ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลมะเร็งสุราษฎร์ธานี

๑. ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสม

ผู้รับผิดชอบ : บุคลากรโรงพยาบาลมะเร็งสุราษฎร์ธานี ทุกแผนกที่ครอบครอง/ใช้งานเครื่องคอมพิวเตอร์ ของโรงพยาบาลมะเร็งสุราษฎร์ธานี

ลำดับที่	ระเบียบปฏิบัติ
๑	จัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย
๒	ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่ทำเครื่องชำรุด หรือสูญหายไปโดยประมาทหรือเลินเล่อ
๓	ไม่เข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ - การพนัน - การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติศาสนา และพระมหากษัตริย์ - สิ่งลามก อนาจาร - สิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม
๔	ห้ามใช้ระบบเครือข่ายเพื่อส่ง กระจาย หรือแจกจ่ายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมทั้ง ข้อมูล ที่เป็นความลับของโรงพยาบาลมะเร็งสุราษฎร์ธานี ไปยังบุคคลที่ไม่ได้รับอนุญาต
๕	ห้ามใช้ระบบเครือข่ายเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของโรงพยาบาลมะเร็งสุราษฎร์ธานี
๖	ตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหากไม่ใช้งาน เกินกว่า ๑๕ นาที
๗	ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมี การยุติการใช้งานเกินกว่า ๓ ชั่วโมง
๘	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในระบบเครือข่าย ของโรงพยาบาลมะเร็งสุราษฎร์ธานี เพื่อให้บุคคลอื่นสามารถเข้าถึงหรือเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย
๙	ให้ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ
๑๐	ต้องขออนุมัติจากผู้มีอำนาจ ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกโรงพยาบาลมะเร็งสุราษฎร์ธานี
๑๑	ระมัดระวังการใช้งาน และดูแลรักษาความสะอาดของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างสม่ำเสมอ

๒. ระเบียบปฏิบัติสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับฐานข้อมูลและสารสนเทศ

ผู้รับผิดชอบ : คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

ลำดับที่	ระเบียบปฏิบัติ
๑	จัดทำ/ทบทวน และปรับปรุงนโยบายความมั่นคงปลอดภัยฯ อย่างสม่ำเสมอ ปีละ ๑ ครั้ง
๒	สื่อสารให้บุคลากรทราบและตระหนักถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยของ ระบบฐานข้อมูลและสารสนเทศของโรงพยาบาลมะเร็งสุราษฎร์ธานี อย่างเคร่งครัดและสม่ำเสมอ
๓	จัดประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยฯ อย่างสม่ำเสมอ อย่างน้อย ปีละ ๑ ครั้ง โดยกำหนดวาระการประชุมที่ต้องหารือกัน ดังนี้ การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ และผลการตรวจสอบ แผนการดำเนินการเชิงป้องกัน/แก้ไขจากผลการตรวจสอบดังกล่าว การปรับปรุง นโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป การประเมินความเสี่ยงและแผนลดความเสี่ยง การจัด ทรัพยากรด้านบุคลากร งบประมาณการบริหารจัดการ และวัตถุดิบให้เพียงพอต่อการจัดการดังกล่าว
๔	ตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯ ปีละ ๑ ครั้ง และจัดทำแผนเพื่อปรับปรุง หรือ แก้ไขปัญหาที่พบ
๕	แจ้งเวียนให้บุคลากรระมัดระวัง และดูแลทรัพย์สินของโรงพยาบาลมะเร็งสุราษฎร์ธานี ที่ตนเองใช้ในการปฏิบัติงาน เพื่อป้องกัน การสูญหาย ปีละ ๑ ครั้ง
๖	กำหนดนโยบายการใช้งานระบบเครือข่าย โดยห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ ๖.๑ การพนัน ๖.๒ การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติศาสนา และพระมหากษัตริย์ ๖.๓ สิ่งลามก อนาจาร ๖.๔ สิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม

๓. ระเบียบปฏิบัติสำหรับการจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

รับผิดชอบ : งานคอมพิวเตอร์

ลำดับที่	ระเบียบปฏิบัติ
๑	จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย และจัดเก็บไว้ในสถานที่ปลอดภัย มีเนื้อหาครอบคลุมระบบงาน เครื่อง server และอุปกรณ์ที่มีความสำคัญ เช่น คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งานและผู้ดูแลระบบ คู่มือการตรวจสอบสถานะของ server และระบบเครือข่าย คู่มือการตรวจสอบ ระบบและอุปกรณ์ต่างๆ คู่มือการสำรองข้อมูล คู่มือการตรวจสอบทรัพยากรของระบบ เป็นต้น
๒	จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น
๓	หากจดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย ต้องป้องกันการเข้าถึงข้อมูล โดยกำหนดรหัสผ่านให้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

๔. ระเบียบปฏิบัติสำหรับการจัดการระบบเครือข่าย

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ลำดับที่	ระเบียบปฏิบัติ
๑	ปรับปรุงผังเครือข่ายให้มีความทันสมัย อย่างน้อยปีละ ๑ ครั้ง
๒	จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่มๆ ตามลักษณะการใช้งาน และ ระบบงานที่มีความสำคัญ
๓	จำกัดการเชื่อมต่อไปยังเครื่อง server ระบบงาน หรืออุปกรณ์ที่มีความสำคัญ โดยกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น
๔	ปิดบริการบนเครื่อง server ที่ไม่มีความจำเป็นในการใช้งาน
๕	ติดตั้ง Patch แบบอตโนมัติ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งานทั้งหมดของโรงพยาบาลมะเร็งสุราษฎร์ธานี
๖	ปรับแต่ง Firewall เพื่อให้เป็นไปตามนโยบายการใช้งานระบบเครือข่ายที่ผู้บริหารได้กำหนดไว้

๕. ระเบียบปฏิบัติสำหรับการจัดการการลาออกของบุคลากรจากโรงพยาบาลมะเร็งสุราษฎร์ธานี

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ลำดับที่	ระเบียบปฏิบัติ
๑	ถอดถอนสิทธิของบุคลากรที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆ ทั้งหมดโดยทันทีที่ได้รับแจ้งจาก งานทรัพยากรบุคคล กลุ่มภารกิจอำนวยการ

๖. ระเบียบปฏิบัติสำหรับการจดการไวรัส

รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ลำดับที่	ระเบียบปฏิบัติ
๑	ตรวจสอบการทำงานของโปรแกรม Anti-virus และการปรับปรุงฐานข้อมูลไวรัส (Virus signature) อย่างสม่ำเสมอ หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข
๒	ติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Realtime Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน
๓	ติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยกับเครื่องคอมพิวเตอร์ทุกเครื่อง

๗. ระเบียบปฏิบัติสำหรับการสำรองข้อมูล

ผู้รับผิดชอบ : ผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มงานดิจิทัลการแพทย์

ลำดับที่	ระเบียบปฏิบัติ
๑	กำหนดชนิดของข้อมูลบนระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้
๒	กำหนดความถี่ในการสำรองข้อมูลของระบบงานดังกล่าว
๓	สำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไว้นั้น ไปเก็บนอกสถานที่ อย่างน้อย๑ ชุด

๘. ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ลำดับที่	ระเบียบปฏิบัติ
๑	ลงทะเบียนผู้ใช้งานใหม่ และกำหนดสิทธิของผู้ใช้งาน ควรให้สิทธิการใช้งานตามความจำเป็น
๒	ทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง ทำบันทึกการทบทวนและจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
๓	ทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน (สำหรับหน่วยงานภายนอก) อย่างน้อยปีละ ๑ ครั้ง ทำบันทึกการทบทวนและจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง

๙. ระเบียบปฏิบัติสำหรับการป้องกันไวรัส

ผู้รับผิดชอบ : บุคลากรทุกคนของโรงพยาบาลมะเร็งสุราษฎร์ธานีที่ใช้งานคอมพิวเตอร์และเชื่อมต่อสัญญาณ WIFI ของโรงพยาบาลมะเร็งสุราษฎร์ธานี

ที่	ระเบียบปฏิบัติ
๑	ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งเจ้าหน้าที่งานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์
๒	Scan Virus ที่ Removable Drive ทุกครั้งที่มีการเชื่อมต่อ
๓	กรณีพบ Virus แต่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ ให้รีบแจ้งเจ้าหน้าที่งานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์ดำเนินการทันที

๑๐. ระเบียบปฏิบัติของการ E-mail ผ่านเครือข่ายอินเตอร์โรงพยาบาล

ผู้รับผิดชอบ : บุคลากรทุกคนของโรงพยาบาลมะเร็งสุราษฎร์ธานีที่ใช้งานคอมพิวเตอร์และเชื่อมต่อสัญญาณ WIFI ของโรงพยาบาลมะเร็งสุราษฎร์ธานี

ที่	ระเบียบปฏิบัติ
๑	ห้ามมิให้เข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
๒	ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
๓	ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
๔	ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
๕	ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
๖	ห้ามปลอมแปลง E-mail ของบุคคลอื่น
๗	ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป
๘	ให้ทำการสำรองข้อมูล E-mail ตามความจำเป็นอย่างสม่ำเสมอ

๑๑. ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์ชนิดพกพา (Notebook)

ผู้รับผิดชอบ : บุคลากรทุกคนของโรงพยาบาลมะเร็งสุราษฎร์ธานีที่ใช้งานคอมพิวเตอร์และเชื่อมต่อสัญญาณ WIFI ของโรงพยาบาลมะเร็งสุราษฎร์ธานี

ที่	ระเบียบปฏิบัติ
๑	เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) ที่ใช้ร่วมกัน ให้ทำการกรอกแบบฟอร์มยืม/คืน เพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย
๒	ตรวจสอบอย่างสม่ำเสมอว่าโปรแกรมป้องกันไวรัสที่ใช้งานอยู่ได้รับการปรับปรุงฐานข้อมูลและรูปแบบไวรัสอย่างสม่ำเสมอ
๓	ระมัดระวังและรักษาเครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เมื่อมีการนำไปใช้งานนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๔	เมื่ออยู่ในที่สาธารณะหรือในห้องประชุม ห้ามทิ้งเครื่องไว้โดยไม่มีผู้ดูแล
๕	ตั้งค่า Screen Saver เพื่อล็อกหน้าจออัตโนมัติ หากไม่ใช้งานเกินกว่า ๑๕ นาที

๑๒. ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ

ผู้รับผิดชอบ : เจ้าของข้อมูลที่เผยแพร่

ที่	ระเบียบปฏิบัติ
๑	ทุกหน่วยงานของโรงพยาบาลมะเร็งสุราษฎร์ธานี ที่เป็นเจ้าของข้อมูลที่ต้องการเผยแพร่สู่สาธารณะผ่านเว็บไซต์ของหน่วยงานต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น
๒	ให้ผู้ที่ได้รับมอบหมายในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะผ่านเว็บไซต์ของโรงพยาบาลมะเร็ง สุราษฎร์ธานี จะต้องดำเนินการผ่านงานคอมพิวเตอร์ กลุ่มงานดิจิทัลการแพทย์เท่านั้น

ประกาศ ณ วันที่ เดือน เมษายน พ.ศ. ๒๕๖๕

(นางสาวนิธิมา ศรีเกตุ)

รักษาราชการในตำแหน่งผู้อำนวยการโรงพยาบาลมะเร็งสุราษฎร์ธานี