ระเบียบปฏิบัติสำหรับการนำฝากเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนภายใน
ห้องศูนย์ข้อมูล Data Center โรงพยาบาลพระมงกุฎเกล้า

ในปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ห้องศูนย์ข้อมูล(DataCenter) ของโรงพยาบาล มีมาตรฐานด้านการดูแลระบบเครือข่ายและการใช้งานระบบสารสนเทศของโรงพยาบาล ที่มีความปลอดภัยสามารถรองรับการให้บริการแก่ผู้ป่วยอย่างต่อเนื่องและสร้างความเชื่อมั่นให้แก่ผู้บริหาร ระดับสูงสายบังคับบัญชา,แพทย์,พยาบาล,นักศึกษาแพทย์และบุคลากรทางการแพทย์ที่เกี่ยวข้อง ศูนย์คอมพิวเตอร์กอ.รพ.รร.๖ จึงได้ออกระเบียบข้อปฏิบัติ โดยมีรายละเอียดดังนี้

๑. วัตถุประสงค์

๑) เพื่อกำหนดแนวทางปฏิบัติ ให้สำหรับผู้ปฏิบัติงานศูนย์คอมพิวเตอร์กอ.รพ.รร.๖,หน่วยงานภายใน และหน่วยงานภายนอก รวมไปถึงเป็นการสร้างมาตรฐานการบริหารจัดการสำหรับเครื่องแม่ข่ายและ เครื่องแม่ข่ายเสมือนที่นำมาฝากในห้องศูนย์ข้อมูล(Data Center) ของโรงพยาบาลให้เกิดความปลอดภัย ทั้งต่อระบบเครือข่ายภายในโรงพยาบาลและระบบสารสนเทศของโรงพยาบาล (HIS)

๒) เพื่อสนับสนุนการใช้เทคโนโลยีร่วมกับระบบสารสนเทศของโรงพยาบาลตามวัตถุประสงค์ของ หน่วยงานนั้นๆที่ต้องการเชื่อมต่อระบบเครือข่ายของโรงพยาบาลเข้ากับอุปกรณ์อื่นๆกับระบบเครือข่ายภายนอก โรงพยาบาล เพื่อใช้ในการรักษาพยาบาลผู้ป่วย ซึ่งตามนโยบายของโรงพยาบาลอัจฉริยะ(Smart Hospital) ที่มุ่งเน้นการรักษาพยาบาลที่ทันสมัย สามารถรองรับนวัตกรรมปัญญาประดิษฐ์(AI)และการวินิจฉัยโรคต่างๆ ได้อย่างแม่นยำเพื่อสำหรับการศึกษาวิจัยทางการแพทย์ในสาขาต่างๆ

๓) เพื่อการดูแลข้อมูลสารสนเทศของโรงพยาบาลมีความปลอดภัย เชื่อถือได้ ทาง ศูนย์คอมพิวเตอร์ฯ จึงได้ปฏิบัติตามกฎหมายว่าด้วยการปกป้องข้อมูล คุ้มครองข้อมูล และคุ้มครองความเป็นส่วนตัวของข้อมูลผู้ป่วย ที่อยู่ภายในระบบเครือข่ายและเครื่องแม่ข่ายที่นำฝากทุกชนิด โดยหน่วยงานที่รับผิดชอบหรือหน่วยงานภายนอก ที่นำฝากจะต้องปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เป็นลำดับความสำคัญ ดังนี้

(๑) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และหลักเกณฑ์ของสำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส./PDPC)

(๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (สกมช.)

(๓) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

(๔) นโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลพระมงกุฎเกล้าและมาตรฐาน ที่เกี่ยวข้องกับการรับรองคุณภาพโรงพยาบาล (เช่น HAIT PLUS)

(๕) กรณีมีการโอนข้อมูลไปยังต่างประเทศหรือเกี่ยวข้องกับนิติบุคคลในสหภาพยุโรปอาจใช้อ้างอิง GDPR เป็นมาตรฐานเสริมตามความจำเป็น

ซึ่งในการดำเนินกิจกรรมตามระเบียบนี้จะอยู่ภายใต้การกำกับ ควบคุม ดูแล ของศูนย์คอมพิวเตอร์ฯและ การพิจารณาของคณะกรรมการสารสนเทศโรงพยาบาลพระมงกุฎเกล้า

๒. ขอบเขต

๒.๑ การขอเชื่อมต่อระบบเครือข่าย ทางหน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องแสดงแผนผังFlow Chart การเชื่อมต่อระหว่างระบบเครือข่ายภายนอกกับระบบเครือข่ายของโรงพยาบาลที่แยกกันให้เห็นอย่างชัดเจน ซึ่งในการจัดสรรช่องทางการเชื่อมต่อเข้ามายังระบบส่วนกลางได้นั้นจะต้องถูกควบคุมเฉพาะช่องทางที่ศูนย์คอมพิวเตอร์ฯกำหนดไว้เช่นNetwork VLAN, Firewall Zone,VPN เท่านั้น และไม่ให้เข้าสู่ระบบด้วยช่องอื่นที่นอกเหนือจากทาง ศูนย์คอมพิวเตอร์ฯ กำหนดไว้โดยเด็ดขาด

๒.๒ การปรนนิบัติบำรุงรักษา หน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องดูแลบำรุงรักษาในส่วนของฮาร์ดแวร์และซอฟต์แวร์ให้เป็นเวอร์ชันปัจจุบัน พร้อมรายงานผลการบำรุงรักษาประจำปี ในรูปแบบเอกสารให้กับทาง ศูนย์คอมพิวเตอร์ฯ ทราบเพื่อเป็นข้อมูลการใช้บริการของหน่วยงานที่นำฝากภายในห้องศูนย์ข้อมูล (Data Center)
อีกด้วย

๒.๓ การดูแลรักษาระบบสารสนเทศของโรงพยาบาล ทางหน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องคอยหมั่นตรวจสอบโปแกรมที่ใช้งานอยู่เสมอ พร้อมติดตั้งอุปกรณ์ป้องกัน(Firewall)และติดตั้งโปรแกรมสแกนAntivirus(หากเป็นระบบปฏิบัติการwindows) ให้เรียบร้อย

๒.๔ ขั้นตอนนำฝากเครื่องแม่ข่าย ทางหน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน สามารถดาวน์โหลดแบบฟอร์มได้ที่หน้าเว็บไซต์https://cc.pm.ac.th ของศูนย์คอมพิวเตอร์ฯได้แก่ แบบฟอร์ม"การขอใช้บริการฝากเซิร์ฟเวอร์และการบำรุงรักษาเซิร์ฟเวอร์" และแบบฟอร์ม"การฝากทรัพย์สินภายในห้องศูนย์ข้อมูล(DataCenter)"โดยทางหน่วยงานจะต้องจัดส่งเอกสารพร้อมรายละเอียดภายใน ๑ สัปดาห์ก่อนวันติดตั้ง

๓. หลักการปฏิบัติตามกฎหมาย

๓.๑ การคุ้มครองข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล หน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องมีมาตรการป้องกันการนำเข้า–ส่งออก ประมวลผล จัดเก็บ และเข้าถึงข้อมูลผู้ป่วย(ข้อมูลสุขภาพ /PHI)และข้อมูลส่วนบุคคลตาม PDPAโดยจัดทำข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement: DPA) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และในกรณีที่จำเป็นอาจจัดทำข้อตกลงที่เทียบเท่า Business Associate Agreement(BAA)ตามมาตรฐานสากล เพิ่มเติมต้องยืนยันว่าเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน และ Application ที่เกี่ยวข้องปฏิบัติตามกฎหมายดังกล่าว ห้ามเก็บหรือส่งออกข้อมูลผู้ป่วยออกนอกพื้นที่ที่ได้รับอนุญาตโดยไม่ผ่านการพิจารณาของ DPO/คณะกรรมการPDPA ของโรงพยาบาล

๓.๒ ความมั่นคงปลอดภัยไซเบอร์ หน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องปฏิบัติตามพรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๒ (สกมช.) และระเบียบข้อกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด เพื่อให้การใช้งานระบบเครือข่ายบนเครื่องแม่ข่ายที่นำฝากมีความปลอดภัยอยู่เสมอ

๓.๓ นโยบายความมั่นคงปลอดภัยสารสนเทศและการตรวจสอบ (Audit) หน่วยงานภายในและหน่วยงานภายนอกที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน จะต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลหรือปฏิบัติตามมาตรฐานISO2071(ระบบการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ) ข้อใดข้อหนึ่งทางโรงพยาบาลขอสงวนสิทธิ์ตรวจสอบ (Audit) Server ของหน่วยงานภายนอกที่นำฝาก เพื่อประเมินความเสี่ยงที่อาจกระทบระบบสารสนเทศหากมีการตรวจพบความผิดปกติ ทาง ศูนย์คอมพิวเตอร์ฯ สามารถดำเนินการระงับยับยั้งการเชื่อมต่อได้โดยไม่ต้องแจ้งล่วงหน้า

๔.หลักเกณฑ์และแนวทางปฏิบัติ

๔.๑ การพิจารณาอนุมัติ

๔.๑.๑ เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝาก จะต้องเป็นเครื่องแม่ข่ายที่ผ่านการอนุมัติขึ้นบัญชีคุมกับทางโรงพยาบาลโดยลงนามมาจากผู้อำนวยการของโรงพยาบาลเรียบร้อยแล้ว(เอกสารแนบประกอบเช่น ชื่อโครงการ,ประเภทงานจ้าง,เอกสารขึ้นบัญชีคุม เป็นต้น) และผ่านการพิจารณาจากทางคณะกรรมการสารสนเทศโรงพยาบาลก่อนการติดตั้งทุกครั้ง

๔.๑.๒ เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝาก จะต้องได้รับการอนุมัติตาม “แบบฟอร์มการขอใช้บริการนำฝากเซิร์ฟเวอร์และการบำรุงรักษาเซิร์ฟเวอร์” โดยยื่นคำร้องขอก่อนเข้าพื้นที่และติดตั้งอุปกรณ์อย่างน้อย ๑ สัปดาห์ เพื่อให้หัวหน้าศูนย์คอมพิวเตอร์ฯ พิจารณาและแจ้งกำหนดวันเวลาในการเข้าดำเนินการให้เจ้าหน้าที่ศูนย์คอมพิวเตอร์ฯทราบ

๔.๑.๓เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝากจะต้องผ่านการตั้งค่าซอฟต์แวร์และระบบเครือข่ายตามหลัก (Confidentiality, Integrity, Availability-CIA Triad) ให้มีความปลอดภัยอยู่เสมอเพื่อไม่ให้เกิดส่งผลกระทบต่อระบบเครือข่ายภายในและระบบงานของโรงพยาบาล (HIS)

๔.๒ การเชื่อมต่อและโครงสร้างเครือข่าย

๔.๒.๑ การเชื่อมต่อเข้ากับฐานข้อมูลของโรงพยาบาล: เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝากจะต้องได้รับการอนุมัติจากหัวหน้าศูนย์คอมพิวเตอร์ฯเรียบร้อยแล้ว หรือเว้นแต่API Gatewayเท่านั้น

๔.๒.๒ การเข้าระบบเครือข่ายภายในของโรงพยาบาล: เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝากจะต้องได้รับอนุญาตในการเปิดPortเฉพาะที่ใช้งาน และได้หมายเลขประจำเครื่องแม่ข่าย IP addressเฉพาะเท่านั้น และทางหน่วยงานไม่สามารถกำหนดชุด IP address ขึ้นเองได้

๔.๒.๓ **การเชื่อมต่อเข้ากับระบบงานโรงพยาบาล:** เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝาก **จะต้องอธิบายวิธีการทำงานของระบบเครือข่ายจากภายนอกเข้ามายังระบบเครือข่ายภายในโดยต้อง** แยกให้ชัดเจน พร้อมแผนการบริหารจัดการข้อมูลผู้ป่วยภายในระบบงานโรงพยาบาล (HIS) หรือการเชื่อมต่อเครือข่ายอินเตอร์เน็ตของโรงพยาบาลที่ปลอดภัยและติดตั้ง Firewall หรือVLAN ตามที่ทาง ศูนย์คอมพิวเตอร์ฯ กำหนดไว้

๔.๒.๔ **การจัดเก็บข้อมูลการทำงานของระบบเครือข่าย(Network Logging):** เครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนที่นำฝาก **จะต้องตรวจสอบสถานะการทำงานของระบบภายในเครื่องแม่ข่ายอยู่เสมอและรายงานผลในห้วง ๓-๖ เดือน ให้กับ ทาง ศูนย์คอมพิวเตอร์ฯสามารถตรวจสอบข้อมูลย้อนหลังทราบ**

๔.๓ มาตรการด้านความปลอดภัยของข้อมูล

๔.๓.๑ หน่วยงานที่รับผิดชอบ จะต้องจัดทำข้อตกลงการรักษาความลับข้อมูลของโรงพยาบาล(NDA) และข้อตกลงความลับการประมวลผลข้อมูลของโรงพยาบาล (DPA)เป็นลายลักอักษรให้กับทางผู้อำนวยการโรงพยาบาลอนุมัติและรับทราบทุกครั้ง

๔.๓.๒ หน่วยงานที่รับผิดชอบ **จะต้องเก็บบันทึกข้อมูลการทำงานของเครื่องแม่ข่าย(Log Server) และสามารถเข้าถึงAccess Log / Audit Trail ได้ไม่น้อยกว่า ๙๐ วัน**

๔.๓.๓ หน่วยงานที่รับผิดชอบ **จะต้องตรวจสอบสถานะการทำงานเครื่องแม่ข่ายโดยให้ทำการอัพเดตซอฟต์แวร์เป็นปัจจุบันและอุปกรณ์ทุกชิ้นควรมีการสำรองข้อมูล(Backup) ของผู้ป่วยให้เป็นปัจจุบันได้มากที่สุดหรือจัดเก็บข้อมูลทุกๆ๖ เดือนเพื่อป้องกันข้อมูลสูญหายหรือหากเครื่องแม่ข่ายเสียหาย**

๔.๓.๔ หน่วยงานที่รับผิดชอบ ที่ต้องการควบคุมจากระยะไกล(Remote Access) ซึ่งทางศูนย์คอมพิวเตอร์ฯ จะเป็นผู้จัดสรรหมายเลขประจำเครื่อง IP Address สำหรับการRemote Access เข้ามาภายในระบบเครือข่ายของโรงพยาบาล ขอให้ทางหน่วยงานใช้ในช่องทางที่มีความปลอดภัยสูงสุด เช่น VPN ร่วมกับการยืนยันตัวตนหลายปัจจัย (MFA/2FA) และให้สิทธิในการเข้าถึงเฉพาะชั้นข้อมูลที่จำเป็นเท่านั้นเพื่อความสะดวกในการบริหารจัดการและสามารถตรวจสอบย้อนหลังได้ของผู้ดูแลระบบเครือข่ายโรงพยาบาล

๔.๓.๕ หน่วยงานที่รับผิดชอบ จะต้องแสดง**แผนการรับมือภัยพิบัติประเภทต่างๆ เช่น ภัยจากธรรมชาติ ,ภัยจากทางไซเบอร์ ,การถูกโจมตีจากเครือข่ายภายนอก**,การเรียกค่าไถ่ข้อมูลทางไซเบอร์ และการเจาะระบบเน็ทเวิร์ค เป็นต้น ในกรณีเกิด**ภัยคุกคามทางไซเบอร์หรือการโจมตีทางไซเบอร์**(Cyber Attack) ในรูปแบบต่างอาทิMalware,DDoS,Man-in-theMiddle(MitM),ZeroDay,InsiderThreat เป็นต้น หากทาง ศูนย์คอมพิวเตอร์ตรวจพบความผิดปกติสามารถเข้าดำเนินการปิดระบบจากเครื่องแม่ข่าย(ที่เป็นสาเหตุ)และทำการปิดกั้นการเชื่อมต่อจากทุกช่องทางบนเครือข่ายได้ทันที โดยไม่ต้องแจ้งให้ทราบล่วงหน้าหรือจนกว่าเจ้าของเครื่องแม่ข่ายจะดำเนินการแก้ไขให้ระบบมีความปลอดภัย จากนั้นจึงแจ้งให้หน่วยงานภายใน ที่เกี่ยวข้องทราบเมื่อสถานการณ์กลับเข้าสู่ภาวะปกติ

๔.๔ การบำรุงรักษาและเข้าถึงเครื่องแม่ข่าย

๔.๔.๑ หน่วยงานที่รับผิดชอบ ต้องแจ้งระบุวันและเวลาในการเข้าพื้นที่ห้องData Center ล่วงหน้าอย่างน้อย๑-๒วัน พร้อมเอกสารการขอเข้าพื้นที่ภายใน(ตามวันและเวลาราชการ) ให้กับเจ้าหน้าที่ศูนย์คอมพิวเตอร์ฯ ทราบทุกครั้ง

๔.๔.๒ หน่วยงานที่รับผิดชอบ ต้องแจ้งระบุวันและช่วงเวลาในการเข้ามาRemote Access จากภายนอก เพื่อให้ผู้ดูแลระบบทำการอนุญาตในการเข้าถึงเครื่องแม่ข่ายของทางหน่วยภายในโรงพยาบาลและใช้ช่องทางVPNตามหมายเลขที่ทาง ศูนย์คอมพิวเตอร์ฯ กำหนดไว้เท่านั้น

๔.๔.๓ หน่วยงานที่รับผิดชอบ ต้องแจ้งระบุวันและช่วงเวลาในการจัดทำ Maintenance Log Sheet และผู้ดำเนินการโดยออกเป็นหนังสือจากทางบริษัท หน่วยงานผู้รับผิดชอบ หรือเอกสารที่ทางราชการออกให้แจ้งมายังศูนย์คอมพิวเตอร์ฯก่อนวันดำเนินการ ๑วัน พร้อมทั้งส่งรายงาน (Report) ให้ศูนย์คอมพิวเตอร์ฯ ทราบอย่างน้อยปีละ ๑ ครั้ง

๔.๕ การจัดการเหตุการณ์ (Incident Response)

๔.๕.๑ หน่วยงานภายในและหน่วยงานภายนอกที่รับผิดชอบ ต้องรายงานสถานการณ์ทันทีเมื่อพบความผิดปกติ อาทิเช่นMalware,การรั่วไหลของข้อมูล, การเจาะผ่านช่องทางที่ไม่ปลอดภัยเข้ามาในระบบจากภายนอก เป็นต้น โดยรายงานให้ทางโรงพยาบาลทราบและดำเนินการประสานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์(NASC) ทราบทันที

๔.๕.๒ หน่วยงานภายในและหน่วยงานภายนอกที่รับผิดชอบ ต้องมีทีมผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์(S-CIRT) เพื่อเข้าดำเนินการแก้ไขกู้คืนระบบโดยไม่ให้เกิดผลกระทบต่อระบบงานอื่นๆของโรงพยาบาล พร้อมทั้งระบบจะต้องกลับมาใช้งานได้ตามปกติ ภายใน ๑ ชั่วโมงหลังแจ้งเหตุไป

๔.๕.๓ หน่วยงานภายในและหน่วยงานภายนอกที่รับผิดชอบ ต้องมีแผนบริหารจัดการIncident Response Plan ที่ชัดเจนเสนอให้ทาง ศูนย์คอมพิวเตอร์ฯ ทราบและต้องจัดสรรบุคลากรที่สำหรับการประสานงานเบื้องต้นไว้ให้กับทีมของโรงพยาบาลด้วยในครึ่งชั่วโมงหลังแจ้งเหตุ

๔.๖ การตรวจสอบและประเมินผล

๔.๖.๑ หน่วยงานภายในและหน่วยงานภายนอก ที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือนต้องยินยอมให้ผู้ดูแลระบบสารสนเทศสามารถเข้าตรวจสอบและประเมินผลการทำงานของเครื่องแม่ข่ายได้ในส่วนของการตรวจเช็คระบบปฏิบัติการ,โปรแกรมป้องกันความปลอดภัยของเครื่องแม่ข่าย หากการตรวจสอบและประเมินแล้วพบว่า ยังมีจุดไหนที่เป็นช่องโหว่หรือเสี่ยงต่อระบบเครือข่ายของโรงพยาบาล ทาง ศูนย์คอมพิวเตอร์ฯ จะรายงานกลับไปยังหน่วยงานที่รับผิดชอบเพื่อให้ดำเนินการแก้ไขปรับปรุงต่อไป ซึ่งนับตั้งแต่เข้าติดตั้งเครื่องภายในห้องเรียบร้อยแล้วถึงจะทำการประเมินทุกๆ ๖เดือน

๔.๖.๒ หน่วยงานภายในและหน่วยงานภายนอก ที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน ต้องยินยอมให้ผู้ดูแลระบบสารสนเทศตรวจสอบเกี่ยวกับด้านความปลอดภัยของระบบเครือข่าย หากทาง ศูนย์คอมพิวเตอร์ฯ ตรวจสอบและประเมินแล้วพบว่า ยังมีจุดไหนที่เป็นช่องโหว่หรือเสี่ยงต่อความเสียหายของระบบเครือข่ายของโรงพยาบาล ทาง ศูนย์คอมพิวเตอร์ฯ จะรายงานกลับไปยังหน่วยงานที่รับผิดชอบทราบ เพื่อให้ดำเนินการแก้ไขปรับปรุงต่อไป ซึ่งนับตั้งแต่คิดตั้งเครื่องภายในห้องเรียบร้อยแล้วถึงจะทำการประเมินทุกๆ ๖เดือน

๔.๖.๓ หน่วยงานภายในและหน่วยงานภายนอก ที่เป็นเจ้าของเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน ต้องยินยอมให้ผู้ดูแลระบบสารสนเทศตรวจสอบเกี่ยวกับแผนการรับมือเผชิญเหตุฉุกเฉิน(Incident) ของระบบเครือข่ายตามที่ทางหน่วยงานจัดทำไว้ หากทาง ศูนย์คอมพิวเตอร์ฯ ตรวจสอบและประเมินแล้วพบว่า ยังมีจุดไหนที่มีความเสี่ยงต่อระบบเครือข่ายของโรงพยาบาล ทาง ศูนย์คอมพิวเตอร์ฯ จะรายงานกลับไปยังหน่วยงานที่รับผิดชอบทราบเพื่อให้ดำเนินการแก้ไขปรับปรุงต่อไป ซึ่งนับตั้งแต่เข้าติดตั้งเครื่องภายในห้องเรียบร้อยแล้วถึงจะทำการประเมินรายปี

๔.๖.๔ ทาง ศูนย์คอมพิวเตอร์ฯ ได้กำหนดระดับผลกระทบความเสี่ยงของระบบสารสนเทศโรงพยาบาล แบ่งเป็น ๓ ระดับ

ระดับที่๑รุนแรงน้อย หมายถึง มีผลกระทบบางจุดบริการ ทำให้ระบบงานโรงพยาบาล ไม่สามารถใช้งาน**ได้ชั่วคราว** โดยใช้ระยะเวลาแก้ไข ภายใน ๐-๓๐นาที

ระดับที่๒รุนแรงปานกลาง หมายถึง มีผลกระทบหลายจุดบริการ ทำให้ระบบงานโรงพยาบาล ไม่สามารถใช้งาน**ได้เกินครึ่งชั่วโมง** โดยใช้ระยะเวลาแก้ไข ภายใน ๑-๒ชั่วโมง

ระดับที่๓รุนแรงมากที่สุด หมายถึง มีผลกระทบทุกจุดบริการ ทำให้ระบบงานโรงพยาบาล ไม่สามารถใช้งาน**ได้เกิน ๒๔ ชั่วโมง** โดยใช้ระยะเวลาแก้ไขนานกว่า ๒ชั่วโมงหรือใช้เวลากู้คืนมากกว่า๑วัน

๔.๗ การยุติการนำฝากเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน(Server)ของโรงพยาบาล

๔.๗.๑ หน่วยงานภายในและภายนอก ที่ต้องการขอต่ออายุนำฝากเครื่องแม่ข่าหรืออัพเดทสถานะของการนำฝากเครื่องและอุปกรณ์กับทางศูนย์คอมพิวเตอร์ ขอให้ทางหน่วยงานที่รับผิดชอบยื่นหนังสือมายังศูนย์คอมพิวเตอร์ฯ เพื่อพิจารณาภายใน ๓๐วัน นับจากวันที่ครบกำหนด

๔.๗.๒ หน่วยงานภายในและภายนอก ที่ต้องการถอนเครื่องแม่ข่ายออกหรือสิ้นสุดการนำฝาก ทางหน่วยงานที่รับผิดชอบจะต้องยื่นเอกสารแบบฟอร์มตามที่กำหนดไว้ โดยขอให้ระบุวัตถุประสงค์ เช่นการถอนเครื่อง/การขอเคลื่อนย้ายเรื่อง/การนำทรัพย์สินออกจากพื้นที่ เพื่อให้ทาง ศูนย์คอมพิวเตอร์ฯ พิจารณาตามหลักการและจะแจ้งผลการอนุมัติภายใน ๑๕ วัน นับตั้งแต่วันที่เอกสาร

๔.๗.๓ หน่วยงานภายในและภายนอก ที่ต้องการยกเลิกการใช้งานเครือข่ายร่วมกับระบบงานของโรงพยาบาล ขอให้ผู้ดูแลเครื่องแม่ข่ายดำเนินการลบข้อมูล เช่น หมายเลข IP ที่ใช้ในการเชื่อมต่อ, หมายเลขในการเข้าควบคุมจากระยะไกล(VPN),การลบบันทึกข้อมูลทางการแพทย์และการลบข้อมูลที่เป็นข้อมูลส่วนบุคคลของผู้ป่วยในโรงพยาบาลออกทั้งหมด เป็นต้น ตามมาตรฐานอย่างปลอดภัย (Secure Erasure) และเมื่อดำเนินการเรียบร้อยขอให้ ทางหน่วยผู้เป็นเจ้าของเครื่องแม่ข่ายแจ้งผลรายงานต่อผู้อำนวยการโรงพยาบาลรับทราบและจัดส่งเอกสารให้ทาง ศูนย์คอมพิวเตอร์ฯทราบ ภายใน ๓๐วัน

ระเบียบฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ ๕ สิงหาคม ๒๕๖๙ เป็นต้นไป

พ.อ.

(ธนกร เทียนศรี)

หน.ศูนย์คอมพิวเตอร์ กอ.รพ.รร.๖