ประกาศโรงพยาบาลทุ่งใหญ่
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ICT Security Policy)
พ.ศ. ๒๕๖๗

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ และประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างราบรื่น รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศที่มีลักษณะไม่ถูกต้อง และจากถูกคุกคามจากภัยต่างๆ โรงพยาบาลทุ่งใหญ่จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด ดังนี้

๑. ประกาศฉบับนี้มีวัตถุประสงค์เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่
๒. ให้บุคลากรทุกระดับของโรงพยาบาลถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศตามประกาศนี้อย่างเคร่งครัด
๓. โรงพยาบาลทุ่งใหญ่สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ ตรวจสอบได้ และพร้อมใช้อยู่เสมอ
๔. โรงพยาบาลทุ่งใหญ่สนับสนุนนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูล เพื่อเป็นการป้องกันและรักษาข้อมูลความลับของผู้ใช้บริการและข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑๐ กรกฎาคม พ.ศ. ๒๕๖๗

(นายปกป้อง เศวตชนะ)
นายแพทย์ชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศโรงพยาบาลทุ่งใหญ่

จัดทำโดย

ศูนย์คอมพิวเตอร์

พ.ศ. ๒๕๖๗

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลทุ่งใหญ่

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

๑.๒ กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๒๒

๑.๓ นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลทุ่งใหญ่ได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ

๑.๖ นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

สารบัญ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“โรงพยาบาล” หมายถึง โรงพยาบาลทุ่งใหญ่

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่

“มาตรการ” หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น

“วิธีปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลทุ่งใหญ่ เช่น ผู้อำนวยการ หัวหน้าหน่วยงาน

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานกระทรวงสาธารณสุข และลูกจ้างชั่วคราว

“ผู้รับจ้างให้บริการจากภายนอก” หมายถึง เจาหนาที่หน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน (Outsource) ที่มีการใชงานหรือให้บริการเกี่ยวกับระบบสารสนเทศโรงพยาบาลทุ่งใหญ่

“หน่วยงานภายนอก” หมายถึง บริษัทที่โรงพยาบาลทุ่งใหญ่ได้ว่าจ้างหรือ มอบหมายให้ดำเนินการในเรื่องระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ ที่ปรึกษา ผู้รับจ้าง ผู้ขาย ผู้ให้บริการ หรือเป็นผู้ใช้บริการ และอื่น ๆ ที่เกี่ยวของ รวมถึงหน่วยงานภายนอกอื่นที่มาขอใชบริการด้วย

“ผู้ใช้งาน/ผู้ใช้บริการ” หมายถึง ขาราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองคกร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใชเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลทุ่งใหญ่

“สิทธิ์ของผู้ใชงาน/สิทธิ์ของผู้ใช้บริการ” หมายถึง สิทธิ์ที่ใชในการเขาถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งใหญ่

“สารสนเทศ” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่รูปของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet)

- **“ระบบแลน (LAN)”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

- **“ระบบอินเตอร์เน็ต (Internet)”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูล และสารสนเทศ เป็นต้น

“เครื่องคอมพิวเตอร์แม่ข่าย/เครื่องเซิร์ฟเวอร์ (Server)” หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย

“อุปกรณ์สำรองไฟฟ้าคอมพิวเตอร์ (UPS)” หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้าเกิดมีปัญหาขึ้นมา เช่นไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่ UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

“ซอฟต์แวร์ (software)” หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้

โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงานของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

“โปรแกรมอรรถประโยชน์” หมายถึง โปรแกรมที่ช่วยอำนวยความสะดวกต่างๆ ในการใช้เครื่องคอมพิวเตอร์ เพื่อทำให้เครื่องคอมพิวเตอร์ทำงานได้อย่างเต็มประสิทธิภาพ จึงถือว่าเป็นโปรแกรมเสริมที่ต้องมีในเครื่องคอมพิวเตอร์ ตัวอย่างเช่น

- ประเภทการจัดแฟ้มข้อมูล (File Manager) เป็นโปรแกรมที่ช่วยในการจัดการเกี่ยวกับแฟ้มข้อมูล เช่น การคัดลอก (Copy), การเปลี่ยนชื่อ(Rename), การแบ่งพาติชัน (Partition) และการจัดรูปแบบดิสก์ (Format)

- ประเภทการลบทิ้งโปรแกรม (Uninstall) เป็นโปรแกรมที่ช่วยในการลบโปรแกรมออกจากระบบปฏิบัติการ ในกรณีที่ไม่ต้องการใช้โปรแกรมนั้นๆ แล้ว โปรแกรมจะทำหน้าที่ในการตามเอา แฟ้มข้อมูลที่เกี่ยวข้องกับโปรแกรมที่ต้องการลบออกทั้งหมด เช่น Add/Remove Programs ในส่วน Control Panel ของ Microsoft Windows

- โปรแกรมจัดการดิสก์ (Disk Utility) เป็นโปรแกรมที่ใช้ในการจัดการปัญหาหรือแก้ไขให้ฮาร์ดดิสก์มีการทำงานที่ดีขึ้น เช่น Disk Cleanup เป็นโปรแกรมช่วยลบไฟล์ที่ไม่จำเป็นทิ้ง ทำให้ฮาร์ดดิสก์มีเนื้อที่ว่างเพิ่มขึ้น และช่วยเพิ่มประสิทธิภาพการทำงานของระบบ เช่น ไฟล์หรือโปรแกรมต่าง ๆ ที่ อาจถูกบันทึกอยู่ในฮาร์ดดิสก์ขณะที่เราท่องไปในเว็บไซต์ต่างๆ ซึ่งจะเรียกว่า temporal internet files ส่วนอีกโปรแกรมที่ช่วยจัดการดิสก์คือ โปรแกรม Disk Defragmenter ซึ่ง เป็นโปรแกรมช่วยรวมไฟล์ที่เคยแยกออกเป็นไฟล์ส่วนเล็กๆ ในขณะที่ทำการจัดเก็บไว้ในฮาร์ดดิสก์ ให้อยู่ในเนื้อที่ต่อเนื่องกัน และยังเป็นการจัดระเบียบเนื้อที่ว่างบนฮาร์ดิสก์ให้อยู่ในรูปแบบที่มีประสิทธิภาพมากที่สุด

- โปรแกรมรักษาหน้าจอ (Screen Saver) เป็นโปรแกรมที่ช่วยรักษาอายุการใช้งานของจอคอมพิวเตอร์ให้มีอายุการใช้งานมากยิ่งขึ้น

- โปรแกรมป้องกันไวรัส ใช้ป้องกันไวรัสคอมพิวเตอร์และโปรแกรมอื่นที่เข้ามาสร้างความเสียหายให้กับระบบคอมพิวเตอร์

- โปรแกรมบีบอัดแฟ้ม ใช้ลดขนาดของไฟล์ เพื่อลดเนื้อที่ในการจัดเก็บ และทำให้สามารถส่งไฟล์ ดังกล่าวทางอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ

“**ไวรัสคอมพิวเตอร์**” หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบ คอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์ เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

“**ทรัพย์สิน**” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“**ความมั่นคงปลอดภัยด้านสารสนเทศ**” หมายถึง การธำรงไวซึ่งความลับ (Confidential) ความถูกต้อง ครบถ้วน (Integrety) และความพรอมใชงาน (Avaliability) ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกตองแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความนาเชื่อถือ

“เหตุการณดานความมั่นคงปลอดภัย” หมายถึง เหตุการณที่ทำใหระบบเทคโนโลยีสารสนเทศและการ สื่อสารของโรงพยาบาลทุ่งใหญ่ ขาดคุณสมบัติดานความลับ (Confidential) ความถูกตองครบถ้วน (Integrity) และความพรอมใชงาน (Availability) อาทิ การปลอมแปลงหนาเว็บไซต การเจาะระบบ การขโมยขอมูลทาง เว็บไซต การแฮกเว็บไซต การรั่วไหลของข้อมูล การแพรระบาดของไวรัสและหนอนอินเทอรเน็ต ระบบลมไม่สามารถใหบริการได้ และการบุกรุกเครือข่าย

“สถานการณ์ความไม่แน่นอนและภัยพิบัติ” หมายถึง บุคลากรของหน่วยงาน สถานการณ์หรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆที่เป็นภัยต่อระบบข้อมูลสารสนเทศ

“แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ” หมายถึง ข้อปฏิบัติในการแก้ไขปัญหาเมื่อเกิดสถานการณ์ความไม่แน่นอน หรือภัยพิบัติ ได้แก่ การนำระบบกลับคืนสู่สภาพปกติ แนวทางปฏิบัติ ผังกระบวนการกรณีเกิดเหตุอัคคีภัย/อุทกภัย ผังกระบวนการกรณีไฟฟ้าดับและผังกระบวนการกรณีโดนเจาะระบบคอมพิวเตอร์

“การป้องกันโปรแกรมชนิดเคลื่อนที่” (Controls against mobile code) หมายถึง การควบคุมการใช้งานโปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง

“PDPA” หมายถึง พระราชบัญญัติคุ้มครองขอมูลสวนบุคคล พ.ศ. ๒๕๖๒

หมวดที่ ๑
มาตรการควบคุมด้านองค์กร
(Organizational controls)

วัตถุประสงค์

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลทุ่งใหญ่ เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่

มาตรการและแนวทางปฏิบัติ

ส่วนที่ ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy for information security)

จัดทำนโยบายความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร (Information Security Policy Document)

๑. ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายดังกล่าวจะต้องได้รับ การอนุมัติจากผู้มีอำนาจสูงสุดของโรงพยาบาลทุ่งใหญ่ ในการนำไปใช้

๒. กำหนดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่ขอโรงพยาบาลทุ่งใหญ่ และผู้ที่เกี่ยวข้องรับทราบ

ส่วนที่ ๒ บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

๑. ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลทุ่งใหญ่ไว้อย่างชัดเจน

๒. ผู้อำนวยการโรงพยาบาลทุ่งใหญ่ต้องตั้งคณะ หรือกลุ่มผู้ทำงานหลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลทุ่งใหญ่

๓. บทบาทหน้าที่แบ่งได้ดังนี้

๓.๑ ระดับนโยบาย ผู้รับผิดชอบ ได้แก

ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

ความรับผิดชอบ

๑) รับผิดชอบในการกำหนดนโยบาย ให้ขอเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แกโรงพยาบาลทุ่งใหญ่หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพรอง ละเลย หรือฝ่าฝืนการปฏิบัติตามฟแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ ระดับบริหาร ผู้รับผิดชอบ ได้แก หัวหน้ากลุ่มงาน/หัวหน้างาน หรือเทียบเทา

ความรับผิดชอบ

๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๓.๓ ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก ผู้ที่ได้รับมอบหมายให้ปฏิบัติหนาที่จากหัวหน้าส่วนราชการโรงพยาบาลทุ่งใหญ่ เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

ความรับผิดชอบ

๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลทุ่งใหญ่

ส่วนที่ ๓ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

ผู้บริหารโรงพยาบาลทุ่งใหญ่ ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงทรัพย์สินของโรงพยาบาลทุ่งใหญ่ หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม

ส่วนที่ ๔ หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ต้องกำหนดให้เจ้าหน้าที่ และผู้รับจ้างให้บริการจากภายนอกรับทราบและปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลทุ่งใหญ่ด้วย

ส่วนที่ ๕ การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

ตองกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

ส่วนที่ ๖ การติดต่อกับกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน (Contact with Special Interest Groups)

ตองกำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่าง ๆ ในอุตสาหกรรมที่โรงพยาบาลทุ่งใหญ่มีส่วนร่วมและเอกสารกำหนดให้มีการระบุวันที่จัดทำเอกสาร

ส่วนที่ ๗ ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย (Threat intelligence)

ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ มีการเก็บรวบรวมและวิเคราะห์ เพื่อประโยชน์ในการดำเนินการป้องกันหรือควบคุมภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลทุ่งใหญ่

ส่วนที่ ๘ ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

๘.๑ ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

๘.๒ กรณีโครงการที่จ้างบริษัทภายนอก โครงการที่หน่วยงานภายนอกดำเนินการให้ และโครงการที่โรงพยาบาลทุ่งใหญ่จัดทำเองต้องดำเนินการตามระเบียบทางราชการ และปฏิบัติตาม PDPA

ส่วนที่ ๙ บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ (Inventory of information and other associated assets)

๑. ต้องจัดทำและเก็บทะเบียนทรัพย์สิน ซึ่งรวมถึง ๑. กระบวนการทำงาน (Business Process) ๒. ข้อมูลและสารสนเทศ (Information) ๓. ฮาร์ดแวร์ (Hardware) ๔. ซอฟต์แวร์ (Software) ๕. เครือข่าย (Network) ๖. บุคลากร (Personnel) ๗. สถานที่ (Site) ๘. องค์กร (Organization) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการทรัพย์สินของโรงพยาบาลทุ่งใหญ่

๒. ตองมีการตรวจสอบทรัพย์สิน (Inventory Check) ตองจัดให้มีการตรวจสอบบัญชีทรัพย์สินทุกประเภท อย่างน้อยปีละ ๑ ครั้ง หรือตามระยะเวลาที่กำหนดไว หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๓. ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของทรัพย์สิน เมื่อมีทรัพย์สินใหม่หรือทรัพย์สินที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

ส่วนที่ ๑๐ การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

๑. จะต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและทรัพย์สินอย่างเหมาะสม

๒. การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

๒.๑ ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่โรงพยาบาลทุ่งใหญ่เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของโรงพยาบาลทุ่งใหญ่ การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๒ เจาหน้าที่ตลอดจนหน่วยงานภายนอกที่ได้รับการว่าจ้างโดยโรงพยาบาลทุ่งใหญ่ จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไวให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความมั่นคงปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูลและระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่

๒.๓ ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของโรงพยาบาลทุ่งใหญ่อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตน

๒.๔ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของโรงพยาบาลทุ่งใหญ่ ตองได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องไดรับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์ โดยระยะเวลาว่างเว้นจากการใช้งานแลว ต่องทำการ Log Off ต่องไมเกิน ๑๕ นาที

๒.๕ ผู้ใช้งานต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ของโรงพยาบาลทุ่งใหญ่

๒.๖ เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในโรงพยาบาลทุ่งใหญ่ อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์

๒.๗ อุปกรณ์คอมพิวเตอร์ของโรงพยาบาลทุ่งใหญ่ ต่องไมถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข่องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของโรงพยาบาลทุ่งใหญ่อย่างเด็ดขาด

๓. การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้

๓.๑ ห้ามเจ้าหน้าที่ ทำการติดตั้งหรือเผยแพร ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของโรงพยาบาลทุ่งใหญ่

๓.๒ ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของโรงพยาบาลทุ่งใหญ่ ทั้งที่ได่มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมาต้องได่รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยโรงพยาบาลทุ่งใหญ่ เจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่

๓.๓ ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต่องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช่งานทั่วไปของโรงพยาบาลทุ่งใหญ่ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

๓.๔ รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได่รับ การจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้อง ครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ ในการทำงานของโรงพยาบาลทุ่งใหญ่เท่านั้น

๔. การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

๔.๑ โรงพยาบาลทุ่งใหญ่ จัดหาบริการอินเทอร์เน็ตไวเพื่อสนับสนุนการดำเนินงานและอำนวยความสะดวกแกเจ้าหน้าที่ในการทำวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของโรงพยาบาลทุ่งใหญ่

๔.๒ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้โรงพยาบาลทุ่งใหญ่ และบุคคลผู้ที่เกี่ยวข้องกับโรงพยาบาลทุ่งใหญ่เสื่อมเสียชื่อเสียง หรือ เกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิด ทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๔.๓ การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ โรงพยาบาลทุ่งใหญ่ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

๔.๔ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๔.๕ ห้ามผู้ใช้งานเขชม ดาวนโหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไมเหมาะสมหรือผิดกฎหมาย

๔.๖ โรงพยาบาลทุ่งใหญ่ ไมสนับสนุนการแสดงความคิดเห็นส่วนตัว หรือเผยแพรข้อมูลส่วนบุคคล ในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด โซเชียลมีเดีย) ของเจ้าหน้าที่ที่อาจทำให้โรงพยาบาล เจ้าหน้าที่ ผู้ป่วยและบุคคลภายนอกเกิดความเสียหาย ทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการกระทำดังกล่าวถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

๕. การอนุญาตให้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) มีดังนี้

๕.๑ ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๕.๒ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่า เจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

๕.๓ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

๕.๔ ผู้ใช้งานต้องไมยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail Account ของตนโดยเด็ดขาด ไมวาบุคคลนั้นจะเป็นผู้บังคับบัญชา หรือบุคคลอื่นใดก็ตาม

๕.๖ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๕.๗ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๕.๘ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

๕.๙ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๕.๑๐ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

๕.๑๑ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๕.๑๒ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๕.๑๓ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๕.๑๔ ห้ามผู้ใช้งานส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรือจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

ส่วนที่ ๑๑ การคืนทรัพย์สิน (Return of assets)

เจ้าหน้าที่โรงพยาบาลทุ่งใหญ่ ซึ่งพ้นจากสภาพการทำงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คูมือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

ส่วนที่ ๑๒ ชั้นความลับของสารสนเทศ (Classification of Information)

๑. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าว เป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความมั่นคงปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยไดกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

๑) ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๒) ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล ซึ่งตาม PDPA ถือว่าเป็นข้อมูลที่มีความอ่อนไหว

๑.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

๓) ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

๑) ข้อมูลลับที่สุด (Top Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางสวนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๒) ข้อมูลลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายร้ายแรง

๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๔) ใช้ภายใน (Internal Use) หรือ เอกสารควบคุม หมายถึง เอกสารที่ใช้สำหรับบุคลากรภายในโรงพยาบาลทุ่งใหญ่เท่านั้น

๕) ข้อมูลทั่วไป หรือ เผยแพรต่อสาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือ เผยแพรทั่วไปได้

๑.๔ จัดแบ่งระดับชั้นการเข้าถึง

๑) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในโรงพยาบาลทุ่งใหญ่

๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำ การเผยแพร่สำหรับผู้ใช้งานทั่วไป ไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้

๓) ระดับชั้นสำหรับบุคลากรทางการแพทย์ สามารถเข้าถึงข้อมูลผู้ป่วยได้ตามสิทธิที่ได้รับมอบหมาย

๔) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ได้รับมอบหมายตามอำนาจหน้าที่

๑.๕ รูปแบบของเอกสารอิเล็กทรอนิกส์ ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ส่วนที่ ๑๓ การจัดทำป้ายชื่อของสารสนเทศ (Labeling of Information)

๑. ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒. ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัย

ส่วนที่ ๑๔ การถ่ายโอนสารสนเทศ (Information Transfer)

๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

๑.๑ ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติ หรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการและมีการปฏิบัติตามเพื่อป้องกันสารสนเทศที่มีการถ่ายโอนกับหน่วยงานภายนอก

๑.๒ ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามขั้นตอนปฏิบัติในการจัดระดับชั้นความลับของข้อมูล

๑.๓ ในการแลกเปลี่ยน ถ่ายโอนข้อมูลส่วนบุคคล ตองปฏิบัติตาม PDPA อย่างเคร่งครัด

๒. การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

๒.๑ ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

๒.๒ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ VPN

๓. การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

๓.๑ พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของโรงพยาบาลทุ่งใหญ่ ตองปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ และต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ในข้อตกลงว่าจะไม่เปิดเผยความลับของโรงพยาบาลทุ่งใหญ่

๓.๒ สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้ เป็นอย่างน้อย

๑) รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ

๒) ระดับการให้บริการ (Service Level)

๓) หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้

๔) ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้

๕) ราคา และเงื่อนไขการชำระเงิน

๖) ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือ พัฒนาขึ้น (ถ้ามี)

๗) การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ

ส่วนที่ ๑๕ การควบคุมการเข้าถึงสารสนเทศ (Access control)

๑. นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑.๑ มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๑.๒ ต่องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๑.๓ ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

๑.๔ ตองมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งใหญ่ และเฝ้าระวังการละเมิดความมั่นคงปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๑.๕ ต่องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑.๖ การเข้าถึงข้อมูลและระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่ จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้นๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้นๆ เท่านั้น ความมั่นคงปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหยดขอบเขตในการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่เสียหายกลับคืนมา

๒. การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๒.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๒.๒ ผู้ใช้งานที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาที่ห้องควบคุมระบบเครือข่าย ต้องลงลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

๒.๓ ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้าออกเป็นประจำทุกเดือน

๒.๔ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

๒.๕ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๒.๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๑) ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมี การลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของ ผู้ใช้งานก่อนทุกครั้ง

๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลข อุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้ หรือไม่สามารถเชื่อมต่อได้

- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลด ผ่านเว็บไซต์ของโรงพยาบาลทุ่งใหญ่

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๑๐) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ เว้นว่างจากการใช้งานเป็นเวลานาน

๑๑) ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการ ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๑๒) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ ติดตั้งก่อนดำเนินการ

๑๓) กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๑๔) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๑๕) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

- บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลทุ่งใหญ่จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลที่ได้รับอนุญาต

- มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

- วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

- การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

- การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในโรงพยาบาลทุ่งใหญ่จากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๑๖) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

- Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุม การเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
- Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน ระบบสารสนเทศภายใน

๑๗) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๘) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑๙) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่เกี่ยวข้อง

๒๐) IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของ ระบบเครือข่ายได้โดยง่าย

๒๑) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติ จากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๓.๑ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ในการใช้งาน ตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๓.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

๓.๔ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

๑) ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ ระบบข้อมูล ผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาลและข้อมูลทางการแพทย์ ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในโรงพยาบาลทุ่งใหญ่

๒) ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ

- มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

- ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิในการเข้าถึงข้อมูล

๓) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงาน จากภายนอกองค์กร

๓.๕ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของ ผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๔. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๔.๑ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๔.๒ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ ดังกล่าวด้วย

๔.๓ ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA๒ (Wi-Fi Protected Access) หรือ ที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

๔.๔ ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และหรือบัญชีผู้ใช้งาน โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายตามที่กำหนดไว้ เท่านั้น

๔.๕ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบ เครือข่ายภายในหน่วยงาน

๔.๖ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๔.๗ ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔.๘ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

๔.๙ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สาย ในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

๔.๑๐ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลทุ่งใหญ่ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

๔.๑๑ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๕. การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๕.๑ หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

๕.๒ การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

๕.๓ ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

๕.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

๕.๕ การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

๕.๖ การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๕.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๕.๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะ เปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ต การเชื่อมต่อนอกเหนือที่กำหนด ต้องทำหนังสือขออนุญาตจากหัวหน้าหน่วยงาน

๕.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หรือผู้ที่ได้รับมอบหมาย โดยต้องระบุข้อมูล ดังนี้

๑) หมายเลข Port ที่ต้องการขอให้เปิด

๒) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๓) วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

๕.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย (Firewall) เป็นประจำทุกเดือนและทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

๕.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มี ลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

๕.๑๒ ผู้ดูแลระบบมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

๕.๑๓ การเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องดำเนินการดังนี้

๑) ขออนุญาตการใช้งานเป็นลายลักษณ์อักษร

๒) เก็บข้อมูล Logfile ที่ Firewall

๓) เก็บ Logfile จากตัว Application

๕.๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการให้บริการทันทีจนกว่าจะได้รับการแก้ไข

๕.๑๕ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๖. การควบคุมการใช้อินเทอร์เน็ต (Internet)

๖.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้น แต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๖.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๖.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๖.๔ ห้ามใช้เครือข่ายอินเทอร์เน็ตขององค์การ เพื่อกระทำการต่อไปนี้

๑) หาประโยชน์ในเชิงธุรกิจส่วนตัว

๒) เพื่อความบันเทิง ได้แก่ การเล่นเกม ดูภาพยนตร์ฟังเพลง

๓) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์การ เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์การ หรือข้อมูลสำคัญที่เป็นความลับขององค์การ

๔) กระทำผิดกฎหมาย เช่น

- นำเข้าหรือเผยแพร่ข้อมูล หรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์
- แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์
- กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้า หรือเผยแพร่สื่อลามก อนาจาร
- กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย
- กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะ อันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่าง ๆ

๕) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๖) ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๗) ในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๘) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความ ที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๙) ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑๐) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๑) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๒) ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/ หรือกฎหมาย ระเบียบวิธีปฏิบัติทางคอมพิวเตอร์ อื่นๆ ที่เกี่ยวข้องอย่างเคร่งครัด

๗. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๗.๑ แนวทางปฏิบัติการใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

๒) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ส่วนบุคคลของหน่วยงาน

๓) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มงานสุขภาพดิจิทัล หรือบุคคล/บริษัทภายนอกที่ได้รับอนุญาต เท่านั้น

๔) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม ป้องกันไวรัส

๕) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๖) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จ สิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๗) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๘) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวบุคคลที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่าย ของหน่วยงาน โดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอย่างเหมาะสมและต้องปฏิบัติ ตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๗.๒ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

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

๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๗.๓ การสำรองข้อมูลและการกู้คืน

๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างสม่ำเสมอ

๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๘. การใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารชนิดพกพา (Mobile device)

๘.๑ แนวทางปฏิบัติการใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ

๒) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่าง ปลอดภัยและมีประสิทธิภาพ

๓) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ ให้มีสภาพเดิม

๔) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่อง คอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๕) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีด ข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๖) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๗) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๘) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่

๙) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๐) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งานหรือได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑๑) การนำอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพา เช่น USB Flash Drive, External Hardisk มาใช้ในการปฏิบัติงานร่วมกับเครื่องคอมพิวเตอร์ลูกข่ายจะต้องทำการตรวจสอบไวรัสคอมพิวเตอร์ทุกครั้ง และผู้ใช้งานต้องไม่ทำการสำเนาข้อมูลที่เป็นความลับของโรงพยาบาลทุ่งใหญ่ลงบนอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพาทุกประเภทเพื่อ นำออกไปใช้ภายนอกโรงพยาบาลทุ่งใหญ่ กรณีเป็นการดำเนินการภายในหน่วยงานเมื่อใช้งานเรียบร้อยแล้วให้ลบข้อมูลนั้นออกจากสื่อบันทึกข้อมูลแบบถาวร (Shift+delete) หรือฟอร์แมต (format) ทันที

๑๒) การนำอุปกรณ์พกพาที่เป็นทรัพย์สินส่วนตัวเข้ามาใช้ร่วมกับระบบเครือข่ายคอมพิวเตอร์ไร้สายของโรงพยาบาลทุ่งใหญ่ เช่น โน้ตบุ๊ค โทรศัพท์มือถือ ต้องลงโปรแกรมป้องกันไวรัสคอมพิวเตอร์และต้องมีการลงชื่อเข้าใช้งานเพื่อยืนยันตัวบุคคลทุกครั้ง

๘.๒ ความปลอดภัยทางด้านกายภาพ

๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๘.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๒) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

๓) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

๘.๔ การสำรองข้อมูลและการกู้คืน

๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและ สื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืน อย่างสม่ำเสมอ

๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๖ การบริหารจัดการอัตลักษณ์ที่ใช้ในการพิสูจน์ตัวตนเข้าระบบ (Indentity management)

ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๗ ข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน (Authentication information)

๑. การบริหารจัดการรหัสผ่าน

๑.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือ เกษียณอายุราชการ หรือยกเลิกการใช้งาน ภายหลังจากได้รับการแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

๑.๒ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๑.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (Email) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๑.๔ กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

๑.๕ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๑.๖ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๑.๗ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับ ว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๑.๘ ในกรณีเกษียณอายุราชการ และยังคงมีการปฏิบัติราชการที่เกี่ยวข้องกับโรงพยาบาลทุ่งใหญ่ สามารถขอให้คงสิทธิ์การใช้งานในระบบสารสนเทศของโรงพยาบาลได้ ซึ่งต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานต้นสังกัดเดิม หรือหน่วยงานที่ปฏิบัติราชการหลังเกษียณอายุราชการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง

๒. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๒.๑ การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

๑) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)
- กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)
- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น “abcdef” “aaaaaa” “๑๒๓๔๕๖” “๑๒๓๔๕๖”
- หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม วันเดือนปีเกิด ที่อยู่
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่าน ให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

๒) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการ รักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เหมาะสมและเป็นมาตรฐานสากล

๓) การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

- การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

- การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

- เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการ พิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๕) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลทุ่งใหญ่ หรือเป็นข้อมูลของบุคคลภายนอก

๖) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ ดูแลของโรงพยาบาลทุ่งใหญ่ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลทุ่งใหญ่หรือผู้ที่ได้รับมอบหมาย

๗) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลทุ่งใหญ่ และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๘) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๙) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลทุ่งใหญ่จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลทุ่งใหญ่ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลทุ่งใหญ่ ซึ่งโรงพยาบาลทุ่งใหญ่อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑๐) ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลทุ่งใหญ่

๑๑) ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการ โจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาลทุ่งใหญ่

๑๒) ห้ามใช้สินทรัพย์ของโรงพยาบาลทุ่งใหญ่เพื่อประโยชน์ทางการค้า

๑๓) ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๑๔) ห้ามกระทำรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๑๕) ห้ามใช้ระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑๖) ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๗) ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่ โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๑๘ สิทธิการเข้าถึงข้อมูล (Access rights)

๑. การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึง ทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ โดยต้องให้สิทธิ์ผู้ใช้งานเฉพาะการปฏิบัติงานในหน้าที่ซึ่งได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรหรือทางระบบอิเล็กทรอนิกส์ที่สามารถยืนยันตัวบุคคลได้ และผู้ดูแลระบบต้องถอดถอนสิทธิ์เมื่อเจ้าหน้าที่โยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบ

๒. การบริหารจัดการสิทธิ์ตามระดับสิทธิ์การเข้าถึง (Management of Privileged Access Right)

๒.๑ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

๒.๒ ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

๓. ผู้ดูแลระบบต้องการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

๓.๑ จัดทำรายชื่อของผู้ที่ยังมีสิทธิ์ในระบบ

๓.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานหรืองานการเจ้าหน้าที่ เพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งาน หรือดำเนินการอื่นใดทางอิเล็กทรอนิกส์เพื่อเป็น การยืนยัน/ทบทวนสิทธิ์

๓.๓ ดำเนินการแก้ไขข้อมูลสิทธิ์ต่างๆ ให้ถูกต้อง

๓.๔ เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้ถอดถอนสิทธิ์ภายใน ๑-๒ วันทำการ

ส่วนที่ ๑๙ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

โรงพยาบาลทุ่งใหญ่จะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างโรงพยาบาลกับผู้ใหบริการภายนอก

ส่วนที่ ๒๐ การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงการให้บริการของผู้รับบริการภายนอก (Addressing information security within supplier agreements)

๑. โรงพยาบาลทุ่งใหญ่ ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างโรงพยาบาลทุ่งใหญ่กับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒. ผู้ดูแลระบบต้องให้สิทธิการเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

๓. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของโรงพยาบาลทุ่งใหญ่จากหนวยงานภายนอก ตองมีการขออนุญาตอยางเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

๔. ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการ ประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

๕. การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของโรงพยาบาลทุ่งใหญ่

๖. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อย เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขต ที่ได้กำหนดไว้

ส่วนที่ ๒๑ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT

ในกรณีที่ผู้ให้บริการหน่วยงานภายนอกมีการใช้บริการต่อจากผู้ให้บริการรายอื่น ต้องจัดให้มีข้อกำหนดดังนี้

๑) ต้องแจ้งส่วนที่ใช้บริการต่อจากผู้ให้บริการรายอื่นต่อโรงพยาบาลทุ่งใหญ่ทราบ และให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของบริการของผู้ให้บริการด้วย โดยต้องมีคุณสมบัติด้านความปลอดภัยเทียบเท่ากับผู้ให้บริการ

๒) ต้องมีการเข้ารหัสในกรณีที่มีการรับส่งข้อมูลระหว่างผู้ให้บริการหน่วยงานภายนอกที่ได้ทำสัญญากับโรงพยาบาลกับผู้ให้บริการรายอื่น

๓) ต้องมีการกำหนดขั้นตอนปฏิบัติงาน และเงื่อนไขการให้บริการอย่างชัดเจน

ส่วนที่ ๒๒ การติดตาม การทบทวน และการบริหารจัดการการเปลี่ยนแปลงของบริการจากผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)

๑. การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

๑.๑ โรงพยาบาลทุ่งใหญ่ ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับโรงพยาบาลทุ่งใหญ่ ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

๑.๒ ต้องมีการทบทวน ติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๑.๓ การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่างๆ ของโรงพยาบาลทุ่งใหญ่

๒. การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

๒.๑ การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของโรงพยาบาลทุ่งใหญ่

๒.๒ การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอน การปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

ส่วนที่ ๒๓ ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการ Cloud (Information security for use of cloud services)

๑. ต้องกำหนดนโยบายหรือระเบียบปฏิบัติการใช้งาน cloud computing โดยอย่างน้อยต้องมีเนื้อหา ดังนี้

๑.๑ ประเมินความเสี่ยงเกี่ยวกับการใช้บริการ

๑.๒ กำหนดประเภทงานที่จะใช้บริการ

๑.๓ กำหนดรูปแบบของการใช้บริการ เช่น software as a service (saas), platform as a service (paas) และinfrastructure as a service (iaas)

๑.๔ กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (due diligence) เช่น ผู้ให้บริการต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล เช่น ได้รับมาตรฐาน ISO ๒๗๐๐๑

๑.๕ กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อประเมินความพร้อมในการให้บริการ

๑.๖ กำหนดความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ใน cloud โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล

๑.๗ กำหนดเงื่อนไขสำหรับผู้ให้บริการในการเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ

๑.๘ กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหาขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อเป็นต้น

๑.๙ จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการใช้บริการและจัดอบรมให้ความรู้แก่เจ้าหน้าที่เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ cloud computing

๑.๑๐ กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภทเพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๑.๑๑ กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่าง ๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

๒. กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการโดยมีลักษณะดังนี้

๒.๑ ผู้ใช้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ

๒.๒ กำหนดประเภทบริการที่จะใช้ cloud computing

๒.๓ ต้องกำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์การป้องกันการโจมตีในลักษณะ DDoS (distributed denial of service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (advanced persistent threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอพพลิเคชั่น (application) การป้องกันการบุกรุกแบบลำดับชั้น (defense-in-depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (hardening) เป็นต้น

๒.๔ กำหนดใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication

๒.๕ ต้องระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบอย่างชัดเจน

๒.๖ กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหา ระดับการให้บริการ (service level agreement) ระยะเวลาในการกลับคืนสู่สภาพปกติของระบบสารสนเทศ (recovery time objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO) อย่างชัดเจน

๒.๗ กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

๒.๘ ผู้ให้บริการต้องไม่มีสิทธิ์เข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่จะแจ้งและได้รับความยินยอมจากผู้ใช้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (cloud server hosting country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (origin country)

๒.๙ ผู้ให้บริการต้องปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล

๒.๑๐ มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (exit plan) เช่น กำหนดระยะเวลารักษาข้อมูล และวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

๓. การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

๓.๑ ต้องติดตามตรวจสอบประสิทธิภาพของการให้บริการรวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

๓.๒ ต้องประเมินความเพียงพอของระบบงานของผู้ให้บริการ (capacity planning) อย่างสม่ำเสมอ

๓.๓ ต้องทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๓.๔ ต้องทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

๔. ต้องกำหนดขั้นตอนการโอนย้ายข้อมูล (data migration) ไปยังผู้ให้บริการรายใหม่อย่างชัดเจน ในกรณีที่มีการเปลี่ยนผู้ให้บริการ ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้องและพร้อมใช้งานอยู่เสมอ

ส่วนที่ ๒๔ วางแผนและเตรียมการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)

๑. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

ตองกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศโรงพยาบาลทุ่งใหญ่ และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได ผล และมีความเป็นระบบระเบียบที่ดี

๒. การรายงานเหตุการณที่เกี่ยวข้อกับความมั่นคงปลอดภัย (Reporting Information Security Events)

๒.๑ ผู้ใช้งานต้องรายงานเหตุการณที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศโรงพยาบาลทุ่งใหญ่

๒.๒ ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไมเหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในโรงพยาบาลทุ่งใหญ่ ต่อผู้บังคับบัญชา หรือโรงพยาบาลทุ่งใหญ่จัดการความมั่นคงปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแกไขปัญหาไดอย่างทันท่วงที

๒.๓ ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ต้องรายงานต่อผู้ดูแลระบบทันที

๒.๔ ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติต้องรายงานต่อผู้ดูแลระบบทันที

๒.๕ ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในโรงพยาบาลทุ่งใหญ่ ตองไมบอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาโรงพยาบาลทุ่งใหญ่จัดการความมั่นคงปลอดภัย (Security Management) และห้ามทำการพิสูจนขอสงสัยเกี่ยวกับจุดออนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

๓. การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

ผู้ดูแลระบบต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลทุ่งใหญ่ ที่สังเกตุพบหรือเกิดความสงสัยในระบบหรือบริการที่ใชงานอยู่

ส่วนที่ ๒๕ ประเมินและตัดสินใจสำหรับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)

๑. สถานการณความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม

๒. จัดทำเกณฑ์ในการตัดสินเหตุการณ์ที่ถือว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๒๖ การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

๑. ระบบป้องกันผู้บุกรุก

ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีแอดเดรสของเครือข่ายที่เป็นผู้โจมตี

๒. ระบบไฟร์วอลล์

๒.๑ ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒.๒ ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีแอดเดรส ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒.๓ กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งต่อผู้บริหารสูงสุดของหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา หรือหากไม่สามารถแก้ไขได้ให้รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือหน่วยงานที่เกี่ยวข้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒

๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ประกอบด้วย มัลแวร์, ไวรัส, หนอนอินเตอร์เน็ต, โทรจัน, สปายแวร์, Backdoor, Rootkit, DDoS Botnet, Spam Mail, Phishing, Snffing, Spam, Hacking, Hacker

๓.๑ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- ภัยคุกคามทางอินเตอร์เน็ตประเภทใดถูกพบเป็นจำนวนมาก
- ภัยคุกคามทางอินเตอร์เน็ตถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

- มีการส่งภัยคุกคามทางอินเตอร์เน็ตจากเครือข่ายภายในโรงพยาบาลทุ่งใหญ่ไปยังภายนอกหรือไม่

๓.๒ ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดภัยคุกคามทางอินเตอร์เน็ตที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของโรงพยาบาลทุ่งใหญ่

๓.๓ หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดภัยคุกคามทางอินเตอร์เน็ตหรือส่งออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดภัยคุกคามทางอินเตอร์เน็ตกับระบบเครือข่ายทันทีแล้วทำการแก้ไขต่อไป

๓.๔ เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคาม หรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต

๓.๕ เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต

๓.๖ ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต หรือถูกใช้เพื่อค้นหาข้อมูลใดๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

๓.๗ ตรวจสอบหรือวิเคราะห์คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใดๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางอินเตอร์เน็ต และแจ้งผลการตรวจสอบแก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ส่วนที่ ๒๗ การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ตองบันทึกเหตุการณละเมิด ความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะไดเรียนรูจากเหตุการณที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ลวงหนา

ส่วนที่ ๒๘ การเก็บรวบรวมหลักฐาน (Collection of evidence)

ตองรวบรวมและจัดเก็บหลักฐานตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข่อง เมื่อพบวาเหตุการณที่เกิดขึ้นนั้นมีความเกี่ยวข่องกับการดำเนินการทางกฎหมายแพงหรืออาญา

ส่วนที่ ๒๙ ความมั่นคงปลอดภัยสารสนเทศในช่วงที่เกิดการหยุดชะงัก (Information security during disruption)

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของโรงพยาบาลทุ่งใหญ่ ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบนโยบาย

การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

๑. องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

๒. ตองจัดทำแนวทางปฏิบัติ ในการจัดทำแผนรองรับเหตุการณฉุกเฉินของระบบเทคโนโลยีสารสนเทศ

๓. การเตรียมความพร่อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของโรงพยาบาลทุ่งใหญ่ และการให้บริการด้านเทคโนโลยีสารสนเทศโรงพยาบาลทุ่งใหญ่

๔. การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแกไขสถานการณฉุกเฉิน เป็นต้น

๕. การดำเนินการเพื่อให้โรงพยาบาลทุ่งใหญ่ สามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกูระบบงานและข้อมูลที่เสียหาย เป็นต้น

๖. การกลับคืนสูการทำงานปกติ เพื่อให้การดำเนินงานโรงพยาบาลทุ่งใหญ่ กลับสูสภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

ส่วนที่ ๓๐ ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

๑. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

ตองจัดทำแผนรองรับเหตุการณฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

๒.๑ ตองกำหนดเวลาการทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ

๒.๒ ตองกำหนดเหตุการณจำลองที่จะใช้ทดสอบและรายละเอียด ในการกำหนดรายละเอียดของเหตุการณจำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผนฉุกเฉิน

๒.๓ ตองกำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย

๒.๔ ตองกำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณปัจจุบัน

๓. การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ (Availability of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

ส่วนที่ ๓๑ ความต้องการที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง (Legal, statutory, regulatory and contractual requirements)

การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

๑. ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับกฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งใหญ่

๒. เจ้าหน้าที่โรงพยาบาลทุ่งใหญ่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด

๓. ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่ถือเป็นทรัพย์สินของโรงพยาบาลทุ่งใหญ่ (ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ โรงพยาบาลทุ่งใหญ่สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๔. เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่ และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายตาง ๆ ของโรงพยาบาลทุ่งใหญ่กำหนดไว

๕. ห้ามเจ้าหน้าที่โรงพยาบาลทุ่งใหญ่ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

๖. การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศไม่ขัดต่อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

ส่วนที่ ๓๒ สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

๑. ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่โรงพยาบาลทุ่งใหญ่จัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๒. ต้องปฏิบัติตามข้อกำหนดที่ระบุไวในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย

๓. ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่ โดยเด็ดขาด

ส่วนที่ ๓๓ การป้องกันข้อมูล (Protection of records)

ตองจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ไดกำหนดไว โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

ส่วนที่ ๓๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

ต้องมีการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบข้อบังคับ หรือตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๓๕ การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)

ตองมีการทบทวนวิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติ ขององค์กร เช่น ทบทวนวัตถุประสงค์มาตรการ นโยบาย วิธีปฏิบัติงานต่างๆ ให้ถูกต้องและเป็นปัจจุบัน ตามรอบระยะเวลาที่กำหนด อย่างน้อยปีละ ๑ ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

ส่วนที่ ๓๖ การปฏิบัติตามนโยบาย กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)

๑. ตองจัดให้มีการตรวจสอบระบบทั้งหมดของโรงพยาบาลทุ่งใหญ่ตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว

๒. ตองมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

ส่วนที่ ๓๗ ขั้นตอนปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

๑. ตองจัดทำคูมือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในโรงพยาบาลทุ่งใหญ่ เช่น ขั้นตอนการสำรองข้อมูล ขั้นตอนการกูคืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วย รายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่ผู้รับผิดชอบ

๒. คูมือและขั้นตอนการปฏิบัติงานตองไดรับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้น ๆ โดยคูมือและขั้นตอนการปฏิบัติงานทุกฉบับต้องไดรับการทบทวนอย่างน้อยปีละ ๑ ครั้ง

๓. มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณผิดปกติหรือการละเมิดความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

หมวดที่ ๒

มาตรการด้านบุคลากร (People controls)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติงานระยะไกลหรือการปฏิบัติงานจากภายนอก และเพื่อให้เหตุการณและจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่ได้รับการดำเนินการที่ถูกต้อง

มาตรการและแนวทางปฏิบัติ

ส่วนที่ ๑ การปฏิบัติงานจากระยะไกล (Remote working)

๑. ตองมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่จากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่โรงพยาบาลทุ่งใหญ่กำหนด

๒. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๓. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความมั่นคงปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๔. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่จากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของโรงพยาบาลทุ่งใหญ่

๕. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของโรงพยาบาลทุ่งใหญ่ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

๖. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๒ การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

๑. ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลทุ่งใหญ่ โดยผ่านช่องทางรายงานที่กำหนดไว้

๒. ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใดๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในโรงพยาบาลทุ่งใหญ่ต่อผู้บังคับบัญชา หรือโรงพยาบาลทุ่งใหญ่จัดการความมั่นคงปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

๓. ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อผู้ดูแลระบบทันที

๔. ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใดๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อผู้ดูแลระบบทันที

๕. ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใดๆ ในโรงพยาบาลทุ่งใหญ่ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชา และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

๖. ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลทุ่งใหญ่ที่สังเกตุพบหรือเกิดความสงสัยในระบบ หรือบริการที่ใช้งานอยู่

หมวดที่ ๓
มาตรการทางกายภาพ (Physical controls)

วัตถุประสงค์

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินของโรงพยาบาลทุ่งใหญ่

มาตรการและแนวทางปฏิบัติ

ส่วนที่ ๑ ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

๑. โรงพยาบาลทุ่งใหญ่จะต้องมีการจำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุมการเข้าออก

๒. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๓. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

๓.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๓.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๓.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๓.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๓.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

๓.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๓.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๔. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๔.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๔.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

ส่วนที่ ๒ การควบคุมการเข้าออกทางกายภาพ (Physical entry)

๑. กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๒. การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitors)

๓. ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔. ผู้มาติดต่อ/บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๕. จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๖. ดูแลผู้มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๗. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๘. สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๙. มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๐. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๑๑. มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๑๒. จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๓. หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ๆ บุคคลภายนอกเข้าถึงได้

๑๔. เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวขณะปฏิบัติหน้าที่ในบริเวณศูนย์คอมพิวเตอร์ และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัวถือเป็นหน้าที่ที่จะต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยโดยทันที

ส่วนที่ ๓ การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

๑. ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับโรงพยาบาลทุ่งใหญ่ ห่องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบข้อมูลสารสนเทศที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก ห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตู หน้าต่างห้องระบบสารสนเทศสำคัญต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๒. เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ

ส่วนที่ ๔ การป้องกันต่อภัยคุกคามทางกายภาพ และด้านสภาพแวดล้อม (Protecting against physical and environmental threats)

ต้องมีการป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น ซึ่งเป็นภัยคุกคามจากภายนอกต้องมีการเตรียมการป้องกันเหตุที่อาจเกิดขึ้น

ส่วนที่ ๕ การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

๑. หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น

๒. หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

ส่วนที่ ๖ โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen)

เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

ส่วนที่ ๗ การจัดวางและป้องกันอุปกรณ์ (Equipment sitting and protection)

เจ้าหน้าที่โรงพยาบาลทุ่งใหญ่ต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

ส่วนที่ ๘ ความมั่นคงปลอดภัยของทรัพย์สินที่มีการใช้งานนอกองค์กร (Security of assets off-premises)

๑. กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๒. ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓. เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ส่วนที่ ๙ สื่อบันทึกข้อมูล (Storage media)

๑. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล

๒. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การตัด ฉีก หรือตัดด้วยเครื่องทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การตัด หรือตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย

ส่วนที่ ๑๐ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๑. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๑) ระบบสำรองกระแสไฟฟ้า (UPS)

๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๓) ระบบระบายอากาศ

๔) ระบบปรับอากาศ และควบคุมความชื้น

๒. ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ส่วนที่ ๑๑ ความมั่นคงปลอดภัยของสายสัญญาณ (Cabling security) ควรปฏิบัติดังนี้

๑. หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒. ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๓. ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

๔. ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๕. จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๖. ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๗. พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

๘. ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ส่วนที่ ๑๒ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑. กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕. ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖. ตรวจสอบการแจ้งเตือนเมื่อถึงรอบการบำรุงรักษาของอุปกรณ์

๗. กำหนดและอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ส่วนที่ ๑๓ ความมั่นคงปลอดภัยสำหรับการจำหน่ายออกหรือการทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

๑. ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๒. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๔
มาตรการควบคุมด้านเทคโนโลยี (Technological controls)

วัตถุประสงค์

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

ส่วนที่ ๑ อุปกรณ์ปลายทางของผู้ใช้งาน (User end point devices)

๑. ต้องมีการกำหนดและปฏิบัติตามนโยบายหรือมาตรการสนับสนุน สำหรับการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Teblet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่นๆ) ที่มีการนำมาใช้งาน เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และควรคำนึงถึงความเสี่ยงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน

๒. เครื่องคอมพิวเตอร์ โน๊ตบุ๊ค เซิร์ฟเวอร์ เราเตอร์ สวิตซ์ โทรศัพท์มือถือ และอุปกรณ์ที่สามารถประมวลผลข้อมูลอื่นๆ ที่ติดต่อสื่อสารผ่านระบบเครือข่ายได้ และมีการใช้งานโดยผู้ใช้งาน ต้องมีการดำเนินการดังต่อไปนี้

- มีการติดตั้งโปรแกรมป้องกันมัลแวร์แบบแพทเทิร์นแมชชิ่ง (pattern matching)
- ติดตั้งโปรแกรมป้องกันมัลแวร์แบบวิธีทางพฤติกรรม (behavior method)
- ดำเนินการตรวจสอบ Log การใช้งานที่น่าสงสัย (EDR)
- มอนิเตอริงข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล (DLP)

๓. ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ ระบบสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย ที่ไม่มีผู้ดูแล

ส่วนที่ ๒ สิทธิการเข้าถึงในระดับพิเศษ (Privileged access rights)

๑. ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

๒. ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้ง เมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศของโรงพยาบาลทุ่งใหญ่

ส่วนที่ ๓ การจำกัดการเข้าถึงข้อมูล (Information access restriction)

๑. ตองมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ไดแก กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้น มีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒. บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ตองไดรับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓. บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของโรงพยาบาลทุ่งใหญ่อย่างเคร่งครัด ก่อนที่จะไดรับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่

ส่วนที่ ๔ การจำกัดการเข้าถึงซอร์สโค้ด (Access to source code)

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง หรือให้บริการ เช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

ส่วนที่ ๕ การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย (Secure authentication)

๑. ผู้ดูแลระบบควรใช้เทคโนโลยีและกระบวนการยืนยันตัวตนที่มีมาตรฐานความปลอดภัย โดยสอดคล้องกับข้อจำกัดการเข้าถึงข้อมูลและนโยบายควบคุมการเข้าถึง

๒ ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง

ส่วนที่ ๖ การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

๑. ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่ำเสมอ

๒. ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน ๑ ปีที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

๓. แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิ การ Tunning , การจัดหาเพิ่มเติม

ส่วนที่ ๗ การป้องกันจากโปรแกรมไม่ประสงค์ดี (Protection against malware)

มาตรการป้องกันโปรแกรมไม่ประสงค์ดี

๑. เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุด และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่องคอมพิวเตอร์

๒. ข้อมูลสารสนเทศ ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๓. ห้ามเจ้าหน้าที่ทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต

๔. ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ หรือไฟล์แชร์ต่างๆ ต้องได้รับการสแกนหาไวรัส

๕. ผู้ใช้งานตองพึงระวังไวรัสและโปรแกรมไมประสงคดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๖. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๗. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของโรงพยาบาลทุ่งใหญ่ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๘. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อนให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาลทุ่งใหญ่ สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการดังนี้

๘.๑ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความมั่นคงปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๘.๒ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๘.๓ พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๘.๔ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟตแวร

๘.๕ นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ส่วนที่ ๘ การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

ส่วนที่ ๙ การบริหารจัดการการตั้งค่าระบบ (Configuration Management)

๑. มีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้อง และปลอดภัย

๒. ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

ส่วนที่ ๑๐ การลบข้อมูล (Information deletion)

หน่วยงานควรมีการลบข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์หรือสื่อบันทึกข้อมูลอื่น ๆ เมื่อไม่มีความต้องการใช้อีกต่อไป โดยปฏิบัติตามแนวทางดังนี้

๑. เลือกใช้วิธีการลบที่เหมาะสมซึ่งเป็นไปตามกฎหมายหรือข้อบังคับที่มีอยู่ เทคนิคต่างๆ ได้แก่ การลบแบบมาตรฐาน การเขียนทับ หรือการลบแบบเข้ารหัส

๒. บันทึกผลลัพธ์ของการลบเพื่อใช้อ้างอิงในการดำเนินการ

๓. ตรวจสอบให้แน่ใจว่าการลบครอบคลุมถึงไฟล์ชั่วคราว ข้อมูลที่แคช สำเนาของข้อมูล

๔. พิจารณาใช้แอปพลิเคชันยูทิลิตี้การลบแบบพิเศษเพื่อลดความเสี่ยง

๕. หากมีการให้ผู้บริการภายนอก เช่น ผู้ให้บริการระบบคลาวด์ ดำเนินการลบข้อมูล หน่วยงานต้องกำหนดข้อกำหนดการลบข้อมูลที่ชัดเจน รวมถึงวิธีการลบและระยะเวลา และให้แน่ใจว่าการลบข้อมูลนั้นจะครอบคลุมภายใต้ข้อตกลง

๖. ตรวจสอบให้แน่ใจว่าผู้ให้บริการระบบคลาวด์ ดำเนินการลบข้อมูลสอดคล้องกับข้อกำหนดการลบข้อมูลของหน่วยงาน

ส่วนที่ ๑๑ การปิดบังข้อมูล (Data masking)

หน่วยงานควรดำเนินการเกี่ยวกับการปกปิดข้อมูลเพื่อจำกัดการเห็นข้อมูลทั้งหมด (data masking) ที่เป็นไปตามนโยบายการควบคุมการเข้าถึง และนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง เพื่อไม่ให้ข้อมูลที่จัดเก็บไว้ในระบบถูกมองเห็น หรือถูกนำไปใช้ประโยชน์อันไม่ควร จึงต้องพิจารณาดำเนินการดังนี้

๑. ซ่อนข้อมูลหรือปกปิดข้อมูลบางส่วนตามคำขอหรือตามลักษณะงานที่ไม่ควรเปิดเผยข้อมูลต่อผู้อื่น และอนุญาตให้เจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงข้อมูลส่วนที่เกี่ยวข้องได้

๒. สร้างการดำเนินการปกปิดข้อมูลตามหลักเกณฑ์ทางกฎหมายและข้อบังคับเฉพาะ

ส่วนที่ ๑๒ การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)

๑. ตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลาย ไม่ซ้ำกับแอคเคาน์อื่น ๆ และเปลี่ยนรหัสผ่านเมื่อพบความผิดปกติ

๒. ตรวจสอบการอัปเดตตบนระบบปฏิบัติการและตั้งค่าเบราว์เซอร์ให้ทันสมัย

๓. ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ เพื่อรักษาตัวเองให้ปลอดภัยจากการติดตามทางออนไลน์

ส่วนที่ ๑๓ การสำรองข้อมูล (Information backup)

๑. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

๒. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๓. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของโรงพยาบาลทุ่งใหญ่ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๔.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ไดแก ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไมสำเร็จ เป็นต้น

๔.๔ ตรวจสอบค่าคอนฟิกกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล

๔.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟตแวร วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๔.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับโรงพยาบาลทุ่งใหญ่ต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไวนอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับโรงพยาบาลทุ่งใหญ่

๔.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๔.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลไดตามปกติ

๔.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว

๔.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๔.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ไดสำรองเก็บไว้

๕. ตองจัดทำแผนเตรียมความพรอมกรณีฉุกเฉินในกรณีที่ไมสามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส เพื่อให้สามารถใชงานสารสนเทศไดตามปกติอย่างต่อเนื่อง โดย

๕.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๕.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม แผ่นดินไหว การชุมนุมประท้วง ทำให้ไมสามารถเข้ามาใช้ระบบงานได เป็นต้น

๕.๓ มีการกำหนดขั้นตอนปฏิบัติในการกูคืนระบบสารสนเทศ

๕.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว

๕.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮารดแวร ซอฟตแวร เปนตน เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๕.๖ การสร้างความตระหนัก หรือให้ความรูแกเจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเรงดวน เปนตน

๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพรอมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคลองกับการใชงานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๗. ตองมีการกำหนดหนาที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพรอมกรณีฉุกเฉินในกรณีที่ไมสามารถดำเนินการดวยวิธีการทางอิเล็กทรอนิกส

๘. ตองมีการทดสอบสภาพพรอมใชงานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพรอมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพรอมใช้งานอยูเสมอ

๙. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพรอมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับไดของโรงพยาบาลทุ่งใหญ่ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๔ การสำรองอุปกรณ์ประมวลผลข้อมูล (Redundancy of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

ส่วนที่ ๑๕ การบันทึกข้อมูลล็อก (Logging)

๑. การบันทึกข้อมูลเหตุการณ์ (Event logging)

ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

๒. การป้องกันข้อมูลล็อก (Protection of Log Information)

ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

๓. ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

ส่วนที่ ๑๖ การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

ตองตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในโรงพยาบาลทุ่งใหญ่ให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลทุ่งใหญ่ ถูกบุกรุกตาม พ.ร.บ. วาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร

ส่วนที่ ๑๗ การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิในระดับพิเศษ (Use of privileged utility programs)

๑. การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๒. ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๒.๑ ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน

๒.๒ ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

๒.๓ จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๒.๔ ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

ส่วนที่ ๑๘ การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

๑. ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

๒. ตองปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่โรงพยาบาลทุ่งใหญ่จัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

๓. ซอฟตแวร (Software) ที่โรงพยาบาลทุ่งใหญ่ไดจัดเตรียมไวให้ผู้ใช้งาน ถือเป็นสิ่งที่จำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แกไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ไดรับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ส่วนที่ ๑๙ ความมั่นคงปลอดภัยของเครือข่าย (Networks security)

การควบคุมการเข้าถึงเครือข่าย (Network Control)

๑. ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๒. การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๓. ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ

๔. ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

๕. บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของโรงพยาบาลทุ่งใหญ่ด้วย

ส่วนที่ ๒๐ ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)

๑. ระบบเครือข่ายทั้งหมดของโรงพยาบาลทุ่งใหญ่ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๒. ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของโรงพยาบาลทุ่งใหญ่ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของโรงพยาบาลทุ่งใหญ่ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายโรงพยาบาลทุ่งใหญ่ได้

๓. ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของโรงพยาบาลทุ่งใหญ่ โดยไม่ได้รับอนุญาต

๔. ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลทุ่งใหญ่โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

๕. ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

๖. ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของโรงพยาบาลทุ่งใหญ่ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่น ในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในโรงพยาบาลทุ่งใหญ่โดยเด็ดขาด

ส่วนที่ ๒๑ การแบ่งแยกเครือข่าย (Segregation in networks)

๑. ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ส่วนที่ ๒๒ การคัดกรองเว็บ (Web filtering)

ต้องดำเนินการกรองข้อมูล/บล็อคเว็บไซต์ที่ไม่เหมาะสม และจำกัดสิทธิการเข้าถึงเข้าเว็บไซต์ที่ไม่ปลอดภัยหรือเว็บเสี่ยงแบบอัตโนมัติ เพื่อป้องการความเสียหายให้แก่ระบบข้อมูลสารสนเทศ เครือข่าย และเครื่องคอมพิวเตอร์ของโรงพยาบาล

ส่วนที่ ๒๓ การใช้การเข้ารหัสข้อมูล (Use of cryptography)

๑. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

โรงพยาบาลทุ่งใหญ่ต้องมีนโยบายการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

๒. การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ โดยองค์กรควรมีการกำหนดมาตรการในการเก็บ Key ที่เป็นข้อมูลลับของแต่ละบุคคล

ส่วนที่ ๒๔ วัฏจักรการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development life cycle)

ตองมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่องค์กรกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนามีช่วงโหวที่รูจักกัน (Common Vulnerabilities and Exposures (CVE)) และตองสามารถแกไขชองโหวที่ตรวจพบได้

ส่วนที่ ๒๕ ความต้องการด้านความมั่นคงปลอดภัยของแอพพลิเคชั่น (Application security requirements)

๑. สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการสงผานเครือขายสาธารณะ ตองไดรับการป้องกันและการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไมไดรับอนุญาต

๒. สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ตองไดรับการปองกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไมไดรับอนุญาต การเปิดเผยข่อมูลโดยไมไดรับอนุญาต การส่งข้อมูลซ้ำโดยไมไดรับอนุญาต

ส่วนที่ ๒๖ สถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยและหลักการวิศวกรรมระบบ (Secure system architecture and engineering principles)

เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ตองมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

ส่วนที่ ๒๗ การทดสอบด้านความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ (Security testing in development and acceptance)

๑. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

๒. การทดสอบเพื่อรับรองระบบ (System acceptance testing)

๒.๑ มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่ และระบบที่ปรับปรุง

๒.๒ ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่นๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้นและให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

ส่วนที่ ๒๘ การพัฒนาระบบโดยหน่วยงานภายนอก (Outsourced development)

ในการทำสัญญาว่าจ้างการพัฒนาระบบของโรงพยาบาลทุ่งใหญ่ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

ส่วนที่ ๒๙ การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบ ออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

ส่วนที่ ๓๐ การบริหารจัดการการเปลี่ยนแปลง (Change management)

๑. เมื่อมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ต้องแจ้งให้ผู้ดูแลระบบทราบทุกครั้ง

๒. เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง

๓. ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อนจะทำการเปลี่ยนแปลง

๔. บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบโดยบันทึกจะต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
- เจาของข่อมูล และผูดูแลระบบ
- วิธีการเปลี่ยนแปลง
- ผลของการเปลี่ยนแปลง (สำเร็จ หรือ ลมเหลว)

ส่วนที่ ๓๑ ข้อมูลสำหรับการทดสอบ (Test information)

ข้อมูลจริงที่จำนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

ส่วนที่ ๓๒ การป้องกันระบบสารสนเทศในช่วงที่มีการทดสอบระบบโดยผู้ตรวจประเมิน (Protection of information systems during audit testing)

ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด