| โรงพยาบาลอุดรธานี Udon Thani Hospital | แนวทางปฏิบัติ<br>เรื่อง : แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ<br>(Access Control Policy) | หน้า 1/5<br>รหัสเอกสาร : PG - IT - 004<br>แก้ไขครั้งที่ : -<br>วันที่แก้ไข : 01 ส.ค. 2568 |
|---|---|---|

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

| ผู้ตรวจสอบ : | ผู้เห็นชอบ : |
|---|---|
| (นายบรรจง แจ่มจันทร์)<br>ตำแหน่ง หัวหน้าศูนย์ข้อมูลสารสนเทศทางการแพทย์ | (นายแพทย์นิพันธ์ ทองบ่อ)<br>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 :**

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

**3. ขอบเขต :**

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับผู้ดูแลระบบสารสนเทศ หรือเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

**4. กลุ่มเป้าหมาย :**

ผู้ดูแลระบบสารสนเทศของโรงพยาบาล ต้องปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

**5. นิยามศัพท์/คำจำกัดความ :**

กฎระเบียบการควบคุมดูแลเครื่องคอมพิวเตอร์และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่าย

1) "โรงพยาบาล" หมายถึง โรงพยาบาลศูนย์อุดรธานี

2) "ศูนย์คอมฯ" หมายถึง กลุ่มงานภารกิจสุขภาพดิจิทัล โรงพยาบาลศูนย์อุดรธานี

3) "เครื่องคอมพิวเตอร์และเครือข่าย" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาลทั้งที่อยู่ภายใน และภายนอกส่วนกลาง รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆภายในโรงพยาบาลตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ ที่มิได้จัดให้เป็นสื่อสาธารณะ

4) "หน่วยงาน" หมายถึง หน่วยงานต่างๆ ของโรงพยาบาลศูนย์อุดรธานี

5) "ผู้ดูแลระบบ" หมายถึง ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ควบคุมดูแลระบบเครื่องคอมพิวเตอร์และเครือข่ายได้

**6. ขั้นตอน/วิธีปฏิบัติ :**

**แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลอุดรธานีมีดังนี้**

**2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ**

2.1.1 โรงพยาบาลอุดรธานี กำหนดระดับการเข้าถึงงานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ โดยจำเป็นต้องมีรายละเอียดดังนี้

1) ข้อมูลผู้ขอเข้าถึงระบบฯ

2) รายการหรือขอบเขตระบบที่ต้องการเข้าถึง

3) ระยะเวลาการเข้าถึง

4) วัตถุประสงค์ที่ต้องการ

5) ความจำเป็นในการเข้าถึง

2.1.2 ผู้ดูแลระบบ (System Administrator) มีหน้าที่กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานนั้น ๆ ก่อนเข้าระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ปัจจุบันโรงพยาบาลมีการแบ่งผู้ดูแลระบบออกตามลักษณะงาน เช่น

ผู้ดูแลระบบทั่วไป (ภาพรวม โดยกลุ่มงานเทคโนโลยีสารสนเทศ) เช่น สร้างผู้ใช้งาน กำหนดกลุ่มสิทธิ์การใช้งาน เป็นต้น

ผู้ดูแลระบบฐานข้อมูลยา (โดยกลุ่มงานเภสัชกร) เช่น กำหนดรายการยา กำหนดหรือปรับปรุงราคายา กำหนดขนาดหรือประมาณยา เป็นต้น

2.1.3 มีการกำหนดขบวนการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

2.1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้ รับการอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

**2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ**

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานระบบฯ ของโรงพยาบาลอุดรธานี กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก การเปลี่ยนตำแหน่งงานภายในหน่วยงาน การกำหนดเวลาหมดอายุ เป็นต้น

2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E - mail) ระบบเครือข่ายไร้สาย (Wireless Lan)ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดย ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.2.3 ผู้ดูแลระบบต้องบริหารจัดการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

2.2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

2.2.3.3 ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

2.2.3.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานตามปกติ

2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับของข้อมูล

2.2.4.1 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.2.4.2 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.2.4.3 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

2.2.4.4 ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

**2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ**

2.3.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

2.3.2 ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้เครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

2.3.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

2.3.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า 1 ชม.

**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 ผู้ที่โรงพยาบาลอนุญาตให้ดูแลควบคุมกำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศได้ ปฏิบัติตามระเบียบ 100 %

**9. ภาคผนวก :**

9.1. ผู้รับผิดชอบ

9.1.1 คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีหน้าที่กำหนดระเบียบปฏิบัติที่เหมาะสมและเป็นไปตามประกาศและระเบียบที่เกี่ยวข้อง

9.1.2 คณะกรรมการบริหารโรงพยาบาล มีหน้าที่ สื่อสารนโยบายและแนวปฏิบัติตามที่ คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้กำหนด รวมถึงกำกับ ติดตาม การปฏิบัติของบุคลากรในหน่วยงานให้เป็นไปในแนวทางเดียวกัน