นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยใน ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลฟากท่า ปี 2567

ศูนย์เทคโนโลยีสารสนเทศ
โรงพยาบาลฟากท่า

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับองค์กรที่เข้ามาช่วยอำนวยความ สะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่นการรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้นซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้ายหรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูและระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัย ด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลฟากท่า จึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสานสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสานสนเทศ จากทุกหน่วยและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้อง กับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการอำนวยการและกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงหวังเป็นอย่างยิ่งว่าแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสานสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริหาร ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่าทุกคนในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการอำนวยการและกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลฟากท่า เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

นางสาวพรสวรรค์ มีชิน
ผู้อำนวยการโรงพยาบาลฟากท่า

สารบัญ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลฟากท่า

1. หลักการและเหตุผล ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวทางปฏิบัติการรักษาความ มั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่า เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลฟากท่าจึงเห็นสมควรกำหนดนโยบายและแนวทาง ปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความ มั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

2. วัตถุประสงค์

2.1. การจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยี สารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและ ประสิทธิผล

2.2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

2.3. นโยบายและแนวทางปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับ ทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบ เทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.5. นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตาม ระยะเวลาอย่างน้อย 1 ครั้ง ต่อปี

3. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลฟากท่า

3.1 โรงพยาบาลฟากท่าส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศ ให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

3.2 โรงพยาบาลฟากท่ามีหน้าที่จำกัด ระงับ เพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสมหากมี การละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญศูนย์เทคโนโลยีสารสนเทศรายงานการฝ่าฝืน ให้ต้นสังกัดหรือโรงพยาบาลเพื่อพิจารณาลงโทษ

3.3 โรงพยาบาลฟากท่าสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อม ใช้งานอยู่เสมอ

3.4 โรงพยาบาลฟากท่าสนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

4. องค์ประกอบของแนวทางปฏิบัติ

4.1. คำนิยาม

4.2. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

4.3. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

4.4. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

4.5. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

4.6. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

4.7. การรักษาความมั่นคงปลอดภัยของอีเมล์

4.8. การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

4.9. การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

4.10. ความมั่นคงปลอดภัยของการสำรองข้อมูล

4.11. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมี มาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลด ความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่าง มั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความ ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลฟากท่า

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจใน ด้านเทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่า ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของ การกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศ หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้าน เทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย ภายในโรงพยาบาลฟากท่า

หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบ เทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่า และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายใน โรงพยาบาลฟากท่า

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลฟากท่า

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้ สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแล รักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่ง โรงพยาบาลฟากท่ากำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลฟากท่า เช่น ผู้อำนวยการโรงพยาบาลฟากท่า รองผู้อำนวยการโรงพยาบาล หัวหน้าตึก หัวหน้ากลุ่มงาน เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มี หน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรม คอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำ โครงการต่างๆ ของโรงพยาบาลฟากท่า

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลฟากท่า อนุญาตให้มีสิทธิ์ใน การเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตาม อำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัด ระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำ หน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น ระบบแลน (LAN) และ

ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่ เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการ ติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายใน

หน่วยงาน ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ หน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้ บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบ เครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบ เทคโนโลยีสารสนเทศ สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ หน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบ อำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทาง กายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความ ถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึง คุณสมบัติในด้าน ความถูกต้องแท้จริง

(authenticity) ความรับผิด (accountability) การห้าม ปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิด เหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบาย ด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจ เกี่ยวข้องกับความมั่นคงปลอดภัย **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตรี และความมั่นคง ปลอดภัยถูกคุกคาม **จดหมายอิเล็กทรอนิกส์ (Email)** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพ กราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือ ชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ ตรงตามคำสั่งที่กำหนดไว้

การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทาให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูลของโรงพยาบาลฟากท่า โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย

1 ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

1) หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต

(1) อนุมัติสิทธิเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

(2) อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

2) ผู้ดูแลห้องควบคุมระบบเครือข่าย

ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ปฏิบัติการให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

2 กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย มีแนวทางปฏิบัติดังนี้

1) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้อง และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูและระบบ (System Administrator) เป็นต้น

