ประกาศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลยางชุมน้อย

โดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ กำหนดให้หน่วยงานของรัฐต้องจัดทำ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น

คณะกรรมการพัฒนาระบบสารสนเทศโรงพยาบาลยางชุมน้อย จังหวัดศรีสะเกษ จึงได้จัดทำแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไป ปฏิบัติอย่างเคร่งครัดและเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลยางชุมน้อย เป็นไปอย่างเหมาะสม เกิด ประสิทธิภาพสูงสุด มีความมั่นคงปลอดภัยด้านสารสนเทศ และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเป็น การป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจาก การถูกคุกคามจากภัย ต่างๆ ซึ่งอาจกอให้เกิดความเสียหายต่อโรงพยาบาลยางชุมน้อย

โดยมีวัตถุประสงค์ ดังนี้

๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยใน การใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

๒. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓. นโยบายนี้ต้องเผยแพรให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลยางชุมน้อย ได้รับทราบและถือปฏิบัติตาม นโยบายนี้อย่างเคร่งครัด

๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหนาที่ และผู้ดูแลระบบตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงาน และ ปฏิบัติตามอย่างเคร่งครัด

๕. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆเข้าล้วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นใน ระบบสารสนเทศโดยมิชอบ

๖. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

(นายชำนาญ สมรมิตร)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรม)
ผู้อำนวยการโรงพยาบาลยางชุมน้อย

สารบัญ


โรงพยาบาลยางชุมน้อย
YANGCHUMNOI HOSPITAL

คำนิยาม

“โรงพยาบาล” หมายถึง โรงพยาบาลยางชุมน้อย

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลยางชุมน้อย

“มาตรการ” หมายถึง วิธีการที่ตั้งเป็น กฎ ข้อกำหนด ระเบียบ หรือกฎหมาย เป็นต้น

“วิธีปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้ กำหนดไวตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุ เป้าหมายได้ง่ายขึ้น

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลยางชุมน้อย

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหนาที่รบผิดชอบในการดูแลรักษา ระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูล ของระบบ เครือข่ายคอมพิวเตอร์

“เจ้าหนาที่” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

“สารสนเทศ” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ใน รูปของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชนใน การบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้ มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหนาที่ ประมวลผลข้อมลู โดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่าง ระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet) - ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายใน หน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศ ภายในหน่วยงาน - ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชนในการ วางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองคประกอบ เช่น ระบบ คอมพิวเตอร์ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศ เป็นต้น

“การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” หมายถึง การตรวจสอบการอนุมัติ และการ กำหนด สิทธิในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้

“เครื่องเซิร์ฟเวอร์(Server)” หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหนาที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็น ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลยางชุมน้อย ลูกข่ายใน ระบบเครือข่าย

“อุปกรณ์UPS” หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้า เกิดมี ปญหาขึ้นมา เช่นไฟตกไฟเกิน ไฟดับหรือไฟกระชาก เป็นต้น โดยที่อุปกรณ์UPS จะจ่ายพลังงาน ออกมา อย่างต่อเนื่องและ มีคุณภาพในทุกสถานการณ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหาย ที่สามารถ เกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์

อิเล็กทรอนิคส (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมี หนาที่ในการจ่ายพลังงานไฟฟ้า สำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือ คอมพิวเตอร์เมื่อเกิดปญหาทาง ไฟฟ้า

“ซอฟต์แวร์(Software)” หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์จึง หมายถึง ลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์คำสั่งเหลานี้เรียงกันเป็น โปรแกรม คอมพิวเตอร์จากที่ทราบมาแล้วว่า คอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียง การกระทำกับ ข้อมลู ที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็น เสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์เพราะเป็นลำดับขั้นตอนการทำงาน ของ คอมพิวเตอร์คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึง หมาย รวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

“ไวรัสคอมพิวเตอร์” หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ใน ระบบคอมพิวเตอร์ได้และถามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆซึ่งอาจเกิด จากการ นำเอา ดิสกที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือ ระบบสื่อสารข้อมูล ไวรัสก็อาจ แพรระบาดได้เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝงตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อย แล้ว เนื่องจากไวรัสเป็นแคโปรแกรมหนึ่ง การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้น จะต้องมีการถูก เรียก ให้ทำงาน ได้ขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่ทราบว่าได้ทำการปลุก คอมพิวเตอร์ไวรัส นั้นๆขึ้นมาทำงาน แล้ว

“เวชระเบียน” หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่เป็นเอกสาร และข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลยางชุมน้อย

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความ มั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิและการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาต จากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเทานั้น

ข้อ ๒. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล จะต้องขออนุญาต เป็นลายลักษณอักษรต่อผู้บริหาร

ข้อ ๓. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของ ผู้ใช้งาน และหนาที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการ เข้าถึงอย่างสม่ำเสมอ ดังนี้

(๓.๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อน,ข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็นลายลักษณอักษร และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓.๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของ ข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็น มาตรการที่

ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และใน การ รักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่ สำคัญไว้ ดั้งนี้

(๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ข้อมูลสถานพยาบาล เป็นต้น (๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด

- ข้อมูลที่มีระดับความสำคัญปานกลาง

- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะกอให้ เกิดความเสียหายอย่างร้ายแรงที่สุด - ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะกอให้ เกิดความเสียหายอย่างร้ายแรง - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะกอให้เกิด ความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพรทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟลที่ผลิตจาก เครื่องมือที่ เป็นซอฟต์แวร์ปกติ เมื่อเปิดไฟลจะสามารถเห็นตัวอักษรในไฟล และพอที่จะ อ่าน ข้อความนั้นได้ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟลที่ผลิตจากเครื่องมือที่ เป็นซอฟต์แวร์มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ ๔. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ ของ หน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๕. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแกไข เปลี่ยนแปลงสิทธิต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๖. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็น

หลักฐานในการตรวจสอบ

ข้อ ๗. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึง ได้ ตลอดเวลา
(๒) ระบบงานภายใน (BackOffice) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

ส่วนที่ ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ดังนี้

(๑) จัดทำแบบฟอรมการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซอน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหนาที่ความรับผิดชอบ ตามข้อ ๓

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณอักษรให้แก่ผู้ ใช้งานเพื่อแสดงถึงสิทธิและหนาที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบ คอมพิวเตอร์โปรแกรมประยุกต(Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไรสาย (Wireless LAN) ระบบ อินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหนาที่ และ ได้รับความเห็นชอบเป็นลาย ลักษณอักษร

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอ อย่างน้อยปละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) จัดทำบัญชีรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และ ตรวจสอบสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแกไขข้อมูล สิทธิต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายใน ต้องดำเนินการภายใน ๗ วัน

ข้อ ๑๑. การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพน จากตำแหน่งหรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยง การใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์(E-Mail) ที่ไม่มีการ ป้องกันในการ ส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใสรหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไวในระบบคอมพิวเตอร์ใน รูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๗) ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการ ใช้ งานทันทีเมื่อพนระยะเวลาดังกล่าวหรือพนจากตำแหน่ง และมีการกำหนดสิทธิพิเศษ ที่ได้รับว่าสามารถ

เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัส ผู้ใช้งาน ตามปกติ

ข้อ ๑๒. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการ เข้าถึง ข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

ส่วนที่ ๓
การกำหนดหนาที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๓. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหนาที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ ร่วมกับผู้อื่น รวมทั้งห้าม ทำการเผยแพร แจกจ่าย ทำให้ผู้อื่นลวงรู้รหัสผ่าน (Password)

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย คอมพิวเตอร์

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไวในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) กำหนดรหัสผ่านเริ่มตนให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับ ผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อย ๑ ครั้งต่อป

ข้อ ๑๔. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการ รักษา ความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็น มาตรฐานสากล ข้อ ๑๕. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้ เป็น ความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วน บุคคล ซึ่งผู้ใช้งาน จะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง ข้อ ๑๖. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของ หน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความ ผิดพลาดใดๆ ก็ดี ผู้ใช้งาน ต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูล ซึ่ง สามารถบงบอกตัวตนบุคคลผู้ใช้งานได้

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการ ล็อกหนาจอทุกครั้ง และต้องทำการ พิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหนาจอ (screen saver) โดยตั้งเวลา อย่าง น้อย ๑๕ นาท

ข้อ ๑๗. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ โรงพยาบาล หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๘. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้าม ไม่ให้ทำการเผยแพร เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๑๙. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลและข้อมูลของ ผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพรโดยไม่ได้รับอนุญาต ผู้ใช้งานต้อง มีส่วนร่วมใน การรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๐. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไวซึ่งความลับ ความถูกต้อง และความพรอมใช้ของข้อมูล ตลอดจน เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่ มีสิทธิ

ข้อ ๒๑. ผู้ใช้งานมีสิทธิโดยขอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม เห็นสมควร โรงพยาบาลยางชุมน้อยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้ บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครอง ข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาล ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับ โรงพยาบาล ซึ่ง โรงพยาบาลอาจแต่งตั้งให้ผู้ทำหนาที่ ตรวจสอบข้อมูลเหลานั้นได้ตลอดเวลา โดยไม่ ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเทาเทียมกัน หมายความ ว่า แต่ละเครื่อง ต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไวเอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรม หรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เทานั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกัน เช่น บิทเทอรเรนท (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟัง เพลง เกมส เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๔. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพรข้อมูล ข้อความ รูปภาพ หรือ สิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของ โรงพยาบาล

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน กอให้เกิดความเสียหาย หรือใช้ในการ โจรกรรม ข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของ โรงพยาบาล

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชนทางการคา

ข้อ ๒๗. ห้ามกระทำการใดๆเพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ใน เครือข่าย ระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆก็ตาม

ข้อ ๒๘. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๒๙. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศ ภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๐. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ ว่ากรณีใดๆ เพื่อประโยชนในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

ข้อ ๓๑. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาล โดย ไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๒. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ ข้อมูลร่วมกันในระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น โรงพยาบาล หรือหน่วยงานที่มาขอเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูล ร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันที่เพียงพอ

ส่วนที่ ๔

การบริหารจัดการสินทรัพย์(Assets Management)

ข้อ ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์(Operation Center หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็น เขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เว้น แต่จะ ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่าย เพื่อการประกอบธุรกิจส่วน บุคคล

ข้อ ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับ อนุญาต

ข้อ ๓๗. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๘. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัด อุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่ จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึง ข้อมูลสำคัญนั้นได้และพิจารณาวิธีการ ทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	- ใช้การทำลายด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	- ใช้วิธีการทุบหรือบดให้เสียหาย
ฮารดดิสก	- ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๙. ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาล

ข้อ ๔๐. ความเสียหายใดๆ ที่เกิดจากการละเมิดตาม

ข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้ งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๕
การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๑. มาตรการควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตร ประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหนาที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำ การ ลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไวในเอกสาร “บันทึกการเข้าออกพื้นที่”

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการ ปฏิบัติงาน มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอรมการขอ อนุญาตเข้าออก ตามที่ระบุไวในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอรมการขอ อนุญาต เข้าออกกับเจ้าหนาที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๒. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่าย ของ หน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งาน ต้องกรอก แบบฟอรม “การขอเชื่อมต่อเครือข่าย”

ข้อ ๔๓. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงาน รับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรม ใด ๆ ที่ส่งผล กระทบ ต่อการกระทำของระบบและผู้ใช้งานอื่นๆ

ข้อ ๔๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเสนทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๔. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับ อนุญาต เทานั้น

(๒) จำกัดเสนทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เสนทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อ ไม่ให้ผู้ใช้งานสามารถใช้เสนทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ หน่วยงานใน ลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้อง มีการลง บันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน

(Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบ เครือข่ายภายในของหน่วยงาน

(๘) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต ของระบบ เครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พรอมทั้งปรับปรุงให้เป็นปจจุบันอยู่ เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่า สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งตนทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอรม “การขอเชื่อมต่อเครือข่าย”
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๖. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการ ดูแล ระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแกไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๗. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงาน ต้องมีการขออนุมัติจากผู้ดูแลระบบก่อน ดำเนินการให้ติดตั้ง

ข้อ ๔๘. กำหนดให้มีการจัดเก็บรหัสตนฉบับ (source code), คลังโปรแกรม (Library) และเอกสาร สำหรับซอฟต์แวร์ของระบบงาน ไวในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๔๙. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความ ถูกต้อง และสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์๒๕๕๐

ข้อ ๕๐. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณอักษร เพื่อขอ อนุญาต จากหัวหน้าหน่วยงาน

(๒) มีการควบคุมชองทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใดๆที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาต จากหัวหน้าหน่วยงาน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมี การลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๑. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึง เครือข่ายที่ไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน ระบบสารสนเทศภายใน

ข้อ ๕๒. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกบั ระบบเครอื ข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปละ ๑ ครั้ง นอกจากนี้การ กำหนด แกไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๓. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้อง เชื่อมต่อ ผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟรวอลล (Firewall) หรือฮารดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์(Malware) ด้วย

ข้อ ๕๔. ต้องมีการติดตั้งระบบตรวจจบั การบกุ รุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่ เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแกไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจ หนาที่เกี่ยวข้อง

ข้อ ๕๕. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอก ที่ เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของ ระบบเครือข่ายได้โดยง่าย

ข้อ ๕๖. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจาก ผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเทาที่จำเป็น

ส่วนที่ ๖
การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๕๗. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการ ใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การ ลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๕๘. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนใน การเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๒) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หนาจอ เป็น เวลานาน

(๓) ซอฟทแวร์ที่โรงพยาบาลจัดเตรียมไวให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำ การติดตั้ง ถอดถอนเปลี่ยนแปลง แกไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๔) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเพื่อประโยชนทางการคา

(๕) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๖) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดย ไม่ได้รับ อนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๕๙. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อ ตรวจสอบความ ถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๖๐. การใช้งานโปรแกรมประเภทยูทิลิตี้(Use of system utilities) ต้องจำกัดและควบคุมการใช้ งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิด สามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการ ละเมิด หรือหลีกเลี่ยง มาตรการความมั่นคงปลอดภัยที่ได้กำหนดไวหรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยัน ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้เพื่อจำกัดและควบคุมการ ใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มี ความจำเป็น ในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๖๑. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทิ้งปิดการใช้งานด้วย หลังจากที่ ไม่มีกิจกรรมการใช้งานชวงระยะเวลา ๑๕ นาที

(๒) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานเร็วขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ ๖๒. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามชวงเวลา การทำงานที่หน่วยงานกำหนดเทานั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดชวงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๗
การควบคุมการเข้าถึงโปรแกรมประยุกตหรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control)

ข้อ ๖๓. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตาม ความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือ การเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๔. ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต (Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไรสาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหนาที่ และต้องได้รับความ เห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณอักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ

ข้อ ๖๕. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบ สารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำ การการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๖๖. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออกหรือพ นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไวในระบบคอมพิวเตอร์ ในรูปแบบ ที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับ ความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและ ระงับการใช้งาน ทันทีเมื่อพนระยะเวลาดังกล่าว หรือพนจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่า เข้าถึงได้ระดับ ใด ได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๖๗. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทขั้นความลับ ในการควบคุมการเข้าถึง ข้อมูลแต่ละประเภทขั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึง วิธีการทำลายข้อมูลแต่ละประเภทขั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทขั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผา น ระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบ ตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละขั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพนระยะเวลาดังกล่าว

(๔) การรับลงข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่ เป็น มาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซอม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๖๘. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดลอมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเทานั้น

ข้อ ๖๙. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพรอมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพรอมใช้ งาน หรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกดัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้ มี การเผยแพรเป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน าที่ที่รับผิดชอบทันที

(๔) เจ้าหนาที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพรอมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้ นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๘
การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี
(Software Licensing and intellectual property and Preventing Malwares)

ข้อ ๗๐. โรงพยาบาลได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงาน อนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหนาที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการ ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิด ลิขสิทธิ์ ถือว่าเป็น ความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๑. ซอฟต์แวร์(Software) ที่หน่วยงานได้จัดเตรียมไวให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้าม มิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แกไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการ อนุญาตจาก หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์

ข้อ ๗๒. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์(Antivirus) ตามที่ หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้า หน่วยงาน

ข้อ ๗๓. บรรดาข้อมูล ไฟล ซอฟต์แวร์หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบ ไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๔. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๕. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ ใช้งาน ต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๗๖. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้า ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๗๗. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็น สินทรัพย์ของหน่วยงานหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๗๘. ห้ามทำการเผยแพรไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆ ที่อาจกอให้เกิด ความ เสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิที่จะพัฒนาโปรแกรมหรือฮารดแวร์ใดๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮารดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้ง การกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือ แกะรหัสผ่านของ บุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮารดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการ ครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับ หนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮารดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือ ขัดต่อ ศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๗๙. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปญ ญาสำหรับรหัสตนฉบับ (source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของ ซอฟต์แวร์ที่ จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไวในสัญญาจ้างที่ทำไวกับผู้ให้บริการภาย นอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อน ดำเนินการ ติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาขอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการ เปลี่ยนรหัสผ่านต่างๆให้พรอมใช้งาน

ส่วนที่ ๙
ภายนอกสำนักงาน (Teleworking)

ข้อ ๘๐. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยี สารสนเทศของหน่วยงานจากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟรวอลลตามที่หน่วยงานกำหนด

ข้อ ๘๑. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และ อุปกรณ์สื่อสารไวไหกับผู้ใช้งานจากระยะไกล

ข้อ ๘๒. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการ ตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๘๓. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ หน่วยงาน จากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใตการควบคุมตามนโยบายความมั่นคงปลอดภัยของ หน่วยงาน

ข้อ ๘๔. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ขั้นความลับของข้อมูลระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๘๕. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ การ เข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐
การควบคุมการเข้าถึงระบบเครือข่ายไรสาย (Wireless LAN Access Control)

ข้อ ๘๖. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไรสาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไรสายให้น้อยที่สุด

ข้อ ๘๗. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดย ปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไรสาย (Access Point) มาใช้งาน และ กำหนดให้ซอน SSID (Service Set Identifier) ข้อ ๘๘. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจาย สัญญาณแบบไรสาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไรสาย

ข้อ ๘๙. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address)และ ชื่อ ผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีลิทธิในการเข้าใช้งานระบบเครือข่ายไรสาย โดยจะ อนุญาตเฉพาะอุปกรณ์ทีมี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ตามที่กำหนดไวเทานั้นให้เข้าใช้ระบบเครือข่ายไรสายได้อย่าง ถูกต้อง

ข้อ ๙๐. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟรวอลล (Firewall) ระหว่างระบบเครือข่ายไรสายกับ ระบบ เครือข่ายภายในหน่วยงาน

ข้อ ๙๑. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไรสายติดต่อสื่อสารกับเครือข่ายภายใน หน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไรสาย ข้อ ๙๒. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไรสาย

ข้อ ๙๓. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮารดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณที่นาสงสัยที่เกิดขึ้นในระบบเครือข่ายไรสาย และ จัดส่งรายงานผลการ ตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไรสายที่ ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที ข้อ ๙๔. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งาน ระบบ เครือข่ายไรสายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

ข้อ ๙๕. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไรสายของโรงพยาบาลจะต้องทำการลงทะเบียนกับผู้ดูแล ระบบ และต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณอักษร

ข้อ ๙๖. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไรสาย ให้เหมาะสมกับหนาที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไรสาย รวมทั้งมีการทบทวน สิทธิ การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๑๑
การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๙๗. หน่วยงานมีหนาที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๙๘. การกำหนดค่าเริ่มตนของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๙๙. ทุกบริการ (Services) และเสนทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูก บล็อก (Block) โดย Firewall

ข้อ ๑๐๐. ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๐๑. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลง ทุก ครั้ง หากมีการเปลี่ยนแปลงค่าต่างๆ ของ Firewall

ข้อ ๑๐๒. การเข้าถึงตัวอุปกรณ์Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแล จัดการ เทานั้น

ข้อ ๑๐๓. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐๔. การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิด พอร์ตการ เชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการ เชื่อมต่อนอกเหนอื ที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๑๐๕. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้อง กำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเทานั้น

ข้อ ๑๐๖. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆของอุปกรณ์Firewall เป็นประจำทุกสัปดาห์ หรือ ทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๐๗. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆภายในหน่วยงาน ที่มี ลักษณะที่ เป็นอินทราเน็ต จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องอนุญาต เป็นกรณีไป

ข้อ ๑๐๘. หน่วยงานมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มี พฤติกรรมการ ใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเลี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแกไข

ข้อ ๑๐๙. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรือ อุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่อง คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นขอบจากหัวหน้าหน่วยงานก่อน

ข้อ ๑๑๐. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ต ทันที

ส่วนที่ ๑๒
การควบคุมการใช้จดหมายอิเล็กทรอนิกส์(E-Mail)

ข้อ ๑๑๑. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไวในระบบคอมพิวเตอร์ ข้อ ๑๑๒. เปลี่ยนรหัสผ่าน (Password) ทุก ๓- ๖ เดือน

ข้อ ๑๑๓. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจาของผูใชงานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์(EMail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์(E-Mail) ของตน

ข้อ ๑๑๔. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์(E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๑๕. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว ให้ใช้ความระมัดระวังในการระบุชื่อ ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๑๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๑๗. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ (Chain Letter)

ข้อ ๑๑๘. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น ข้อ ๑๑๙. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๐. ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อ ๑๒๑. ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๒๒. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบ ไฟล โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟลที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ ๑๒๓. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รูจัก

ข้อ ๑๒๔. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูล อันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๒๕. ผู้ใช้งานต้องตรวจสอบตูเก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน ควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออก จากระบบ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๒๖. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไวในตูจดหมายอิเล็กทรอนิกส์

ข้อ ๑๒๗. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติ คณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารใน ภาครัฐ

ส่วนที่ ๑๓
การควบคุมการใช้อินเตอร์เน็ต (Internet)

ข้อ ๑๒๘. ผู้ดูแลระบบ ต้องกำหนดเสนทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไวเทานั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านชองทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความ จำเป็น และต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ อักษร

ข้อ ๑๒๙. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์(Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดชอง โหวของ ระบบปฏิบัติการ

ข้อ ๑๓๐. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๑. ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชนในเชิงพาณิชยเป็นการส่วน บุคคล และทำการเข้าสู่เว็บไซตที่ไม่เหมาะสม เช่น เว็บไซตที่ขัดต่อศีลธรรม เว็บไซตที่มีเนื้อหาอัน อาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซตที่เป็นภัยต่อ สังคม หรือ ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจกอให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๑๓๒. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็น ทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ ๑๓๓. ระมัดระวังการดาวนโหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๓๔. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ หน่วยงาน ข้อ ๑๓๕. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของ หน่วยงานอื่นๆ

ข้อ ๑๓๖. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความ มั่นคงแหงราชอาณาจักร อันเป็นความผิดเกี่ยวกับการกอการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการ เผยแพรหรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อ ๑๓๗. หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์ เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่น ๆ ข้อ ๑๓๘. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งาน โดย บุคคลอื่น ๆ

ข้อ ๑๓๙. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๔
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๔๐. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงาน ราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานดัดลอกโปรแกรมต่างๆ และ นำไปติดตั้งบน เครื่องคอมพิวเตอร์ส่วนตัว หรือแกไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแกไขเปลยี่ นแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วน บุคคลของหน่วยงาน

(๔) การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซอมจะต้องดำเนินการโดยเจ้าหนาที่ของโรงพยาบาลเทานั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกัน ไวรัส

(๖) ผู้ใช้งาน มีหนาที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จ สิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหนาที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ ๑๔๑. การใช้รหัสผ่าน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไวหนาเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓- ๖ เดือน

ข้อ ๑๔๒. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟลที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟลที่ ดาวนโหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำ ให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูก แกไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว

ข้อ ๑๔๓. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไวบนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหนาที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไวในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกูคืนข้อมูลที่สำรองไวอย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไวบน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญ เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของ หน่วยงาน

ส่วนที่ ๑๕
การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๑๔๔. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ ในงานราชการ

(๒)โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่ หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไป ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแกไข หรือนำไปให้ผู้อื่นใช้งาน โดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคูมือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

(๔)ไม่คัดแปลงแกไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอรให้ มี สภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใสกระเป๋าสำหรับเครื่อง คอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโตะทำงาน หรือ หลุดมือ เป็นต้น

(๖) หลีกเสี่ยงการใช้นิ้วหรือ ของแข็ง เช่น ปลายปากกา กดสัมผัสหนาจอ LCD ให้เป็นรอย ขีด ขวน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของทับบนหนาจอและแปนพิมพ

(๘) การเข็ดทำความสะอาดหนาจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทาง เดียวกัน ห้ามเข็ดแบบหมุนวน เพราะจะทำให้หนาจอมีรอยขีดขวนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ต้อง ปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใตแปนพิมพ ห้ามย้ายเครื่องโดยการดึงหนาจอภาพขึ้น

ข้อ ๑๔๕. ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหนาที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรลอกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไวในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนสูง ความขึ้น ฝุนละออง และต้องระวังป้องกันการตกกระทบ

ข้อ ๑๔๖. การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบบาพกพา

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีและรัดกุม

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใสรหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หนาจอเป็นเวลานาน

ข้อ ๑๔๗. การใช้รหัสผ่านให้ผู้ใช้งาน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไวหนาเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓- ๖ เดือน

ข้อ ๑๔๘. การสำรองข้อมูลและการกูคืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา และสื่อต่างๆ เพื่อป้องกัน การสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไวในสถานที่ ที่เหมาะสม ไม่ เสี่ยง ต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไวจะต้องทำการทดสอบการกูคืน อย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไวบน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญ เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสีย จะไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๖
การตรวจจับการบุกรุก
(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ ๑๔๙. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัย ของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคง ปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรกุเครอือข่าย พรอมกับบทบาทและความรับผิดชอบที่ เกี่ยวข้อง

ข้อ ๑๕๐. IDS/IPS Policy ครอบคลุมทุกโฮสต (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเสนทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ตทุกเสนทาง

ข้อ ๑๕๑. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจาก ระบบ IDS/IPS

ข้อ ๑๕๒. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๕๓. โฮสต (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการ ตรวจสอบ

ข้อ ๑๕๔. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๕๕. ต้องมีการตรวจสอบเหตุการณ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณ ข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๕๖. IDS/IPS จะทำงานภายใตกฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่าย ของระบบ สารสนเทศตามปกติ

ข้อ ๑๕๗. เครื่องแม่ข่ายที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๕๘. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตี ระบบ พฤติกรรมที่นาสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะตองมี การรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ

ข้อ ๑๕๙. พฤติกรรม กิจกรรมที่นาสงสัยหรือระบบการทำงานที่ผิดปกติที่ถูกคนพบจะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๖๐. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไวไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๖๑. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบ ของเหตุการณต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณที่ อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๖๒. หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครอื ข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการ บุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานลวงหนา

ข้อ ๑๖๓. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบ สารสนเทศ จะ

ถูก ระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคลองกับกฎหมาย ว่าด้วยการ กระทำความผิดที่เกี่ยวกับคอมพิวเตอร์หรือเป็นการกระทำที่ลงผลให้เกิดความ เสียหาย ต่อข้อมูล และทรัพยากร ระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗
การติดตั้งและกำหนดค่าของระบบ
(System Installation and Configuration)

ข้อ ๑๖๔. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address

(๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการ ที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรบั ปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการ สแกนและปรับปรุงโปรแกรม

ข้อ ๑๖๕. การบริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ ๑๖๖. การปรับปรุงการรักษาความปลอดภัย/Anti-Virus (System Security & Anti-virus Update)

(๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์การเข้าใช้ระบบ

(๒) ประสิทธิภาพของระบบ (Performance) หรือตรวจสอบจากระบบรักษาความปลอดภัย ที่ ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปญหา

(๔) ปรับปรุงโปรแกรม Anti-virus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

ข้อ ๑๖๗. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

(๓) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและ สิทธิการใช้

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปญหาอยู่เสมอ

ข้อ ๑๖๘. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ/ กำหนดค่าระบบของโปรแกรม กำหนดผู้ใช้ และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรม หรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้น กำหนด

(๔) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อ รหัสผ่าน และ สิทธิ การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว

(๕) กำหนดเกณฑการสำรอง สำเนา ทดสอบกูคืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

ส่วนที่ ๑๘
การจัดเก็บข้อมูลจราจรคอมพิวเตอร์(Log)

ข้อ ๑๖๙. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) ไวในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดขั้นความลับในการ เข้าถึง

ข้อ ๑๗๐. ห้ามแกไขข้อมูลจราจรคอมพิวเตอร์(Log) ที่เก็บรักษาไว

ข้อ ๑๗๑. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบปองกนัการบุกรกุ เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ ระบบ เป็นต้น เพื่อประโยชนในการใช้ตรวจสอบและต้องเก็บบันทึกไวอย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุด ลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๗๒. ต้องมีวิธีการป้องกันการแกไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหลานั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเทานั้น

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรูเข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑. กำหนดสิทธิและความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้ กำหนดกลุ่ม ผู้ใช้งาน และสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การ กำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ปอนข้อมูล
- แกไข
- อนุมัติ
- ไม่มีสิทธิ

(๒.๒) กำหนดเกณฑการระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การ เข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็น ลายลักษณอักษร และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับ มอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำ รับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชยที่ให้บริการ เช่น ข้อมูลดัชนีเศรษฐกิจ

การคา ข้อมูลการคาระหว่างประเทศของไทย ข้อมูลเศรษฐกิจการคาจังหวัด เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะกอให้ เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมากหมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้ เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะกอให้เกิด ความเสียหาย - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพรทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนชองทางที่สามารถเข้าถึง

ข้อ ๒. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ เข้าใช้ หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทาง ราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒

ข้อ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้ งาน และโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชนในการตรวจสอบความถูกต้องของการ ใช้งาน ฐานข้อมูล

ข้อ ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส วน ราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับ หน่วยงาน ภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะ มีการ ขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหนาที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือ แลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหนาที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อ เป็น การป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิด เหตุการณความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์หรืออื่นๆ ที่มี ความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พรอ มใช้ งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๗. กำหนดหนาที่และความรับผิดชอบของเจ้าหนาที่ในการสำรองข้อมูล

ข้อ ๘. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พรอมทั้งกำหนด ระบบ สารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพรอมกรณีฉุกเฉิน อย่างน้อยปละ ๑ ครั้ง

ข้อ ๙. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการ สำรอง ข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มี วิธีการสำรอง ข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ผู้ดำเนินการ วัน/เวลาชื่อ ข้อมูลที่ สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบค่าคอนฟกกูเรชัน (Configuration) ต่างๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถ แสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไวอย่าง ชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไวนอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับ หน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไวนอกสถานที่นั้น ในกรณีที่เกิดภัย พิบัติกับหน่วยงาน

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอก สถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกูคืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกูคืน ข้อมูล อย่างสม่ำเสมอ อย่างน้อยปละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว

ข้อ ๑๐. ต้องจัดทำแผนเตรียมความพรอมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหนาที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหลานั้น และกำหนดมาตรการ เพื่อลด ความเสี่ยงเหลานั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม น้ำท่วม แผ่นดินไหว การชุมนุมประทวงทำ ให้ไม่สามารถเข้ามาใช้ระบบงานได้เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกูคืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกูคืนข้อมูลที่สำรองไว

(๕) มีการกำหนดชองทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร ดแวร ซอฟต์แวร์เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือใหความรูแก่เจ้าหนาที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งดวน เป็นต้น

ข้อ ๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพรอมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ อย่าง เหมาะสม และสอดคลองกับการใช้งานตามภารกิจ อย่างน้อยปละ ๑ ครั้ง ข้อ ๑๒. ต้องมีการกำหนดหนาที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพรอมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

ข้อ ๑๓. ต้องมีการทดสอบสภาพพรอมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผน เตรียมพรอมกรณีฉุกเฉิน อย่างน้อยปละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่างๆ ที่จะ เกิดขึ้น เพื่อให้ระบบมีสภาพพรอมใช้งานอยู่เสมอ

ข้อ ๑๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพรอมกรณีฉุกเฉิน ที่ เพียงพอ ต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความ มั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึง ประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของ หน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่าง น้อยปละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย สารสนเทศ โดยมี แนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงดังนี้

ข้อ ๑. จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒. คนหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพรอมข้อเสนอแนะ

ข้อ ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบ สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่าง เดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างลำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บ ไวโดยมีการ ป้องกัน เป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหาร จัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลแสดงการ เข าถึง นั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้ง เครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการ จัดเก็บ ป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่างๆได้๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหนาที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหนาที่ หรือบุคลากรของหน่วยงานขาดความรูความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้เกิดการ ชะงักหรือ หยุด ทำงาน และอาจส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็ม ประสิทธิภาพ จึงได้กำหนดแนวทางการดำเนินการเบื้องตนเพื่อลดปญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยี สารสนเทศไว ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหนาที่ของหน่วยงาน ให้มีความรูความเชาใจในด้าน Hardware และ Software เบื้องตน เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหนาที่มี ความรูความเข้าใจ การใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงทีเกิดจาก Human error ลด น้อยลง

(๒) จัดทำคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่าง ถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบ เครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์(Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), มาโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหลานี้อาจ รบกวน การทำงาน และกอให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขึ้นทำให้ระบบเครือข่าย คอมพิวเตอร์ใช้งานไม่ได้จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหนาที่ในการกำหนดสิทธิการ เข้าใช้ งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์Anti-virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถ ตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ ประเภทที่ ๓ ภัยจากไฟไหม หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ ระบบ เทคโนโลยีสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบ เครื่อง แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถ ให้ บริการ ได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไวอย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณกระแสไฟฟ้าขัดข้องหรือมีควัน ไฟ เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษา ความ ปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันทวงที ซึ่งมีการตรวจสอบความ พรอมของ อุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไวใช้ในกรณีเหตุ ฉุกเฉิน (อัคคีภัย) โดยมีการตรวจสอบความพรอมของอุปกรณ์และทดลองใช้งานโดย สม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัย ร้ายแรง ที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับ สถาน การณ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณอากาศของกรม อุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไวในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดตัวตัดไฟเครื่องปรับอากาศ เพื่อป้องกัน เครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหนาที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุม เครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่และเตรียมความพรอมห้องควบคุมระบบเครือข่าย สำหรับติดตั้ง เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พรอมทั้งทดสอบ การใช้ งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ตรวจสอบ ระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูก ข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถ ให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดลอม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือ เข้าถึง พื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมี ผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยี สารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบ คอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของ บุคลากรทางคอมพิวเตอร์รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และอุปกรณ์ประกอบที่ ติดตั้งประจำโตะทำงาน

ข้อ ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญ แล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บงบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อก หรือใสกุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหนาที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณ ดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้ง ไว เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ดังนี้

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อ จุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้ง ป้องกัน ความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้ง จัดทำ แผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจ แบง ออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่ จัดเก็บ ข้อมูลคอมพิวเตอร์(Data Storage Area) และพื้นที่ใช้งานเครือข่ายไรสาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔. การควบคุมการเข้าออก อาคารสถานที่

(๑) กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และชวงเวลาที่มีสิทธิในการผ่านเข้าออก ใน แต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหนาที่รักษา ความ ปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตร ประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้ว ทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอรมการเข้าออกพรอม กับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเดนชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเดนชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องคอมพิวเตอร์ แม่ข่าย (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจาก ไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑหรือข้อกำหนด ต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้าออกใน พื้นที่หรือบริเวณที่มีความสำคัญ (ห้องคอมพิวเตอร์แม่ข่าย Server Room ,Data Center)

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานใน พื้นที่ หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่าง น้อยป ละ ๑ ครั้ง

ข้อ ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อ ความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้ - ระบบสำรองกระแสไฟฟ้า (UPS) - เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) - ระบบระบายอากาศ - ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหลานั้นอย่างน้อยปละ ๑ ครั้ง เพื่อให้ มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการลมเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้อง เครื่อง

ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปใน บริเวณที่ มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยทอสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัด สายสัญญาณ เพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวน ของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเสน

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใสสลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคล ภายนอก

(๗) พิจารณาใช้งานเสนใยแกวนำแสงแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณ แบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับ สัญญาณ โดยผู้ไม่ประสงค์ดี

ข้อ ๗. การบำรุงรักษาอุปกรณ์(Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามดำแนะนาในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการ ตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปญหาและข้อบกพรองของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและ ปรับปรุง อุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดสองดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษา อุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจาก ภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคลองกับระยะเวลาที่อนุญาตและ ตรวจสอบ การชำรุดเสียหายของอุปกรณ์

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไวเป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือ ทรัพย์สิน ของ หน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไวโดยลำพังในที่สาธารณะ

(๓) เจ้าหนาที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญใน อุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมลู สำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองเหตุการณความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณละเมิดความปลอดภัย ระบบ สารสนเทศ ให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑. ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการ ตรวจสอบมีดังต่อไปนี้ - มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด

- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด - หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒. ระบบไฟรวอลล

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟรวอลล สิ่งที่ต้อง ตรวจสอบมี ดังต่อไปนี้

- Packet ที่ไฟรวอลลได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณละเมิดความปลอดภัยระบบสารสนเทศ ให้ แจ้ง หัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแกไขปญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์(Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัย คุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมิดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลฯ ไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแกไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่า กระจายอยู่ในเครือข่ายโรงพยาบาล

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้าง นอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแกไขเครื่องนั้นทันท

หมวดที่ ๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรูความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของ โรงพยาบาล

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ โดย ไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปจจุบันอยู่เสมอ อย่างน้อยปละ ๑ ครั้ง

ข้อ ๒. จัดฝกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝกอบรม โดยใช้วิธีการ เสริม เนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆตามแผนการฝกอบรมของหน่วยงาน

ข้อ ๓. จัดสัมมนาเพื่อเผยแพร นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการ ดำเนินงานปละไม่ น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และ มีการเชิญวิทยากรจาก ภายนอกที่มีประสบการณด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมา ถ่ายทอดความรู

ข้อ ๔. ติดประกาศประชาสัมพันธ์ให้ความรูเกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรูหรือข้อระวัง ใน รูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรูอยู่เสมอ

ข้อ ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความ ต้องการของผู้ใช้งาน

ข้อ ๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหนาที่มีความรูความ เข้าใจ และสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้อง ดำเนินการ อย่างไร

ข้อ ๗. สร้างความรูความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณด้านความมั่นคงปลอดภัยที่ เกิดขึ้น และสถานการณด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตาม นโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้ง กฎระเบียบ ของโรงพยาบาลฯ และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตาม กฎหมายดังกล่าว ถือ ว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

หมวดที่ ๗
หนาที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหนาที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหนาที่ ตลอดจนผู้ ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับผู้อำนวยการ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหนาที่ในระดับปฏิบัติงาน

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือ ข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆแก่องคกรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความ บก พรอง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ

ข้อ ๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่ม/หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือ เทียบเท่า หัวหน้ากลุ่ม

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติงาน ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยี สารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบ ฐานข้อมูล

ข้อ ๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ผู้ที่ได้รับมอบหมายให้ปฏิบัติหนาที่จากหัวหน้าส่วนราชการ โรงพยาบาล เช่น นักวิชาการคอมพิวเตอร์เจ้าหนาที่เครื่องคอมพิวเตอร์

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแกไขบัญหาระบบความมั่นคงปลอดภัยของ ฐานข้อมูลและสารสนเทศ จากสถานการณความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่อง คอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่ กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแกไขปญหาการถูกเจาะเข้าระบบฐานข้อมูลจาก บุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศของโรงพยาบาล


โรงพยาบาลยางชุมน้อย
YANGCHUMNOI HOSPITAL

ภาคผนวก


โรงพยาบาลยางชุมน้อย
YANGCHUMNOI HOSPITAL

การจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตาม ประกาศนี้มี๒ ส่วน ดังนี้

๑.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่าง น้อยครอบคลุมตามข้อ ๔

๑.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหา อย่างน้อย ครอบคลุมตามข้อ ๔-๑๔

ข้อ ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๒.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมใน การทำ นโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณอักษร โดยประกาศให้ผู้ใช้งานทราบและ สามารถ เข้าถึง ได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาล

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปละ ๑ ครั้ง

๒.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๔) การสร้างความรูความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ ๓. มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ(access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึง การใช้งานและ ความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑเกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่ เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้น ความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และชองทางการเข้าถึง

ข้อ ๔. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) อย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทำข้อปฏิบัติสำหรับการควบคุมการ เข้าถึงสารสนเทศ

(๒) มีการปรับปรุงให้สอดคลองกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนด ด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ หลักการ
“ตามความจำเป็นที่ต้องรู”

ข้อ ๕. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึง ระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ ซึ่งไม่ได้รับอนุญาต อย่างน้อย ดังนี้

(๑) สร้างความรูความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึง ภัยและผลกระทบ ที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรูเทาไม่ถึงการณ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทาง ปฏิบัติสำหรับ การลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการ ตัด ออกจาก ทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการ ควบคุม และจำกัด สิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ จำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights) ต้องจัดให้มี กระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่ กำหนดไว

ข้อ ๖. มีการกำหนดหนาที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การลวงรูหรือการลักลอบทำสำเนาข้อมูล สารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน ใน การกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์กำหนดแนวปฏิบัติที่ เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์(Clear Desk And Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึก ข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้อง กำหนดให้ ผู้ใช้งาน ออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็น ความลับ โดยให้ปฏิบัติตาม ระเบียบ การรักษา ความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๗. มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกัน การเข้าถึงบริการทาง เครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศ ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเทานั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (UserAuthentication For External Connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลกอ นที่จะ อนุญาตให ผู้ใช้งานที่อยู่ ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของ หน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification เท Networks) ต้องมีวิธีการที่ สามารถระบุอุปกรณ์บนเครือข่ายได้และควรใช้การระบุอุปกรณ์บนเครือข่าย เป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับ ตรวจสอบและ ปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation In Networks) ต้องทำการแบ่งแยก เครือข่าย ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้อง ควบคุมการ เข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคลองกับ แนว ปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเสนทางบนเครือข่าย (Network Routing Control) ต้อง ควบคุมการจัด เสนทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือ ไหลเวียนของ ข้อมูลหรือสารสนเทศสอดคลอ งกบั แนวปฏิบัติการควบคุมการเข้าถึง หรือการ ประยุกตใช้งาน ตามภารกิจ


โรงพยาบาลยางชุมน้อย
YANGCHUMNOI HOSPITAL