
# นโยบายความมั่นคงปลอดภัยและการสำรองข้อมูล

กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศ

โรงพยาบาลท่าชนะ

# นโยบายความมั่นคงปลอดภัยและการสำรองข้อมูล
## (Backup Policy)

**1.วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรฐานในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักในการทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้ เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

**2. แนวทางปฏิบัติในการสำรองข้อมูล**

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบซอฟต์แวร์ วันที่ เวลา ที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานทีอื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรอง อย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเกตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ ภายในระยะเวลาที่เหมาะสม

**โรงพยาบาลท่าชนะ ประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ พ.ศ.2563**

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลลับแลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะ เกิดขึ้นจากการใช้งานในระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลลับแลจึงเห็นสมควรกำหนดนโยบาย ดังนี้

1. โรงพยาบาลท่าชนะส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

2. โรงพยาบาลท่าชนะมีหน้าที่ จำกัด ระงับ เพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสม หากมี การละเมิดหรือฝ่าฝืนแนวปฏิบัติ ในกรณีสำคัญคณะกรรมการสารสนเทศและคอมพิวเตอร์รายงานการฝ่าฝืนให้ ต้นสังกัดหรือโรงพยาบาลพิจาณาลงโทษ

3. โรงพยาบาลท่าชนะสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์ และ พร้อมใช้งานอยู่เสมอ

4. โรงพยาบาลท่าชนะสนับสนุนการรักษาความปลอดภัยของข้อมูลตามแนวปฏิบัติ เพื่อ การปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ 4 มกราคม พ.ศ.2564

(นายแพทย์กฤษนันท์ เหล่ายัง)
ผู้อำนวยการโรงพยาบาลท่าชนะ

# แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
# (Network and Server Policy)

**1.วัตถุประสงค์**

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และ ระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของ หน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

**2.แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย**

โรงพยาบาลท่าชนะ กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server)
ดังนี้

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น
โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุก รุกได้อย่างเป็นระบบ

2.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบ เครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

2.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่ หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการ กระทำของระบบและผู้ใช้บริการอื่นๆ

2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้ง เพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

2.5 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

2.5.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะ ระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบ เครือข่ายที่มีการใช้งานร่วมกัน

2.5.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยัง เครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้

2.5.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

2.5.4 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งาน ระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

2.5.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้อง มีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication)เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

2.5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

2.5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อม ทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.5.8 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจาก ผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.5.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบใน การดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

2.6 โรงพยาบาลท่าชนะ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

2.6.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับ อนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือ บุคคลที่หน่วยงานมอบหมาย

2.6.2 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึก การเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน CommandLine และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บ บันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

2.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

2.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆและจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2.7 โรงพยาบาลท่าชนะ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

2.7.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและ เครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์ อักษร เพื่อขออนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกัน สุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์

2.7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์ และสารสนเทศทางการแพทย์

2.7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

# แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล
# (Backup Policy)

**1.วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรฐานในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลัก ในการทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

**2. แนวทางปฏิบัติในการส ารองข้อมูล**

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรอง ข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงาน จากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูล สำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเกตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ ภายในระยะเวลาที่เหมาะสม

# แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
# (Physical and Environment Security)

**1.วัตถุประสงค์**

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้ งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญ ของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบ เทคโนโลยีสารสนเทศของหน่วยงาน

**2.แนวทางปฏิบัติการรักษาความมั่งคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม**

2.1 ให้กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ เป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนแสดง ตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2.2 ให้กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ เป็นผู้กำหนด สิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.3 ให้กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ เป็นผู้กำหนด มาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรือ อุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายใน แบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และ ต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

# แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

**1. วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความ เสียหายแก่ข้อมูล หรือการท างานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถ ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่าง ถูกต้อง

**2.แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ**

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่าชนะ มี ดังนี้

**2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ**

2.1.1 โรงพยาบาลท่าชนะ กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขอ อนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยีสารสนเทศ

2.1.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบ ข้อมูลให้เหมาะสมกับการเข้าใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ใน การปฏิบัติงานก่อนเข้าระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.1.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบเทคโนโลยี สารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

2.1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลง สิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับการอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

**2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ**

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลท่าชนะกำหนดให้ มีขั้นตอน ปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการ เปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่นระบบ คอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E - mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดย ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับ บัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.2.3 ผู้ดูแลระบบต้องบริหารจัดการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

2.2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

2.2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยง การใช้บุคคลอื่นหรือส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกัน ในการส่งรหัสผ่าน

2.2.3.3 ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

2.2.3.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ใน รูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานตามปกติ

2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึง ระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับของข้อมูล

2.2.4.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.2.4.4 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่น SSL VPN หรือ XML Encryption เป็นต้น

2.2.4.5 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความ สำคัญของข้อมูล

2.2.4.6ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

**2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ**

2.3.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของ เครื่องคอมพิวเตอร์ของหน่วยงาน

2.3.2 ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้เครื่อง คอมพิวเตอร์ของหน่วยงานร่วมกัน

2.3.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้ งาน

2.3.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า 1 ชม.

# แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต
# (Internet Security Policy)

**๑. วัตถุประสงค์**

เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลท่าชนะ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ ต่างๆ ที่ ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพ กฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเตอร์เน็ต เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

**๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเตอร์เน็ต**

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลท่าชนะมีหน้าที่และความรับผิดชอบที่ต้อง ปฏิบัติดังนี้

๒.๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการ เครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลท่าชนะ โดยสามารถใช้งานได้ ๑ วัน เพื่อรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งาน โดยผู้ใช้งานต้องเป็นบุคลากร สังกัดโรงพยาบาลท่าชนะ สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒.๒ ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชนในเชิงพาณิชย์เป็นการส่วน บุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่ มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๓ ผู้ใช้งานอินเตอร์เน็ตจึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ ส่งผ่านระบบเครือข่าย

๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การ ละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๒.๕ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการ อัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๒.6 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ เฟสบุค โปรแกรมอื่น ๆ ที่มีลักษณะ คล้ายกัน โดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับ บุคลากรของหน่วยงานอื่นๆ

2.7 หลังการใช้งานระบบอินเตอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจาก เครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

## แนวทางปฏิบัติการรักษาความมั่นคง
## จดจำง่ายด้วย

### ปกปิด

ต้องเก็บ Username และ Password
เป็นความลับ ไม่เปิดเผยต่อผู้อื่น
เป็นสิทธิ์ใช้งานเฉพาะบุคคล

### ปกป้

ต้อง Login
หลังเลิกใช้
อย่าทิ้งหน้าจอไว้

### เปิดเผย


ต้องได้รับการอนุมัติ
เป็นลายลักษณ์อักษรก่อนการเผยแพร่
ข้อมูลในเว็บไซต์โรงพยาบาล

### ปลด

ห้ามนำอุปกรณ์
กับระบบเน็ตเวิร์ค
โดยไม่ได้