

# คู่มือการปฏิบัติงาน (Work Manual)

กระบวนการงาน การบริการ ระเบียบปฏิบัติ



งานเทคโนโลยีสารสนเทศและคอมพิวเตอร์  
โรงพยาบาลบ้านไร่

# คู่มือการปฏิบัติงาน (Work Manual)

กระบวนการงาน การบริการ ระเบียบปฏิบัติ

งานเทคโนโลยีสารสนเทศและคอมพิวเตอร์  
โรงพยาบาลบ้านไร่

จัดทำโดย	งานเทคโนโลยีสารสนเทศและคอมพิวเตอร์	ลายมือชื่อ
ผู้ตรวจสอบ	นางสาวรัตนภรณ์ รุทธะกาญจน์ หัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์	รัตนภรณ์ รุทธะกาญจน์
ผู้อนุมัติ	นายแพทย์วิชาญ แป้นทอง ผู้อำนวยการโรงพยาบาลบ้านไร่	

สารบัญ	หน้า
1. วัตถุประสงค์.....	3
2. ขอบเขต.....	3
3. คำจำกัดความ.....	3
4. หน้าที่ความรับผิดชอบ.....	4
5. Work Flow กระบวนการ.....	5
6. ขั้นตอนการปฏิบัติงาน.....	6
7. มาตรฐานคุณภาพงาน.....	8
8. ระบบติดตามประเมินผล.....	8
9. เอกสารอ้างอิง.....	9
10. แบบฟอร์มที่ใช้.....	9

#### ภาคผนวก

1. กฎระเบียบ/คำสั่ง
2. ตัวอย่างแบบฟอร์ม
3. รายชื่อผู้จัดทำ

## วัตถุประสงค์

๑. เพื่อวางแผนปฏิบัติ การใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กร ให้ปฏิบัติเป็นแนวทางเดียวกัน
๒. เพื่อให้ผู้ปฏิบัติงานใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย
๓. เพื่อให้การใช้งานเครือข่าย ระบบคอมพิวเตอร์ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ
๔. เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่าย ระบบคอมพิวเตอร์ ในลักษณะที่ไม่ถูกต้อง
๕. เพื่อให้ผู้ใช้งานรับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
๖. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

## คำนิยาม

๑. **องค์กร** หมายถึง โรงพยาบาลบ้านไร่
๒. **หน่วยงาน** หมายถึง กลุ่มงาน งาน ภายใต้โครงสร้างการบริหารงานโรงพยาบาลบ้านไร่
๓. **ผู้บริหารหน่วยงาน** หมายถึง ผู้มีอำนาจด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมและการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์
๔. **ผู้ใช้งาน** หมายความว่า บุคลากร และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือ จดหมายอิเล็กทรอนิกส์ ที่ทางงานเทคโนโลยีสารสนเทศและคอมพิวเตอร์ จัดสรรให้
๕. **ผู้ดูแลระบบ** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศหรือระบบเครือข่าย หรือระบบคอมพิวเตอร์
๖. **เจ้าหน้าที่** หมายความว่า เจ้าหน้าที่องค์กร ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ของโรงพยาบาลบ้านไร่
๗. **สิทธิ์ของผู้ใช้งาน** หมายความว่า สิทธิ์ทั่วไป สิทธิ์เฉพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลบ้านไร่
๘. **สินทรัพย์** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของโรงพยาบาลบ้านไร่ เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
๙. **การเข้าถึงและการควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
๑๐. **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
๑๑. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายความว่า การเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๑๒. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑๓. **ระบบเครือข่าย** หมายความว่า กลุ่มของคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และสื่อสัญญาณ ที่ถูกนำมา เชื่อมต่อกัน ผ่านอุปกรณ์ด้านสื่อสารหรือสื่ออื่นใด และทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและ ใช้อุปกรณ์หรือทรัพยากรต่าง ๆ ของเครือข่ายร่วมกันได้ โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายใน (Local Area Network : LAN) ซึ่งอาจจะใช้การเชื่อมต่อแบบมีสายหรือไร้สายก็ได้ และเครือข่ายบริเวณกว้าง (Wide Area Network : WAN) ของโรงพยาบาลบ้านไร่

๑๔. **ระบบสารสนเทศ** หมายความว่า ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ฮาร์ดแวร์ (Hardware), ซอฟต์แวร์ (Software), บุคคล(People), ข้อมูล (Data) และขบวนการ (Procedure) ซึ่งทุกองค์ประกอบดังกล่าว ข้างต้นจะทำงานร่วมกัน เพื่อกำหนด รวบรวม จัดเก็บ และประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และผู้ใช้งานจะนำ สารสนเทศที่ได้มาช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และ ติดตามผลการดำเนินงานของโรงพยาบาลบ้านไร่

๑๕. **การใช้งานอินเทอร์เน็ต** หมายความว่า การใช้บริการต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต ของโรงพยาบาล บ้านไร่

๑๖. **คอมพิวเตอร์** หมายความว่า เครื่องมือหรืออุปกรณ์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์และ อินเทอร์เน็ต ของโรงพยาบาลบ้านไร่

๑๗. **ข้อมูลคอมพิวเตอร์** หมายความว่า ข้อมูล ข้อความ คาสั่ง ชุดคำสั่ง ซอฟต์แวร์ แฟ้มข้อมูล หรือสิ่งอื่นใดที่ ป้อนเข้าไปหรืออยู่ในคอมพิวเตอร์ ในสภาพที่คอมพิวเตอร์อาจประมวลผลได้ และให้หมายรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๘. **รหัสผ่าน** หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัว บุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยี สารสนเทศ

๑๙. **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดย ผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข้อมูลดังกล่าวไปยังผู้รับคนเดียวหรือหลายคนก็ได้

๒๐. **ชุดคำสั่งไม่พึงประสงค์** หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือ ชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมข้อขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่ กำหนดไว้

## **แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ**

### **วัตถุประสงค์**

- (๑) เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- (๒) เพื่อกำหนดหลักเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของผู้บริหาร วิทยาลัยพยาบาลบ้านไร่
- (๓) เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

## แนวปฏิบัติ

### ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ หรือเจ้าของข้อมูล หรือเจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านไร่ จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการโรงพยาบาลบ้านไร่ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๑.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๑.๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านไร่ จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการโรงพยาบาลบ้านไร่ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๒.๑) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๒.๒) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความ

เสียหายร้ายแรงที่สุด

เสียหายร้ายแรง

- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความ

- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๒.๓) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

ข้อ ๔ ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของโรงพยาบาล บ้านไร่ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลง สิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๖ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งระบบสารสนเทศเพื่อเป็นหลักฐานในการ ตรวจสอบ

ข้อ ๗ กำหนดระยะเวลาเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา

(๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่โรงพยาบาลบ้านไร่ กำหนด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ

๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้เพื่อ แสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙ ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ อินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์ อักษร

ข้อ ๑๐ ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อ ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้า ใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน ทำการ หรือ เมื่อเปลี่ยนแปลงตำแหน่งต้องดำเนินการภายใน ๗ วัน ทำการ

ข้อ ๑๑ การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้และรหัสผ่านต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๗) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นกำหนดระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับ ว่าสามารถเข้าถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๑๒ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) กำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นาสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๗) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ ๑๓ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้ผู้อำนวยการพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างโรงพยาบาลบ้านไร่ กับหน่วยงานที่มาขอเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล



- (๓) พิจารณาวามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน
- (๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- (๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกัน

เพียงพอ

### ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔ การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- (๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน
- (๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)
- (๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว
- (๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- (๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- (๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- (๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๕ การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

ข้อ ๑๖ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้ เป็นความรับผิดชอบ ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๗ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของโรงพยาบาลบ้านไร่ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากใส่รหัสผิดเกิน ๓ ครั้งก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- (๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนก่อนการใช้งานทุกครั้ง
- (๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
- (๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย

๑๕ นาที

ข้อ ๑๘ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าจะข้อมูลนั้นจะเป็นของโรงพยาบาลบ้านไร่ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของโรงพยาบาลบ้านไร่ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้อำนวยการ

ข้อ ๒๐ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลบ้านไร่ และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๒ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลบ้านไร่ จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้อำนวยการที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลบ้านไร่ ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลบ้านไร่ ซึ่ง โรงพยาบาลบ้านไร่อาจแต่งตั้งให้ผู้ที่ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๓ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายความว่า วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้มข้อมูล (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิททอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการ

ข้อ ๒๔ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างปฏิบัติงาน

ข้อ ๒๕ ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านไร่ ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลบ้านไร่

ข้อ ๒๖ ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านไร่ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้การโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาลบ้านไร่

ข้อ ๒๗ ห้ามใช้สินทรัพย์ของโรงพยาบาลบ้านไร่ เพื่อประโยชน์ทางการค้า ที่มีใช้ภารกิจของโรงพยาบาลบ้านไร่

ข้อ ๒๘ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะ เป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลบ้านไร่ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๙ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลบ้านไร่ ต้องหยุดชะงัก

ข้อ ๓๐ ห้ามใช้ระบบสารสนเทศของโรงพยาบาลบ้านไร่ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๑ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๒ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลบ้านไร่ โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

#### ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๓ ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Operation Center หมายความว่า สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๕ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๖ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

ข้อ ๓๗ ผู้ใช้งานต้องทำลายข้อมูลในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	- ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีทุบหรือบดให้เสียหาย

ข้อ ๓๘ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่โรงพยาบาลบ้านไร่ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset Lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือการคืนสินทรัพย์ จะถูกบันทึกและการตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๓๙ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบต่อสินทรัพย์ของโรงพยาบาลบ้านไร่ ที่ได้รับมอบหมาย

ข้อ ๔๐ ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหาย ตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๑ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่ากรณีใด ๆ เว้นแต่การยืมนั้นได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๔๒ ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่โรงพยาบาลบ้านไร่ จัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลบ้านไร่ เท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์ของระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่โรงพยาบาลบ้านไร่ ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาลบ้านไร่

ข้อ ๔๓ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

## ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๔ มาตรการควบคุมการเข้า-ออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกในสมุดบันทึก “ขออนุญาตเข้า-ออกห้อง Server (บุคคลภายนอก)”

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในรูปแบบฟอร์มการขออนุญาต “ขอใช้งานระบบอินเทอร์เน็ต (บุคคลภายนอก)” ให้ถูกต้องชัดเจน

ข้อ ๔๕ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของโรงพยาบาลบ้านไร่ ต้องได้รับอนุญาตจากผู้อำนวยการและต้องปฏิบัติตามแนวปฏิบัตินี้โดยเคร่งครัดโดยผู้ใช้ต้องกรอกแบบฟอร์ม “แบบขอใช้บริการอินเทอร์เน็ตผ่านเครือข่ายโรงพยาบาลบ้านไร่”

ข้อ ๔๖ การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งานอื่น

ข้อ ๔๗ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณ (Switch) อุปกรณ์เชื่อมต่อระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๘ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของโรงพยาบาลบ้านไร่ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายทั้งหมดต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลบ้านไร่ ในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในโรงพยาบาลบ้านไร่ โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของโรงพยาบาลบ้านไร่

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ที่สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้ หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “แบบขอใช้บริการอินเทอร์เน็ตผ่านเครือข่ายโรงพยาบาลบ้านไร่”

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้ใช้อุปกรณ์

ข้อ ๔๙ ผู้ดูแลระบบ ต้องบริหาร ควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๕๐ การติดตั้งหรือปรับปรุงซอฟต์แวร์ระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบก่อนดำเนินการ

ข้อ ๕๑ กำหนดให้มีการจัดเก็บซอร์สโค้ด โลบาร์ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๒ การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๕๐

ข้อ ๕๓ กำหนดมาตรฐานควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกโรงพยาบาลบ้านไร่ เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคลากรจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาลบ้านไร่ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการ

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าถึงข้อมูลและระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการ

(๔) การเข้าถึงระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินการกับโรงพยาบาลบ้านไร่ อย่างเพียงพอ

(๕) การเข้าถึงระบบเครือข่ายภายในและระบบสารสนเทศในโรงพยาบาลบ้านไร่ จากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน ด้วยการใส่รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๔ กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามความจำเป็นในการใช้งาน เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๕๕ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งให้บุคคลที่เกี่ยวข้องได้รับทราบทุกครั้ง

ข้อ ๕๖ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกโรงพยาบาลบ้านไร่ ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๗ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบ้านไร่ ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๘ IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้อุปกรณ์ภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๕๙ การใช้งานเครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

## ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๐ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลบ้านไร่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในโรงพยาบาลบ้านไร่ เป็นต้น

ข้อ ๖๑ กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งานทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านไร่ ร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่ได้อยู่ที่หน้าจอเป็นเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการ

(๘) ซอฟต์แวร์ที่โรงพยาบาลบ้านไร่ ใช้นิสิทธิ์ ผู้ใช้งานสามารถขอใช้ได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟต์แวร์ที่โรงพยาบาลบ้านไร่ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทาสีเนาเพื่อนำไปใช้งานที่อื่น

(๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลบ้านไร่ เพื่อประโยชน์ทางการค้า

(๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม  
กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๒) ห้ามผู้ใช้งานของโรงพยาบาลบ้านไร่ ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้  
อำนวยการ

ข้อ ๖๒ การระบุยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตน  
ด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๖๓ การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรม  
ยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยง  
มาตรการป้องกันทางด้านความมั่นคงของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความปลอดภัยที่ได้  
กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการ  
เข้าใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้  
งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๖๔ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งาน  
สามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงาน  
กำหนดเท่านั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง  
(ในที่สาธารณะหรือพื้นที่ภายนอกโรงพยาบาลบ้านไร่) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

## ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๕ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น  
รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยน  
ตำแหน่งภายในโรงพยาบาลบ้านไร่ เป็นต้น

ข้อ ๖๖ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง  
ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการลงบันทึกเข้าใช้  
งานก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๖๗ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิก  
การใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(ก) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(ข) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากระหัสผู้ใช้งานตามปกติ

ข้อ ๖๘ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นาสินทรัพย์ออกนอกโรงพยาบาลบ้านไร่ เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๖๙ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

ข้อ ๗๐ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น



## ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malware)

ข้อ ๗๑ โรงพยาบาลบ้านไร่ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่โรงพยาบาลบ้านไร่ อนุญาตให้ใช้งานหรือที่โรงพยาบาลบ้านไร่ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้ได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่า เป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๒ ซอฟต์แวร์ ที่โรงพยาบาลบ้านไร่ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำ การ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากผู้อำนวยการหรือ ผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๗๓ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่โรงพยาบาลบ้านไร่ ได้ ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากผู้อำนวยการ

ข้อ ๗๔ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๕ ผู้ใช้งานต้องการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๖ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ ผู้ดูแลระบบ

ข้อ ๗๗ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๗๘ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของ โรงพยาบาลบ้านไร่ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้อำนวยการ

ข้อ ๗๙ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ ทรัพย์สินของโรงพยาบาลบ้านไร่ สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ ดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำใน ลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแก็งรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครอง ทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับ หนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์ (License) การใช้ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณี อันติงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๘๐ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มียุติในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทากับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอกโรงพยาบาลบ้านไร่ ต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

#### ส่วนที่ ๙ การควบคุมการเข้าระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๘๑ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๘๒ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สายมาใช้งาน

ข้อ ๘๓ ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย

ข้อ ๘๔ ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งานและรหัสผ่าน ของผู้ใช้งานที่มีสิทธิ์ในการใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๘๕ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายนอกโรงพยาบาลบ้านไร่

ข้อ ๘๖ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในโรงพยาบาลบ้านไร่ผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกจากระบบเครือข่ายไร้สาย

ข้อ ๘๗ ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๘๘ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ รายงานต่อผู้อำนวยการทราบทันที

ข้อ ๘๙ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินเทอร์เน็ต และฐานข้อมูลภายในต่าง ๆ

ข้อ ๙๐ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลบ้านไร่ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการอย่างเป็นทางการเป็นลายลักษณ์อักษร

ข้อ ๙๑ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

## แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล วัตถุประสงค์

- (๑) เพื่อให้ระบบสารสนเทศของโรงพยาบาลบ้านไร่ สามารถให้บริการได้อย่างต่อเนื่อง
- (๒) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับโรงพยาบาลบ้านไร่ อย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
- (๓) เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

