

โรงพยาบาลรัฐประเทศ จังหวัดสระแก้ว	หน้า:
นโยบายและระเบียบปฏิบัติเลขที่:	ฉบับที่:                               แก้ไขครั้งที่:
เรื่อง: การรักษาความมั่นคงด้านสารสนเทศ	วันที่:
แผนก: กลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์	แผนกที่เกี่ยวข้อง: ห้องบัตร, ประกันสุขภาพ, ER, OPD, IPD, ห้องยา, LAB, LR, X-Ray, OR, การเงิน, ปฐมนุ้, กายภาพบำบัด, แพทย์แผนไทย, ทันตกรรม, บริหาร,
ผู้จัดทำ: คณะกรรมการ IM	ผู้ทบทวน: ประธานทีมIM
	ผู้อนุมัติ: ..... ผู้อำนวยการโรงพยาบาลรัฐประเทศ

**นโยบาย**

เพื่อให้มีแนวปฏิบัติการเข้าถึงสารสนเทศของโรงพยาบาล และให้ทุกหน่วยงานปฏิบัติตามแนวทางเพื่อป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

**วัตถุประสงค์**

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัย
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง และการกำหนดสิทธิ์
3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

**ระเบียบปฏิบัติ**

1. จัดทำนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของหน่วยงาน ครอบคลุมทุกระดับ

ได้แก่

- 1.1 การควบคุมการเข้า – ออก ห้องปฏิบัติการระบบเครือข่าย
- 1.2 การควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC) คอมพิวเตอร์พกพา(Notebook)

และโทรศัพท์เคลื่อนที่

- 1.3 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN)
2. กำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจนเป็นลายลักษณ์อักษร
3. เผยแพร่โยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศทางเว็บไซต์ของหน่วยงาน

## 1. นโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของหน่วยงาน

### 1.1 การควบคุมการเข้า – ออก ห้องปฏิบัติการระบบเครือข่าย

- กำหนดเป็นเขตหวงห้ามไม่ให้บุคคลภายนอกเข้า
- ปิดล็อกห้องเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
- ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณห้องควบคุม
- ติดป้ายเตือน ห้ามสูบบุหรี่ ห้ามนำอาหารและเครื่องดื่ม เข้ามารับประทาน หน้าห้องควบคุม
- กำหนดให้เจ้าหน้าที่คอมพิวเตอร์เป็นผู้ควบคุม ได้แก่
  - ลำดับที่ 1. นาย ยงยุทธ หารจันทร์ ผู้ควบคุมหลัก
  - ลำดับที่ 2. นาย ณิชพงศ์ เงามาม
  - ลำดับที่ 3. นาย ปัญญา จันทรสีนวล
  - ลำดับที่ 4. นาย จักรภานุ พองเรศ

### 1.2 การควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC) คอมพิวเตอร์พกพา (Notebook)

#### และโทรศัพท์เคลื่อนที่

- เครื่องคอมพิวเตอร์ทุกเครื่องทำการตั้งเวลาพักหน้าจอ (Screen saver)
- ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิงเช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างปฏิบัติงาน
- ห้ามติดตั้งอุปกรณ์หรือกระทำใด ๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาล โดยไม่ได้รับอนุญาต จากหัวหน้ากลุ่มงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบ หากเกิดการสูญเสีย/สูญหายโดยนำไปใช้ในทางที่ผิด ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย
- การกระทำใด ๆ ที่เกิดจากการใช้งาน อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง
- ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาล
- ห้ามบุคลากรทำการคัดลอกข้อมูลให้กับบุคคลภายนอก เว้นแต่ข้อมูลที่มีการเผยแพร่เป็นการทั่วไป
- เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และโทรศัพท์เคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่ รับผิดชอบทันที

### 4. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN)

- ผู้ดูแลระบบกำหนดค่าในการเข้ารหัสข้อมูล (Password) อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ทุกจุดบริการที่มีการติดตั้งอุปกรณ์ ทุกจุดมีรหัส Wifi
- ควบคุมดูแลไม่ให้อุปกรณ์หรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ ระบบและฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน