นโยบาย มาตรฐานและ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โรงพยาบาลสูงเม่น อ.สูงเม่น จ.แพร่
ปีงบประมาณ ๒๕๖๗

งานข้อมูลและสารสนเทศ
โรงพยาบาลสูงเม่น

คำนิยาม

“โรงพยาบาล” หมายถึง โรงพยาบาลสูงเม่น

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสูงเม่น

“มาตรการ” หมายถึง วิธีการที่ตั้งเป็น กฎ ข้อกำหนด ระเบียบ หรือกฎหมาย เป็นต้น

“วิธีปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐาน ที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลสูงเม่น

“ผู้ดูแลระบบ”หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแล รักษาระบบ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการ ฐานข้อมูลของระบบ เครือข่ายคอมพิวเตอร์

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

“สารสนเทศ” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ ในรู้ปของตัวเลขข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูล โดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเทอร์เน็ต (Internet)

- ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงาน เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

- ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบ คอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศเป็นต้น

“การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” หมายถึง การตรวจสอบการอนุมัติ และการกำหนด สิทธิในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้งาน

“เครื่องเซิร์ฟเวอร์ (Server)” หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือ โปรแกรมคอมพิวเตอร์ ที่เป็นลูกข่ายใน ระบบเครือข่าย

“อุปกรณ์ UPS” หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้า เกิดมีปัญหาขึ้นมา เช่นไฟตกไฟเกิน ไฟดับหรือไฟกระชาก เป็นต้น โดยที่อุปกรณ์ UPS จะจ่ายพลังงาน ออกมาอย่างต่อเนื่องและ มีคุณภาพในทุกสถานการณ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหาย ที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้า สำรองจากแบตเตอรีให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิด ปัญหาทางไฟฟ้า

“ซอฟต์แวร์ (Software)” หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์ จึงหมายถึง ลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็น โปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่า คอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียง การกระทำากับข้อมูล ที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รู้ปภาพ หรือแม้แต่เป็น เสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงาน ของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกัน ได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์ จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

“ไวรัสคอมพิวเตอร์” หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ใน ระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิด จากการนำเอาดิสกที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือ ระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปผังตัวอยู่ในหน่วยความจำ คอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสเป็นแค่โปรแกรมหนึ่ง การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้น จะต้อง มีการถูกเรียกให้ทำงานได้ ขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่ทราบว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสนั้นๆ ขึ้นมาทำงาน

“เวชระเบียน” หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บปวด และการตรวจรักษาทั้งที่เป็นเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลสูงเม่น

แนวทางป้องกันและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
หน่วยบริการโรงพยาบาล

ปัจจุบันปัญหาเรื่องภัยคุกคามทางไซเบอร์ (Cyber Security)ยังคงเกิดขึ้นอย่างต่อเนื่องตาม เทคโนโลยีที่ทันสมัย และมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น ดังนั้นหน่วยงานจึงจำเป็นต้อง ตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามแนวทางในการจัดการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ เพื่อเป็นการป้องกันและรับมือจากภัยคุกคามที่เกิดขึ้นได้อย่างทันท่วงที

โรงพยาบาลจึงได้จัดทำแนวทางในการจัดการความเสี่ยงด้านความมั่นคง ปลอดภัยทาง ไซเบอร์ที่สอดคล้องกับประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศกระทรวงสาธารณสุข พ.ศ.๒๕๖๕ (https://ict.moph.go.th/th/extension/download/1083) โดยอาศัยอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒, พระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วน บุคคล พ.ศ.๒๕๖๒ เพื่อเป็นแนวทางให้หน่วยบริการในจังหวัดแพร่ปฏิบัติตามอย่างเคร่งครัด ดังนี้

๑. ตรวจสอบ และจำกัดสิทธิของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและ ฐานข้อมูลในระบบ ได้แก่ HDC, HosXP, HosXP PCU, HosMerge,MOPH-IC, MOPH PHR และระบบอื่นๆ ที่มีการ เข้าถึงข้อมูลส่วนบุคคล

๒. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของไวรัส Web Application, Firewall, หรือ DDoS Protection

๓. เจ้าหน้าที่ของหน่วยงานจะต้องมีความระมัดระวังในการใช้งานอินเตอร์เน็ต โดยหลีกเลี่ยงข้อความ ไฟล์จาก Social Media

๔. หากพบความผิดปกติที่สงสัยว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมี ความล่าช้าผิดปกติควรตรวจสอบ Log การ Login ย้อนหลังทุกๆ เดือน

๕. หลีกเลี่ยงการเชื่อมต่ออินเตอร์เน็ตภายนอกกับ HIS ของสถานพยาบาล

๖. สถานพยาบาลทุกแห่งมีแนวทางการจัดการความเสี่ยง (Risk Management) ด้าน Cyber Security ตามแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Information Security Management System)

๗. หน่วยบริการทุกแห่งมีระบบ Security ในการป้องกันความปลอดภัยของข้อมูลตามเกณฑ์ ดังนี้

๗.๑ มีนโยบาย ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศ เช่น การ Login ด้วย User และจำกัดสิทธิ์การเข้าถึงข้อมูลเท่าที่จำเป็น, มีการป้องกันการเข้าถึงเว็บไซต์ ที่ไม่ปลอดภัย เป็นต้น

๗.๒ มีการสำรองข้อมูลของ Server และ Client เป็นประจำทุกวัน

๗.๓ หน่วยบริการทุกแห่งมีระบบ Antivirus ของ Server และ Client

๗.๔ โรงพยาบาลทุกแห่งมีระบบ Firewall เพื่อตรวจจับการบุกรุกของระบบเครือข่าย ดังนี้

รพ.ระดับ S เกณฑ์ขั้นต่ำคือ Next-generation Firewall (Firewall ขั้นสูงสามารถรักษา ความมั่นคงปลอดภัยจากเครือข่ายอื่นๆ และตรวจจับการบุกรุกทั้งจากการรับ-ส่งข้อมูล, IP Address และแอปพลิเคชันต่างๆ ที่สามารถรับ-ส่งข้อมูลจากภายนอกได้ เช่น อีเมลล์ เป็นต้น)

รพ.ระดับ F1, F2 และ F3 เกณฑ์ขั้นต่ำคือ Entry Level Firewall (Firewall ที่ ตรวจสอบการบุกรุกจากช่องทางการรับ-ส่งข้อมูล, IP Address หรือป้องกันเพียงบางเครือข่ายเท่านั้น)

๘. หน่วยบริการมีระบบ Log เก็บข้อมูลติดต่อภายนอก

๙. การจัดการปัจจัยเสี่ยง ที่ทำให้เกิดช่องโหว่ทาง Cyber อื่นๆ ที่อาจนำไปสู่ความผิด PDPA

๙.๑ หลีกเลี่ยงการอัปโหลดไฟล์ที่มีความสำคัญขึ้นบนหน้าเว็บไซต์ทั้งภายใต้โดเมน (moph.go.th) และภายนอก (Development Platform ต่างๆ เช่น github) ที่ทำให้ผู้โจมตีใช้ประโยชน์ได้ เช่น ไฟล์ที่ประกอบด้วย Username, Password สำหรับเข้าใช้งานระบบ, Source Code ของระบบ

๙.๒ อัปเดตซอฟต์แวร์ที่ใช้งานให้เป็นเวอร์ชันปัจจุบัน

๙.๓ ถอนการติดตั้งแพลตฟอร์มหรือโปรแกรมเสริมที่ใช้จัดการเว็บไซต์และฐานข้อมูล (CMS Plugins) ที่ไม่ได้ใช้งานแล้ว

๙.๔ การเข้ารหัสข้อมูลสำคัญเฉพาะคนที่มีสิทธิ์เข้าถึงเท่านั้น เช่น เลขประจำตัวประชาชน

๙.๕ หลีกเลี่ยงการเปิดให้เข้าถึงไฟล์ได้จากอินเตอร์เน็ตโดยไม่มีการตรวจสอบ เช่น เปิดหน้า Index Directory ไว้ ทำให้เห็นไฟล์ต่างๆ

๙.๖ กำหนด IP Address ที่จะเข้าถึง Service ที่มีความอ่อนไหว เช่น MySQL, SSH

๙.๗ กำหนด Rate-Limitation ในการเข้าถึง Service ว่าหากเกิด Connection failed หลายครั้งจะต้องถูกปิดกั้น

๙.๘ มีการตรวจสอบ User Input เช่น SQL Injection, XSS Attack ที่ทำให้สามารถพัฒนา เป็นช่องโหว่ที่ใช้โจมตีได้

๙.๙ ปิดกั้น exposed ของ website configuration, database configuration, website directory

๙.๑๐ หลีกเลี่ยงการเปิดให้เชื่อมต่อ port 3306 จากสาธารณะ โดยไม่ผ่าน VPN

๙.๑๑ หลีกเลี่ยงการแชร์ข้อมูลส่วนบุคคลในพื้นที่สาธารณะ เช่น google drive, one drive, โดยไม่เข้ารหัสไฟล์ หรือแชร์เฉพาะบุคคล เป็นต้น

๙.๑๒ ตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติ ควรแก้ไขโดยทันที

๑๐. การเผยแพร่ข้อมูล โดยเฉพาะข้อมูลส่วนบุคคลควรได้รับการเห็นชอบ (อย่างมีหลักฐาน) จาก ผู้บริหารสูงสุดของหน่วยงานก่อนเผยแพร่สู่สาธารณะ (ทั้ง Internet และ Intranet)

โรงพยาบาลสูงเม่น จ.แพร่
1 ตุลาคม 2566

สารบัญ

มาตรฐานด้านเทคโนโลยีสารสนเทศ

ความเป็นมา

การพัฒนาคุณภาพโรงพยาบาลในประเทศไทยได้เริ่มดำเนินการมาเป็นเวลานานพอสมควรแล้ว และเทคโนโลยีสารสนเทศโรงพยาบาลเป็นส่วนหนึ่งที่ช่วยให้คุณภาพการดูแลผู้ป่วยมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ดีหากการจัดการระบบเทคโนโลยีสารสนเทศโรงพยาบาลขาดมาตรฐานที่เหมาะสม ย่อมเป็น ความเสี่ยงที่จะทำให้ผู้ป่วยได้รับอันตราย

ในมาตรฐานโรงพยาบาลและบริการสุขภาพของสถาบันพัฒนาและรับรองคุณภาพโรงพยาบาลแต่เดิมได้ กล่าวถึงเรื่องมาตรฐานด้านเทคโนโลยีสารสนเทศโรงพยาบาลไว้อย่างกว้างๆ แต่ในปัจจุบันการ ใช้เทคโนโลยี สารสนเทศมีความซับซ้อนยิ่งขึ้น ซึ่งทำให้เกิดทั้งโอกาสใหม่ๆ และเกิดความเสี่ยงใหม่ๆ ด้าน เทคโนโลยีสารสนเทศเป็นอย่างมาก ดังนั้นสถาบันพัฒนาและรับรองคุณภาพโรงพยาบาลจึงปรึกษาสมาคมเวชสารสนเทศไทย (TMI) ให้ช่วยพัฒนามาตรฐานคุณภาพในด้านเทคโนโลยีสารสนเทศโรงพยาบาลขึ้น เพื่อใช้เป็นแนวทางในการพัฒนา และรับรอง คุณภาพโรงพยาบาลต่อไป

TMI ได้ตั้งคณะทำงานขึ้นศึกษา และดำเนินการในเรื่องนี้ตกลงเริ่มจากการพัฒนามาตรฐานเทคโนโลยีเทคโนโลยีสารสนเทศที่เหมาะสมร่วมกันเป็นอันดับแรก โดยกระบวนการนี้

คณะทำงานศึกษาเอกสารที่เกี่ยวข้องกับมาตรฐาน Hospital Accreditation (HA) และมาตรฐานการจัดการสากลด้านIT ก่อนการประชุม ได้แก่

- มาตรฐานโรงพยาบาลและบริการสุขภาพฉบับเฉลิมพระเกียรติฉลองสิริราชสมบัติ ครบ ๖๐ ปี พ.ศ. ๒๕๔๙
- SPA(Standards Practice Assessment) สถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล
- มาตรฐาน JCI (Joint Commission International)
- Baldrige National Quality Program ๒๐๐๙ - ๒๐๑๐
- มาตรฐาน CoBIT (Control Objectives for Information and related Technology)
- มาตรฐาน ITIL (Information Technology Infrastructure Library)
- มาตรฐาน ISO/I EC ๒๗๐๐๒

คณะทำงานเสนอให้ร่าง มาตรฐานเทคโนโลยีสารสนเทศโรงพยาบาล (Hospital Information Technology) เพื่อเป็นแนวทางให้โรงพยาบาลในประเทศไทยพัฒนาเทคโนโลยีสารสนเทศในองค์กรเพื่อสนับสนุนการพัฒนาคุณภาพโรงพยาบาล (HA) เพิ่มเติมจากมาตรฐานโรงพยาบาลและบริการสุขภาพ ของสถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล

เนื่องจาก Information System (IS) กับ Information Technology (IT) มีความสัมพันธ์ใกล้ชิดกันมากจนบางครั้งแยกออกจากกันยาก การศึกษาแนวทางการดำเนินงาน (guideline) ของทั้งสองระบบจึงคาบเกี่ยวกัน อย่างไรก็ตามทั้งสองระบบก็มีมิติที่มีข้อพิจารณาเฉพาะระบบแยกจากกัน ดังนั้นในร่างแรกจะเน้นการบริหารจัดการงานบริการเทคโนโลยีสารสนเทศก่อน หลังจากนั้นแล้วจะพัฒนาบูรณาการ กับระบบข้อมูลสารสนเทศ (Information System) เป็นภาพรวมของระบบสารสนเทศโรงพยาบาล (Hospital Information Systems)

ร่างแนวทาง(Guideline) ที่เสนอใช้กรอบแนวคิด (Framework) ที่บูรณาการ CobIT (Control Objectives for Information and related Technology) , ITIL (Information Technology Infrastructure Library), ISO ๒๗๐๐๒ (ISO ๑ ๗๗๙๙ เดิม)(ISO ๒๗๗๙๙ for healthcare) ตามการศึกษาของ Angeli Hoekstra & Nicolette Conradie จาก Price Water House Cooper (๒๐๐๒) ร่วมกับแนวทางการเขียนมาตรฐานของ Joint Commission International (JCI)

กรอบแนวคิดนี้ได้ผ่านการทดสอบและนำไปใช้เบื้องต้นในการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศของโรงพยาบาลนำร่องในโครงการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศของสมาคมเวชสารสนเทศไทย จำนวน ๑๓ โรงพยาบาล ปัจจุบันเป็น version ๑.๑

กรอบแนวคิด (Framework)

คณะทำงานตกลงร่วมกันที่จะใช้ CobIT, ITIL และ ISO 17799 เป็น framework หลักของการพัฒนามาตรฐานเทคโนโลยีสารสนเทศโรงพยาบาล เนื่องจากเป็นมาตรฐานที่เป็นที่ยอมรับ และครอบคลุมการทำงานของโรงพยาบาลได้เป็นอย่างดี คณะทำงานตระหนักดีว่า โรงพยาบาลในประเทศไทยมีความพร้อมในการพัฒนาคุณภาพในด้านนี้ไม่เท่ากัน อันเนื่องมาจากบุคลากร งบประมาณ และการบริหาร จัดการอื่นๆ หากนำเอามาตรฐานทั้งหมดของต่างประเทศมาใช้ทันที จะมีโรงพยาบาลจำนวนมากประสบปัญหา คณะทำงานจึงได้ปรับมาตรฐานให้มีความยืดหยุ่นแต่มีความท้าทาย เพื่อเป็น การกระตุ้นการพัฒนาต่อไปในอนาคต

๑. โครงสร้าง และ บทบาท (Structure and Role)

โรงพยาบาลมีการกำหนดเป้าหมายนโยบาย แผนงาน และโครงสร้างหน่วยงานที่ รับผิดชอบด้านเทคโนโลยีสารสนเทศอย่างชัดเจน รวมถึงมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วย ได้อย่างต่อเนื่อง ปลอดภัย และเกิดประโยชน์สูงสุด โดยควรมีการดำเนินการในสิ่งต่อไปนี้

๑.๑.จัดให้มีทีมดูแลด้านระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลและผู้ใช้งานระบบร่วมกำหนดทิศทาง วางแผน จัดการ และติดตาม การดำเนินงานด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมระบบรัฐบาลเทคโนโลยีสารสนเทศ (IT Governance) และระบบบริหารจัดการเทคโนโลยีสารสนเทศ (IT Management)

๑.๒.จัดให้มีแผนแม่บทเทคโนโลยีสารสนเทศ (IT Master Plan) ของโรงพยาบาล

การจัดทำแผนแม่บทหรือแผนยุทธศาสตร์เทคโนโลยีสารสนเทศโรงพยาบาล โดยกำหนดเป้าหมายและแนวทางการพัฒนาและใช้งานข้อมูลและสารสนเทศไว้อย่างชัดเจน การจัดทำแผนฯ จัดทำโดยการมีส่วนร่วมของบุคลากรที่เกี่ยวข้องทั้ง ผู้บริหาร และผู้ปฏิบัติซึ่งเป็นผู้ใช้งานระบบเทคโนโลยีสารสนเทศในด้านต่างๆ เพื่อให้แผนแม่บทมีความสอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และเข็มมุ่งของโรงพยาบาล และตอบสนองต่อความต้องการของผู้ปฏิบัติงานในการดูแลผู้ป่วย /บริการสุขภาพให้มีคุณภาพยิ่งขึ้น

มีการสื่อสารแผนแม่บทให้ผู้เกี่ยวข้องรับทราบ และดำเนินการในแนวเดียวกัน มีการตรวจสอบ การติดตามประเมินผลการดำเนินการตามแผน และนำผลการประเมินมาปรับแผน ให้ดีขึ้น

๑.๓.มีนโยบายและแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

มีการกำหนดนโยบาย และแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศที่ชัดเจน ครอบคลุมนโยบายด้านความครบถ้วนถูกต้องของข้อมูลความปลอดภัยของระบบ การรักษาความลับของ ผู้ป่วย การเก็บสารสนเทศต่างๆ ระยะเวลาในการเก็บข้อมูลผู้ป่วย ข้อมูลดิบและสารสนเทศ การทำลายข้อมูลดิบและสารสนเทศด้วยความเหมาะสม และนโยบายกำกับดูแล ติดตามการดำเนินงาน ด้านเทคโนโลยีสารสนเทศ

มีการสื่อสารนโยบายด้านเทคโนโลยีสารสนเทศของโรงพยาบาลให้ผู้เกี่ยวข้องรับทราบ และดำเนินการในทิศทางเดียวกัน

๑.๔. จัดโครงสร้าง และอัตรากำลังของหน่วยงานข้อมูลและสารสนเทศโรงพยาบาลที่เหมาะสม

โรงพยาบาลมีการจัดโครงสร้างให้มีหน่วยงานที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ รวมถึงกำหนดตำแหน่ง อัตรากำลังและสายการบังคับบัญชาและอำนาจหน้าที่ ที่ชัดเจนและเหมาะสม เพื่อให้สามารถดำเนินการ ด้านเทคโนโลยีสารสนเทศให้สามารถสนับสนุนงานตาม บริบทของโรงพยาบาลได้อย่างมีประสิทธิภาพ

๑.๕. มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆที่จำเป็น สอดคล้องกับมาตรฐาน ของประเทศหรือ มาตรฐานสากล ได้แก่ มาตรฐานข้อมูลมาตรฐานรหัสข้อมูล(ซึ่งรวมถึง รหัสโรค รหัสผ่าตัด สัญลักษณ์ ตัวย่อ คำจำกัดความ) มาตรฐานการปฏิบัติงาน มาตรฐานด้านความปลอดภัย มาตรฐานระบบ เครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและ สภาพแวดล้อม

๑.๖. มีการตอบสนองความต้องการของผู้ใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม

มีการสำรวจความต้องการสารสนเทศของผู้ปฏิบัติงาน หัวหน้าหน่วยงาน ผู้บริหารโรงพยาบาล และ จัดระบบเทคโนโลยีสารสนเทศให้ตอบสนองความต้องการของผู้ใช้ มีการคำนึงถึงบริบท ของโรงพยาบาล โดยนำสารสนเทศมาช่วยในการพัฒนาการบริการให้มีความ ถูกต้อง ปลอดภัย มีประสิทธิภาพ สะดวก รวดเร็ว รวมทั้งนำสารสนเทศมาช่วยสนับสนุนการตัดสินใจ ในการบริหารจัดการตลอดจนการศึกษาวิจัย ตอบสนองต่อภารกิจและพันธกิจทุกด้าน

๒. เทคโนโลยี (Technology)

การเลือกใช้เทคโนโลยีที่เหมาะสม จัดให้มีการใช้เทคโนโลยีอย่างเป็นระบบ มีความสำคัญยิ่งต่อการพัฒนาเทคโนโลยีสารสนเทศโรงพยาบาล ซึ่งนับว่าเป็นหัวใจของการใช้งานอย่างคุ้มค่า สะดวก ปลอดภัย อย่างไรก็ดีเทคโนโลยีสารสนเทศมาพร้อมกับความเสี่ยง ซึ่งรวมถึงการสะดุดหยุดลงของงาน การสูญเสียข้อมูลที่สำคัญทั้งโดยบังเอิญจากความผิดพลาดของระบบและการจงใจจากผู้ประสงค์ร้าย รวมทั้งการถูกล้วงความลับข้อมูลของโรงพยาบาลโดยผู้ไม่มีสิทธิ จึงจำเป็นต้องมีการจัดการเทคโนโลยีอย่าง เหมาะสม เพื่อลดความเสี่ยงที่อาจเกิดขึ้นให้น้อยที่สุด

โรงพยาบาลจำเป็นต้องมีการจัดการด้านเทคโนโลยีดังต่อไปนี้

๒.๑. จัดให้มี Data center

Data center ของโรงพยาบาล ได้แก่ที่ตั้งของ Servers และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัยเป็นต้น data center นี้ต้องมีการจัดการอย่างเหมาะสม เพื่อให้แน่ใจได้ว่า จะสามารถใช้งานระบบได้อย่าง ปลอดภัย ปราศจากการหยุด หรือสะดุดของระบบ ซึ่งต้องคำนึงถึงสิ่งต่อไปนี้

๑) ห้อง สถานที่และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย เช่นมีการปรับอากาศที่ดีรักษา ความปลอดภัยจากบุคคลภายนอก การป้องกันอัคคีภัย (รวมถึงระบบตรวจจับควันและระบบเตือนภัย เครื่องดับเพลิง และระบบดับเพลิงอัตโนมัติ)

๒) มีระบบป้องกันการเสียหายของข้อมูลและระบบ (data integrity and fault tolerance) ซึ่งรวมถึง UPS และระบบไฟฟ้าสำรอง, ระบบ RAID, Redundant power supply และ Redundant Servers

๓) มีระบบสำรองข้อมูลทั้งภายใน และภายนอก data center

๔) มีการจัดการ network ที่เหมาะสม

๒.๒. มีการกลั่นกรอง/เลือกใช้ Technology อย่างเหมาะสม

มีการวิเคราะห์ความเหมาะสม คำนึงถึงประโยชน์ มาตรฐาน ความเสี่ยง และความคุ้มค่า ในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และการเลือก software ที่เหมาะสม กับ เป้าหมายสอดคล้องกับบริบท และแผนแม่บทเทคโนโลยีสารสนเทศของโรงพยาบาล

มีการทบทวนความก้าวหน้าเทคโนโลยีสารสนเทศทางการแพทย์อย่างสม่ำเสมอเพื่อนำมาพัฒนา และปรับปรุง ระบบเทคโนโลยีสารสนเทศให้เกิดประโยชน์สูงสุด

๒.๓. จัดเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยและคุ้มครองความลับข้อมูลส่วนบุคคลและการเข้าถึงข้อมูลผู้ป่วย

ความเป็นส่วนตัวของผู้ป่วยเป็นสิ่งสำคัญ ซึ่งเป็นความเสี่ยงอย่างหนึ่งจากการใช้เทคโนโลยี จำเป็นต้องจัดการให้มีระบบที่ป้องกันผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลของผู้ป่วย ดังนี้

๑) ระบบมีบัญชีรายชื่อผู้ใช้งาน และรหัสผ่าน (username and password) และกลไกการ ยืนยันตัวบุคคล

๒) สร้างระบบการเข้าถึงข้อมูลผู้ป่วยให้รัดกุม (ใคร สามารถเข้าถึงข้อมูลส่วนไหน ด้วยวิธีใดเป็นต้น)

๓) สามารถระบุตัวบุคคลผู้เข้าถึงข้อมูลผู้นำข้อมูลผู้รับบริการเข้าสู่ระบบ ผู้ที่แก้ไขข้อมูลและ วันเวลาที่เข้าถึง หรือนำข้อมูลผู้รับบริการเข้าสู่ระบบ หรือแก้ไขข้อมูลได้มีเทคโนโลยี ด้านความมั่นคงของระบบ เช่น firewall ระบบป้องกันไวรัสและโทรจัน มาใช้

๔) การแยกระบบ internet และระบบงานโรงพยาบาล การจัด private network เป็นต้น

๓. บุคลากร (People)

มีการจัดการทรัพยากรบุคคลด้านเทคโนโลยีสารสนเทศ ที่เหมาะสม เพื่อให้การพัฒนาและใช้งานเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ

๓.๑. มีบุคลากรด้านเทคโนโลยีสารสนเทศที่เพียงพอ โดยมีการกำหนดสมรรถนะที่จำเป็นของแต่ละตำแหน่งอย่างเหมาะสม อันได้แก่

๑) Chief Information officer (CIO) ได้แก่บุคลากรระดับบริหารของโรงพยาบาลที่ทำหน้าที่เป็นผู้นำในการบริการด้านเทคโนโลยีสารสนเทศ พัฒนาระบบเทคโนโลยีสารสนเทศ โรงพยาบาลอยู่ในทีมนำของโรงพยาบาล โดยมีหน้าที่หลักดังนี้

- กำหนดเป้าหมายการดำเนินงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ให้ สอดคล้องกับวิสัยทัศน์พันธกิจ และเข็มมุ่งของโรงพยาบาล รวมทั้งแนวทางในการนำเทคโนโลยีด้านสารสนเทศที่เหมาะสมมาใช้งาน และการพัฒนาคุณภาพ เทคโนโลยีสารสนเทศให้ได้มาตรฐาน โดยผ่านการเห็นชอบจากทีมนำของโรงพยาบาล และสอดคล้องกับกฎหมายและข้อบังคับต่างๆ
- จัดให้มียุทธศาสตร์แผนงาน โครงการเพื่อบรรลุวัตถุประสงค์ดังกล่าว
- ควบคุม กำกับ และประเมินผล ให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างเหมาะสมและราบรื่น

คณะทำงานควรเป็นผู้ที่มีความรู้/ผ่านการอบรม/ หรือมีประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ และติดตามความก้าวหน้าดังกล่าวอย่างสม่ำเสมอ เนื่องจากความรู้และพัฒนาการ ทั้งในด้านอุปกรณ์ ระบบงาน มาตรฐาน กฎระเบียบและกฎหมาย รวมถึงภัยคุกคามด้านเทคโนโลยีสารสนเทศเป็นไปอย่างรวดเร็ว

๒) หัวหน้าหน่วยงานข้อมูลและสารสนเทศ (Head of IT unit) บริหารจัดการและดูแลการบริการด้านเทคโนโลยีสารสนเทศ (IT service management) อย่างเป็นระบบ ประเมินความเสี่ยง จัดการป้องกัน ดูแล และแก้ปัญหาต่างๆ ที่เกิดขึ้นในการดำเนินงานติดตามการทำงานและปัญหาที่เกิดขึ้นในด้านเทคโนโลยีสารสนเทศและดำเนินการแก้ไข เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลดำเนินการไปได้อย่างราบรื่นและต่อเนื่อง รวมทั้งการพัฒนาหน่วยงานข้อมูลและสารสนเทศให้มีระดับคุณภาพที่สูงขึ้น

๓) บุคลากรอื่นๆ หน่วยงานมีการวิเคราะห์ความจำเป็นด้านบุคลากรเทคโนโลยีสารสนเทศ ตามบริบทของโรงพยาบาล และจัดให้มีบุคลากรด้านนี้อย่างพอเพียงและเหมาะสม ตัวอย่างบุคลากรที่จำเป็น เช่น

I. IT technician ผู้ดูแลระบบงานทั่วไป เช่นแก้ไขเมื่อคอมพิวเตอร์ หรือเครือข่ายมีปัญหา ติดตั้งโปรแกรม ดูแลเครื่องแม่ข่าย สำรองข้อมูลเป็นต้น

II. IT security personnel ผู้ดูแลความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ

III. IT staffs อื่นๆ เช่น นักพัฒนาระบบ(developer) โปรแกรมเมอร์ วิศวกรด้านคอมพิวเตอร์ เจ้าหน้าที่ Service desk ฯลฯ

IV. Health Information Management officer เช่น เจ้าหน้าที่เวชระเบียน ผู้ดูแลเกี่ยวกับข้อมูลสารสนเทศต่างๆ ที่อยู่ในระบบ ให้มีความถูกต้องเที่ยงตรง

V. Clinical Informatician เป็นผู้ที่มีความรู้ความเข้าใจงานทางคลินิก งานด้านสาธารณสุข และงานด้านเทคโนโลยีสารสนเทศในระดับที่สามารถเป็นตัวเชื่อมการทำงาน ระหว่างบุคคลากรด้าน IT กับบุคคลากรผู้ให้บริการทางการแพทย์และ สาธารณสุขได้อย่างมีประสิทธิภาพ รวมถึงสามารถนำสารสนเทศโรงพยาบาลมาประมวลผล และใช้งานให้มีประสิทธิภาพ ทั้งด้านการดูแลผู้ป่วย และการบริหารจัดการองค์กร

๓.๒. มีการประเมินสมรรถนะบุคลากรด้านเทคโนโลยีสารสนเทศและนำผลการประเมินมาพัฒนาบุคลากรเพื่อให้บุคลากรมีความรู้ความสามารถที่จำเป็นต่อการปฏิบัติและพัฒนางานอยู่ตลอดเวลา

๓.๓. มีกระบวนการในการรักษาบุคลากรไว้ในระบบ และป้องกันความเสี่ยงในการสูญเสียบุคลากร ด้านเทคโนโลยีสารสนเทศที่จะไม่ก่อให้เกิดปัญหาร้ายแรงต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ อย่างต่อเนื่อง

๓.๔. มีการพัฒนาผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ผู้ใช้งานระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างถูกต้องและเป็นไปตามบริบทและนโยบายด้านเทคโนโลยีสารสนเทศขององค์กรทั้งด้านความถูกต้องครบถ้วนของข้อมูลการรักษาความลับของผู้ป่วย และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ การพัฒนานี้รวมถึงผู้บริหารระดับสูงและผู้เกี่ยวข้องได้รับการพัฒนาให้เข้าใจเกี่ยวกับ หลักการการจัดการสารสนเทศ (Principles of Information Management) ที่จำเป็นโดยมุ่งเน้น ให้เกิดวัฒนธรรมการใช้งานสารสนเทศที่ดี อัตรากำลังของหน่วยงาน เทคโนโลยีสารสนเทศ โรงพยาบาลนั้น อาจมีความยืดหยุ่นได้ เช่นงานบางอย่างด้านเทคโนโลยีสารสนเทศอาจจัดจ้างบุคคลภายนอกดูแล แต่ต้องมีการจัดการที่แน่ใจได้ว่าจะสามารถดำเนินการด้านเทคโนโลยีสารสนเทศได้อย่างราบรื่น ปลอดภัย รวมทั้งจะไม่กระทบต่อภารกิจหลัก ของโรงพยาบาล และไม่กระทบต่อความลับของผู้ป่วย

๔. กระบวนการ (Processes)

มีการออกแบบและการจัดการระบบงาน กระบวนการการให้บริการและสนับสนุนงานด้านเทคโนโลยีสารสนเทศที่ตอบสนองต่อบริบทของโรงพยาบาล เพื่อให้แน่ใจว่าการให้บริการด้านสุขภาพ เป็นไปอย่างสม่ำเสมอ ต่อเนื่อง เป็นมาตรฐานเดียวกัน และมีการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ได้แก่

๔.๑. ระบบสนับสนุนการใช้งานด้านเทคโนโลยีสารสนเทศ

ในโรงพยาบาลควรมีระบบสนับสนุนงานด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมุ่งเน้นที่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศให้ได้รับความสะดวก ลดข้อผิดพลาด และใช้งานได้ราบรื่นต่อเนื่อง รวมทั้งการรวบรวม แก้ไขอุบัติการณ์และปัญหาต่างๆ ที่เกิดขึ้น ในส่วนการสนับสนุนงานด้านเทคโนโลยีสารสนเทศ โรงพยาบาลควรมีกระบวนการบริหารจัดการที่สำคัญคือ

๑) มีจุดติดต่อ (contact point) กับหน่วยงานข้อมูลและสารสนเทศ เช่น ศูนย์ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Service desk) เพื่อผู้ใช้งานสามารถเข้าถึงได้ง่ายเมื่อมีอุบัติการณ์หรือปัญหาเกิดขึ้น รวมทั้งเป็นช่องทางการสื่อสารกับผู้ใช้งาน เพื่อรับฟังปัญหา อุปสรรค และความต้องการของผู้ใช้งานด้วย

๒) มีระบบจัดการอุบัติการณ์ และปัญหาด้านเทคโนโลยีสารสนเทศ (incident and problem management) มีการรวบรวมสถิติและวิเคราะห์ซึ่งครอบคลุมตั้งแต่ปัญหาง่ายๆ ที่จัดการ ได้ ณ จุดเกิดอุบัติการณ์จนถึงปัญหาที่สลับซับซ้อน รวมถึงมีการวิเคราะห์หาสาเหตุราก (root cause) เพื่อการแก้ไขอย่างถาวร ทั้งนี้เพื่อให้การใช้งานข้อมูลและสารสนเทศเป็นไป อย่างราบรื่นหรือเกิดผลกระทบต่อการทำงานน้อยที่สุดหากมีการหยุดชะงัก

๓) มีระบบบริหารการเปลี่ยนแปลง (Change Management) การเปลี่ยนแปลงใน พื้นฐาน หรือสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศเกิดขึ้น ได้ตลอดเวลา ซึ่งอาจเกิดจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงของเทคโนโลยี ความต้องการด้านกฎหมาย ด้านการเงิน ระบบประกัน ฯลฯ หรือปัจจัยภาย'ใน เช่น ข้อตกลงระดับบริการ (service level agreement) การปรับเปลี่ยนหรือพัฒนาระบบให้ดียิ่งขึ้น รวมทั้งการปรับปรุง software hardware หรือ network ด้วย ฯลฯ จึงต้องมีการบริหาร จัดการเพื่อให้มั่นใจว่า การเปลี่ยนแปลงที่เกิดขึ้น จะไม่ส่งผลกระทบต่อการทำงานและคุณภาพการบริการ หรือเกิดผลกระทบน้อยที่สุด โดยมีคณะกรรมการเฉพาะเพื่อพิจารณา และอนุมัติการเปลี่ยนแปลง

๔.๒. มีระบบบริหารจัดการด้านการให้บริการเทคโนโลยีสารสนเทศ จัดให้เกิดระบบข้อมูลสำหรับทุกคนที่เข้ามารับบริการ มีการจัดการข้อมูลผู้รับบริการด้วยระบบที่มีประสิทธิภาพ เพื่อให้ผู้รับบริการได้รับบริการที่ปลอดภัย ถูกต้อง สะดวกรวดเร็ว และต่อเนื่อง โดยมีการประกัน คุณภาพตามข้อตกลงการจัดบริการ (Service Level Agreement-SLA) ของโรงพยาบาล

๔.๓. มีการจัดการและจัดสรรทรัพยากรที่เพียงพอ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ เหมาะสมกับปริมาณงาน (Capacity Management)

๔.๔. มีการออกแบบระบบคงทนต่อความผิดพลาด (fault tolerance) มีการบำรุงรักษาอย่างสม่ำเสมอ มีการจัดการเพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง (Availability Management) และสามารถกู้คืนระบบได้แม้จะมีเหตุการณ์ไม่คาดฝนเกิดขึ้น (IT Service

Continuity Management) โดยมีการวิเคราะห์และจัดทำแผนสำรองฉุกเฉิน (Business Continuity Plan) และแผนกู้คืนระบบ (Disaster Recovery Plan) รวมทั้งมีการทบทวนและ ซักซ้อมแผนอย่างสม่ำเสมอ

๔.๕. มีการจัดการข้อมูลให้แน่ใจว่า ข้อมูลสำคัญได้รับการบันทึก และจัดเก็บในระบบ อย่างถูกต้อง และครบถ้วน ประกอบไปด้วย

๑) การบันทึก อาการสำคัญประวัติ ผลการตรวจร่างกาย และคำวินิจฉัยโรค ในบัตรผู้ป่วย นอก และ/หรือ เวชระเบียนอิเล็กทรอนิกส์โดยต้องไม่จัดเก็บรหัส ICD แทนคำวินิจฉัยโรค

๒) บันทึกประวัติตรวจร่างกายแรกรับ บันทึกความก้าวหน้า และการสรุปเวชระเบียนเมื่อ สิ้นสุดการรักษา (Discharge Summary) ในแฟมผู้ป่วยใน

๓) รายงานการผ่าตัด ในผู้ป่วยทุกรายที่ได้รับการผ่าตัด

๔) การให้รหัส ICD ทั้งรหัสกลุ่มโรค และรหัสการผ่าตัด

๕) การบันทึกเวชระเบียนให้สอดคล้องกับมาตรฐานข้อมูลทางการแพทย์อื่นๆ

๕. การควบคุม (Control)

การมีระบบการควบคุมการดำเนินงานด้านเทคโนโลยีสารสนเทศจะทำให้แน่ใจได้ว่าการดำเนินงาน จะเป็นไปตามระบบ และแผนงานที่วางไว้ การควบคุมด้านเทคโนโลยีสารสนเทศถือเป็นส่วนหนึ่งของการควบคุมภายในของหน่วยงาน ซึ่งประกอบด้วยกลไกที่สำคัญดังนี้

๕.๑. มีระบบควบคุมทั่วไป (General control) เพื่อให้แน่ใจว่า ระบบสารสนเทศจะสามารถใช้งานได้อย่างถูกต้อง ปลอดภัย การควบคุมทั่วไปได้แก่ การควบคุมในกรณีต่อไปนี้

๑) สร้างวัฒนธรรมการใช้งานข้อมูลและสารสนเทศที่ปลอดภัย และสอดคล้องกับทิศทางขององค์กร

๒) การจัดสร้าง/ต่อเติม software ให้เป็นไปอย่างมีประสิทธิภาพ รวมทั้งกำกับดูแล source code/version ของ software

๓) ระบบควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) มีกระบวนการควบคุมที่ทำให้แน่ใจได้ว่าระบบและข้อมูลได้รับการปกป้องจากการ เข้าถึงหรือโจมตีโดยผู้ไม่ประสงค์ดี การใช้งานที่ไม่ถูกต้องหรือไม่ได้รับอนุญาต ประกอบไปด้วย

๓.๑) ความปลอดภัยด้านกายภาพ เช่น มาตรการการเข้าออก data center

๓.๒) ด้าน software และการใช้งาน เช่น การเลือกใช้ database

๓.๓) การควบคุมการเข้าถึง (Access Control) การจัดการการเข้าถึงของผู้ใช้งาน (User access management) รวมถึงการทำบัญชีรายชื่อผู้ใช้งาน การกำหนดสิทธิผู้ใช้งาน การรักษาความลับรหัสผ่านของผู้ใช้แต่ละบุคคล รวมถึงยืนยันตัวบุคคล (Authentication)

๓.๔) การควบคุมให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นสามารถเข้าถึงข้อมูล(Business requirements of access control)

๓.๕) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๓.๖) การควบคุมการเข้าถึงระบบ (System and application access control)

๓.๗) การบันทึกข้อมูล Log และการเฝ้าระวัง (Logging and Monitoring)

๓.๘) การบริหารจัดการช่องโหวทางเทคนิค (Technical Vulnerability Management)

๓.๙) ด้านเครือข่าย เช่น การเชื่อมโยง Internet การป้องกันการบุกรุกเครือข่าย

๓.๑๐) การบำรุงรักษาระบบโดยบุคคลภายนอก มีมาตรการควบคุม

๓.๑๑) การป้องกันไวรัสในระบบคอมพิวเตอร์ และเครื่องมือแพทย์(Protection from Malware)

๓.๑๒) การใช้ Social Media ในการสื่อสารข้อมูลผู้ป่วย

๔) ด้าน hardware/software เมื่อมีการเปลี่ยนแปลงระบบงานเกิดขึ้นเช่น การลงระบบงาน การติดตั้งโปรแกรมครั้งใหม่ ตั้งค่าระบบ(configuration) การเพิ่มหน่วยความจำใน เครื่องคอมพิวเตอร์ เป็นต้น

๕.๒. มีระบบควบคุมด้วย application (Application control) เพื่อให้แน่ใจว่า ข้อมูลสารสนเทศที่มีอยู่ในระบบเป็นข้อมูลที่ถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลา โดยมีระบบควบคุมตรวจสอบดังนี้

๑) การตรวจสอบความครบถ้วน (completeness check) มีระบบที่ทำให้แน่ใจว่ามีการบันทึกข้อมูลผู้รับบริการทุกรายที่เข้ามารับบริการในโรงพยาบาลอย่างครบถ้วน

๒) ข้อมูลผู้รับบริการทุกคนที่มารับบริการ ถูกบันทึกข้อมูลไว้ในระบบอย่างเป็นระบบแบบแผน (Input control)

๓) การตรวจสอบความถูกต้อง (validity check) มีระบบที่ทำให้แน่ใจว่าข้อมูลต่างๆ ที่นำเข้าระบบสารสนเทศ มีความถูกต้อง เที่ยงตรง รวมทั้งมีระบบการเรียกดูข้อมูลผู้รับบริการ และตรวจสอบความครบถ้วนของข้อมูลผู้รับบริการอย่างสม่ำเสมอ โดยการเรียกดูแบบ สุ่มตัวอย่างดำเนินการนำและผู้เกี่ยวข้องที่มีอำนาจหน้าที่ในการนำ ข้อมูลเข้า หรือ เรียกดูข้อมูลได้ การเรียกดูข้อมูลผู้รับบริการเน้นไปที่ความตรงต่อเวลา ความครบถ้วนของข้อมูล การแยกดูข้อมูลครอบคลุมทั้งผู้ที่กำลังรับบริการอยู่และที่กลับไปแล้ว

๔) การระบุเจ้าของข้อมูล (identification) มีการควบคุมที่ทำให้แน่ใจว่า มีการระบุบุคคลได้ อย่างชัดเจน ไม่มีข้อมูลซ้ำ (ข้อมูลผู้ป่วย ๒ ราย ถูกระบุเป็นคนเดียวกันในระบบ) และ ข้อมูลที่นำเข้าเป็นของผู้ป่วยรายนั้นจริง

๕) การระบุตัวผู้เข้าใช้ระบบ และควบคุมให้ผู้มีสิทธิเท่านั้นที่เข้าใช้งานระบบได้ตามสิทธิ มีการบันทึกข้อมูลการเข้าใช้งาน

๕.๓. มีระบบบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT risk management) ในด้านต่างๆ ดังนี้

๑) ความเสี่ยงต่อความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ (hardware software network data)

๒) ความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย

๓) ความเสี่ยงต่อความเป็นส่วนตัวของข้อมูลผู้ป่วย

๔) ความเสี่ยงในการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management Failure)

๕.๔. มีระบบควบคุมคุณภาพข้อมูลให้แน่ใจว่า ข้อมูลสำคัญที่บันทึก และจัดเก็บไว้ในระบบ มีคุณภาพที่ดีขึ้นอย่างต่อเนื่อง โดยมีกระบวนการประเมินคุณภาพข้อมูลที่สำคัญ ดังนี้

๑) คุณภาพการบันทึก อาการสำคัญประวัติผลการตรวจร่างกาย และคำวินิจฉัยโรคในบัตร ผู้ป่วยนอก และ/หรือ เวชระเบียนอิเล็กทรอนิกส์

๒) คุณภาพการบันทึกประวัติตรวจร่างกายแรกรับ บันทึกความก้าวหน้า และการสรุปเวชระเบียนเมื่อสิ้นสุดการรักษา (Discharge Summary) ในแฟ้มผู้ป่วยใน

๓) คุณภาพการบันทึกรายงานผ่าตัด ในผู้ป่วยทุกรายที่ได้รับการผ่าตัด

๔) ความถูกต้องของการให้รหัส ICD ทั้งรหัสกลุ่มโรคและรหัสการผ่าตัดและมีการนำผลการประเมินมาวิเคราะห์เพื่อหาแนวทางปรับปรุงระบบให้ดีขึ้นอย่างต่อเนื่อง

๖. การวัด (Metrics)

มีการกำหนดตัวชี้วัด และวัดผลที่สามารถใช้ในการติดตามเฝ้าระวังและตรวจสอบการ ดำเนินงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ว่าเป็นไปอย่างถูกต้องเหมาะสมและบรรลุวัตถุประสงค์การวัดและประเมินผลควรกระทำในทุกๆหมวดของกรอบการพัฒนา เพื่อลดการใช้ความเห็นของบุคคลในการตัดสินใจ การวัดที่สำคัญ ได้แก่

๖.๑. วัดและติดตาม กระบวนการทำงานด้านเทคโนโลยีสารสนเทศ เช่น จำนวนครั้งและระยะเวลาที่ ต้องหยุดให้บริการ (down time) ระยะเวลาในการแก้ไขอุบัติการณ์ต่างๆ ค่าใช้จ่ายในการ บำรุงรักษาระบบ

๖.๒. วัดและติดตามความเสี่ยง การควบคุมภายใน ด้านความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๖.๓. วัดและติดตามความถูกต้อง ครบถ้วน เชื่อถือได้ ทันเวลาของข้อมูลสารสนเทศ

๖.๔. ตรวจสอบการปฏิบัติตามนโยบายและระเบียบปฏิบัติ

๖.๕. ประเมินและวัดผลการดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศ การพัฒนาสมรรถนะบุคลากร การพัฒนาความสามารถของระบบ

๗. ข้อมูลสารสนเทศ (Data & Information)

วัตถุประสงค์หลักของการมีระบบเทคโนโลยีสารสนเทศในโรงพยาบาลคือ การมีข้อมูลและสารสนเทศที่จำเป็นสำหรับบุคลากร ผู้บริหาร ผู้ป่วย ผู้รับผลงาน องค์กรภายนอก มีความพร้อมใช้งาน เอื้อต่อการดูแลผู้ป่วย การบริหารจัดการ การตรวจสอบทางคลินิก การพัฒนาคุณภาพ การศึกษา และการวิจัย ความจำเป็นของข้อมูลและสารสนเทศขึ้นอยู่กับขนาดและความซับซ้อนตามบริบทของโรงพยาบาล

๗.๑. มีข้อมูลที่เพียงพอกับการให้บริการผู้ป่วยอย่างมีคุณภาพ

ข้อมูลสามารถนำมาใช้ระบุตัวบุคคล สนับสนุนการวินิจฉัยโรค ช่วยพิจารณาการรักษา ช่วยติดตามการรักษา บันทึกผลการรักษา และใช้สนับสนุนการรักษาดูแลอย่างต่อเนื่อง จัดทำเป็นมาตรฐานอยู่ในเวชระเบียนอิเล็กทรอนิกส์ปราศจากการซ้ำซ้อน หรือขัดแย้งซึ่งกันและกัน

๗.๒. ผู้ใช้สามารถเข้าถึงข้อมูลและสารสนเทศได้อย่างสะดวกและเหมาะสม

ผู้ใช้งานเข้าถึงข้อมูลและสารสนเทศสำหรับการปฏิบัติงานในความรับผิดชอบได้โดยได้รับข้อมูลและสารสนเทศตามกำหนดเวลา ตรงตามรูปแบบที่ช่วยการใช้งาน

ผู้ป่วยสามารถเข้าถึงข้อมูลของตนเองเพื่อนำไปใช้ในการดูแลรักษาสุขภาพ และหน่วยงานเครือข่ายที่เกี่ยวข้องได้รับข้อมูลเพื่อนำไปใช้พัฒนาบริการสุขภาพ

๗.๓. สารสนเทศถูกนำมาใช้อย่างเหมาะสม (Appropriate use of information)

มีการวิเคราะห์ข้อมูลที่มีอยู่ในระบบ รวมถึงข้อมูลที่จำเป็นต่อการใช้งานแต่ยังไม่มีอยู่ในระบบเพื่อจัดการให้มีข้อมูลสารสนเทศที่เหมาะสมเพิ่มขึ้น รวมทั้งบูรณาการข้อมูลผู้ป่วยและข้อมูลบริหาร เข้าหากันเพื่อสนับสนุนการติดสินใจและพัฒนาคุณภาพอย่างต่อเนื่อง

๗.๔. หน่วยงานสามารถใช้ข้อมูลจากแหล่งข้อมูลภายนอกต่างๆ

หน่วยงานใช้และบูรณาการข้อมูลจากแหล่งต่างๆ เพื่อ

๑) สนับสนุนการติดสินใจในการดูแลผู้ป่วย

๒) สนับสนุน การศึกษา การวิจัย

๓) สนับสนุนการบริหารจัดการและวางแผน ยุทธศาสตร์ มีสารสนเทศทางวิทยาศาสตร์และด้านอื่นๆ ที่เป็นปัจจุบัน ที่สนองต่อความต้องการของ ผู้ใช้งานภายในเวลาที่เหมาะสม

หมวดที่ ๑
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิและการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ๒. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล จะต้องขออนุญาต เป็นลายลักษณ์อักษรต่อผู้บริหาร

ข้อ๓. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการ เข้าถึงอย่างสม่ำเสมอดังนี้

(๓.๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

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

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

(๓)ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงาน หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓.๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับ ของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็น มาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่ เหมาะสม ในการ จัดการเอกสารอิเล็กทรอนิกส์และใน การรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่ สำคัญไว้ดังนี้

(๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่ เป็นซอฟต์แวร์ปกติ เมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์ และพอที่จะอ่านข้อความนั้นได้ซึ่งมีรูป แบบย่อยอีกหลายรูปแบบเช่น TEXT Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ๔. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ ของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ๕. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ๖. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ๗. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึง ได้ตลอดเวลา

(๒) ระบบงานภายใน (BackOffice) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ(ตามข้อ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษร ให้แก่ผู้ใช้ งาน เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ๙. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบ คอมพิวเตอร์ โปรแกรมประยุกต์(Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และ ได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) จัดทำบัญชีรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และตรวจสอบสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูลสิทธิต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายใน ต้องดำเนินการภายใน ๗ วัน

ข้อ๑๑. การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการ ส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใสรหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๗)ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษได้รับว่าสามารถ เข้าถึงได้ถึงระดับใดได้บาง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัส ผู้ใช้งานตามปกติ

ข้อ๑๒. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้า ถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูล แต่ละประเภทชั้นความลับ มีดังต่อไปนี้

ระดับที่ ๑ ข้อมูลทีมีสามารถเผยแพร่สู่สาธารณะ ได้ในทุกรูปแบบรวมทั้งเชื่อมโยงไปสู่แหล่งข้อมูลอื่นๆ ในบริบทที่เกี่ยวข้องกันได้ อยู่ภายใต้เงื่อนไขและข้อกำหนดของสัญญาอนุญาตของศูนย์ข้อมูลเปิดภาครัฐ

ระดับที่ ๒ ข้อมูลที่สามารถเปิดเผยให้กับบุคคลหรือองค์กรเป็นรายกรณี แต่ต้องมีการจำกัดตัวแปรอื่นที่อาจเชื่อมโยงถึงบุคคลใดบุคคลหนึ่งได้

ระดับที่ ๓ ข้อมูลที่สามารถเปิดเผยได้เฉพาะข้อมูลเชิงสรุปหรือเชิงสถิติเท่านั้น

ระดับที่ ๔ ข้อมูลที่เปิดเผยได้เฉพาะหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย

ระดับที่ ๕ ข้อมูลที่ไม่เปิดเผยหรือไม่จำเป็นต้องเปิดเผยให้หน่วยงานหรือบุคคลภายนอกองค์กร จะเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ๑๓. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้าม ทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ(save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อย ๑ ครั้งต่อปี

ข้อ๑๔. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ๑๕. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งาน จะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ๑๖. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งาน ต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการ พิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่ง สามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการ ล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

ข้อ๑๗. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาล หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ๑๘. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๑๙. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลและข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ๒๐. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อ๒๑. ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาล จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่ง บุคคลใด ทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาล ซึ่ง โรงพยาบาลอาจแต่งตั้งให้ผู้ทำหน้าที่ ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ๒๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่าย

คอมพิวเตอร์ ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่อง ต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรม หรือแฟ้ม ข้อมูลของคอมพิวเตอร์ เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกัน เช่น บิทเทอรเรนท์ (Bittorrent), อีเมล (Email) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟัง เพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ๒๔. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูลข้อความ รูป ภาพ หรือสิ่งอื่น ใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาล

ข้อ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรม ข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาล

ข้อ๒๖. ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชน์ทางการค้า

ข้อ๒๗. ห้ามกระทำการใดๆเพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆก็ตาม

ข้อ๒๘. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ๒๙. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศ ภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ๓๐. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่ากรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

ข้อ๓๑. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาล โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ๓๒. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันใน ระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น โรงพยาบาลหรือหน่วยงานที่มาขอเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันที่เพียงพอ

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Operation Center หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๓๔. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่าย เพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ๓๗. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ๓๘. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูลแฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	- ใช้การทำลายด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของ กระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการ เขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
เทป	- ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ๓๙.ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ

ไปใช้ใน กิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาล

ข้อ๔๐. ความเสียหายใดๆ ที่เกิดจากการละเมิดตาม ข้อ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ๔๑. มาตรการควบคุม การเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการ ปฏิบัติงาน มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาต เข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ๔๒. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัดโดยผู้ใช้งานต้องกรอก แบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

ข้อ๔๓. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบ ต่อการกระทำของระบบและผู้ใช้งานอื่นๆ

ข้อ๔๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์ จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล(Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๔๕. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย(Malware) ด้วย

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

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้อง มีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

(๘) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต ของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้ หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ๔๖. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ๔๗. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงาน ต้องมีการขออนุมัติจากผู้ดูแลระบบก่อน ดำเนินการให้ติดตั้ง

ข้อ๔๘. กำหนดให้มีการจัดเก็บรหัสต้นฉบับ (source code), คลังโปรแกรม (Library) และเอกสาร สำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ๔๙. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๕๐

ข้อ๕๐. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จาก ผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาต จากหัวหน้าหน่วยงาน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ๕๑. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ๕๒. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือ เปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ๕๓. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ๕๔. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก(IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่าน ระบบเครือข่าย การใช้งานใน ลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่ เกี่ยวข้อง

ข้อ๕๕. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ๕๖. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ๕๗. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ๘) ในการ ใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ๕๘. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๒) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

(๓) ซอฟต์แวร์ที่โรงพยาบาลจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

(๔) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเพื่อประโยชน์ทางการค้า

(๕) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๖) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดย ไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๕๙. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ๖๐. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถ ทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยง มาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการ ใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็น ในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ๖๑. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งาน ด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

(๒) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานเร็วขึ้นสำหรับระบบสารสนเทศ ที่มีความเสี่ยงสูง

ข้อ๖๒. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งาน ได้ตามช่วงเวลา

การทำงานที่หน่วยงานกำหนดเท่านั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ(Application and Information Access Control)

ข้อ๖๓. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ๘) ในการใช้งานตาม ความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ๖๔. ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ

ข้อ๖๕. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนเขาระบบสารสนเทศอีกครั้ง

ข้อ๖๖. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือ พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและ ระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนด สิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัส ผู้ใช้งานตามปกติ

ข้อ๖๗. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึง วิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

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

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ๖๘. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

ข้อ๖๙. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ใน สภาพพร้อมใช้ งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้ มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

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

ข้อ๗๐. โรงพยาบาลได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งาน ทำการ ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐาน ละเมิดลิขสิทธิ์ ถือว่าเป็น ความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ๗๑. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการ อนุญาตจาก หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์

ข้อ๗๒. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๗๓. บรรดาข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ๗๔. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ๗๕. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ๗๖. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ๗๗. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูลข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นสินทรัพย์ ของหน่วยงานหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๗๘. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ สามารถดำเนินการได้ แต่ต้องไม่ ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการ กระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะ เช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือ ขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบน เครือข่ายคอมพิวเตอร์

ข้อ๗๙. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ (source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำไว้กับ ผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆให้พร้อมใช้งาน

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ๘๐. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ๘๑. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูลและอุปกรณ์ สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ๘๒. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ๘๓. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ หน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ๘๔. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูลระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ๘๕. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ๘๖. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้ รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายให้น้อยที่สุด

ข้อ๘๗. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ ซ่อน SSID (Service Set Identifier)

ข้อ๘๘. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ๘๙. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และ ชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้ อย่างถูกต้อง

ข้อ๙๐. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ๙๑. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายใน

หน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย
ข้อ๙๒. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
ข้อ๙๓. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที
ข้อ๙๔. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน
ข้อ๙๕. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร
ข้อ๙๖. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็น ในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ๙๗. หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของ Firewall ทั้งหมด
ข้อ๙๘. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)
ข้อ๙๙. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall
ข้อ๑๐๐. ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง
ข้อ๑๐๑. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลง ทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่างๆ ของ Firewall
ข้อ๑๐๒. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
ข้อ๑๐๓. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน
ข้อ๑๐๔. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ต การเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน
ข้อ๑๐๕. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น
ข้อ๑๐๖. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์ หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า
ข้อ๑๐๗. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆภายในหน่วยงาน ที่มีลักษณะที่

เป็นอินทราเน็ต จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องอนุญาตเป็นกรณีไป

ข้อ๑๐๘. หน่วยงานมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการ ใช้งานที่ผิดนโยบาย หรือเกิดจากการทำ งานของโปรแกรมที่มีความเลี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ๑๐๙. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อ๑๑๐. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ต ทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส (E-Mail)

ข้อ๑๑๑. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ๑๑๒. เปลี่ยนรหัสผ่าน (Password) ทุก ๓ - ๖ เดือน

ข้อ๑๑๓. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

ข้อ๑๑๔. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ๑๑๕. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลE-Mail ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังใน การระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ๑๑๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ๑๑๗. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ๑๑๘. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ๑๑๙. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ๑๒๐. ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อ๑๒๑. ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ๑๒๒. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ๑๒๓. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ๑๒๔. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูล อันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ๑๒๕. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน ควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ๑๒๖. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตูจดหมายอิเล็กทรอนิกส์

ข้อ๑๒๗. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ๑๒๘. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ๑๒๙. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ๑๓๐. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ๑๓๑. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือ ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ๑๓๒. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ๑๓๓. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ๑๓๔. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ๑๓๕. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากร ของหน่วยงานอื่นๆ

ข้อ๑๓๖. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความ

มั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ๑๓๗. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ๑๓๘. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ๑๓๙. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ๑๔๐. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดย เจ้าหน้าที่ของโรงพยาบาลเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม ป้องกันไวรัส

(๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ๑๔๑. การใช้รหัสผ่าน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

ข้อ๑๔๒. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

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

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ๑๔๓. การสำรองข้อมูลและการกู้คืน

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

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ๑๔๔. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้าม ผู้ใช้งาน คัดลอกโปรแกรมต่างๆ และนำไป ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๖) หลีกเสี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ๑๔๕. ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนสูง ความชื้น ฝุนละออง และต้องระวังป้องกันการตกกระทบ

ข้อ๑๔๖. การควบคุมการเข้าถึงระบบปฏิบัติการ

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

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีและรัดกุม

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ต้องใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ๑๔๗. การใช้รหัสผ่านให้ผู้ใช้งาน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓- ๖ เดือน

ข้อ๑๔๘. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา และสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืน อย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสีย จะไม่กระทบต่อการ ดำเนินการของหน่วยงาน

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

ข้อ๑๔๙. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคง ปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาท และความรับผิดชอบที่เกี่ยวข้อง

ข้อ๑๕๐. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ต ทุกเส้นทาง

ข้อ๑๕๑. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ๑๕๒. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ๑๕๓. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ๑๕๔. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ๑๕๕. ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ๑๕๖. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่าย ของระบบสารสนเทศตามปกติ

ข้อ๑๕๗. เครื่องแม่ข่ายที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ๑๕๘. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมี การรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ

ข้อ๑๕๙. พฤติกรรม กิจกรรมที่น่าสงสัยหรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการ รายงานให้หัวหน้าหน่วยงานทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ๑๖๐. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ๑๖๑. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้าย ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ๑๖๒. หน่วยงานมสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยง ต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ๑๖๓. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบ สารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมาย

ว่าด้วยการ กระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความ เสียหาย ต่อข้อมูลและทรัพยากร ระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ๑๖๔. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

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

(๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบ ระบบการสแกนและปรับปรุงโปรแกรม

ข้อ๑๖๕. การบริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

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

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ๑๖๖. การปรับปรุงการรักษาความปลอดภัย/Anti-Virus (System Security & Anti-virus Update)

(๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

(๒) ประสิทธิภาพของระบบ (Performance) หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง /กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

(๔) ปรับปรุง โปรแกรม Anti-virus และ Definition ให้ทันสมัยเป็นประจำ ทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อ๑๖๗. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล(Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูลตามความต้องการของระบบงานที่หน่วยงานใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

(๓) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล(Database Admin) ชื่อผู้ใช้งานอื่น และสิทธิการใช้

(๔) ปรับปรุง /กำหนดค่าระบบให้ เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

ข้อ๑๖๘. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ/ กำหนดค่าระบบของโปรแกรม กำหนดผู้ใช้ และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตาม ระบบงานนั้นกำหนด

(๔) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิการเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง สำเนา ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มี การสร้างหรือปรับปรุง

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ๑๖๙. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริงระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้น ความลับในการเข้าถึง

ข้อ๑๗๐. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ๑๗๑. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำ ความผิด เกี่ยวกับ คอมพิวเตอร์

ข้อ๑๗๒. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ๑. กำหนดสิทธิและความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูลการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

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

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหารเช่นข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ เช่น ข้อมูลดัชนีเศรษฐกิจการค้า ข้อมูลการค้าระหว่างประเทศของไทย ข้อมูลเศรษฐกิจการค้าจังหวัด เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมากหมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ๒. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิเข้าใช้ หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับ ทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ๑๒

ข้อ๔. หน่วยงานเจ้าของฐานข้อมูลผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติ ของผู้ใช้งาน และโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มี แฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการหรือแลกเปลี่ยน หรือขอใช้ข้อมูลจาก

ส่วนราชการ ให้จัดทำข้อตกลงการใช้ข้อมูลหรือสำหรับการแลกเปลี่ยนสารสนเทศ ระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึก ข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูลเช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือ ซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูลซอฟต์แวร์ หรืออื่นๆที่มีความสำคัญเช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ๖. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้ งานโดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ๗. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ๘. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนด ระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ๙. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อย กำหนดให้มีความถี่ ในการสำรอง ข้อมูลมากขึ้น โดยให้มีวิธีการสำรอง ข้อมูลดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูลได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่ สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบค่าคอนฟิกกูเรชัน (Configuration) ต่างๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง

กับหน่วยงาน ต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่ จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถ เข้าถึงข้อมูลได้ ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้ สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของ ขั้นตอนปฏิบัติในการ กู้คืนข้อมูล อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ๑๐. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ น้ำท่วม แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ทเกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ๑๒. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์

ข้อ๑๓. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ๑๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอ ต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคง ปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ๑. จัดลำดับความสำคัญของความเสี่ยง

ข้อ๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบ สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บ ป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยใน ระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่ หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงาน และอาจส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศ ได้อย่างเต็มประสิทธิภาพ จึงได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหา ความเสี่ยง ที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑.๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการ เครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๑.๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm),ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวน การทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขึ้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๒.๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการ กำหนดสิทธิการเข้าใช้ งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกัน การบุกรุกจากภายนอก

(๒.๒) ติดตั้งซอฟต์แวร์ Anti-virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ ระบบเทคโนโลยีสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๓.๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแส ไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๓.๒) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้อง หรือมีควันไฟ เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าว จะส่งสัญญาณแจ้งเตือนที่หน่วยรักษา ความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของ อุปกรณ์อย่างสม่ำเสมอ

(๓.๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (อัคคีภัย) โดยมีการตรวจสอบความพร้อมของ อุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม(อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรง ที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของ กรมอุตุนิยมวิทยาตลอดเวลา

(๒) นำอุปกรณ์ Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดตัวตัดไฟเครื่องปรับอากาศ เพื่อป้องกัน เครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอรแม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบ ระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศข้อมูลซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยี สารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของ บุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณีดังกล่าว

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บงบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อคหรือใสกุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออก มาจากบริเวณ

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกลาวเป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ดังนี้

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้ รับอนุญาต รวมทั้ง ป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจแบ่ง ออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงาน

ของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่ จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ๔. การควบคุมการเข้าออกอาคารสถานที่

(๑) กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการ ผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความ ปลอดภัย จะต้องให้มีการแลกบัตร ที่ใช้ระบุตัวตน ของบุคคลนั้นๆ เช่น บัตร ประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้ว ทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอร์มการเข้าออกพร้อม กับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลา การทำงาน

(๖) จัดเก็บบันทึกการเข้า- ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องคอมพิวเตอร์แม่ข่าย (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนด ต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูดการใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า- ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (ห้องคอมพิวเตอร์แม่ข่าย Server Room, Data Center)

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกใน ขณะที่ปฏิบัติงานในพื้นที่ หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่าง น้อยปีละ ๑ ครั้ง

ข้อ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลว ในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้อง เครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่ มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวน ของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณ ผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานเส้นใยแก้วนำแสงแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณ โดยผู้ไม่ประสงค์ดี

ข้อ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและ ปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและ ตรวจสอบการชำรุดเสียหายของอุปกรณ์

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือ ทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญใน อุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มี การเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ๑. ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ๒. ระบบไฟร์วอลล์

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลฯ ไปยังภายนอกหรือไม่

(๒) ศึกษาแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่า กระจายอยู่ในเครือข่ายโรงพยาบาล

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

หมวดที่ ๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของโรงพยาบาล

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอโดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ๓. จัดสัมมนาเพื่อเผยแพร่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงาน ปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจาก ภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ๔. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความ ต้องการของผู้ใช้งาน

ข้อ๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความ เข้าใจ และสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่า ต้องดำเนินการอย่างไร

ข้อ๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตาม นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้ง กฎระเบียบของโรงพยาบาลฯ และข้อตกลงระหว่างประเทศอย่างเคร่งครัดทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือ ว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งาน จะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับผู้อำนวยการ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติงาน

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆแกองค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความ บกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่ม/หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้ากลุ่ม

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติงาน ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการ โรงพยาบาล เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่อง คอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) ทำการสำรองข้อมูลและเรียกค้นข้อมูล(Backup and Recovery) ตามรอบระยะเวลา ที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูล จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศของโรงพยาบาล

ภาคผนวก

การจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ๑. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๑.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ๔

๑.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ๔-๑๔

ข้อ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๒.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถ เข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาล

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๒.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ๓. มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ(access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูลลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ๔. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) อย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทำข้อปฏิบัติสำหรับการควบคุมการเข้าถึงสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ หลักการ “ตามความจำเป็นที่ต้องรู้”

ข้อ๕. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบ ที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เทาไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุม และจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ๖. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน ในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk And Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสทธิ และต้องกำหนดให้ ผู้ใช้งาน ออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบ การรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ๗. มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียง

บริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication For External Connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของ หน่วยงานได้
(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification เท Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่าย เป็นการยืนยัน
(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย
(๕) การแบ่งแยกเครือข่าย (Segregation In Networks) ต้องทำการแบ่งแยกเครือข่าย ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง
(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือ ไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกบแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

แผนรองรับสถานการณ์ฉุกเฉิน

๑. กรณีการแพร่กระจายของไวรัสคอมพิวเตอร์

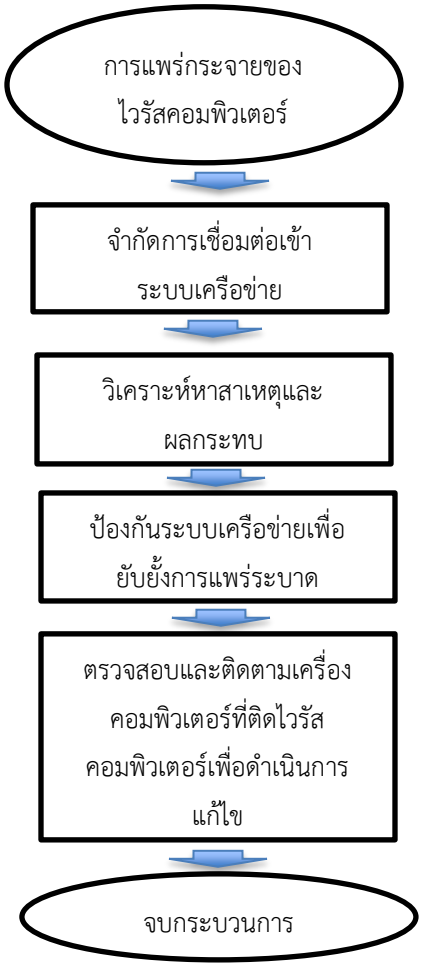
๑) เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องคอมพิวเตอร์ลูกข่ายอื่น ๆ ในระบบเครือข่าย เป็นการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

๒) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสคอมพิวเตอร์ที่ระบาด

๓) ดำเนินการป้องกันระบบเครือข่ายคอมพิวเตอร์เพื่อหยุดยั้งการระบาดของไวรัสคอมพิวเตอร์

๔) ตรวจสอบและติดตามเครื่องคอมพิวเตอร์ที่ติดไวรัสคอมพิวเตอร์เพื่อดำเนินการแก้ไข

๕) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้ผู้ประสบปัญหาแจ้งเหตุให้เจ้าหน้าที่งานข้อมูลและสารสนเทศหรือกรณีมีเหตุอื่นทำให้งานข้อมูลและสารสนเทศไม่สามารถ ดำเนินการให้บริการด้านเครือข่ายได้กลุ่มเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกกลุ่มงาน ในหน่วยงานทราบ



ผู้รับผิดชอบ
ได้แก่ เจ้าหน้าทกลุ่มเทคโนโลยี
สารสนเทศ/เจ้าหน้าที่ที่ได้รับ
มอบหมายให้ปฏิบัติงานด้าน IT ของ
แต่ละกลุ่มงาน

๒. กรณีมีการบุกรุกระบบ (Hack)

๑) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องตัดการเชื่อมต่อระบบเครือข่ายของเครื่องนั้น ๆ ก่อน เพื่อหยุดยั้ง การทำลายหรือขโมยข้อมูลที่มากขึ้น

๒) เจ้าหน้าที่ CIRT แจ้งผู้บริหารเทคโนโลยีสารสนเทศให้ทราบโดยด่วน

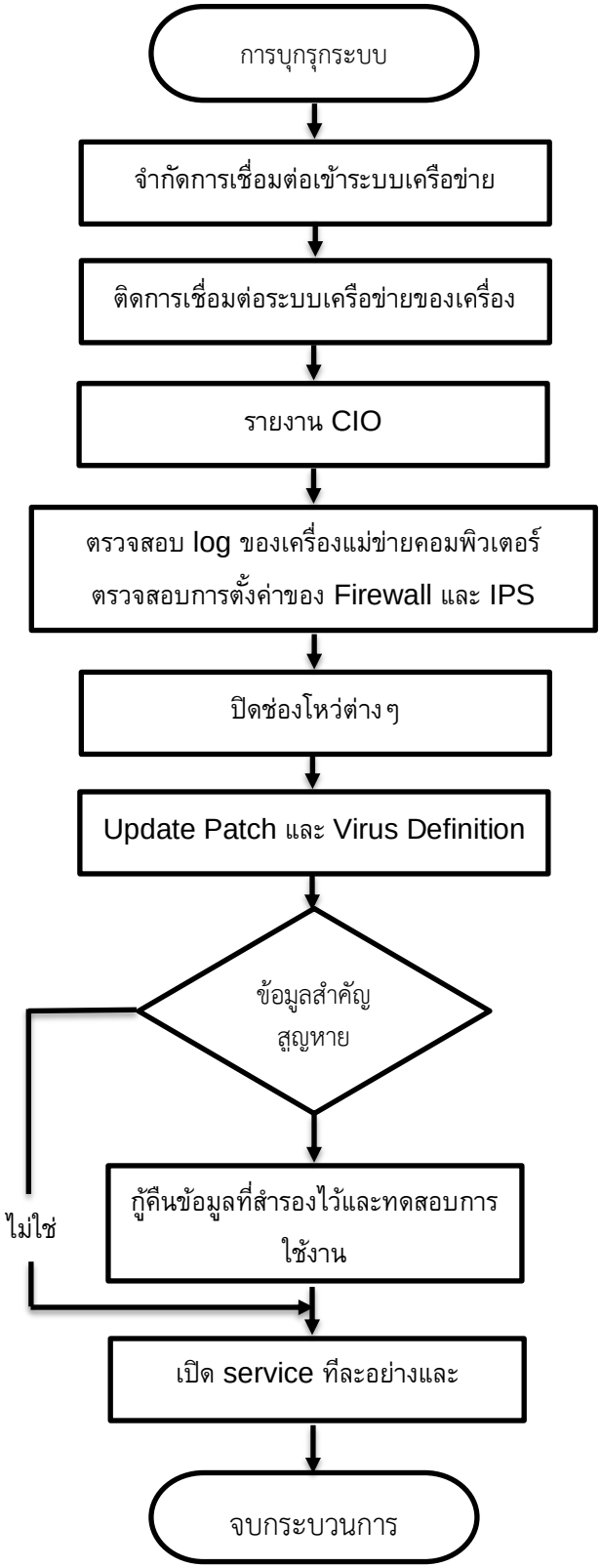
๓) วิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log ของเครื่องแม่ข่ายคอมพิวเตอร์และตรวจสอบการตั้งค่าของFirewall และ IPS

๔) ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

๕) Update Patch ต่าง ๆ ของเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์ให้เป็นปัจจุบัน ตรวจสอบการทำงานของโปรแกรม Antivirus ที่ติดตั้งในเครื่องแม่ข่ายคอมพิวเตอร์ และ Update Virus Definitions ให้เป็นปัจจุบัน

๖) กรณีที่ข้อมูลสำคัญสูญหายให้ทำการกู้คืนระบบ (Recovery) ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้อง และทดสอบการใช้งาน

๗) เมื่อดำเนินการขั้นตอนต่างๆ เรียบร้อยแล้ว ให้เปิด Service ของระบบทีละ Service เพื่อตรวจสอบ ผลการแก้ไข และเปิด Service เฉพาะเท่าที่จำเป็นของเครื่องแม่ข่ายคอมพิวเตอร์แต่ละเครื่อง



ผู้รับผิดชอบ

ได้แก่ เจ้าหน้าทกลุ่มเทคโนโลยีสารสนเทศ/เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละกลุ่มงาน

๓. กรณีการเชื่อมโยงเครือข่ายล้มเหลว

๑) ดำเนินการวิเคราะห์หาจุดเกิดปัญหา

๒) หากสายเคเบิ้ลขาดให้รีบติดต่อเจ้าหน้าที่บริษัทที่ให้บริการระบบเครือข่าย เพื่อดำเนินการซ่อมแซม สายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

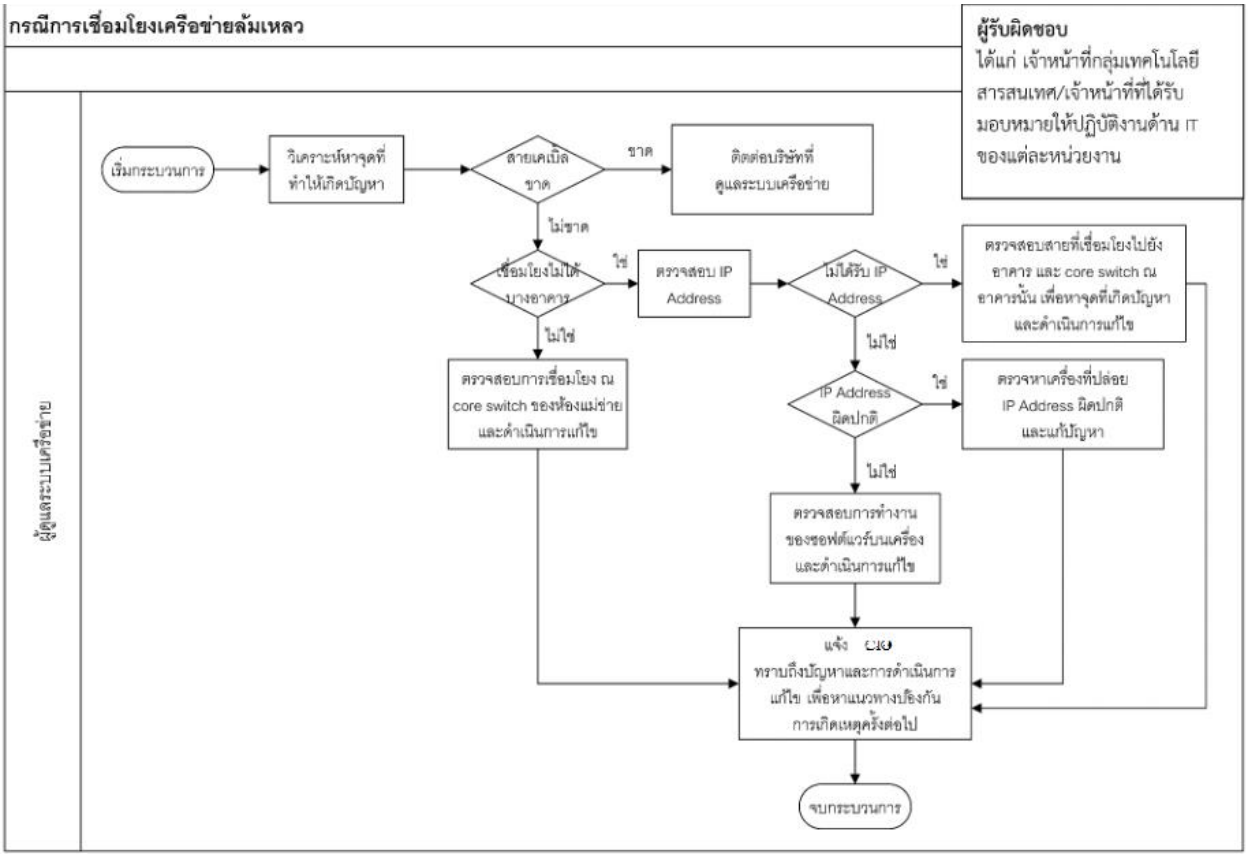
๓) หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคารให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

๔) ตรวจสอบอุปกรณ์เครือข่าย(Ethernet Switch) ณ จุดที่การเชื่อมโยงเครือข่ายล้มเหลว ว่าชำรุดหรือไม่ เพื่อดำเนินการแก้ไข

๕) ตรวจสอบเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการระบบอินเตอร์เน็ต เพื่อตรวจดูว่าชำรุดหรือไม่ เพื่อ ดำเนินการแก้ไข

๖) ตรวจสอบการให้บริการของเครื่องแม่ข่ายคอมพิวเตอร์ว่าสามารถให้บริการเป็นปกติหรือไม่ เพื่อดำเนินการแก้ไข

๗) ติดต่อผู้ให้บริการบำรุงรักษาและซ่อมแซมระบบคอมพิวเตอร์เพื่อแจ้งอาการชำรุดและดำเนินการซ่อมแซมอุปกรณ์ที่ชำรุด

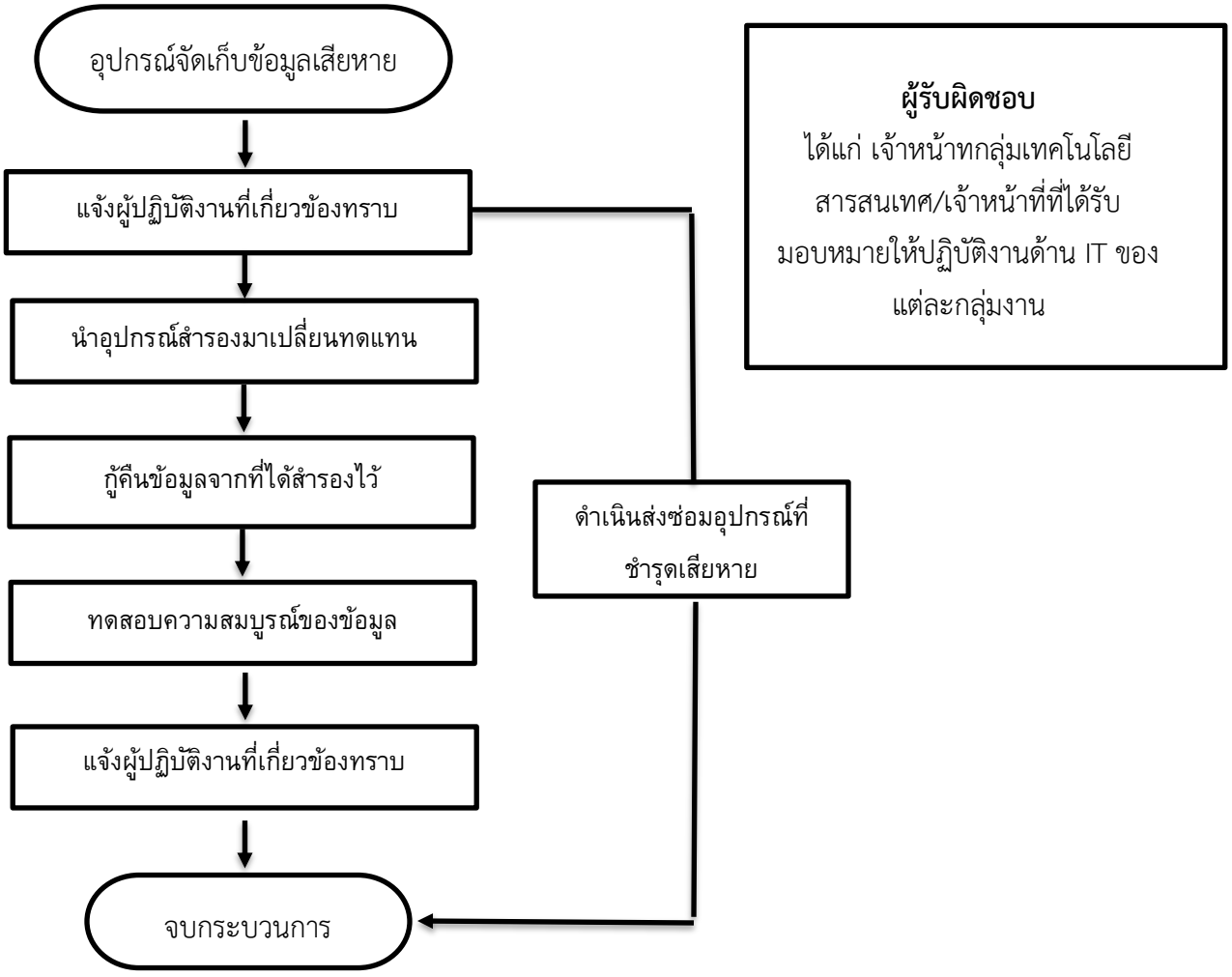

กรณีการเชื่อมโยงเครือข่ายล้มเหลว
ผู้รับผิดชอบ
ได้แก่ เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ/เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน
ผู้ดูแลระบบเครือข่าย
เริ่มกระบวนการ
วิเคราะห์หาจุดที่ทำให้เกิดปัญหา
สายเคเบิลขาด
ขาด
ติดต่อบริษัทที่ดูแลระบบเครือข่าย
ไม่ขาด
เชื่อมโยงไม่ได้บางอาคาร
ใช่
ตรวจสอบ IP Address
ไม่ได้รับ IP Address
ใช่
ตรวจสอบสายที่เชื่อมโยงไปยังอาคาร และ core switch ณ อาคารนั้น เพื่อหาจุดที่เกิดปัญหาและดำเนินการแก้ไข
ไม่ใช่
ตรวจสอบการเชื่อมโยง ณ core switch ของห้องแม่ข่าย และดำเนินการแก้ไข
IP Address ผิดปกติ
ใช่
ตรวจหาเครื่องที่ปล่อย IP Address ผิดปกติ และแก้ปัญหา
ไม่ใช่
ตรวจสอบการทำงานของซอฟต์แวร์บนเครื่อง และดำเนินการแก้ไข
แจ้ง CIO ทราบถึงปัญหาและการดำเนินการแก้ไข เพื่อหาแนวทางป้องกันการเกิดเหตุครั้งต่อไป
จบกระบวนการ

๔. กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

๑) แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

๒) รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว

๓) ทดสอบความสมบูรณ์ของข้อมูลและแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ



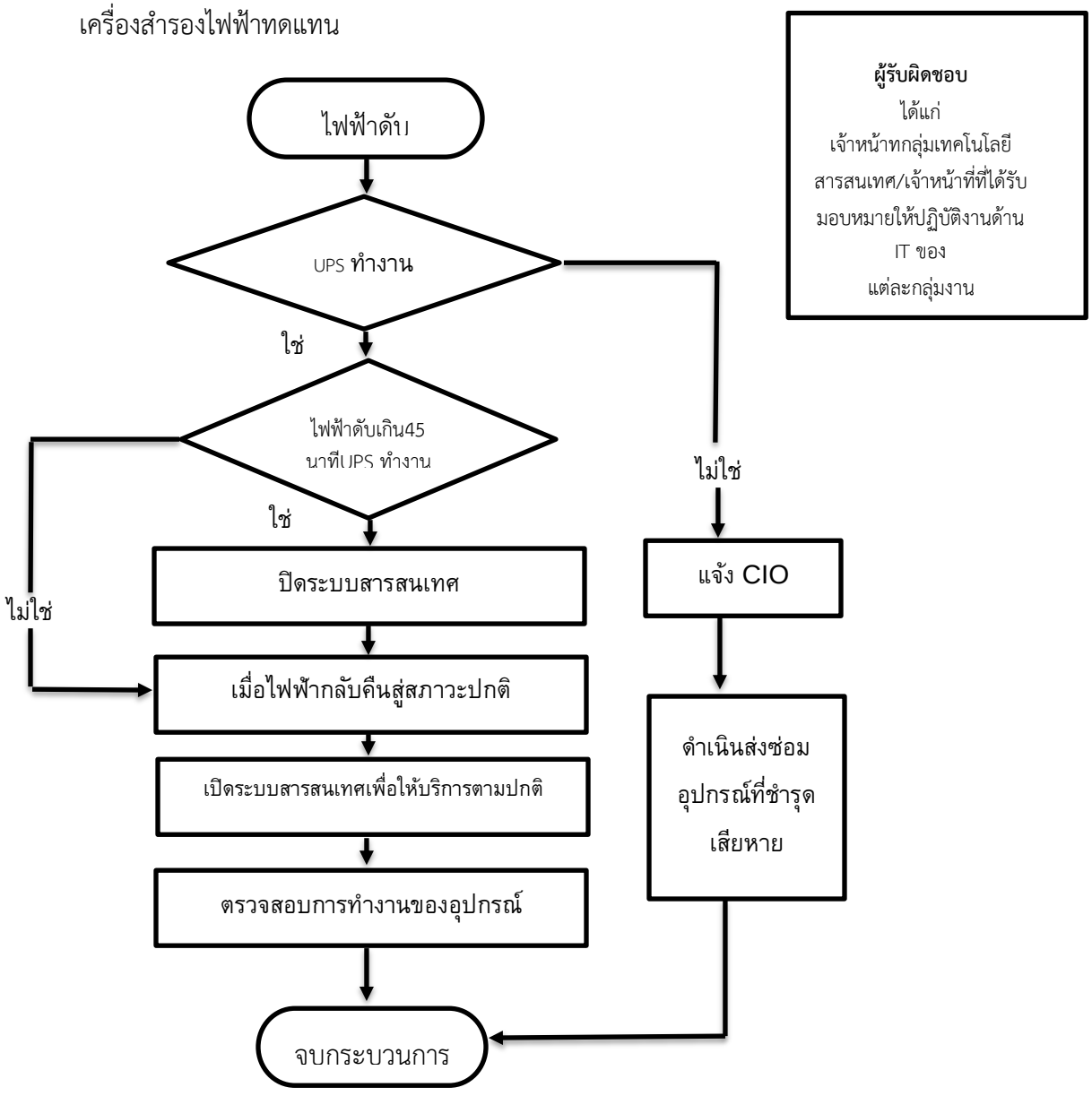
๕. กรณีไฟฟ้าขัดข้อง

๑) ระบบฐานข้อมูลและสารสนเทศ ณ ห้องแม่ข่ายคอมพิวเตอร์ของหน่วยงานสามารถ สำรองกระแสไฟฟ้าได้ไม่น้อยกว่า ๑ ชั่วโมง

๒) หากใกล้ครบ ๑ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติให้มีการแจ้งเตือนไปยังผู้บริหารเทคโนโลยีสารสนเทศ

๓) ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย

๔) หากเครื่องสำรองไฟฟ้ามีปัญหาแจ้งผู้บังคับบัญชาเพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน



๖. กรณีไฟไหม้

๑) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอก ตัวอาคารให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

๒) หากไม่สามารถควบคุมไฟได้ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคารผู้ติดต่อประสานงานโทรแจ้งผู้รับผิดชอบอาคารสถานที่และยานพาหนะทันทีและโทรแจ้งสถานีดับเพลิง

๓) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วไม่มีปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการ จัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้และออกแบบติดตั้งระบบ ตรวจจับไฟ และดับไฟอัตโนมัติ

๔) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง