บันทึกข้อความ

ส่วนราชการ งานเวชสารสนเทศ โรงพยาบาลบางสะพานน้อย . โทร. ๐๓๒-๖๙๙-๐๒๕ ต่อ ๒๒๕

ที่ .....**วันที่**.....

เรื่อง ขออนุมัติและประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลบางสะพานน้อย

เรียน ผู้อำนวยการ (ผ่านหัวหน้าฝ่ายบริหารงานทั่วไป)

ตามพระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้ง ป้องกันปัญหาที่อาจเกิดขึ้นจากาการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง

ดังนั้น งานเวชสารสนเทศโรงพยาบาลบางสะพานน้อยเป็นหน่วยงานที่อยู่ภายใต้การกำกับดูแลของกลุ่มงานบริหารงานทั่วไป ซึ่งรับผิดชอบดูแลด้านการให้บริการระบบสนเทศนั้น ได้ดำเนินการจัดทำ “นโยบายและแนวปฏิบัติการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบางสะพานน้อย” เพื่อให้การใช้งานระบบสารสนเทศของโรงพยาบาลบางสะพานน้อยมีความปลอดภัย และสอดคล้องตามหลักกฎหมาย จึงควรประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบางสะพานน้อย ควบคุมการดำเนินการใดๆ ที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลบางสะพานน้อย

จึงเรียนมาเพื่อโปรดพิจารณาประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบางสะพานน้อย จะเป็นพระคุณ

(นางระวิวรรณ หิรัญ)
ตำแหน่ง เจ้าพนักงานเวชสถิติชำนาญการ
หัวหน้างานเวชสารสนเทศ

(นางสาวนันทนา กำบัง)
ตำแหน่ง พยาบาลวิชาชีพชำนาญการ
ปฏิบัติงานแทนหัวหน้ากลุ่มงานบริหารทั่วไป

ประกาศโรงพยาบาลบางสะพานน้อย

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบางสะพานน้อย

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลบางสะพานน้อย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสารารถและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่าง ๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลบางสะพานน้อย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่นๆ ที่เกี่ยวข้องโรงพยาบาลบางสะพานน้อยจึงเห็นสมควร กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลบางสะพานน้อย ทำให้ดำเนินงานได้อย่างปลอดภัย และต่อเนื่อง

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลบางสะพานน้อยได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูและระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลบางสะพานน้อย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะมีการทบทวนนโยบายปีละ ๑ ครั้ง

อาศัยอำนาจตามในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โรงพยาบาลบางสะพานน้อย จึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบางสะพานน้อย ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลบางสะพานน้อย” เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ใช้ประกาศนี้แทน

ข้อ ๓ การรักษาความปลอดภัยด้านสารสนเทศของโรงพยาบาลบางสะพานน้อย กำหนดประเด็นสำคัญดังต่อไปนี้

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

- ๓.๑.๑ ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย
- ๓.๑.๒ นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาลราชวิถี
- ๓.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน
- ๓.๑.๔ กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง
- ๓.๑.๕ กำหนดให้ทบทวนและปรับปรุงนโยบายปีละ ๑ ครั้ง

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๓ ส่วน คือ

ส่วนที่ ๑ คำนิยามและคำจำกัดความ

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลบางสะพานน้อย พ.ศ. ๒๕๖๐ ซึ่งกำหนดผู้รับผิดชอบตามนโยบาย แบ่งสาระสำคัญออกเป็น ๑๔ หมวด ซึ่งสาระสำคัญจะสอดคล้องตามมาตรา ๕ และมาตรา ๗ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙

(๑) นโยบายควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

(๑) ผู้อำนวยการโรงพยาบาลบางสะพานน้อย

(๒) หัวหน้ากลุ่มงานบริหารงานทั่วไป

(๓) หัวหน้างานเวชสารสนเทศ

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๒) นโยบายการสำรองและกู้คืนข้อมูล กำหนดให้มีการจัดทำระบบสำรองข้อมูลของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้ และกำหนดให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อป้องกันการหยุดชะงักในการบริการสารสนเทศของโรงพยาบาลบางสะพานน้อย

กำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลบางสะพานน้อย

๒) หัวหน้ากลุ่มงานบริหารงานทั่วไป

๓) หัวหน้างานเวชสารสนเทศ

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๒) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อกำกับดูแลการดำเนินงาน การบริหารจัดการระบบสารสนเทศให้มีความปลอดภัย ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้

แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสนักงาน

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๓ การควบคุมการใช้อินเตอร์เน็ต

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ส่วนที่ ๑๖ การตรวจจับการบุกรุก

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ส่วนที่ ๒ การสำรองข้อมูล

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอัตรายต่อระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติในการรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม

แนวปฏิบัติในการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

แนวปฏิบัติในการสร้างความตระหนักในเรื่องการักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

การจัดทำประกาศแนวนโนบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติ เมื่อเกิดฟิชชิง (Phishing) ที่เว็บเซิร์ฟเวอร์ของโรงพยาบาล

ข้อที่ ๔ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลบางสะพานน้อยเกิดความเสียหาย หรือได้รับอันตรายจากภัยคุกคามทางด้านต่าง ๆ ผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย ละเว้น หรือฝ่าฝืน การปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาลราชวิถีเป็นผู้ขอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อที่ ๕ ให้ใช้แนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แบบท้ายประกาศนี้

ข้อที่ ๖ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ .....พ.ศ. ๒๕๖๕

(นายสมพงษ์ พัฒนกิจโพโรจน์)
ผู้อำนวยการโรงพยาบาลบางสะพานน้อย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลบางสะพานน้อย

พ.ศ. ๒๕๖๕- ๒๕๗๐

งานเวชสารสนเทศโรงพยาบาลบางสะพานน้อย

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลบางสะพานน้อย

โดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ดังนั้น

คณะกรรมการพัฒนาเทคโนโลยีสารสนเทศและการบริหารสารสนเทศโรงพยาบาลบางสะพานน้อย จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด และเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบางสะพานน้อยเป็นไปอย่างเหมาะสมเกิดประสิทธิภาพสูงสุดมีความมั่นคงปลอดภัยด้านสารสนเทศและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลบางสะพานน้อยนั้น โดยมีวัตถุประสงค์ดังนี้

๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยให้ใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

๒. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓. นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลบางสะพานน้อย ได้รับทราบและถือปฏิบัตินโยบายนี้อย่างเคร่งครัด

๔. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหารเจ้าหน้าที่และผู้ดูแลความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๕. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆเข้าล่วงรู้ข้อมูล แก้ไข หรือลายข้อมูลสารสนเทศโดยมิชอบ

๖. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

"การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ" หมายถึง การตรวจสอบการอนุมัติ และการกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้

"เครื่องเซิร์ฟเวอร์ (Server)"หมายถึงเครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย

"อุปกรณ์ UPS" หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการเกิดมีปัญหาขึ้นมาไฟตกเช่นไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้นอุปกรณ์โดยที่UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ตลอดจนเป็นอุปกรณ์ที่ช่วย ป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้าและอุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะคอมพิวเตอร์และ เชื่อมต่อ) รวมถึงหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ คอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

"ซอฟต์แวร์ (Software)" หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงานซอฟแวร์จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งหลักโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่งฐานเป็นเพียงการทำงานพื้นการกระทำกับข้อมูลที่เป็นตัวเลขฐานสองซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ เสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งที่ต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน แต่ซอฟต์แวร์จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

"ไวรัสคอมพิวเตอร์" หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ ระบบคอมพิวเตอร์ได้ และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่าย ระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำของคอมพิวเตอร์เรียบร้อยแล้วเนื่องจากไวรัสเป็นแค่โปรแกรมหนึ่งการที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำจะต้องมีการถูกได้นั้นเรียกให้ทำงานได้ขึ้นอยู่กับประเภทของไวรัสแต่ละตัวปกติผู้ใช้มักจะไม่ทราบว่าได้ทำการปลุก คอมพิวเตอร์ไวรัสนั้นขึ้นมาทำงานแล้ว

"เวชระเบียน" หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลบางสะพานน้อย

ข้อ๑ คำนิยาม

"โรงพยาบาล" หมายถึง โรงพยาบาลบางสะพานน้อย

"การรักษาความมั่นคงปลอดภัย" หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศโรงพยาบาลบางสะพานน้อย

"มาตรการ" หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น

"วิธีปฏิบัติ" หมายถึงรายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งได้กำหนดไว้ตามวัตถุประสงค์

"แนวทางปฏิบัติ" หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อบรรลุเป้าหมายได้ง่ายขึ้น

"ผู้บริหาร" หมายถึง ผู้มีอำนาจในระดับสูงของโรงพยาบาลบางสะพานน้อย

"ผู้ดูแลระบบ"หมายถึงเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อกำหนดฐานข้อมูลของเครือข่ายคอมพิวเตอร์

"เจ้าหน้าที่" หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

"สารสนเทศ" หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลอยู่รูปของตัวเลข ข้อความ หรือภาพให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจ และอื่นๆ

"ระบบคอมพิวเตอร์"หมายถึงอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าโดยได้มีการกำหนดคำสั่งชุดคำสั่ง และแนวทางปฏิบัติงานให้อุปกรณ์หรือสิ่งอื่นใดหรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆของโรงพยาบาลได้ เช่น ระบบแลนLAN) ระบบอินเตอร์เน็ต (Internet)

- **ระบบแลน (LAN)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกและสารสนเทศภายในหน่วยงาน
- **ระบบอินเตอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

"ระบบเทคโนโลยีสารสนเทศ" หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประกอบการวางแผนบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศ เป็นต้น

สารบัญ

หมวดที่๑

การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์และการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดรวมถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่๑ การควบคุมการเข้าถึงสารสนเทศ Access(Control)

ข้อ๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่ออนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ๒. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของจะต่อขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหาร

ข้อ๓. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทำการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๑.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องา เช่น

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

(๑.๒) กำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการเข้าถึงของผู้ใช้งานUser Access (Management) ที่ได้กำหนดไว้

(๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานผู้ดูแลระบบที่ได้รับมอบหมาย

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ ๒๕๔๔ ซึ่งระเบียบ พ.ศ. ดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สคัญไว้ดังนี้

(๒.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบายข้อมูลยุทธศาสตร์และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วยข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(๒.๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับคัญมากที่สุด
- ข้อมูลที่มีระดับคัญปานกลาง
- ข้อมูลที่มีระดับคัญน้อย

(๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไป

(๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๒.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ Text (Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในโฟล์พอที่จะอ่านข้อความนั้นได้ซึ่งมีรูปแบบอีกหลายรูปแบบ TEXT เช่น Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ Image(Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้JPEGเช่นFormat, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ๔. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ๕. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ๖. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า –ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ๗. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการe-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา

(๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งานUserAccess(Management)

ข้อ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ดังนี้

(๑) จัดทำแบบฟอร์มการการลงทะเบียนผู้ใช้งานหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าเทคโนโลยีสารสนเทศ

ข้อ๙. ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN)ระบบอินเตอร์เน็ต(Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าทีและได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งานสิทธิการใช้งานสิทอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) จัดทำบัญชีรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และตรวจสอบสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูลต่างๆสิทธิให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือ ขอเปลี่ยนก็ต่อเมื่อตำแหน่งภายในต้องดำเนินการภายใน ๗ วัน

ข้อ๑๑. การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ากัน

(๓) ส่งมอบรหัสผ่าน (Password)ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๗) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้น จะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดด้บ้างกำหนดให้รหัสผู้ใช้งานต่างจากรหัสการดังกล่าวและต้องผู้ใช้งานตามปกติ

ข้อ๑๒. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับการในการควบคุมเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

ส่วนที่๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(UserResponsibilities)

ข้อ๑๔. การใช้งานรหัสผ่านผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username)ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน(Password)

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

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (savepassword) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) กำหนดรหัสผ่านเริมต้นให้กับผู้ใช้งานให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน(Password) อย่างน้อย ๑ ครั้งต่อปี

ข้อ๑๕. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการพ.ศ.๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ๑๖. การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตามให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ๑๗. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใดๆ ก็ดีผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทางดังนี้

(๑) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้งและต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

ข้อ๑๘. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ๑๙. ข้อมูลที่เป็นความลับหรือมีระดับความสคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงานห้าม ไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทาลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๒๐. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาล และข้อมูลของผู้รับบริการหากเกิดการสูญหายโดยน ไปใช้ในทางที่ผิดการเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ๒๑. ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อ๒๒. ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาล จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นยกเว้นในกรณีที่โรงพยาบาล ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาล ซึ่งโรงพยาบาล อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึงวิธีการจัดเครือข่ายคอมพิวเตอร์ที่กหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกันหมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเการจัดแบบนี้ทึบไว้เองให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (FileServer) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่นบิทเทอร์เรนท์ (Bittorrent), อีมูล(Emule) เป็นต้นเว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๒๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบัน เช่นทิงการดูหนังฟังเพลงเกมส์เป็นต้นในระหว่างเวลาปฏิบัติราชการ

ข้อ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูลข้อความรูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศกฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาล

ข้อ๒๖. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวนก่อให้เกิดความเสีหรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของโรงพยาบาล

ข้อ๒๗. ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชน์ทางการค้า

ข้อ๒๘. ห้ามกระทำการใดๆ เพื่อการดักข้อไม่ว่าจะเป็นข้อควูลภาพม เสียงหรือสิ่งอื่นใด เครื่อขายระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ๒๙. ห้ามกระทำการรบกวนทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ๓๑. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่ากรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้หรือมูลเพื่อการใช้ทรัพยากร

ข้อ๓๒. ห้ามติดตั้งอุปกรณ์หรือกระทการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ๓๓. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่างๆก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกันเช่นโรงพยาบาลหรือหน่วยงานที่มาขอ เชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุมป้องกันและบริหารจัดการการใช้ข้อมูลร่วมกัน
(๒) พิจารณาจกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน
(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่ป้องกันที่เพียงพอ

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์(Assets Management)

ข้อ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (OperationCenter หมายถึง สถานที่ที่ใช้สาหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย)ที่เป็นเขตหวงห้าม โดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๓๔. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กับการใช้งานก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

ข้อ๓๗. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูลแฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สาหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภทดังนี้

ประเภทสื่อบันทึกข้อ	วิธีทำลาย
กระดาษ	ใช้การทำลายด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive แผ่นCD/DVD	- ให้การทลายข้อมูลบนFlash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกาซึ่งเป็นมาตรฐานการทลายข้อมูลโดยกาเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหายใช้การทำลายด้วยเครื่องหั่นทลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทลาย
ฮาร์ดดิสก์	- ใช้การทลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกาซึ่งเป็นมาตรฐานการทลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ๔๒. ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่างๆทีหน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้นห้ามมิให้ผู้ใช้งานนสินทรัพย์และระบบสารสนเทศต่างๆไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อโรงพยาบาล

ข้อ๔๓. ความเสียหายใดๆที่เกิดจากการละเมิดตาม

ข้อ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่๕ การควบคุมการเข้าถึงเครือข่าย(Network Access Control)

ข้อ๔๔. มาตรการควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตนเช่นบัตร ประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ(Visitor)แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร **"บันทึกการเข้าออกพื้นที่"**

(๒) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปกิบัติงานนำมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้าออกตามที่ระบุไว้ในเอกสาร**"บันทึกการเข้าออกพื้นที่"** ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของข้อมูลในสมุดแบบบันทึกฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ๔๕. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วย และต้องปฏิบัติตามนโยบายนั้น โดยเคร่งครัดโดยผู้ใช้งานต้องกรอกแบบฟอร์ม"การขอเชื่อมต่อเครือข่าย"

ข้อ๔๖. การขออนุญาตใช้งานพื้นที่WebServer ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทบของระบบและผู้ใช้งานอื่นๆ

ข้อ๔๗. ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหากการใดที่มีผลกระทบต่ออุปกรณ์ส่วนกลางได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล(Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ๔๘. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพดังต่อไปนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานาระบบเครือข่ายที่ได้รับฉพาะอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ หน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกรวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย(Malware) ด้วย

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

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วย โดยงานผ่านทางระบบอินเตอร์เน็ตจเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นIPAddressภายในของระบบเครือข่ายภายในของหน่วยงาน

(๘) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่ายได้แก่รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IPAddress และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอกต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IPAddress ของทั้งต้นทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม"การขอเชื่อมต่อเครือข่าย"
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ๔๙. ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)

ข้อ๕๐. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ๕๑. กำหนดให้มีการจัดเก็บรหัสต้นฉบับ (source code), คลังโปรแกรม(Library)และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ๕๒. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางพ...คอมพิวเตอร์๒๕๕๐

ข้อ๕๓.กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากการกำหนดผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าหน่วยงาน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

(๒) การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๓) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน(Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ๕๔. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยตามอาคารต่างๆๆ เพื่อควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ๕๕. กำหนดการป้องกันเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายต่างๆ อย่างชัดเจน และต้องทบทวนการกำหนดค่าParameterต่างๆเช่น IP Address อย่างน้อยปีละ ๑ ครั้งนอกจากนี้การกำหนดการแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ๕๖. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำPacketFiltering เช่นการใช้ไฟร์วอลล์ (Firewall)หรือฮาร์ดแวร์อื่นๆรวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ๕๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอนาจหน้าที่เกี่ยวข้อง

ข้อ๕๘. IP address ของระบบงานเครือข่ายภายในจเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างเครือข่ายได้โดยง่าย

ข้อ๕๙. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ๖๐. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ๑๐) เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงานเป็นต้น

ข้อ๖๑. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screensaver) เพื่อทำการล็อกหน้าจอภาพ เมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username)และรหัสผ่าน(Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภทPeer-to-Peer หรือโปรแกรมที่มีความเสี่ยงวันแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานโรงพยาบาล

(๘) ซอฟต์แวร์ที่โรงพยาบาลฯ ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามความจเป็นใน หน้าที่และห้ามไม่ให้ผู้ใช้งานทการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟท์แวร์ที่โรงพยาบาลจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจห้ามมิให้ผู้ใช้งานทการติดตั้งถอดถอนเปลี่ยนแปลงแก้ไขหรือทสำเนาเพื่อนไปใช้งานที่อื่น

(๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเพื่อประโยชน์ทางการค้า

(๑๑) ห้ามผู้ใช้งานนำเสอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่ เหมาะสมหรือขัดต่อศีลธรรมกรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๒) ห้ามผู้ใช้งานของหน่วยงานควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๖๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (UserIdentification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ๖๓. การใช้งานโปรแกรมประเภทยูทิลิตี้(Useof system utilities) ต้องจกัดและควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ไหนไว้หรือที่มีอยู่แล้วให้ดเนินการดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบและต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สาหรับระบบงาน

(๔) มีการจกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี

ข้อ๖๔. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

(๒) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานเร็วขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ๖๕. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจากัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กหนดและกำหนดให้ใช้งานได้ตามช่วงเวลา การทำงานที่หน่วยงานกำหนด

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงกว่าระบบงานที่มีการใช้งานในระบบเทคโนโลยีสารสนเทศที่มีความสคัญสูงาระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ๖๖. ผู้ดูแลระบบต้องกหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ๘) ในการใช้งานตามความจุเป็นรวมทั้งขั้นตอนปฏิบัติสาหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ๑๐) เช่นการลาออกหรือ การเปลี่ยนตำแหน่งงานภายในหน่วยงานเป็นต้น

ข้อ ๖๗. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สาคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN)ระบบอินเตอร์เน็ต (Internet)เป็นต้นโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสมำเสมอ

ข้อ๖๘. ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาทีระบบจะยุติการใช้งานผู้ใช้งานต้องที่การการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ๖๙. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งงานหรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์รูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานโดยมีการกหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ๗๐. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลัยดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่นSSL, VPN หรือXML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กหนดของระดับความสคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นสินทรัพย์ออกนอกหน่วยงานบำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนเป็นต้น

ข้อ๗๑. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงให้ ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเองโดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

ข้อ๗๒. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้วให้รีบนส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malwares)

ข้อ๗๓. โรงพยาบาลได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้น ซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์การตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ๗๔. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจเป็นต่อการทำงานห้ามมิให้ผู้ใช้งานทำการถอดถอดอำนาจเปลี่ยนแปลงแก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์

ข้อ๗๕. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่หน่วยงานได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาโดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๗๖. บรรดาข้อมูลไฟล์ซอฟต์แวรร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนมาใช้งานหรือบันทึกทุกครั้ง

ข้อ๗๗. ผู้ใช้งานต้องการปรับปรุงข้อมูลสหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ๗๘. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ๗๙. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ๘๐. ห้ามลักลอบทำสำเนา เปลี่ยนแปลงลบทิ้งซึ่งข้อมูลข้อความเอกสาร หรือสิ่งใดๆที่เป็นสินทรัพย์ของหน่วยงานหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ๘๑. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงานสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆสามารถดำเนินการได้แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการ กระทำในลักษณะเป็นการแอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทให้ผู้ใช้งานมีสิทธิและลดับความสคัญาในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำซ้อนตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไว้รัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทลายระบบจ กัดสิทธิการใช้ (License) ซอฟต์แวร์

(๔) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทยกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ๘๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ (source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำไว้กับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทการติดตั้งก่อน ดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายหน่วยงานต้องดอกเนินการเปลี่ยนรหัสต่างๆให้พร้อมใช้งาน

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสนักงาน (Teleworking)

ข้อ๘๓. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ๘๔. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ๘๕. ผู้ใช้งานจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่านหรือวิธีการเข้ารหัสเป็นต้น

ข้อ๘๖.ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนหน่วยงานจากระยะไกลหากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ๘๗. ต้องกหนดชนิดของงานชั่วโมงการทำงานชั้นความลับของข้อมูลระบบงานและบริการต่าง ๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ๘๘. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการขอยกเลิกการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ๘๙. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ๙๐. ผู้ดูแลระบบต้องทำการเปลี่ยนค่าSSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย(Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย(Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier)

ข้อ๙๑. ผู้ดูแลระบบต้องกำหนดค่าWireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access)ในการเข้ารหัสข้อมูลระหว่างWireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย(Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ๙๒. ผู้ดูแลระบบเลือกใช้วิธีการควบคุมMACAddress (Media Access Control Address) และชื่อผู้ใช้งาน(Username) รหัสผ่าน(Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MACaddress (Media Access Control Address) และชื่อผู้ใช้งาน(Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ทำให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ๙๓. ผู้ดูแลระบบต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ๙๔. ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ๙๕. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ๙๖. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายและจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือนและในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ๙๗. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆของหน่วยงาน

ข้อ๙๘. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ๙๙. ผู้ดูแลระบบต้องทำการลงทะเบียนกหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (FirewallControl)

ข้อ๑๐๐. หน่วยงานมีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของFirewall ทั้งหมด

ข้อ๑๐๑. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ๑๐๒. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตPolicyจะต้องถูกามบล็อก(Block) โดย Firewall

ข้อ๑๐๓. ผู้ใช้งานอินเตอร์เน็ตจะต้องทการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ๑๐๔. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่างๆขอ Firewall

ข้อ๑๐๕. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูจัดการเท่านั้น

ข้อ๑๐๖. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์Firewallจะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ๑๐๗. การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ทเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งานซึ่งหากมีความจเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ๑๐๘. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อทีเป็นต่อการให้บริการเท่านั้น

ข้อ๑๐๙. จะต้องมีการสรองข้อมูลการกหนดค่าต่างๆของอุปกรณ์ Firewall เป็นประจทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ๑๑๐. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในหน่วยงานที่มีเป็นอินทราเน็ตจะต้องไม่อนุญาตการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ตตให้มีเว้นแต่มีความจเป็นาโดยจะต้องอนุญาตเป็นกรณีไป

ข้อ๑๑๑.หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายทีมีการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ๑๑๒. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายและจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อ๑๑๓. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ส่วนที่๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ๑๑๘. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ๑๑๙. เปลี่ยนรหัสผ่าน (Password) ทุก๓ - ๖ เดือน

ข้อ๑๒๐. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-MailAddress) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์(E-Mail)ของตน

ข้อ๑๒๑. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ๑๒๒. การส่งข้อมูลที่เป็นความลับควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว้ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กของผู้รับให้เพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ๑๒๓. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ๑๒๔. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (ChainLetter)

ข้อ๑๒๕. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ๑๒๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ๑๒๗. ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อ๑๒๘. ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล E-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่า ดังนั้น E-Mail ที่เก่ามากๆ จำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ๑๒๙. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็นExecutable file เช่น.exe .com เป็นต้น

ข้อ๑๓๐. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้

ข้อ๑๓๑. ผู้ใช้งานต้องใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ๑๓๒. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการจากระบบเพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ๑๓๓. ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ๑๓๔. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม๒๕๕๐ เรื่องการพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่๑๓ การควบคุมการใช้อินเตอร์เน็ต (Internet)

ข้อ๑๓๕. ผู้ดูแลระบบต้องกหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้นเช่นProxy, Firewall,IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นเช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทาการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ๑๓๖. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาก่อนทรเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ๑๓๗. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ๑๓๘. ไม่ใช้ระบบอินเตอร์เน็ต(Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคมละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ๑๓๙. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ๑๔๐. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ๑๔๑. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เปิดเผยข้อมูลที่สคัญและเป็นความลับของหน่วยงาน

ข้อ๑๔๒. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงานการทลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ๑๔๓. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรอันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพลักษณะอันไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อ๑๔๔. หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้วให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้ งานโดยบุคคลอื่นๆ

ข้อ๑๔๕. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้วให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ๑๔๖. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่าง เคร่งครัด

ส่วนที่๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ๑๔๗. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมหน่วยงานได้ซื้อลิขสิทธิมาอย่างถูกต้องตามกฎหมายดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลเท่านั้น

(๕)ก่อนการใช้งานสื่อบันทึกพกพาต่างๆต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการตั้งค่าScreen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาทีเพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายหน่วยงานยกเว้นจะรับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ๑๔๘. การใช้รหัสผ่าน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓–๖ เดือน

ข้อ๑๔๙. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆเช่นFloppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๓) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๔) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยซึ่งมีผลทำให้ชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคสั่งอื่นเกิดความเสียหายถูกทำลาย แก้ไข เปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคสั่งที่กาหนดไว้

ข้อ๑๕๐. การสำรองข้อมูลและการกู้คืน

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

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (BackupMedia) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บ HardDisk ไม่ควรจะเป็นข้อมูลที่สำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ๑๕๑. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้งานราชการ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือนเช่น การตกจากโต๊ะทำงานหรือหลุดมือเป็นต้น

(๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็งเช่นปลายปากกา กดสัมผัสหน้าจอLCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุดและต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทกรยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ๑๕๒. ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อกเครื่องขณะที่ไม่ได้ใช้งานไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนความชื้นฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ๑๕๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

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

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีและรัดกุม

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (ScreenSaver) โดยตั้งเวลาประมาณ ๑๕ นาทีให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเวลานาน

ข้อ๑๕๔. การใช้รหัสผ่านให้ผู้ใช้งาน

(๑) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

(๒) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

(๓) ควรเปลี่ยนรหัสผ่านทุก ๓–๖ เดือน

ข้อ๑๕๕. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหล เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่างๆที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บ HardDisk ไม่ควรจะเป็นข้อมูลส่วนที่สำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียจะไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่๑๖ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ๑๕๖. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงานความมั่นคงปลอดภัยเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทความรับผิดชอบที่เกี่ยวข้อง

ข้อ๑๕๗. IDS/IPS Policy ครอบคลุมทุกโฮสต์Host) (ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ตทุกเส้นทาง

ข้อ๑๕๘. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบระบบ IDS/IPS

ข้อ๑๕๙. ระบบทั้งหมดในDMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ๑๖๐. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPSจะต้องมีการบันทึกผลการตรวจสอบ

ข้อ๑๖๑. ระบบ IDS/IPS จะต้องมีการตรวจสอบและUpdate Patch/Signature เป็นประจำ

ข้อ๑๖๒. ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ๑๖๓. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ๑๖๔. เครื่องแม่ข่ายที่มีการติดตั้งHost-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ๑๖๕. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก ระบบพฤติกรรมที่น่าสงสัยหรือการพยายามเข้าระบบประสบความสำคัญทั้งที่สำเร็จและไม่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้อง มีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ

ข้อ๑๖๕. พฤติกรรมกิจกรรมที่น่าสงสัยหรือระบบการทางานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการทำรายงานให้หัวหน้าหน่วยงานทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ๑๖๖. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ๑๖๗. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ผลการตรวจพบรายงานของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตเนินการตามแผน

ข้อ๑๖๘. หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ๑๖๙. ผู้ที่ถูกตรวจสอบว่าพยายามทำการอันใดที่เป็นการละเมิดนโยบายของกระทำโรงพยาบาลการพยาบาลเข้าถึงระบบโดยมิชอบ การโจมตีระบบมีพฤติกรรมเสี่ยงต่อการทางานของระบบสารสนเทศหรือ จะถูกระงับการใช้ เครือข่ายทันทีหากการกระทำ ดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลพยากรและทรัพยากรระบบของหน่วยงานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ๑๗๐. การปรับปรุงระบบปฏิบัติการOperating (System Update)

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

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

(๕) ปรับปรุง /กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มีService Patch Update)

(๖) ติดตั้งโปรแกรมAntivirus/ปรับปรุงVirus Definition และ กำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ๑๗๑.การบริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User) (Account Management)

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ System (Administrator)

(๒) กำหนดชื่อผู้ใช้งาน User Name และรหัสผ่าน Password

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ๑๗๒. การปรับปรุงการรักษาความปลอดภัย/Anti-Virus (System Security & Anti-virus Update)

(๑) การเข้าใช้ระบบติดตาม เฝ้าระวัง ระบบการทงานของคอมพิวเตอร์

(๒) ประสิทธิภาพของระบบ (Performance) หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

(๔) ปรับปรุงโปรแกรมAnti-virus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการScan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อ๑๗๓. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพตามระบบฐานข้อมูลที่กำหนด

(๓) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล Database(Admin) ชื่อผู้ใช้งานอื่นและสิทธิการใช้

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเปิดปัญหาอยู่เสมอ

ข้อ๑๗๔. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ/กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนาระบบโปรแกรม

(๒) กำหนดค่าหรือโปรแกรมหรือบริการงานร่วมกับระบบปฏิบัติการให้เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และท การทดสอบการให้บริการตามระบบงานนั้นกหนดา

(๔) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้ดยแจ้งรายชื่อโรหัสผ่าน และสิทธิการเข้าใช้ระบบและฐานข้อมูลตามที่กหนดไว้า

(๕) ก หนดเกณฑ์การสรองา สำเนา ทดสอบกู้คืนRestore (Test)

(๖) บันทึกข้อกหนดา ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

ส่วนที่๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ๑๗๕. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ะข้อมูลที่ใช้ในการจัดเก็บและกำหนดชั้นต้องความลับในการเข้าถึง

ข้อ๑๗๖. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์Log) ที่เก็บรักษาไว้

ข้อ๑๗๗. กำหนดให้มีการบันทึกการทงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึก–การเข้าระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ๑๗๘. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้ก หน่วยงานอย่างเคร่งครัด และตระหนักถึงความสคัญของการรักษาความมั่นคงปลอดภัย
๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กหนดโดยเคร่งครัดและตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่๑การรักษาความปลอดภัยฐานข้อมูล

ข้อ๑. กำหนดสิทธิและความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนด กลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต กำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

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

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานUser Access (Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูและได้รับมอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ เช่น ข้อมูลดัชนีเศรษฐกิจการ การค้าระหว่างประเทศของไทย ข้อมูลเศรษฐกิจการค้าจังหวัด เป็นต้น

(๓.๒) จัดแบ่งระดับความสคัญของข้อมูลา ออกเป็น๓ระดับ คือ

- ข้อมูลที่มีระดับคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุดหมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดค เสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ๒. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้หรือดำเนินการรวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัยที่

ข้อ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๑ ข้อหมวดที่๑๒

ข้อ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงานเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการหรือแลกเปลี่ยนขอใช้ข้อมูลจากส่วนราชการหรือ แลกเปลี่ยนขอใช้ข้อมูลจากส่วนหรือ ราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงาน ภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรฐาน เพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลแลกเปลี่ยน ข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสาหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูลซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ๖. พิจารณาคัดเลือกระบบสารสนเทศที่สญและจัดทาระบบสา รองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ๗. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ๘. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ๙. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อย กำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทาการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมของการสำรองข้อมูล ได้แก่การลง วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบค่าคอนฟิกกูเรชัน (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถนที่เพื่อไม่ให้เกิดภัยพิบัติกับหน่วยงาน

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสมำเสมอ เพื่อตรวจสอบว่ายังสามารถเข้าถึงข้อมูล ได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสาหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่เสมอ อย่างน้อยปีละ๑ครั้ง หรือตามความเหมาะสมโดยคนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการหัสข้อมูลกับข้อมูลลับที่ได้สเข้รองเก็บไว้

ข้อ๑๐. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานานน้าท่วมไฟไหม้แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์อฟต์แวร์ซ เป็นต้น เมื่อเกิดเหตุจเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ๑๒. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ๑๓. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้งหรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสียงที่ยอมรับได้ของแต่ละหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

หมวดที่๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงทีอันตรายต่อระบบสารสนเทศเป็น

แนวปฏิบัติ

ส่วนที่๑การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน Internal(Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกExternal(Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ๑. จัดลำดับความสำคัญของความเสี่ยง
ข้อ๒. ค้นหาวิธีการดเนินการเพื่อลดความเสี่ยง
ข้อ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
ข้อ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
ข้อ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
ข้อ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สคัญๆ
(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ หนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศสามารถแยกเป็นภัยต่างๆ ๔ ได้ประเภท ดังนี้

ประเภทที่๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงานHumanError)(เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงานและอาจส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพกำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้านHardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางสารสนเทศ ทั้งทางด้าน HardwareและSoftware ได้อย่างมีประสิทธิภาพยิ่งขึ้นทำให้รับความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกร์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ประกอบด้วยไวรัสคอมพิวเตอร์ (Virus Computer), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจันTrojan(Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้กำหนดแนวทางปฏิบัติ เพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่ายหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์Anti-virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที ๓ ภัยจากไฟไหม้ หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทความเสียหายให้แก่ ระบบเทคโนโลยีสารสเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนหน่วยรักษาความปลอดภัย เพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที การตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉินอัคคีภัย (โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานอย่างสม่ำเสมอ)

ประเภทที่๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับ สถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา
(๒) ถอดเทป Back up ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย
(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเครื่องปรับอากาศไฟ เพื่อป้องกันเครื่องควบคุมเสียหายและ ป้องกันภัยจากไฟฟ้า
(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย
(๕) กรณีลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่าย ว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่
(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งหน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้ตามปกติ

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคลและหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของ คอมพิวเตอร์ระบบเครือข่ายหรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ ติดตั้งประจำโต๊ะทำงาน

ข้อ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออกของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อกหรือใส่กุญแจประตูหน้าต่างเสมอหรือเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างอย่างเหมาะสมๆ เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตาแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นฐานทั่วไป (Working Area General) พื้นที่ทำงานของผู้ดูแลระบบ (Administrator Area System) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ IT(Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สายWireless LAN(Coverage Area) เป็นต้น

ข้อ๔. การควบคุมการเข้าออก อาคารสถานที่

(๑) กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออก ในแต่ละพื้นที่ใช้งานระบบอย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น ประชาชน ใบอนุญาตขับขี่ เป็นต้น การลงบันทึกข้อมูลบัตรในสมุดบันทึกและแล้ว รับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาติดต่อ(Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญเช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น -เพื่อควบคุมการออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Center Data)

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ๕. ระบบและอุปกรณ์สนับสนุนการทงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องใช้งานโดยให้มีระบบดังต่อไปนี้

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

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทางานภายในห้องเครื่องทำงานผิด

ข้อ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆของการดักจับสัญญาณ เพื่อป้องหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าบุคคลภายนอก

(๗) พิจารณาใช้งานเส้นใยแก้วน าแสงแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบcoaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนาโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนาในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกมาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสคัญโดยผู้รับจาให้บริการจากทางภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้อนุญาต

ข้อ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนาอุปกรณ์ออกนอกหน่วยงาน กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงานเมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๓) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำรวมอุปกรณ์ส่งคืน

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

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สิน

ข้อ๑๐. การกำจัดอุปกรณ์หรือการนอุปกรณ์กลับมาใช้งานอีกครั้งSecure Disposal(or re-use of Equipment)

(๑) ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนาอุปกรณ์นำไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่๕
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตีหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ๑. ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใดและเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ๒. ระบบไฟร์วอลล์

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูกBlock เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินดำเนินการแก้ไขปัญหาใจ

ข้อ๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) (ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจันงสปายแวร์รวมถึง

(๑) ดำเนินการตรวจสอบLog File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจานวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลฯ ไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่พบว่ากระจาย อยู่ในเครือข่ายโรงพยาบาล

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกข้างนอกต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

หมวดที่๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของโรงพยาบาล

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ๑. จัดให้มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปี ๑ ครั้ง

ข้อ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมตามแผนการฝึกอบรมของหน่วยงานต่างๆ

ข้อ๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศและมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ๔. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และ สำรวจความต้องการของผู้ใช้งาน

ข้อ๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดเกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดใช้งานปฏิบัติบัติตามเพื่อให้ผู้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆที่ได้ประกาศใช้ในประเทศไทยรวมกฎหมายกฎระเบียบของโรงพยาบาลฯ และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติ ดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

หมวดที่๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ๑. **ระดับนโยบาย**ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับผู้อนวยการ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ ปรึกษาตลอดจนติดตามกำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆแก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ๒. **ระดับบริหาร**ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่ม/หัวหน้าศูนย์เทคโนโลยีสารสนเทศเทียบเท่าหัวหน้ากลุ่ม

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ๓. **ระดับปฏิบัติ**ผู้รับผิดชอบ ได้แก่ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการโรงพยาบาล เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุมแลดูรักษาความปลอดภัย และบำรุงรักษาระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูลา(Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลฯ

ภาคผนวก

การจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ๑. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๑.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๔

๑.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ๕ – ๑๔

ข้อ๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ ๒ ส่วนมีดังนี้

๒.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าทีปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาล

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๒.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ๓. มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตกำหนดสิทธิการเข้าถึงหรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูลที่สำคัญหรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ๔. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทข้อปฏิบัติสาหรับการควบคุมการเข้าถึงสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกหนดการใช้งานตามภารกิจ และข้อกหนดด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ“ตามหลักการ ความจำเป็นที่ต้องรู้”

ข้อ๕. มีการบริหารจัดการการเข้าถึงของผู้ใช้งานUserAccess (Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (Registration User) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (Management User) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิเฉพาะสิทธิพิเศษและสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

ข้อ๖. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (Responsibilities User) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (User Password) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่าน

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์กำหนดแนวปฏิบัติที่เหมาะสม เพื่อกำหนดแนวปฏิบัติที่เหมาะสม เพื่อกำหนดการป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงาน

(๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (ClearDesk And Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานเข้ารหัสการใช้ข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ๗. มีการควบคุมการเข้าถึงเครือข่าย (Access Control Network) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อยดังนี้

(๑) การใช้บริการเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (UserAuthentication For External Connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification In Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้การระบุอุปกรณ์บนเครือข่ายและควรใช้วิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้การระบุอุปกรณ์บนเครือข่าย และควรใช้เป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สหรับตรวจสอบและปรับแต่งระบบต้องควบคุมการเข้าถึงพอร์ตที่ใช้สหรับ ตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่ายต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่ายต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่ายต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อคอมพิวเตอร์และการส่งผ่านไหวเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือ การประยุกต์ใช้งานตามภารกิจ

ข้อ๘. มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (UserIdentification And Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Management SystemPassword) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation Of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ๙. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้ในการเข้าถึงสารสนเทศและฟังก์ชัน(Function) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และงานจากการปฏิบัติภายนอกหน่วยงาน

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่กำหนดแนวปฏิบัติและต้องมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ๑๐. จัดทำระบบสำรองสำหรับระบบสารสนเทศตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกได้

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ๑๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นระบบสารสนเทศ (Information Security Audit And Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ๑๒. ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่ายปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

แนวปฏิบัติ เมื่อเกิดฟิชชิง (Phishing) ที่เว็บเซิร์ฟเวอร์ของหน่วยงาน

วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหายและส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

แนวปฏิบัติ

ข้อ๑. เมื่อผู้ดูแลระบบเครือข่ายของโรงพยาบาลฯได้รับแจ้งหรือตรวจพบว่าเว็บเซิร์ฟเวอร์เป็นช่องทางให้ผู้ไม่หวังดีทำฟิชิง (Phishing) ผู้ดูแลระบบของโรงพยาบาลฯจะดำเนินการ ดังนี้

(๑) ดำเนินการบล็อก IP Address ของเว็บเซิร์ฟเวอร์ที่โดนฟิชชิงนั้น หรือแจ้งผู้ให้บริการ เส้นทางเครือข่ายของหน่วยงานดเนินการโดยเร่งด่วน

(๒) แจ้งผู้ดูแลเว็บเซิร์ฟเวอร์ของหน่วยงานที่ถูกทำฟิชชิทางจดหมายอิเล็กทรอนิกส์ หรือทางโทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

ข้อ๒. เมื่อหน่วยงานดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังผู้ดูแลระบบเครือข่ายของโรงพยาบาลหรือผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานบล็อกเพื่อปลด IPAddress

ข้อ๓. ผู้ดูแลเว็บเซิร์ฟเวอร์ของหน่วยงานต้องตรวจสอบเว็บเวอร์และเว็บไซต์ภายในหน่วยงานของตนเอง รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทฟิชชิง

หมายเหตุ: ทางผู้เสียส่วนใหญ่หากเป็นหน่วยงานที่มีกาธุรกรรมอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการเงินธนาคาร เว็บไซต์ที่เกี่ยวกับการซื้อขายออนไลน์ ฯลฯ หากการดำเนินการแก้ไขปัญหาดังกล่าวล่าช้าและมีความเสียหายอาจมีผลทางกฎหมายต่อหน่วยงานของท่าน