โรงพยาบาลอุดรธานี Udon Thani Hospital	นโยบาย เรื่อง : ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ใช้ระบบสารสนเทศ	หน้า 1/5 รหัสเอกสาร : QM - IT - 003 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 :

1) เพื่อสร้างความเข้าใจเกี่ยวกับแนวการป้องกันการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของโรงพยาบาลศูนย์อุดรธานี

2) เพื่อให้ ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ใช้เครื่อง คอมพิวเตอร์และเครือข่ายได้ปลอดภัยตามแนวทางปฏิบัติ

3. ขอบเขต :

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับเจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศของโรงพยาบาลอุดรธานี

4. กลุ่มเป้าหมาย :

ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายได้

5. นิยามศัพท์/คำจำกัดความ :

กฎระเบียบการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่าย

1) "โรงพยาบาล" หมายถึง โรงพยาบาลศูนย์อุดรธานี

2) "ศูนย์คอมฯ" หมายถึง กลุ่มงานภารกิจสุขภาพดิจิทัล โรงพยาบาลศูนย์อุดรธานี

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

4) "หน่วยงาน" หมายถึง หน่วยงานต่างๆ ของโรงพยาบาลศูนย์อุดรธานี

5) "ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายได้

6) "บทลงโทษ" หมายถึง บทลงโทษที่โรงพยาบาลเป็นผู้กำหนด หรือ บทลงโทษตามกฎหมาย

6. ขั้นตอน/วิธีปฏิบัติ :

6.1 กฎระเบียบการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

1) เครื่องคอมพิวเตอร์และเครือข่ายของโรงพยาบาลเป็นสมบัติของทางราชการ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต

2) ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไขในการรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่โรงพยาบาลกำหนดขึ้นโดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย ของส่วนราชการ มิได้

3) โรงพยาบาลให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

4) บัญชีผู้ใช้งาน (User Account) ที่โรงพยาบาลให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

5) ห้ามผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือ ศีลธรรมอันดีแห่งสาธารณชนโดยผู้ใช้งานรับรองว่าหากมีการกระทำการ ใดๆดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของโรงพยาบาลอุดรธานี

6) ห้ามผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และ เครือข่ายเช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการการให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคล ทั่วไปเพื่อแสวงหากำไร

7) ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาตการบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในโรงพยาบาล หรือหน่วยงานอื่นๆ การเผยแพร่ ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่นการใช้ภาษาหรือ รูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียวโรงพยาบาลไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

8) โรงพยาบาลจะไม่ควบคุมเนื้อหาของข้อมูลข่าวสารที่เก็บและรับส่งผ่านเข้าออก เครื่องคอมพิวเตอร์ของหน่วยงานและจะไม่รับประกันในคุณภาพของการเก็บ การรับส่งข้อมูลข่าวสารและการไม่สามารถใช้งานได้ของระบบบางส่วนหรือ ทั้งหมดและจะไม่รับผิดชอบในความเสียหายของการใช้งานอันเนื่องมาจากวงจร สื่อสารชำรุดจานแม่เหล็กชำรุด ความล่าช้า แฟ้มข้อมูลหรือจดหมายส่งไปไม่ถึงปลายทาง หรือส่งผิดสถานที่และความผิดพลาดในข้อมูลหรือความเสียหายอัน เกิดจากการล่วงละเมิดโดยผู้ใช้งาน อื่นๆ

9) ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่โรงพยาบาล กำหนดไว้ และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสมซึ่งจะมีผลบังคับใช้ โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

10) โรงพยาบาลทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อ และ/หรือการใช้งาน และทรง ไว้ซึ่งสิทธิที่จะยกเลิก หรือระงับการเชื่อมต่อ และ/หรือการใช้งานใดๆ ของ ผู้ใช้งานที่ล่วงละเมิด หรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของส่วนราชการ

11) ให้ผู้ซึ่งต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามกฎระเบียบข้อกำหนดโดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่าง ๆ เป็นไปตามมาตรฐานสากลและไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาล การขออนุญาตใช้งานเครือข่ายย่อย หมายเลขไอพี (Subnet) และชื่อโดเมน (Domain Name) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องติดต่อขออนุญาตมายังศูนย์คอมฯ เพื่อพิจารณาดำเนินการ

12) โรงพยาบาลไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้ายหรือทำการใดๆต่อ อุปกรณ์ส่วนกลางโดยพลการเพราะอาจก่อให้เกิดความเสียหายแก่อุปกรณ์ ส่วนกลางและระบบเครือข่ายของโรงพยาบาลได้

6.2 ผู้ใช้งานระบบ

6.2.1. การรักษารหัสผ่านการใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

2) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

3) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม

4) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

5) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

6) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

7) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

8) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

6.2.2 การรักษาข้อมูลผู้ป่วย

การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบกระทรวงสาธารณสุขว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ.2561

6.2.3 การใช้งานระบบสารสนเทศโรงพยาบาล

ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดีผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

1) คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

2) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

3) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

5) ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลา 10 นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

6.3 บทลงโทษ

หากผู้ใช้งานไม่ปฏิบัติตามกฎระเบียบดังกล่าว ก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อสมบัติของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

- โทษขั้นต้น
- โทษขั้นกลาง
- โทษขั้นสูง
- โทษขั้นร้ายแรงหากการละเมิดฝ่าฝืนก่อให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินทั้งของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบส่วนราชการ หรือ รับโทษ ตามกฎหมายโดยลำดับต่อไป

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 ผู้ที่โรงพยาบาลอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายได้ ปฏิบัติตามระเบียบ 100 %

9. ภาคผนวก :

9.1 ผู้รับผิดชอบ

9.1.1 คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล มีหน้าที่กำหนดระเบียบปฏิบัติที่เหมาะสมและเป็นไปตามประกาศและระเบียบที่เกี่ยวข้อง

9.1.2 คณะกรรมการบริหารโรงพยาบาล มีหน้าที่ สื่อสารนโยบายและแนวปฏิบัติตามที่คณะทำงานพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้กำหนด รวมถึงกำกับ ติดตาม การปฏิบัติของบุคลากรในหน่วยงานให้เป็นไปในแนวทางเดียวกัน