1/3, 3.1

# บันทึกข้อความ

**ส่วนราชการ** งานประกันสุขภาพ โรงพยาบาลยางสีสุราช จังหวัดมหาสารคาม

**ที่** มค ๐๐๓๒.๓๐๑/๑๑/๓๙ **วันที่** ๒๐ เมษายน ๒๕๖๔

**เรื่อง** ขออนุมัติและประกาศใช้นโยบายแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เรียน ผู้อำนวยการโรงพยาบาลยางสีสุราช

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องเหมาะสม

ดังนั้นคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศ โรงพยาบาลยางสีสุราช ได้ดำเนินการจัดทำ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลยางสีสุราช เพื่อให้การใช้งานระบบสารสนเทศของโรงพยาบาลยางสีสุราชมีความปลอดภัย และสอดคล้องตามหลักกฎหมาย จึงควรประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลยางสีสุราช ควบคุมการดำเนินการใด ๆ ที่เกี่ยวข้องกับระบบสารสนทศของโรงพยาบาลยางสีสุราช

จึงเรียนมาเพื่อทราบและโปรดพิจารณาอนุมัติ

(นางมยุรฉัตร อุทปา )
พยาบาลวิชาชีพชำนาญการ

เรียน ผู้อำนวยการโรงพยาบาลยางสีสุราช
-เห็นควรอนุมัติ

(นางศุภลักษณ์ ทองจันทร์)
เจ้าพนักงานการเงินและบัญชีชำนาญงาน

คำสั่ง ผู้อำนวยการโรงพยาบาลยางสีสุราช
-อนุมัติ

(นายภาคภูมิ อินทร์ม่วง)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลยางสีสุราช

# ประกาศโรงพยาบาลยางสีสุราช

**เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลยางสีสุราช**

เพื่อให้การดำเนินการใด ๆ ต่อระบบสารสนเทศโรงพยาบาลยางสีสุราช เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่าง ๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลยางสีสุราช และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง โรงพยาบาลยางสีสุราชจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของโรงพยาบาลยางสีสุราชทำให้ดำเนินงานได้อย่างปลอดภัย และต่อเนื่อง

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลยางสีสุราชได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะมีการทบทวนนโยบายปีละ 1 ครั้งอาศัยอำนาจตามในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โรงพยาบาลยางสีสุราชจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลยางสีสุราช ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศโรงพยาบาลยางสีสุราช"เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลยางสีสุราช กำหนดประเด็นสำคัญดังต่อไปนี้

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๓.๑.๑ ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๓.๑.๒ นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาลยางสีสุราช

๓.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๓.๑.๔ กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓.๑.๕ กำหนดให้ทบทวนและปรับปรุงนโยบายปีละ ๑ ครั้ง

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๓ ส่วน คือ

ส่วนที่ ๑ คำนิยามและคำจำกัดความ

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลยางสีสุราช พ.ศ.๒๕๖๐ ซึ่งกำหนดผู้รับผิดชอบตามนโยบาย แบ่งสาระสำคัญออกเป็น ๑๔ หมวด ซึ่งสาระสำคัญจะสอดคล้องตามมาตรา ๕ และมาตรา ๗ พระราชกฤษฎีกากำหนดหลักกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๙ ดังต่อไปนี้

**(๑) นโยบายควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผล**

สารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลยางสีสุราช

๒) หัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

๓) หัวหน้างานประกันสุขภาพ โรงพยาบาลยางสีสุราช

๔) นักวิชาการคอมพิวเตอร์

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

**(๒) นโยบายการสำรองและกู้คืนข้อมูล กำหนดให้มีการจำทำระบบสำรองข้อมูลของสารสนเทศ**

ซึ่งอยู่ในสภาพพร้อมใช้ และกำหนดให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อป้องกันการหยุดชะงักในการให้บริการสารสนเทศของโรงพยาบาลยางสีสุราช

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลยางสีสุราช

๒) หัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

๓) หัวหน้างานประกันสุขภาพ โรงพยาบาลยางสีสุราช

๔) นักวิชาการคอมพิวเตอร์

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๒) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อกำกับดูแลการดำเนินงาน การบริหารจัดการระบบสารสนเทศให้มีความปลอดภัย ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับนโยบายความมั่นคงปลอดสารสนเทศ ดังต่อไปนี้

แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน

ส่วนที่ ๑๐ การควบคุมการเข้าระบบเครือข่ายไร้สาย

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย

ส่วนที่ ๑๒ ระเบียบปฏิบัติการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๓ การควบคุมการใช้อินเตอร์เน็ต

ส่วนที่ ๑๔ การใช้งานคอมพิวเตอร์ส่วนบุคคล

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ส่วนที่ ๑๖ การตรวจจับการบุกรุก

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ

ส่วนที่ ๑๘การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

แนวปฏิบัติในการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

แนวปฏิบัติในการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

แนวปฏิบัติสำหรับการจัดซื้อจัดจ้างระบบสารสนเทศของโรงพยาบาลยางสีสุราช

แนวปฏิบัติความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

ข้อที่ ๔ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลยางสีสุราชเกิดความเสียหาย หรือได้รับอันตรายจากภัยคุกคามทางด้านต่าง ๆ ผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย ละเว้น หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาลยางสีสุราชเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อที่ ๕ ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แบบท้ายประกาศนี้

ข้อที่ ๖ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ เมษายน ๒๕๖๔

(นายภาคภูมิ อินทร์ม่วง)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลยางสีสุราช