



ประกาศโรงพยาบาลท่าตะเกียบ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลท่าตะเกียบ พ.ศ. 2567

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลท่าตะเกียบ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลท่าตะเกียบและหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องได้ โรงพยาบาลท่าตะเกียบจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลท่าตะเกียบ
มีวัตถุประสงค์ ดังต่อไปนี้

1.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลท่าตะเกียบ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่โรงพยาบาลท่าตะเกียบและผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

1.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งานผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลท่าตะเกียบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาลท่าตะเกียบในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

2. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลท่าตะเกียบ กำหนดประเด็นสำคัญดังต่อไปนี้

2.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

2.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

2.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดง

ตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยตามที่โรงพยาบาลท่าตะเกียบจัดสรรไว้ เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

2.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

2.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่างๆ รวมถึง จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

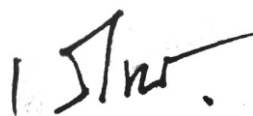
2.2 การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

2.3 ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

4. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลท่าตะเกียบ พ.ศ. 2567 ตามที่แนบท้ายประกาศนี้

ณ วันที่ 12 เดือน กุมภาพันธ์ พ.ศ. 2567



(นายแพทย์เกริกภัทร ลิ้มปวยอม)

ผู้อำนวยการโรงพยาบาลท่าตะเกียบ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลท่าตะเกียบ พ.ศ. 2567

ตามประกาศโรงพยาบาลท่าตะเกียบ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลท่าตะเกียบ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อนั้น โรงพยาบาลท่าตะเกียบกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้คำนิยาม

“หน่วยงาน” หมายถึง โรงพยาบาลท่าตะเกียบ

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

“ผู้บริหาร” หมายถึง ผู้อำนวยการโรงพยาบาลท่าตะเกียบ

“ผู้ดูแลระบบ” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล ระบบเครือข่าย และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานถือครอง

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ ได้แก่ ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ เอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิดชอบ และความน่าเชื่อถือ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน (Access Control) ครอบคลุมทุกระดับ

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ และการมอบอำนาจของหน่วยงานของรัฐ
3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ 1 การเข้าถึงหรือควบคุมการเข้าถึงสารสนเทศ

ข้อ 1. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ 2. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหาร หรือหัวหน้าหน่วยงาน แล้วแต่กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

ข้อ 3. กำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอโดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญาตนั้น ดังนี้

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

(3) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้

(3.1) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(3.2) กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างสม่ำเสมอ

(3.3) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

ข้อ 4. จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสาร

อิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

(1) จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร - ระดับชั้นสำหรับผู้ใช้งานทั่วไป - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(2) จัดแบ่งลำดับชั้นความลับของข้อมูล - ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรงที่สุด - ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรงมาก - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(3) จัดแบ่งประเภทของข้อมูล - ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี - ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการรักษา ผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

(4) จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชา ในหน่วยงานนั้น - ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ หรือ ได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ ที่ได้รับมอบหมายตามอำนาจหน้าที่

(5) รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรม ทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของ ข้อมูลอิเล็กทรอนิกส์ พ.ศ.2443

ข้อ 5. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุม การเข้าถึงข้อมูล แต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(1) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและผ่านระบบ

(2) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของ ข้อมูลแต่ละระดับ

(5) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา 20 นาที

(6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษาตรวจสอบให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

ข้อ 6. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

(1) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบ สารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(2) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ 7. การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(1) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน
ดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) ระบบปรับอากาศและควบคุม
ความชื้น

(2) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและ
ลดความเสี่ยงจากความล้มเหลวในการทำงาน

(3) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data
Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

(4) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอกและให้
แยกอุปกรณ์ที่มีความสำคัญเก็บไว้ที่พื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(5) ตรวจสอบสื่อดูดข้อมูลและสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่
ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในห้องศูนย์ข้อมูล (Data Center)

(6) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่าน
เข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกัน หนู นก กระรอก
แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับ สัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความ
เสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(7) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณ สื่อสารและ
สายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณ ซึ่งกันและกัน แล้วให้จัดเก็บ
สายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้
ที่ไม่มีส่วนเกี่ยวข้อง

การควบคุมการเชื่อมต่อ VPN FTP หรือ Telnet กับระบบเครือข่ายหลัก

วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การใช้งานการควบคุมการเชื่อมต่อ VPN FTP
หรือ Telnet กับระบบเครือข่ายหลัก เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดย
เคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ไม่อนุญาตให้ดำเนินการ เชื่อมต่อ VPN FTP หรือ Telnet กับระบบเครือข่ายหลัก

หากมีความจำเป็นในการเปิดใช้งาน VPN FTP หรือ Telnet จะต้องควบคุม โดยผู้ดูแลระบบของ
โรงพยาบาลท่าตะเกียบ และต้องมีบันทึกข้อความเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้างานทราบ
และรายงานให้อำนาจการโรงพยาบาลท่าตะเกียบเป็นผู้อนุมัติเท่านั้น เพื่อการรักษาความมั่นคงปลอดภัยของ
ระบบเครือข่ายหลัก

2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

**สร้างความรู้ความเข้าใจให้กับผู้ใช้งานถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่
ระมัดระวังหรือรู้เท่าไม่ถึงการณ์**

การสร้างความรู้ความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อเป็นการ
ให้ความรู้ต่อผู้ใช้งาน User และการสร้างความปลอดภัยที่อาจเกิดขึ้นได้จากผู้ใช้งาน โดยการให้ความรู้ส่งไปทาง
ไลน์ เพื่อกระตุ้นให้เห็นถึงความสำคัญและความเสี่ยงต่อการใช้งานระบบสารสนเทศได้

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของ
โรงพยาบาลท่าตะเกียบ

2. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
3. เพื่อป้องกันและลดการกระทำผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

- ข้อ 1. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง
- ข้อ 2. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
- ข้อ 3. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า 1 ครั้ง โดยจะจัดรวมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
- ข้อ 4. ตีตประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
- ข้อ 5. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน
- ข้อ 6. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
- ข้อ 7. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
- ข้อ 8. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของโรงพยาบาลท่าตะเกียบ และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

- ข้อ 8. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (User Registration) ดังนี้
 - (1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
 - (2) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน
 - (3) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ 3) (4) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบ เทคโนโลยีสารสนเทศ
- ข้อ 9. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยมีระบบที่เกี่ยวข้อง คือ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบ เครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงาน ในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร
- ข้อ 10. ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่าง

น้อย ปีละ 1 ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างโดยปฏิบัติตาม แนวทาง ดังนี้

- (1) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน
- (2) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและ สิทธิ การเข้าใช้งานว่าถูกต้องหรือไม่
- (3) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน
- (4) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิ ใน ระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน
- (5) เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยน หน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ถอดถอนสิทธิภายใน 1 สัปดาห์

ข้อ 11. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- (1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือ พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (2) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- (3) ส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้ บุคคล อื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
- (4) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)
- (5) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง
- (6) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ใน รูปแบบที่ไม่ได้ป้องกันการเข้าถึง

ข้อ 12. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลาย ข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

- (1) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธี ปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่าน ระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ
- (2) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- (3) ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงข้อมูลโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน ข้อมูลในแต่ละชั้นความลับข้อมูล
- (4) มีการกำหนดให้เปลี่ยนรหัสผ่าน ทุกๆ 90 วัน
- (5) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอก หน่วยงาน เช่น บำรุงรักษา ตรวจสอบให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อ บันทึกก่อน เป็นต้น
- (6) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- (7) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของ บุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ 13. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้ หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจ

ใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน

- (1) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน
- (2) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- (3) พิจารณาวามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน
- (4) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- (5) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ 4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ 14. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- (1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- (2) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical Character) และตัวอักษร (Alphabet)
- (3) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุล ของตนเองหรือตรงกับคำในพจนานุกรม
- (4) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (5) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- (6) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- (7) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- (8) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 90 วันหรือทุกครั้งที่ไม่การแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 15. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ 16. ผู้ใช้งานระบบสารสนเทศของหน่วยงาน หากมีปัญหา ไม่ว่าจะเกิดจากการเข้าใช้งานไม่ได้ ลืมรหัสผ่าน หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- (1) การใช้งาน HIS ของหน่วยงาน ต้องมีการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
- (2) การใช้งานอินเทอร์เน็ต (Internet) ต้องมีการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
- (3) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการลงบันทึกออก (Logout) ทุกครั้ง
- (4) ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลา 10 นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

ข้อ 17. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงาน หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 18. เอกสารที่เป็นความลับหรือมีระดับความสำคัญ ซึ่งพิมพ์ออกจากเครื่องพิมพ์ (Printer) ตลอดจนข้อมูลที่เป็นความลับในรูปอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังนี้

- (1) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก
- (2) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ
- (3) การเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่เป็นเจ้าของ

(4) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

(5) ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้

ข้อ 19. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 20. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อ 21. ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคล หนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาล ซึ่งโรงพยาบาลอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ 22. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูล ของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิตทอร์เรนต์ (Bittorrent) หรือ อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 23. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนังเล่นเกม เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ 24. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมไว้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาล

ข้อ 25. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกระทรวงสาธารณสุข

ข้อ 26. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อประโยชน์ทางการค้า

ข้อ 27. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของหน่วยงาน โดยเด็ดขาด ไม่ว่าจะทำด้วยวิธีการใด ๆ ก็ตาม

ข้อ 28. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ 29. ห้ามใช้ระบบสารสนเทศของหน่วยงาน เพื่อการควบคุมคอมพิวเตอร์หรือระบบ สารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ 30. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 31. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงาน โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3 การควบคุมการเข้าถึงเครือข่ายและระบบปฏิบัติการ (Network and Operation System Access Control)

ส่วนที่ 3.1 ห้องปฏิบัติงานหรือห้องควบคุมระบบเครือข่ายเป็นพื้นที่เฉพาะบุคคลที่ได้รับอนุญาตและต้องมีการแบ่งพื้นที่เป็นส่วนชัดเจน ดังนี้

1. ส่วนปฏิบัติการ (Operation Zone) ให้แยกเป็นพื้นที่ที่ง่ายต่อผู้ดูแลระบบเข้าไปใช้งาน
2. ส่วนเครื่องแม่ข่าย (Server Zone) ให้เป็นพื้นที่สำหรับวางเครื่องแม่ข่ายของระบบแม่ข่ายหลักของโรงพยาบาลทั้งเครื่องแม่ข่ายหลักและเครื่องแม่ข่ายรอง เพื่อง่ายต่อการจัดการอุปกรณ์
3. ส่วนเครื่องสำรองไฟ (UPS Zone) แบ่งสัดส่วนภายในตู้ Rack และเครื่องแม่ข่ายเพื่อการใช้งานที่ง่ายขึ้น
4. ส่วนถังดับเพลิงสีเขียวในห้อง ง่ายต่อการใช้งานหากเกิดอุบัติเหตุกรณีไฟไหม้ในห้อง Server ทั้งนี้ ให้ผู้รับผิดชอบดูแลระบบจัดสัดส่วนให้มีความพร้อมใช้งานตามความเหมาะสม

ส่วนที่ 3.2 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ 43. มาตรการควบคุมการเข้า-ออก ห้องแม่ข่าย

- (1) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- (2) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเข้าออกพื้นที่ เป็นประจำทุกเดือน
- (3) หากไม่มีการเข้าใช้งานห้องแม่ข่าย ให้ดำเนินการล็อกกุญแจทุกครั้ง เพื่อความปลอดภัยและการเข้าถึงห้องแม่ข่ายโดยไม่พึงประสงค์

ข้อ 44. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ หรือระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบ และต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด โดยผู้ใช้งานจะต้องแจ้งให้ผู้ดูแลระบบทราบทุกครั้ง

ข้อ 45. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 46. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- (1) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- (2) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- (3) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- (4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งาน ของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(7) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

(8) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(9) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอใช้งานระบบเครือข่ายอินเทอร์เน็ต ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอใช้งานระบบเครือข่ายอินเทอร์เน็ต” ที่กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

(10) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อเว้น ว่างจากการใช้งานเป็นเวลานาน

ข้อ 47. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 48. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ ติดตั้งก่อนดำเนินการ

ข้อ 49. กำหนดให้มีการจัดเก็บซอร์สโค้ด (Source code) ไบรารี และเอกสารสำหรับซอฟต์แวร์ ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ 50. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

ข้อ 51. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการใช้งานระบบเครือข่ายและ เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขอ อนุญาตจากหัวหน้าหน่วยงาน

(2) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(3) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับ การอนุญาตจากหัวหน้าหน่วยงาน

(4) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(5) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกล ต้องมี การลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบ ความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ 52. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้ (1) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุม การเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต (2) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน ระบบสารสนเทศภายใน

ข้อ 53. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ 54. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ 55. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่ใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจ หน้าที่เกี่ยวข้อง

ข้อ 56. IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้นักภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ 57. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติ จากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ 4 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ 58. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงาน ภายในหน่วยงาน เป็นต้น

ข้อ 59. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(2) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการ ล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่ รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(3) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(4) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(5) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็น เวลานาน

(6) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานโรงพยาบาลท่าตะเกียบ

(7) ซอฟต์แวร์ที่โรงพยาบาลท่าตะเกียบใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตาม หน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใด ที่ไม่มีลิขสิทธิ์หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(8) ซอฟต์แวร์ที่โรงพยาบาลท่าตะเกียบ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(9) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลท่าตะเกียบ เพื่อประโยชน์ทาง การค้า

(10) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(11) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดย ไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 60. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง (โดยปฏิบัติตามส่วนที่ 2 ข้อ 11)

ข้อ 61. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System utilities) ต้องจำกัดและควบคุมการ ใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลักเสี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

- (1) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตน สำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุม การใช้งาน
- (2) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์
- (3) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน
- (4) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
- (5) ต้องยกเลิกหรือลบทั้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มี ความจำเป็นใน การใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งาน โปรแกรมยูทิลิตี้ได้

ส่วนที่ 5 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ 62. แนวทางปฏิบัติการใช้งานทั่วไป

- (1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ ในงานราชการ
- (2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรม ที่หน่วยงานได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอก โปรแกรมต่าง ๆ และนำไป ติดตั้งบนเครื่อง คอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใน เครื่องคอมพิวเตอร์ ส่วน บุคคลของหน่วยงาน
- (4) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการ โดยเจ้าหน้าที่ ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ โรงพยาบาลท่า ตะเกียบ เท่านั้น
- (5) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดย โปรแกรมป้องกันไวรัส
- (6) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง คอมพิวเตอร์ (7) ปิด เครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งาน ประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการ ใช้งานเกินกว่า 1 ชั่วโมง
- (8) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้ มีการล็อกหน้าจอ หลังจากที่ไม่ได้ใช้งานเกินกว่า 10 นาที เพื่อป้องกันบุคคลอื่นมาใช้งาน ที่เครื่องคอมพิวเตอร์
- (9) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวบุคคลที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบ เครือข่ายของ หน่วยงาน โดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอย่างเหมาะสม และต้องปฏิบัติตามนโยบาย การรักษาความ มั่นคงปลอดภัยด้านสารสนเทศของ หน่วยงานอย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจาก ผู้ดูแลระบบ ของ หน่วยงานก่อนการใช้งาน

ข้อ 143. การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทาง “คู่มือปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ สำหรับผู้ใช้งาน”

ข้อ 63. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- (1) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- (2) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- (3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- (4) อุปกรณ์สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายตามวิธีการที่กำหนดไว้ (โดยปฏิบัติตามส่วนที่ 4 ข้อ 36)

ข้อ 64 การสำรองข้อมูลและการกู้คืน

- (1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก อื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- (2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างสม่ำเสมอ
- (3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูล สำคัญ เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อ การดำเนินการของหน่วยงาน (4) การสำรองข้อมูล การทำงานเบื้องต้นอื่นๆ เช่น ข้อมูลการทำงานส่วนตัว ฯลฯ เป็นหน้าที่ของเจ้าของ ข้อมูลนั้นๆ ในการเก็บสำรองข้อมูล

ส่วนที่ 6 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ 65 แนวทางปฏิบัติการใช้งานทั่วไป

- (1) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของ หน่วยงานเพื่อใช้ใน งานราชการ
- (2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็น โปรแกรมที่ หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งาน ดัดลอกโปรแกรมต่าง ๆ และนำไป ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (3) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งาน อย่างปลอดภัยและมี ประสิทธิภาพ
- (4) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของ คอมพิวเตอร์ให้มี สภาพเดิม
- (5) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับ เครื่อง คอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากโต๊ะทำงาน หรือ หลุดมือ เป็นต้น
- (6) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็น รอยขีดข่วนหรือ ทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- (7) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (8) การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปใน แนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- (9) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศ ร้อนจัด ต้องปิด เครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งาน ใหม่อีกครั้ง

(10) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้ แบนพัมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ 66 ความปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพา ในสถานที่ที่มีความร้อน/ ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

ข้อ 67 การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการ เข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(2) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลา ประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(3) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

ข้อ 68 การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน เอกสาร

“คู่มือปฏิบัติงาน กระบวนการ การบริการ ระเบียบปฏิบัติ สำหรับผู้ใช้งาน”

ส่วนที่ 7 การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ 69 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งาน อินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้น แต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ 70 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์(Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัปเดตของ โหมว ของระบบปฏิบัติการ

ข้อ 71 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ 72 ห้ามใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อกระทำการต่อไปนี้

(1) หาประโยชน์ในเชิงธุรกิจส่วนตัว

(2) เพื่อความบันเทิง ได้แก่ การเล่นเกม โหลดภาพยนตร์ โหลดเพลง

(3) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์กร เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์กร หรือข้อมูลสำคัญที่เป็นความลับขององค์กร

(4) กระทำผิดกฎหมาย เช่น - นำเข้าหรือเผยแพร่ ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์ - แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์ - กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นเกมออนไลน์การนำเข้า หรือเผยแพร่สื่อลามก อนาจาร - กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย - กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือ คัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย - กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะ อันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิด ความเสียหายต่าง ๆ

ข้อ 74 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ 75 รมั้ดระวังการดาวนโหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 76 ในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ 77 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความ ที่ยั่ว ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากร ของหน่วยงานอื่น ๆ

ข้อ 78 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ 79 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ 80 เมื่อใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการลงบันทึกออก (Logout) เพื่อป้องกันการเข้า ใช้งานโดยบุคคลอื่น ๆ

ข้อ 81 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/ หรือกฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์ อื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

ส่วนที่ 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ 82 ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 83 ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า เริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ ดังกล่าวด้วย

ข้อ 84 ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้ แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ 85 ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และหรือบัญชีผู้ใช้งาน โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายตามที่กำหนด ไว้เท่านั้น

ข้อ 86 ผู้ดูแลระบบ ต้องมีการติดตั้งไฟรอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ 87 ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่าย ภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่าย ไร้สาย

ข้อ 88 ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย

ข้อ 89 ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณี ที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ 90 ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้อุบัติหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

ข้อ 91 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลท่าตะเกียบจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นทางการ

ข้อ 92 ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่าย ไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการ ทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ 93 การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

(1) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน เมื่อมีการว่างเว้นจาก การใช้งาน เป็นเวลา 20 นาที ต้องยุติการใช้งานระบบสารสนเทศ (Session Time-out) นั้น

(2) ระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งาน ระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม หรือเป็นเวลา 20 นาที

ข้อ 94 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

(1) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับ ระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้

- กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับ ระบบสารสนเทศ เพื่อให้ผู้ใช้งาน สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ 8 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง

- กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีการจำกัดช่วงระยะเวลา การใช้งานต้องมีการลงบันทึกเข้าใช้งาน (Login) และต้องทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อเข้าใช้ งานทุกครั้ง

ส่วนที่ 9 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ 95 ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามส่วนที่ 2 ข้อ 8) ในการใช้งาน ตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามส่วน ที่ 2 ข้อ 10) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ 96 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าว อย่างสม่ำเสมอ

ข้อ 97 ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน 20 นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ 98 ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกการรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(4) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้ งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึง ระดับใดได้บ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ 99 ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและ การเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการ ตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(5) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับ ความสำคัญของข้อมูล

(6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ ออกนอก หน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูล ที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(7) ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอ โดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ

(8) ไม่เก็บข้อมูลสำคัญขององค์การไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และข้อมูลดังกล่าวจะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน

(9) ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์การ โดยถูกจัดเก็บไว้บนอุปกรณ์ แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงาน และธุรกรรม และทำการเข้ารหัสข้อมูล และระบบเครือข่ายไร้สายก่อนเท่านั้น

(10) การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เจ้าของระบบงานและ ธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว

ข้อ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(1) ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ ระบบข้อมูล ผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาลและข้อมูลทางการแพทย์ ระบบบุคลากรที่เป็นข้อมูล ส่วนบุคคลของเจ้าหน้าที่ภายในโรงพยาบาลท่าตะเกียบ

(2) ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ

(2.1) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับ มอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

(2.2) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึง ข้อมูล

(3) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงาน จากภายนอก องค์การ ข้อ

ข้อ 100 การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพ พร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รับนำ ส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่รับคืนด้วย

(5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของ ผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ 10 การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

ข้อ 101 โรงพยาบาลท่าตะเกียบได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากมีการตรวจสอบพบความผิด ฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 102 ซอฟต์แวร์(Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการ ทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้น ได้รับการอนุญาต จากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ 103 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 104 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 105 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 106 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 107 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 108 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซิงข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 109 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการ ดังนี้

(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูล บุคคลอื่นหรือแกะรหัสผ่าน ของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญ ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความ รูปภาพไม่เหมาะสมหรือ ขัดต่อศีลธรรม ประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์

ข้อ 110 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด (Source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(3) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของ ซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้าง ที่ทำกับผู้ให้บริการภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้ง ก่อนดำเนินการติดตั้ง

(5) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้อง ดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

(6) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

(7) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบายและแนว ปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลท่าตะเกียบ

ส่วนที่ 11 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ 111 ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ 112 ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ 113 ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ 114 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ 115 ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ 116 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุง สิทธิ์การเข้าถึงระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ 12 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ 117 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วนถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนด ชั้นความลับในการเข้าถึง

ข้อ 118 ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ 119 กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ 120 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2 การสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องเพื่อให้เป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

2. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแนวปฏิบัติ

ส่วนที่ 1 การสำรองข้อมูล

ข้อ 1. การสำรองข้อมูลแบบ Offline

มีการจัดการสำรองข้อมูลโดยนักวิชาการคอมพิวเตอร์ มีให้ผู้ที่ปฏิบัติหน้าที่นอกเวลา ดำเนินการสำรองข้อมูลทุกวันลงใน External Hard Disk เพื่อความปลอดภัยของข้อมูล

มีการปฏิบัติงานดังนี้

1.ดำเนินการโดยนักวิชาการคอมพิวเตอร์ผู้รับผิดชอบเวรนอกเวลา บันทึกข้อมูลลงใน External Hard Disk

2.หลังจากบันทึกข้อมูลลงแล้วให้ตรวจสอบของวันก่อนหน้าและส่งข้อมูลไปให้กับหัวหน้างานสารสนเทศทางการแพทย์

3.หัวหน้าตรวจสอบข้อมูลการบันทึกข้อมูลและลงลายมือชื่อในใบตรวจสอบความพร้อมใช้งานของระบบคอมพิวเตอร์

ข้อ 2. การสำรองข้อมูลแบบอัตโนมัติ

มีการจัดการสำรองข้อมูลผ่านระบบ Auto Backup ด้วย ระบบแยกตึกและในตึก ดังนี้

1.ในห้อง Server 1 เครื่อง โดยจะสำรองเวลา 03.00 น. ถึง 08.00 น.

2.ในห้องประชุมเล็ก 1 เครื่อง 01.00 น. ถึง 06.00 น.

ส่วนที่ 2 แผนเตรียมความพร้อมกรณีฉุกเฉิน

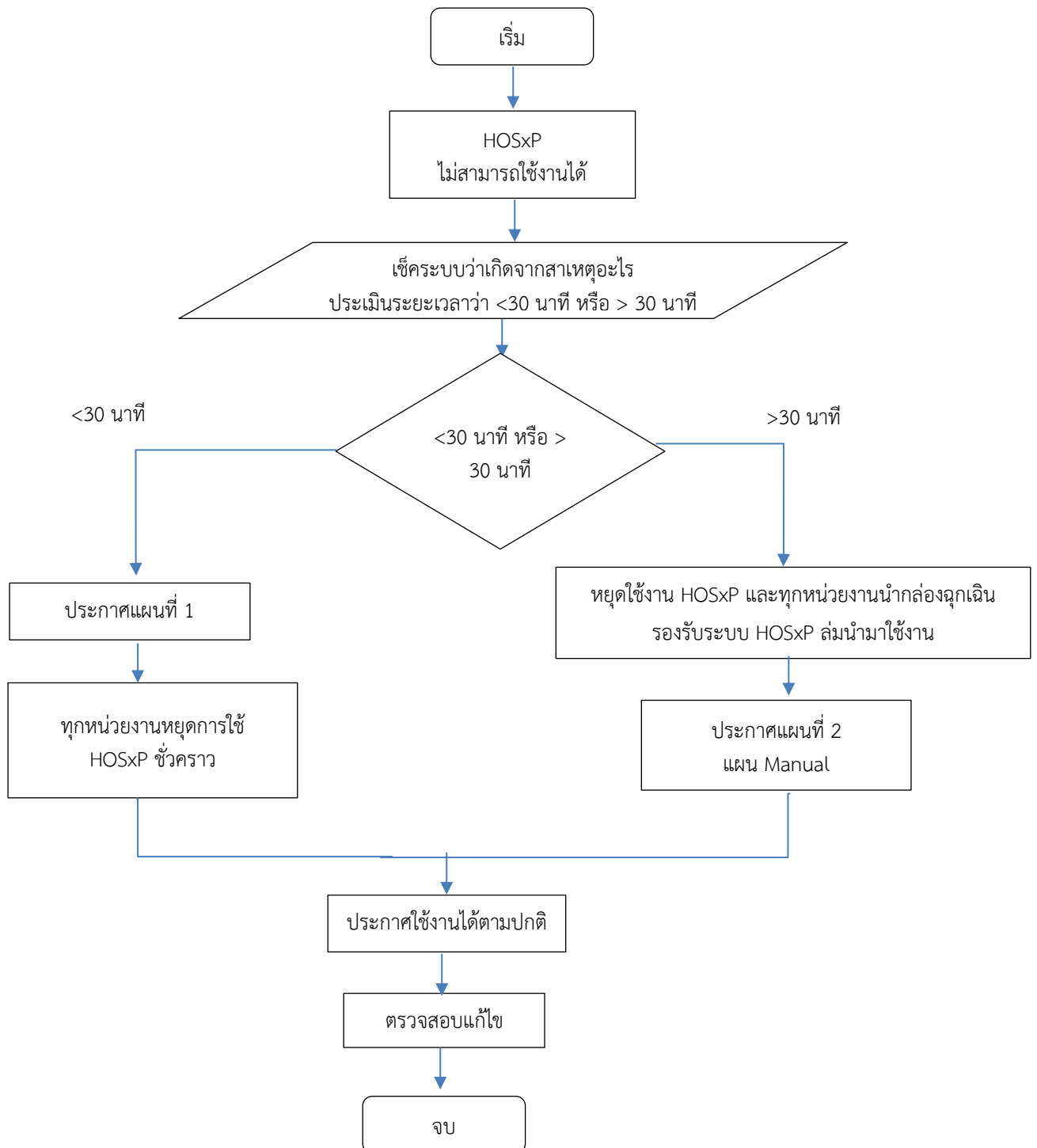
แผนที่ 1 ระยะเวลา ไม่เกิน 30 นาที

ให้หัวหน้างานสารสนเทศทางการแพทย์แจ้งให้ประชาสัมพันธ์ประกาศให้ทุกหน่วยงานทราบ หยุดการใช้งาน HOSXP ไม่เกิน 30 นาที

แผนที่ 2 แผน Manual

ระยะเวลาเกิน 30 นาที ประกาศใช้แผน Manual ประกาศโดยประธาน IM หรือหัวหน้ากลุ่มงานยุทธศาสตร์ งานประกันและสารสนเทศทางการแพทย์ โดยจะทำการตรวจสอบระบบจนกว่าจะมีการตรวจสอบเสร็จและกู้ระบบกลับมาใช้งานได้ตามปกติ

Flowchart ขั้นตอนการใช้แผนเมื่อระบบ HOSxP ล่ม



3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ 1 การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

1. จัดลำดับความสำคัญของความเสี่ยง
2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
4. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
5. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
6. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
 - (1) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลทั้ง ที่เป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
 - (2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
 - (3) กำหนดให้มีการระบุและจัดสรรทรัพยากรทั้ง ที่เป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
 - (4) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ
 - (5) ในกรณีที่มียุทธศาสตร์สำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนี้จากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ 4 ประเภท ดังนี้

ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

- (1) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(2) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ 2 ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสดังกล่าว (Computer Virus) หนอนอินเทอร์เน็ต(Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(1) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(2) ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ 3 ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลได้อย่างปลอดภัย

(2) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(3) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ 4 ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรง ที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(1) ฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(2) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(3) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศเพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(4) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(5) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์ แม่ข่าย และอุปกรณ์เครือข่าย

(6) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(7) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