2) สิทธิในการเข้าออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

3) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

4) การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มหรืออุปกรณ์บันทึกข้อมูลการเข้าออกพื้นที่

3 แนวปฏิบัติการจัดทำเอกสารระบุสิทธิในการเข้าถึงพื้นที่ มีดังนี้

1) กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและช่วงเวลาที่มีสิทธิในการผ่านเข้าออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

2) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ ที่ออกโดยหน่วยงานราชการ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทาการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

3) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในโรงพยาบาลฟากท่า

4) เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้องและต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

5) บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับ

เจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

6) ผู้ใช้จะได้รับสิทธิให้เข้าออกพื้นที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

7) หากมีบุคคลอื่นที่ไม่ใช้ผู้ใช้ขอเข้าพื้นที่ โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจาตัวที่หน่วยงานราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

มาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลฟากท่าได้อย่างถูกต้อง

วัตถุประสงค์

1) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของโรงพยาบาลฟากท่า

2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับโรงพยาบาล ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1) ศูนย์เทคโนโลยีสารสนเทศ
2) ผู้ดูแลระบบที่ได้รับมอบหมาย
3) เจ้าหน้าที่ที่ได้รับมอบหมาย
4) ผู้ใช้งาน

แนวทางปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

1.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ

การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ให้ผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง มีดังนี้

1) สิทธิ์อ่านอย่างเดียว
2) สิทธิ์การเพิ่มข้อมูล
3) สิทธิ์การแก้ไขข้อมูล

4) สิทธิ์การลบข้อมูล
5) สิทธิ์การอนุมัติ/อนุญาต
6) ไม่มีสิทธิ์

1.2 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

การแบ่งประเภทของข้อมูลและการจัดลาดับความสำคัญหรือลาดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และพระราชบัญญัติข้อมูลข่าวสารของราชการพ.ศ. 2540 ซึ่งเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

1) **การจัดแบ่งประเภทของข้อมูล** ออกเป็น
(1) ข้อมูลที่เปิดเผยได้ทั่วไป
(2) ข้อมูลที่เปิดเผยเฉพาะ ที่มีการจากัดการเข้าถึง ได้แก่ ข้อมูลเชิงบริหาร ข้อมูลส่วนบุคคล ข้อมูลการรักษา

2) **การจัดแบ่งระดับความสำคัญของข้อมูล** ออกเป็น 4 ระดับ คือ
(1) ข้อมูลที่มีระดับความสำคัญมากที่สุด
(2) ข้อมูลที่มีระดับความสำคัญมาก
(3) ข้อมูลที่มีระดับความสำคัญปานกลาง
(4) ข้อมูลที่มีระดับความสำคัญน้อย

การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูล ด้วยวิธีการประเมินผลกระทบของปัญหา คุณภาพข้อมูลที่มีต่อองค์กร ซึ่งฐานข้อมูลแต่ละระบบจะมีความสำคัญต่อกระบวนการทำงานไม่เท่ากัน หากข้อมูลใดมีปัญหา ไม่สมบูรณ์ จะมีผลกระทบต่อกระบวนการทำงานหลักมาก ทำให้หน่วยงานไม่สามารถดำเนินงานที่สำคัญได้ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูล มีดังนี้

[1] พิจารณาจากวิธีการเชื่อมโยงข้อมูล โดยเปรียบเทียบประโยชน์และความเป็นไปได้

[2] พิจารณาจากความพยายามที่จะเชื่อมโยงข้อมูล

[3] พิจารณาว่าข้อมูลรายการนั้นมีผลกระทบต่อกระบวนการทำงานโดยรวม เนื่องจากเป็นข้อมูลที่ใช้ร่วมกันในกระบวนการทำงานหลายๆ อย่าง หากผลกระทบโดยรวมดังกล่าว ทาให้การทำงานใดงานหนึ่งถึงขั้นล้มเหลว ย่อมถือว่าสำคัญมาก

[4] พิจารณาจากความยากง่ายของการได้มาของข้อมูลแต่ละรายการ ซึ่งอาจขึ้นอยู่กับปัจจัยหลายประการเช่น ความพร้อมของหน่วยงานเจ้าของข้อมูล การทำสัญญาข้อตกลงระหว่างหน่วยงานในการขอใช้ข้อมูล งบประมาณสนับสนุน ค่าใช้จ่ายที่จะเกิดขึ้นในการเชื่อมโยงระบบข้อมูล

[5] สรุปผลการพิจารณา จากขั้นตอนที่ 1-4 เพื่อหาลาดับความสำคัญของข้อมูลแต่ละรายการ

3) **การจัดแบ่งลำดับชั้นความลับของข้อมูล**
(1) ข้อมูลลับที่สุด หากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียงหายอย่างร้ายแรงที่สุด
(2) ข้อมูลลับมาก หากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
(3) ข้อมูลลับ หากเปิดเผยทั้งหมดหรือบางส่วนจะก่อให้เกิดความเสียหาย
(4) ข้อมูลทั่วไป ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

การกำหนดชั้นความลับ ให้พิจารณาจากความสำคัญของเนื้อหา แหล่งที่มาของข้อมูล วิธีการนาไปใช้ประโยชน์ จำนวนบุคคลที่ควรรับทราบ ผลกระทบหากมีการเปิดเผย และหน่วยงานที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ ทั้งนี้**ให้มีการจัดทำข้อตกลงการรักษาความลับที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ที่จะเปิดเผยได้เฉพาะบุคคล เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลแล้วเท่านั้น**

4) **การจัดแบ่งระดับชั้นการเข้าถึง** โดยแบ่งสิทธิการเข้าถึงตามประเภทของข้อมูล

(1) ประเภทของข้อมูลทั่วไป กำหนดสิทธิให้สามารถเข้าถึงข้อมูลได้ทุกคน

(2) ประเภทของข้อมูลที่ต้องกำหนดสิทธิการเข้าถึง มีระดับการเข้าถึงดังนี้

[1] ระดับผู้ปฏิบัติงาน

[2] ระดับผู้ตรวจสอบข้อมูล

[3] ระดับผู้ลงนามรับรองผล/อนุมัติ

[4] ระดับการเข้าถึงรายงานสรุปผล

[5] ระดับผู้ดูแลระบบระดับหน่วยงาน

[6] ระดับผู้ดูแลระบบย่อย ตามคาสั่งหน่วยงานผู้รับผิดชอบข้อมูล

[7] ระดับผู้ดูแลระบบสูงสุด

กรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆเพื่อเป็นหลักฐานในการตรวจสอบ ดังนี้

[1] Server เก็บ LOG ระยะเวลาตามกฎหมาย

[2] ระบบที่มีความสำคัญ มีการเก็บประวัติการเข้าใช้งาน

5) **การกำหนดเวลาที่ได้เข้าถึงระบบสารสนเทศ** ดังนี้

(1) ระบบงานบริการ (Front Office) สำหรับผู้ใช้งานทั่วไป เข้าถึงได้ตลอดเวลา

(2) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายใน ผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลาดังนี้

[1] การเข้าถึงในเวลาราชการ (08.30-16.30 น)

[2] การเข้าถึงนอกเวลาราชการ (นอกช่วงเวลา 08.30-16.30 น.)

[3] การเข้าถึงในช่วงเวลาวันหยุดราชการและวันหยุดนักขัตฤกษ์

[4] การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุเป็นช่วงเวลา ระยะเวลาการเข้าถึง

6) **การกำหนดจานวนช่องทางที่สามารถเข้าถึง**

(1) ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

(2) ระบบโทรศัพท์ (เข้าถึงได้ในเวลาราชการ)

(3) หนังสือหรือบันทึกข้อความ (เข้าถึงได้ทุกช่วงเวลา)

(4) ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

(5) ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

(6) ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

(7) ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

(8) เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนดเวลา)

(9) การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และช่วงเวลาพิเศษเป็นรายครั้ง)

1.3 ข้อกำหนดการใช้งานตามภารกิจ

1) **การใช้งานตามภารกิจ**

โรงพยาบาลจัดให้บริการสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใช้ประโยชน์ตามภารกิจของโรงพยาบาล ได้แก่ การรักษา การเรียนการสอน การวิจัย การบริการวิชาการ และการบริหารงาน ทั้งนี้การใช้งานตามภารกิจ ต้องอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่น เคารพและปฏิบัติให้ถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใดๆ โดยกำหนดสิทธิ์การเข้าถึงจะแบ่งตามลาดับชั้นการบริหารจัดการของผู้บริหาร ไว้ดังนี้

(1) ผู้บริหารระดับสูง ได้แก่ ผู้อำนวยการ สามารถเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายในการกำกับดูแล

(2) ผู้บริหารระดับหน่วยงาน ได้แก่ หัวหน้าหน่วยงาน สามารถเข้าถึงข้อมูลภายใต้ความรับผิดชอบดูแล

(3) ผู้ปฏิบัติงาน สามารถเข้าถึงได้เฉพาะส่วนที่ตนเองได้รับมอบหมาย

2) **การกำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ** ดังนี้

(1) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

(2) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

(3) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

3) **ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจากัดสิทธิ์สำหรับผู้ใช้งาน** มีดังนี้ ตำแหน่งงาน หน่วยงานต้นสังกัด คำสั่งมอบหมายงานและหน้าที่รับผิดชอบ ระยะเวลาการจ้างงาน/ระยะเวลาการปฏิบัติงาน

การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตเป็นต้นเพื่อให้การควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล เป็นไปอย่างมั่นคงปลอดภัย มีแนวทางปฏิบัติดังนี้

1.แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

1) ผู้อำนวยการกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2) การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

(1) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการ

(2) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทาการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้ เหตุผลในการขอใช้ระยะเวลาในการใช้ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย และการตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

3) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(1) หน่วยงานภายนอกที่ ทำงานให้กับโรงพยาบาลทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในโรงพยาบาลหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของโรงพยาบาล โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(2) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(3) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของโรงพยาบาลฟากท่า ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(4) โรงพยาบาลฟากท่า มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่าโรงพยาบาลฟากท่า สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(5) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

1 การใช้งานทั่วไป

1) ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

2) เครื่องคอมพิวเตอร์และเครือข่ายของโรงพยาบาลฟากท่าเป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น

3) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาล ต้องเป็นโปรแกรมที่โรงพยาบาลได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนาไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนาไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

4) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดาเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบารุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับโรงพยาบาลเท่านั้น

5) ห้ามการใช้งานสื่อบันทึกพกพาต่างๆ

6) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

7) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น ตกหรือหลุดมือ ฯลฯ

8) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

9) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

10) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทาการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

11) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำกาแฟ และเครื่องดื่มต่าง ๆ ฯลฯ

12) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

13) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

14) ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

15) ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น (อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ) ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

16) ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนาที่โรงพยาบาลฟากท่ากำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

17) หากผู้ใช้งานกระทำการล่วงละเมิด หรือ พยามยามจะล่วงละเมิด ศูนย์เทคโนโลยีสารสนเทศ ในฐานะผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของโรงพยาบาล ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือการใช้งานใดๆ ตามความเหมาะสม

18) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

19) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

20) ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง

21) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

22) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

23) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือศูนย์เทคโนโลยีสารสนเทศ

24) ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

25) ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟท์แวร์ที่โรงพยาบาลจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนาไปใช้งานที่อื่น

26) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาล เพื่อประโยชน์ทางการค้า

27) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

28) ห้ามผู้ใช้งานใช้ระบบสารสนเทศของโรงพยาบาล เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

11.2 การสำรองข้อมูลและการกู้คืน แนวปฏิบัติ มีดังนี้

1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD และ External Hard Disk ฯลฯ

2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

3) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Hard Disk ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทางาน

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลฟากท่าได้ โดยกำหนดแนวปฏิบัติ ดังนี้

1 การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

1) มีการเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศให้ผู้ใช้งานได้รับทราบ

2) มีการฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

2 การกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration)

1) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

2) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

3) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

4) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

5) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

6) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการอนุญาตจากผู้อานวยการ

7) มีหลักเกณฑ์ในการยกเลิก เพิกถอน การอนุญาต ให้เข้าถึงระบบสารสนเทศและการตัด ออกจากทะเบียนของผู้ใช้งาน เมื่อมีการ ลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง

8) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบ ต้องทาการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

9) มีการแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน อย่างน้อยทุก 3 เดือน

3 การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

1) ผู้ดูแลระบบ ต้องกำหนดรหัสผู้ใช้ รหัสผ่าน และสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ ตามหน้าที่ความรับผิดชอบของแต่ละกลุ่มผู้ใช้งาน เพื่อใช้ในการตรวจสอบยืนยันตัวตนของผู้ใช้งาน

2) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ทั้งนี้ต้องได้รับหนังสือจากต้นสังกัดโดยให้มีการพิจารณาควบคุมการใช้งาน ดังนี้

(1) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบนั้นๆ

(2) ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้มีการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) มีการเปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะนานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน

4 มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

1) กระบวนการจัดสรร หรือแจกจ่ายรหัสผ่านให้กับผู้ใช้งาน

(1) กำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

(2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(3) ส่งมอบรหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน

(4) ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกาลังใส่ข้อมูลล็อกอิน

(5) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจารหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

2) ข้อกำหนดการเปลี่ยนรหัสผ่าน

(1) อนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง

(2) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(3) ผู้ใช้งาน ควรทาการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทาการเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

5 การทบทวนสิทธิการเข้าถึงผู้ใช้งาน (Review of User Access Rights)

1) ผู้ดูแลระบบ ทบทวนสิทธิการเข้าถึงของผู้ใช้งานปีละ 1 ครั้งเป็นอย่างน้อย มีแนวทางปฏิบัติ ดังนี้

(1) จัดทำหนังสือถึงเจ้าหน้าที่ เพื่อขอข้อมูลบุคลากรพ้นสภาพบุคลากร ยกเว้นกรณีเกษียณอายุราชการ

(2) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งจากหน่วยงาน

2) ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

3) ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลง การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

4) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

6 การเพิกถอนสิทธิการเข้าถึงของผู้ใช้งาน

1) ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพบุคลากร ของโรงพยาบาลฟากท่ายกเว้นกรณีเกษียณอายุราชการ โดยดำเนินการแจ้งเจ้าของข้อมูล เพื่อขอรายชื่อบุคลากร พ้นสภาพอย่างน้อยปีละ 1 ครั้ง

2) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศทันที เมื่อผู้ใช้งานนั้นพ้นจากสภาพบุคลากร ยกเว้นกรณีเกษียณอายุราชการ โดยอ้างอิงจากบันทึกจากเจ้าหน้าที่

3) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานเปลี่ยนตำแหน่งงาน โดยมีบันทึกข้อความจากเจ้าหน้าที่เป็นหลักฐานการเปลี่ยนตำแหน่งงานโอนย้ายข้ามหน่วยงานราชการ

4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

4.1 การใช้บริการเครือข่าย

1) มีการกำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้ใช้งานได้

2) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น

3) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ฯลฯ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ 1 ครั้ง

4.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกโรงพยาบาล (User Authentication for External Connection) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคล ดังนี้

1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

2) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง ด้วยการใช้รหัสผ่าน การใช้สมาร์ทการ์ด หรือการใช้ User Token ที่มีเทคโนโลยี PKI โดยจะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของโรงพยาบาล 1 วิธี

3) การเข้าสู่ระบบสารสนเทศจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

4.3 การระบุอุปกรณ์บนเครือข่าย (Equipment Identifiction in Network)

มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

1) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

2) มีการควบคุมการใช้งานอย่างเหมาะสม

3) จากัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึง ทั้งทางกายภาพและเครือข่าย ดังนี้

1) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

17

2) กำหนดวิธีการป้องกันช่องทางที่ใช้บารุงรักษาระบบผ่านเครือข่าย

3) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจอบและปรับแต่งระบบให้ใช้งานได้อย่างจากัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

4.5 การแบ่งแยกเครือข่าย (Segregation in Network)

แนวทางปฏิบัติ

1) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรออกเป็นเครือข่ายภายใน และภายนอก

2) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรออกเป็นเครือข่ายย่อยๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

3) กำหนดให้มีการควบคุมการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเหล่านั้น ทั้งนี้เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเหล่านั้นและทาการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่ายหรืออื่นๆ โดยไม่ได้รับอนุญาต

4) กำหนดมาตรการความมั่นคงปลอดภัยที่เหมาะสมกับเครือข่ายย่อย เหล่านั้น เช่นใช้ไฟร์วอลล์กั้นและป้องกันเครือข่ายย่อยเหล่านั้นจากการถูกบุกรุก หรือเข้าถึงโดยไม่ได้รับอนุญาต

5) กำหนดให้มีการใช้เกตเวย์เช่น ไฟร์วอลล์เพื่อกั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

กรองหรือจากัดการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น และควบคุมการเข้าถึงเครือข่ายย่อยภายในโรงพยาบาลโดยไม่ได้รับอนุญาต

6) กำหนดให้มีการใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย (ทั้งจากภายใน และภายนอกองค์กร) ให้สอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานระบบเครือข่ายของโรงพยาบาล

7) กำหนดให้มีการใช้ขีดความสามารถของอุปกรณ์เครือข่าย เช่น การทา IP Switching เพื่อแบ่งแยกเครือข่ายออกเป็นส่วนๆ รวมทั้งควบคุมการไหลของข้อมูล ระหว่างเครือข่ายย่อยเหล่านั้น

8) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ความต้องการในการเข้าถึงเครือข่ายหรือระบบงาน เช่น ความต้องการของผู้ใช้งานกลุ่มต่างๆ หรือของผู้บริหาร เป็นต้น รวมถึงคุณค่าและชั้นความลับของข้อมูลที่ใช้งานอยู่ภายในเครือข่ายของโรงพยาบาล

9) กำหนดให้มีการแยกวงของเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของโรงพยาบาล

10) กำหนดให้มีการประเมินความเสี่ยงและกำหนดมาตรการป้องกันที่ เหมาะสมก่อนแบ่งแยกวงเครือข่ายไร้สาย เช่น การกำหนดมาตรการการพิสูจน์ ตัวตนที่มีความมั่นคงปลอดภัย วิธีการที่มีการเข้ารหัสข้อมูล เป็นต้น

18

4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

แนวปฏิบัติการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน มีดังนี้

1) มีการตรวจสอบการเชื่อมต่อเครือข่าย

2) จากัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

3) ระบุอุปกรณ์ เครื่องมือ ที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

4) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

5) ควบคุมไม่ให้มีการเปิดให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

4.7 การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control) มีการควบคุมดังนี้

1) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address Plan)

2) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

3) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจากัดสิทธิในการใช้บริการเครือข่าย

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

5.1 ผู้ดูแลระบบ (System Adminstrator)

ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ให้บริการสารสนเทศของโรงพยาบาล และกำหนดชื่อผู้ใช้งานให้กับเครื่องคอมพิวเตอร์

5.2 กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบเสร็จสมบูรณ์ และกำหนดให้ระบบมีการหน่วงเวลาการเชื่อมต่อ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

5.3 ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identififation and Atuhentication)

กำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้
1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ
2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงาน หรือด้านเทคนิค
3) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่นสมาร์การ์ด RFID เครื่องอ่านลายนิ้วมือ ฯลฯ
19

5.4 การบริหารจัดการรหัสผ่าน (Password Management System)
มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

5.5 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ดำเนินการดังนี้
1) จากัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้งานโปรแกรม
2) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป
3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจา
4) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้
5) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

5.6 การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)
กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเกิน 30 นาที ตามความเหมาะสม ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้มีการพิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญ

5.7 การจากัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Network Usage Idle Time)
กำหนดหลักเกณฑ์การยุติการใช้งานระบบเครื่อข่ายเมื่อว่างเว้นจากการใช้งานเป็นเวลาเกิน 1 ชั่วโมง หากต้องการเชื่อมต่อ ต้องเข้ารหัสผ่านเพื่อยืนยันตัวตนอีกครั้ง

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access control)

6.1 การจากัดการเข้าถึงสารสนเทศ (Information Access Restriction)
ต้องจากัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจากัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

6.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อโรงพยาบาล ดำเนินการดังนี้
1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อโรงพยาบาล
2) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ
3) มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกโรงพยาบาล (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
20

6.3 การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนาไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

2) การยืมใช้อุปกรณ์ ต้องมีการบันทึกรายละเอียดการยืมใช้งานอย่างเป็นลายลักษณ์อักษร

3) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นาไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

4) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนาส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

5) เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

6) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาณอย่างร้ายแรงของผู้นาไปใช้ ผู้นาไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

7. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1) **ผู้ใช้งาน** ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลฟากท่า จะต้องทาการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

2) **ผู้ดูแลระบบ** ต้องดำเนินการดังนี้

(1) ต้องทาการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่าเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(2) ต้องทาการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(3) ต้องกำหนดตาแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

(4) ควรเลือกใช้กาลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสารวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

(5) ควรทาการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นาอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(6) ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(7)__

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่ เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตาม ความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สนที่มีค่าและอาจ จำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมี ส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยี สารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบ เครือข่ายไร้สาย เป็นต้น

๒.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยี สารสนเทศ

๒.๓ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบ เทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่อง คอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลง นาม

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
(Access Control Policy)

1. วัตถุประสงค์ เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และ ป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะ สร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่ามี ดังนี้

2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1.1 โรงพยาบาลฟากท่า กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจาก หน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยี สารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้า ศูนย์เทคโนโลยีสารสนเทศ

2.1.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยี สารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.1.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบ เทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความ ปลอดภัย ที่มีต่อระบบข้อมูล

2.1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลฟากท่า กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้ งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมาย อิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ อินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานใน หน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.2.3 ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของ บุคลากรดังต่อไปนี้

2.2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้ งาน

2.2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยง

การใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

2.2.3.3 ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

2.2.3.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบ คอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ใน การควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้น ความลับ ดังต่อไปนี้

2.2.4.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการ เข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2.2.4.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้น ความลับของข้อมูล

2.2.4.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าว

2.2.4.4 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับ การเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.2.4.5 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของ ระดับความสำคัญของข้อมูล

2.2.4.6 ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลใน กรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่ เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น 2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

2.3.2 ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้า ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

2.3.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อค หน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการ ต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

2.3.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็น เวลานานมากกว่า 1 ชม.

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
(Network and Server Policy)

1. วัตถุประสงค์ เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและ ข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย โรงพยาบาลฟากท่า กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ ข่าย (Server) ดังนี้

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

2.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่ หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำ ของระบบและผู้ใช้บริการอื่นๆ

2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับ ระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

2.5 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้

2.5.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งาน เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการ เข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

2.5.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

2.5.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

2.5.4 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

2.5.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

2.5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

2.5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียด เกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และ อุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.5.8 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติ จากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.5.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และ รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

2.6 โรงพยาบาลฟากท่า กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตาม แนวทาง ดังต่อไปนี้

2.6.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถ รักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและ ผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบ ระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงาน มอบหมาย

2.6.2 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของ ผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุก รุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้ งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้ บริการสิ้นสุดลง

2.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

2.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การ เข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2.7 โรงพยาบาลฟากท่า กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

2.7.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและ เครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขอ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ

2.7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ

2.7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความ จำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

(Wireless Policy)

1. วัตถุประสงค์ เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจาก ระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่าย ไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของโรงพยาบาลฟากท่า มีหน้าที่และ ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์ กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

2.3 ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

2.4 กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

2.4.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดย จะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการ รับรองและการเข้ารหัสด้วย (Authentication, Encryption)

2.4.2 ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้ เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่าย ไร้สายได้อย่างถูกต้อง

2.4.3 ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิด คุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

2.4.4 ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

2.4.5 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควร กำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

2.4.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับ อนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

2.4.7 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัย ของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่า สงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบ ทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ ผิดปกติ ให้ผู้ดูแลระบบรายงานให้หัวหน้าศูนย์เทคโนโลยีสารสนเทศทราบ ทันที

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

(Firewall Policy)

1. วัตถุประสงค์ เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

2. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของโรงพยาบาลฟากท่ามีหน้าที่และ ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของ ไฟร์วอลล์ทั้งหมดของโรงพยาบาลฟากท่า

2.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

2.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

2.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัส ผู้ใช้ (User account) และรหัสผ่าน (User password)

2.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

2.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ ดูแลจัดการเท่านั้น

2.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่ อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อย กว่า 90 วัน

2.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิด พอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลฟากท่า อนุญาตให้ใช้ งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้อง ได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ ก่อน

2.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยี สารสนเทศ โดยต้องระบุข้อมูลดังนี้

2.9.1 หมายเลข Port ที่ต้องการขอให้เปิด

2.9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

2.9.3 วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

2.9.4 วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

2.10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุก สัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

2.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้ มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็น กรณีไป

2.12 โรงพยาบาลฟากท่า มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลฟากท่า หรือ กฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัย ของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

2.13 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบ ของโรงพยาบาลฟากท่า หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความ ปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบ สารสนเทศของหน่วยงาน ทางศูนย์เทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

2.14 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการ ขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และ จะต้องได้รับความเห็นชอบจากโรงพยาบาลฟากท่าก่อน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

1. วัตถุประสงค์ เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่ง ผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บน เครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์ กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำ ของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบ เครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลฟากท่า มีหน้าที่และความรับผิดชอบที่ ต้องปฏิบัติ ดังนี้

2.1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอก ข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงาน โดยยื่นคำขอกับ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลฟากท่า

2.2 เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดย ทันที

2.3 ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

2.4 ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

2.5 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของ จดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของ ตน

2.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของโรงพยาบาลฟากท่า ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลฟากท่าเท่านั้น ห้ามไม่ให้ ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ โรงพยาบาลฟากท่า ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

2.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

2.8 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการ ปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็น ความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของโรงพยาบาลฟากท่า หรือก่อให้เกิด ความเสียหายต่อโรงพยาบาลฟากท่า

2.9 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลฟากท่า เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของโรงพยาบาลฟากท่า ตลอดจนเป็นการรบกวนผู้ใช้งาน อื่น รวมทั้งผู้รับบริการของโรงพยาบาลฟากท่า

2.10 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย อิเล็กทรอนิกส์

2.11 การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน 10 เมกะไบท์

2.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

(Internet Security Policy)

1. วัตถุประสงค์ เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลฟากท่า ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพ กฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะ ทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้เครือข่ายอินเตอร์เน็ต ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลฟากท่ามีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการ เครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยี สารสนเทศ โรงพยาบาลฟากท่า หรือทำการสมัครผ่านระบบอินทราเน็ตของโรงพยาบาลฟากท่า โดยสามารถใช้งานได้ 1 วัน เพื่อรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งาน โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลฟากท่า สำหรับบุคคลภายนอกจะต้อง ได้รับอนุญาตจากหัวหน้าศูนย์เทค โนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

2.2 ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วน บุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่ มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่ อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

2.3 ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการ ละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็น ผู้รับผิดชอบ

2.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

2.6 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการ อัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

2.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ เพสบุค โปรแกรมอื่น ๆที่มีลักษณะ คล้ายกัน โดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอ ความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อเสียต่อชื่อเสียง ของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

2.8 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจาก การเครือข่ายอินเตอร์เน็ตด้วย การ Logout จากการ Authentication เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่นๆ

นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

1. วัตถุประสงค์ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่าย ภายในโรงพยาบาลฟากท่า ให้มีความมั่นคงปลอดภัย

2. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุก เครือข่าย เป็นดังนี้

2.1 IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลฟากท่าและ เครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่าย อินเทอร์เน็ตทุกเส้นทาง

2.2 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการ ตรวจสอบจากระบบ IDS/IPS

2.3 ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

2.4 โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผล การตรวจสอบ

2.5 มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

2.6 มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึก ปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

2.7 IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่าย ของระบบเทคโนโลยีสารสนเทศตามปกติ

2.8 เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

2.9 พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การ โจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จ และไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

2.10 พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมี การรายงานให้ผู้บังคับบัญชาทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

2.11 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

2.12 มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของ เหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

2.13 โรงพยาบาลฟากท่า มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มี พฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

2.14 ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลฟากท่า การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการ ทำงานของระบบเทคโนโลยีสารสนเทศ จะ

ถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความ เสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลฟากท่า จะต้องถูกดำเนินคดีตาม ขั้นตอนของกฎหมาย

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

(Backup Policy)

1. วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมี เหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

2. แนวทางปฏิบัติในการสำรองข้อมูล

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการ สำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบ เทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่ง ติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมา ได้ภายในระยะเวลาที่เหมาะสม

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์ เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจน สามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ

2.1 จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้ วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของ หน่วยงาน

2.2 จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนา ควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจาก ภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

2.3 ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือ ข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

2.4 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการของผู้ใช้บริการ

(แพทย์หญิงพรสวรรค์ มีชิน)
ผู้อำนวยการโรงพยาบาลฟากท่า
วันที่ 1 ตุลาคม 2566