## แนวปฏิบัติ

### ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- บ้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านไร่ จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการวิจัย การพัฒนา การให้บริการและเทคโนโลยีที่เกี่ยวข้อง เช่น สถิติผู้ใช้บริการ ผลงานวิจัย เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง

- ข้อมูลที่มีระดับความสำคัญน้อย
- (๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล
  - ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
  - ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
  - ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
  - ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) การกำหนดเวลาที่ได้เข้าถึง

(๓.๕) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒ ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานะข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ เรื่อง แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ข้อ ๑๒

ข้อ ๔ หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างหน่วยงาน หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากหน่วยงานภายนอกให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างโรงพยาบาลบ้านไร่ กับหน่วยงานภายนอกดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิ์การเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

## ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดหาระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจาเป็นมากไปน้อย

ข้อ ๗ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง ต้องห่างกันเพียงพอเพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติ

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๐ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

ข้อ ๑๓ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่เกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๔ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

## แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

### วัตถุประสงค์

(๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

(๒) เพื่อการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ

(๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

### แนวปฏิบัติ

#### ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงาน ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑ จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทाराายงานพร้อมข้อเสนอแนะ

ข้อ ๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจสอบประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือที่เข้าถึง โดยไม่ได้รับอนุญาต

## ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

**ประเภทที่ ๑** ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงาน ขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมหรือประชาสัมพันธ์สำหรับเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนเรื่องระเบียบปฏิบัติในการใช้งานคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

**ประเภทที่ ๒** ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกหลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti-Virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

**ประเภทที่ ๓** ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า ถือเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

**ประเภทที่ ๔** ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำให้ความเสียหายให้กระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

- (๑) เผื่อสำรองภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา
- (๒) ถอดเทป Backup ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย
- (๓) ดำเนินการตัดระบบไฟฟ้าในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ โดยปิดเบรกเกอร์ที่เกี่ยวข้อง เพื่อป้องกันอุปกรณ์เสียหาย และป้องกันภัยจากไฟฟ้า
- (๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง
- (๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องปฏิบัติการเครือข่ายคอมพิวเตอร์สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
- (๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถใช้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่
- (๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

## **แนวปฏิบัติในการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม**

### **วัตถุประสงค์**

(๑) เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการใช้งานหรือเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

### **แนวปฏิบัติ**

ข้อ ๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายความว่า ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

- (๑) กำหนดเป็นเขตห้ามห้ามนัดเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี
- (๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า - ออก ของบุคคลเป็นจำนวนมาก
- (๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว
- (๔) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
- (๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกจากบริเวณดังกล่าว
- (๖) อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด
- (๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต



ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้าออก อาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งาน มีสิทธิ์ผ่านเข้า - ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) ให้มีการบันทึกวันและเวลาการเข้า - ออก พื้นที่สำคัญของผู้ที่มาติดต่อ

(๓) จัดเก็บบันทึกการเข้า - ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้อง Server เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๔) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๕) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงาน ที่เพียงพอต่อความต้องการใช้งานโดยมีระบบ ดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้น อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีทีระบบสนับสนุนการทำงานภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงาน ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

ข้อ ๘ การนำทรัพย์สินของหน่วยงาน ออกจากหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของ สช. ออกจากใช้งานนอก สช. เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอก สช. (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของ สช. ออกจากใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของ สช. ไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

### 3. คำจำกัดความ

มาตรฐาน คือ สิ่งที่เราเป็นเกณฑ์สำหรับเทียบกำหนด ทั้งในด้านปริมาณ และคุณภาพ(พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542)มาตรฐานการปฏิบัติงาน (Performance Standard) เป็นผลการปฏิบัติงานในระดับใดระดับหนึ่งซึ่งถือว่าเป็นเกณฑ์ที่น่าพอใจหรืออยู่ในระดับที่ผู้ปฏิบัติงานส่วนใหญ่ทำได้ โดยจะมีกรอบในการพิจารณากำหนดมาตรฐานหลาย ๆ ด้าน อาทิ ด้านปริมาณ คุณภาพ ระยะเวลา ค่าใช้จ่าย หรือพฤติกรรมของผู้ปฏิบัติงานIT

Help Desk = ศูนย์บริการให้ความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่าย

ผู้รับบริการ = ชำราชการและเจ้าหน้าที่ผู้ปฏิบัติงานของโรงพยาบาลน่าน

ผู้ประสานงานด้านเทคนิค = เจ้าหน้าที่ผู้ประสานงานด้านการให้ความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่ายของศูนย์เทคโนโลยีสารสนเทศ

เจ้าหน้าที่ผู้ปฏิบัติงาน = เจ้าหน้าที่ผู้รับมอบหมายให้ดำเนินการให้ความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่ายของศูนย์เทคโนโลยีสารสนเทศ

SLA (Service Level Agreement) = ข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับผู้รับบริการ เพื่อเพิ่มความมั่นใจแก่ผู้รับบริการว่าเจ้าหน้าที่จะสามารถให้บริการได้ตามระยะเวลาแต่ละกระบวนการที่กำหนดไว้ ไม่ถือเป็นข้อผูกพัน อาจมีการเปลี่ยนแปลงได้

ไบเสนอส/ส่งซ่อม/ติดตั้ง = แบบบันทึกการรับแจ้งขอความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่าย

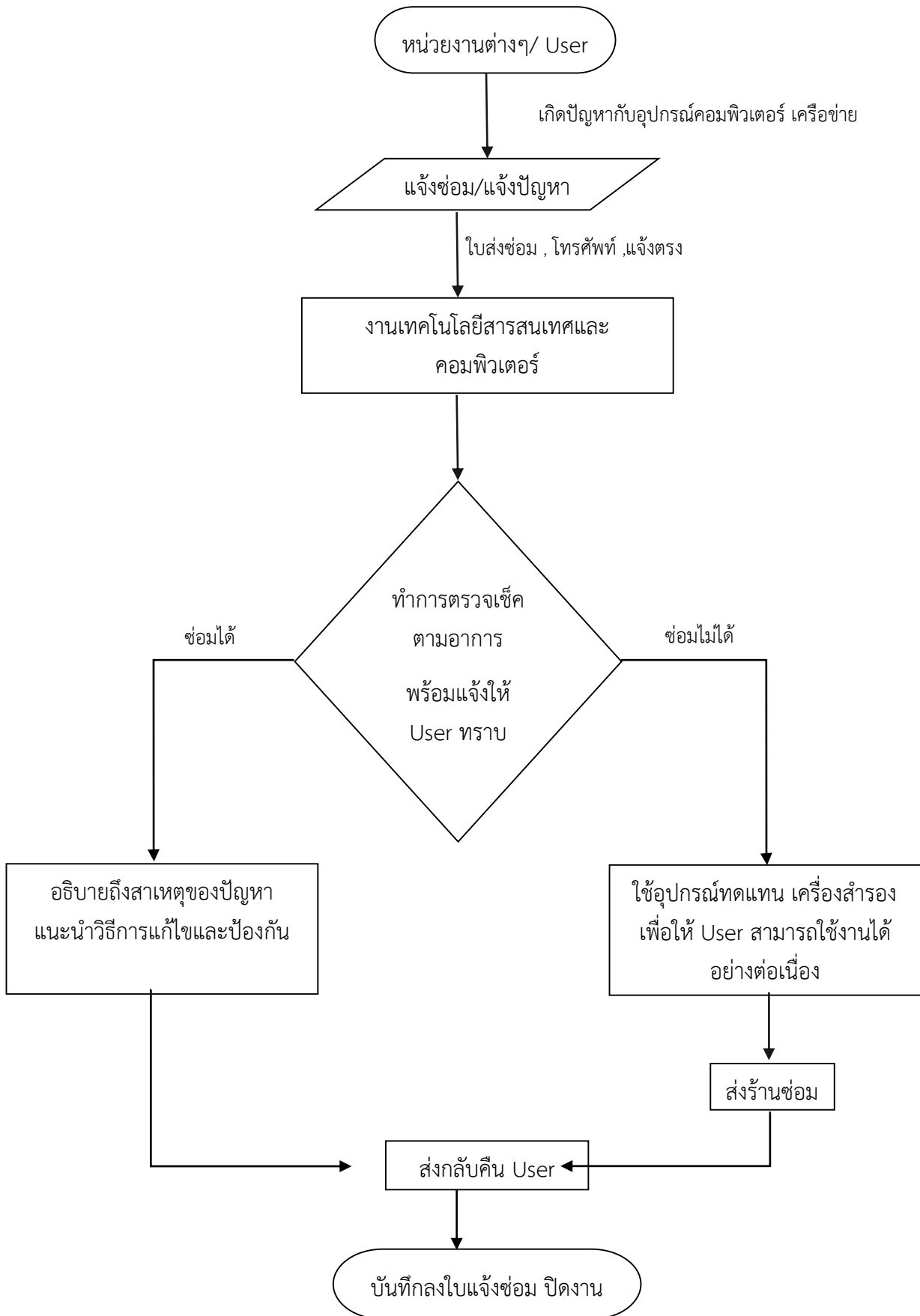
### 4. หน้าที่ความรับผิดชอบ

1. ผู้อำนวยการโรงพยาบาลบ้านไร่ทำหน้าที่อนุมัติแผนการดำเนินงานพร้อมทั้งมอบหมายกำกับ ติดตามการปฏิบัติงานของผู้ที่ได้รับมอบหมาย
2. คณะทำงานบริการและจัดการความรู้ด้านเทคโนโลยีสารสนเทศและคอมพิวเตอร์มีหน้าที่ความรับผิดชอบดังต่อไปนี้
  - 2.1 จัดทำแผนการดำเนินงานและแนวทางการบริหารจัดการระบบการให้บริการและจัดการด้านความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
  - 2.2 บริหารจัดการระบบการให้บริการและจัดการด้านความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารให้สามารถดำเนินการตามแผนและแนวทางได้อย่างมีประสิทธิภาพ
  - 2.3 ประสาน ติดตามการดำเนินงาน และรวบรวมข้อมูล รวมถึงรายงานผลการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้บริหาร
  - 2.4 ส่งเสริมให้เกิดการถ่ายทอดองค์ความรู้ระดับหน่วยงานและผู้ปฏิบัติงาน ให้สามารถนำความรู้ไปใช้สนับสนุนในการปฏิบัติงาน

### 5. Work Flow กระบวนการการปฏิบัติงานการบริการด้านระบบคอมพิวเตอร์และเครือข่าย

#### 5.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์ หมายเลข 121

ผังงาน (Flowchart) กระบวนการทำงานบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย



## 6. ขั้นตอนการปฏิบัติงาน

### 6.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์

ผู้รับบริการ

1. แจ้งปัญหา/ขอรับบริการขอความช่วยเหลือผ่านทางโทรศัพท์หมายเลข 121
2. รับคำตอบหรือวิธีการแก้ไขปัญหาผู้ประสานงานด้านเทคนิค
  1. เมื่อผู้รับบริการแจ้งขอรับความช่วยเหลือ ผู้ประสานงานด้านเทคนิคต้องทำการบันทึกค่าแจ้งลง ใบเสนอ/ส่งซ่อม/ติดตั้ง
  2. ทำการวิเคราะห์ปัญหาที่ได้รับแจ้ง
  3. ทำการตอบคำถามหรือแนะนำวิธีการแก้ไขปัญหา
    - 3.1 ในกรณีที่สามารถตอบได้ทันที ผู้ประสานงานด้านเทคนิคจะทำการแนะนำวิธีการแก้ไขปัญหาให้ผู้รับบริการทราบทันที
    - 3.2 ในกรณีที่ไม่สามารถตอบได้ทันที ผู้ประสานงานด้านเทคนิคจะต้องดำเนินการดังนี้
      - ทำการแจ้งเวลาโทรกลับให้ผู้รับบริการทราบ
      - ประสานนักวิชาการหรือผู้เชี่ยวชาญให้คำตอบหรือวิธีการแก้ไขปัญหาทำการแจ้งวิธีการแก้ไขปัญหาให้ผู้รับบริการทราบ