์ของโรงพยาบาลอ่างทอง และจะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหา จะต้องรับผิดชอบต่อความผิดพลาดนั้น

๗. ผู้ใช้งาน จะต้องรับผิดชอบต่อเพียงฝ่ายเดียว โรงพยาบาลอ่างทอง ไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายอันเกิดจากการละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มีชื่อของตน โดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในโรงพยาบาลอ่างทอง โดยไม่ได้รับอนุญาต

๘. โรงพยาบาลอ่างทอง ทรงไว้ซึ่งสิทธิ์ที่จะปฏิเสธการติดตั้งโปรแกรมที่ไม่ได้ซื้อสิทธิ์มาอย่างถูกต้องตามกฎหมาย การเชื่อมต่อ และ/หรือการใช้งาน ที่ขัดต่อประโยชน์ของทางราชการ และทรงไว้ซึ่งสิทธิ์ที่จะยกเลิกหรือระงับการเชื่อมต่อ และ/หรือการใช้งานใดๆ ของผู้ใช้งาน ที่ล่วงละเมิด หรือพยายามจะล่วงละเมิดระเบียบนี้ของโรงพยาบาลอ่างทอง

หมวดที่ ๔ แนวทางปฏิบัติสำหรับ การเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์

๑. การนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องขออนุมัติอย่างเป็นทางการเป็นลายลักษณ์อักษร และแจ้งให้ผู้ดูแลระบบทราบ เพื่อให้การเชื่อมต่ออุปกรณ์ต่าง ๆ เป็นไปตามมาตรฐานสากล และไม่เกิดผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาลอ่างทอง เช่น อุปกรณ์กระจายสัญญาณ Wireless Access Point กล้อง Webcam

๒. การนำเครื่องคอมพิวเตอร์ส่วนบุคคล เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ เจ้าของเครื่องคอมพิวเตอร์ ต้องขออนุมัติอย่างเป็นทางการเป็นลายลักษณ์อักษร

๓. การเคลื่อนย้าย หรือทำการใดๆ ต่อเครื่องคอมพิวเตอร์ หรืออุปกรณ์ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ เพราะอาจก่อให้เกิดความเสียหายแก่อุปกรณ์ และระบบเครือข่ายของโรงพยาบาล

กรณีระบบคอมพิวเตอร์ หรือ ข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด หรือต่อสิทธิประโยชน์ของทางราชการ อันเนื่องจากความบกพร่อง ละเลย หรือ ฝ่าฝืนการปฏิบัติตามระเบียบ และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลอ่างทอง จะต้องรับโทษทางวินัย เว้นแต่มีเหตุอันควรงดโทษตามที่บัญญัติไว้ในหมวด ๗ การดำเนินการทางวินัย (พรบ.ระเบียบข้าราชการพลเรือน พ.ศ. ๒๕๕๑) หรือรับโทษ ตามกฎหมาย

ประกาศ ณ วันที่ ๑๑ เมษายน พ.ศ. ๒๕๕๙



(นายพงษ์นรินทร์ ชาตธีรสรค์)
ผู้อำนวยการโรงพยาบาลอ่างทอง