โรงพยาบาลอุดรธานี Udon Thani Hospital	แนวทางปฏิบัติ เรื่อง : แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)	หน้า 1/5 รหัสเอกสาร : PG - IT - 006 แก้ไขครั้งที่ : - วันที่แก้ไข : 01 ส.ค. 2568

ชื่อหน่วยงานผู้จัดทำ : ศูนย์ข้อมูลสารสนเทศทางการแพทย์ กลุ่มงานภารกิจสุขภาพดิจิทัล
วันที่บังคับใช้ : 01 ส.ค. 2568

ผู้ตรวจสอบ :	ผู้เห็นชอบ :
(นายบรรจง แจ่มจันทร์) ตำแหน่ง หัวหน้าศูนย์ข้อมูลสารสนเทศทางการแพทย์	(นายแพทย์นิพันธ์ ทองบ่อ) ตำแหน่ง รองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัล

ผู้อนุมัติ :

(นายแพทย์ทรงเกียรติ เล็กตระกูล)
ตำแหน่ง ผู้อำนวยการโรงพยาบาลอุดรธานี

บันทึกรายการแก้ไข

ครั้งที่	หน้า	รายการแก้ไข	วัน/เดือน/ปี
00	ทุกหน้า	ฉบับใหม่	01 ส.ค. 2568

*** หมายเหตุ หน้าที่ 1 QIC จะเป็นผู้บันทึก****

1. นโยบาย :

ระเบียบปฏิบัติงานนี้เพื่อเป็นแนวทางการบริหารความมั่นคงปลอดภัย การควบคุม และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโรงพยาบาลอุดรธานี

2. วัตถุประสงค์ :

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตาม เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

3. ขอบเขต :

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับผู้ดูแลระบบสารสนเทศ หรือเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาลอุดรธานี

4. กลุ่มเป้าหมาย :

ผู้ดูแลระบบสารสนเทศของโรงพยาบาลอุดรธานี ต้องปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

5. นิยามศัพท์/คำจำกัดความ :

กฎระเบียบการควบคุมดูแลเครื่องคอมพิวเตอร์และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่าย

1) "โรงพยาบาล" หมายถึง โรงพยาบาลศูนย์อุดรธานี

2) "ศูนย์คอมฯ" หมายถึง กลุ่มงานภารกิจสุขภาพดิจิทัล โรงพยาบาลศูนย์อุดรธานี

3) "เครื่องคอมพิวเตอร์และเครือข่าย" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาลทั้งที่อยู่ภายใน และภายนอกส่วนกลาง รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในโรงพยาบาล ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ ที่มิได้จัดให้เป็นสื่อสาธารณะ

4) "หน่วยงาน" หมายถึง หน่วยงานต่างๆ ของโรงพยาบาลศูนย์อุดรธานี

5) "ผู้ดูแลระบบ" หมายถึง ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ควบคุมดูแลระบบเครื่องคอมพิวเตอร์และเครือข่ายได้

6. ขั้นตอน/วิธีปฏิบัติ :

แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

โรงพยาบาลอุดรธานีมีการกำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

6.1 มีการกำหนดและแบ่งกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย ออกเป็นกลุ่ม ๆ และมี Firewall กั้นและกรองการเข้าระบบเครื่องที่มีเครื่องคอมพิวเตอร์แม่ข่าย เช่น

6.1.1 กลุ่ม Server ที่สามารถให้บุคคลภายนอกเข้าถึงได้ (Web Zone)

6.1.2 กลุ่ม Server ที่ใช้งานภายในองค์กร (Server Zone)

6.1.3 กลุ่ม Server ที่มีปัญหาด้านความปลอดภัย (Quarantine Zone)

6.1.4 กลุ่ม Computer Client ที่ใช้ระบบ HIS ภายในองค์กร (HIS Internal Computer)

6.1.5 กลุ่ม Computer Client ที่ใช้ระบบอินเตอร์เน็ต และโปรแกรมสำนักงาน (VC-Staff Only) เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

6.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลอุดรธานี หรือรองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัลหรือหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

6.3 การขอพัฒนาระบบงานภายใน Intranet web application และ Internet web application/ Information จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการโรงพยาบาลอุดรธานี หรือรองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัลและหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ เพื่อควบคุมผลกระทบด้าน Cyber Security ต่อการกระทำของระบบและผู้ใช้บริการ

6.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้ง เพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์กระจายสัญญาณไร้สาย (WIFI Router/Access Point) และอุปกรณ์ เครื่องมือแพทย์ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ โดยไม่ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลอุดรธานี หรือรองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัล และหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ เพื่อเป็นผู้ควบคุมผลกระทบด้าน Cyber Security ต่อการกระทำของระบบและผู้ใช้บริการ

6.5 กลุ่มงานเทคโนโลยีสารสนเทศต้องสามารถควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

6.5.1 มีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น และมีการจำกัดเส้นทาง/บริการต่าง ๆ ของระบบเครือข่ายที่มีการใช้งานร่วมกัน

6.5.2 มีการกำหนดวิธีการเข้าถึง เพื่อจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ไปยัง เครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถเข้าถึงระบบฯ ที่ตนเองไม่มีสิทธิ์

6.5.3 ระบบเครือข่ายของโรงพยาบาลอุดรธานี มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก (สาขา) และระบบเครือข่ายภายนอกอื่นๆ (อินเตอร์เน็ต) ได้มีการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall)รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ได้

6.5.4 การเข้าสู่ระบบเครือข่ายภายในหน่วยงานผ่านทางระบบอินเตอร์เน็ต มีการบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ มีการลงทะเบียน เพื่อเข้าสู่ระบบ (Login) โดยมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

6.5.5 มีการปกปิดเลขหมายที่อยู่ไอพี (Internal IP Address) ของระบบเครือข่ายภายในมิให้หน่วยงานภายนอกล่วงรู้ได้

6.5.6 มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และการเชื่อมต่ออุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6.5.7 มีการใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย เพื่อให้ได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็นได้

6.5.8 ผู้ดูแลระบบต้องบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) และควบคุมรวมถึงดูแลระบบคอมพิวเตอร์แม่ข่าย ให้อยู่ในการกำหนดเงื่อนไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

6.6 โรงพยาบาลอุดรธานี มีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Computer Access Log) เพื่อให้สามารถระบุถึงตัวตน และตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

6.6.1 มีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Computer Access Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

6.6.2 มีการกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และFirewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บ บันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

6.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

6.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

6.7 โรงพยาบาลอุดรธานี กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

6.7.1 บุคคลจากหน่วยงานภายนอก ที่มีความต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและข้อมูลภายในเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน จะต้องจัดทำหนังสือขออนุญาตและเหตุผลความจำเป็นเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการโรงพยาบาลอุดรธานี หรือรองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัล และหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ เพื่อเป็นผู้ควบคุมผลกระทบด้าน Cyber Security ต่อการกระทำของระบบและผู้ใช้บริการ

6.7.2 มีการควบคุมช่องทางสื่อสาร (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

6.7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการโรงพยาบาลอุดรธานี หรือรองผู้อำนวยการกลุ่มภารกิจสุขภาพดิจิทัลและหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ เพื่อเป็นผู้ควบคุมผลกระทบด้าน Cyber Security ต่อการกระทำของระบบและผู้ใช้บริการ

6.7.4 การเข้าสู่ระบบคอมพิวเตอร์จากระยะไกล Remote Access / Remote Desktop ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ และจะให้กระทำผ่านเครื่องคอมพิวเตอร์ของแผนกไอทีเท่านั้น (มีผู้ดูการกระทำต่าง ๆ บนหน้า Computer Desktop)

6.7.5 กลุ่มงานเทคโนโลยีสารสนเทศ ไม่มีการเปิดให้ใช้ระบบ VPN

6.7.6 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

7. เอกสารอ้างอิง :

7.1 ประกาศโรงพยาบาลอุดรธานี เรื่อง ระเบียบปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ พ.ศ. 2566 (สำหรับเจ้าหน้าที่ทั่วไปของโรงพยาบาลอุดรธานี) ลงวันที่ 14 กรกฎาคม 2566

7.2 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ.2561

7.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553

7.4 ระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561

8. ตัวชี้วัด :

ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ดูแลควบคุมมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลอุดรธานี ปฏิบัติตามระเบียบ 100 %

9. ภาคผนวก :

9.1. ผู้รับผิดชอบ

9.1.1 คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีหน้าที่กำหนดระเบียบปฏิบัติที่เหมาะสมและเป็นไปตามประกาศและระเบียบที่เกี่ยวข้อง

9.1.2 คณะกรรมการบริหารโรงพยาบาล มีหน้าที่ สื่อสารนโยบายและแนวปฏิบัติตามที่ คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้กำหนด รวมถึงกำกับ ติดตาม การปฏิบัติของบุคลากรในหน่วยงานให้เป็นไปในแนวทางเดียวกัน