ประกาศโรงพยาบาลเมืองจันทร์

เรื่องนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

.....

ตามที่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ ๒ พ.ศ.๒๕๖๐ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓ และที่เกี่ยวข้อง รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ ที่มีผลกระทบต่อประชาชนโดยตรงจากการเชื่อมโยงข้อมูลด้านสุขภาพ

สถานพยาบาลพยาบาลควรต้องมีการกำหนดนโยบายและวัตถุประสงค์ระบบการจัดการและกำหนดขั้นตอนในการนำไปปฏิบัติ พร้อมทั้งชี้ให้เห็นความสำเร็จตามเกณฑ์ที่กำหนด เพื่อให้เกิดวงจรการปรับปรุงพัฒนาระบบการจัดการคุณภาพอย่างต่อเนื่องมีการดำเนินงานตามเกณฑ์มาตรฐาน อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และสามารถให้บริการได้อย่างต่อเนื่อง สามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆเพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเขาใช่บริการในระบบบริการสุขภาพ จำเปนตองมีความมั่นคงปลอดภัยไซเบอรในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ

โรงพยาบาลเมืองจันทร์ตระหนักถึงการปฏิบัติงานต่างๆ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเมืองจันทร์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลเมืองจันทร์ จึงได้จัดทำนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเผยแพร่ให้บุคลากรทุกระดับผู้รับบริการได้รับทราบและขอความร่วมมือให้ปฏิบัติตามอย่างเคร่งครัด จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลเมืองจันทร์ เรื่องนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓. โรงพยาบาลเมืองจันทร์ได้จัดทำนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของโรงพยาบาลเมืองจันทร์เป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ ประกอบด้วยเนื้อหาอย่างน้อยครอบคลุมตามประกาศ ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดในข้อ ๔

๓.๒ ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนด ในข้อ ๕ – ข้อ ๑๔

ข้อ ๔. นโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ตามประกาศนี้ มีดังนี้

๔.๑ การจัดทำนโยบายต้องมีผู้บริหาร เจ้าหน้าที่ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

๔.๒ นโยบายต้องจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ และสามารถเข้าถึงได้อย่างสะดวก ผ่านทางเว็บไซต์ของโรงพยาบาลเมืองจันทร์

๔.๓ มีการกำหนดผู้รับผิดชอบตามนโยบาย/ระเบียบปฏิบัติดังกล่าวไว้ชัดเจน

๔.๔ มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๖ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๔.๗ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

๔.๘ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรอง ระบบสารสนเทศ และระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๔.๙ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔.๑๐ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑๑ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๔.๑๒ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๕. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ ประกอบด้วย

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

๕.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๕.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับขั้นความลับของข้อมูล รวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทาง การเข้าถึง

ข้อ ๖. การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ซึ่งได้รับการสร้างความตระหนักเรื่องความมั่นคง ปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ประกอบด้วย

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อไม่การอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิก เพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน ต้องจัดการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและ

ใช้งานระบบสารสนเทศแต่ละชนิด ตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน ต้องจัดกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ต้องจัดกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ ตามระยะเวลาที่กำหนดไว้

ข้อ ๗. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ประกอบด้วย

๗.๑ การใช้งานรหัสผ่าน กำหนดระเบียบปฏิบัติที่ดีสำหรับผู้ใช้งาน ในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดระเบียบปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยง ต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘. การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาต ประกอบด้วย

๘.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน สามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของหน่วยงานได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับระเบียบปฏิบัติการควบคุม การเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ

สอดคล้องกับระเบียบปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙. การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ประกอบด้วย

๙.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการ กล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๙.๓ การบริหารจัดการรหัสผ่าน ต้องจัดทำ หรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบหรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศ

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยง หรือมีความสำคัญสูง

ข้อ ๑๐. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ประกอบด้วย

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดระเบียบปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดระเบียบปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงาน จากภายนอกหน่วยงาน

ข้อ ๑๑. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

๑๑.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อขออนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

๑๑.๒ หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๑๑.๓ สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงานให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษา ความพร้อมที่จะให้บริการ

๑๑.๔ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขต ที่กำหนดไว้

ข้อ ๑๒. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ประกอบด้วย

๑๒.๑ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

๑๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๒.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑๒.๖ มีศูนย์คอมพิวเตอร์สำรอง ซึ่งตั้งอยู่ในสถานที่ที่ปลอดภัย พร้อมระบบคอมพิวเตอร์เพื่อสนับสนุนการปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน

ข้อ ๑๓. การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ประกอบด้วย

๑๓.๑ ต้องมีการจัดทำแผนด้านระบบสารสนเทศ

๑๓.๒ ต้องมีการจัดทำแผนด้านระบบคอมพิวเตอร์และระบบเครือข่าย

๑๓.๓ ต้องมีการจัดทำแผนด้านบุคลากรผู้รับผิดชอบ สถานที่ในการปฏิบัติงาน เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน

ข้อ ๑๔. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

๑๔.๑ ต้องมีการจัดทำแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

๑๔.๒ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑๔.๓ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายใน

ของหน่วยงาน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๕. โรงพยาบาลเมืองจันทร์ กำหนดความรับผิดชอบให้เป็นไปตามเอกสารแนบท้ายประกาศ ส่วนที่ ๖

๑๕.๑ ระดับนโยบาย

กำหนดให้ผู้บริหาร เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบาย และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหาร เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

๑๕.๒ ระดับปฏิบัติ

๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ ผู้รับผิดชอบได้แก่

๑.๑) ผู้บังคับบัญชา

๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน ผู้รับผิดชอบ ได้แก่

๒.๑) ผู้บังคับบัญชา

๒.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๓) ผู้ใช้งาน

๓) การควบคุมการเข้าถึงเครือข่าย ผู้รับผิดชอบได้แก่

๓.๑) ผู้บังคับบัญชา

๓.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓) ผู้ใช้งาน

๔) การควบคุมการเข้าถึงระบบปฏิบัติการ ผู้รับผิดชอบ ได้แก่

๔.๑) ผู้บังคับบัญชา

๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๕) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ ผู้รับผิดชอบ ได้แก่

๕.๑) ผู้บังคับบัญชา

๕.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๖) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบได้แก่

๖.๑) ผู้บังคับบัญชา

๖.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๖.๓) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

๗) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ผู้รับผิดชอบ ได้แก่
๗.๑) ผู้บังคับบัญชา
๗.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๘) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่
๘.๑) ผู้บังคับบัญชา
๘.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๙) การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ผู้รับผิดชอบ ได้แก่
๙.๑) ผู้บังคับบัญชา
๙.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๑๐) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่
๑๐.๑) ผู้บังคับบัญชา
๑๐.๒) ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบจาก ภายนอก
๑๐.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย
๑๑) นโยบายการสร้างความรู้ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่
๑๑.๑) ผู้บังคับบัญชา
๑๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
๑๑.๓) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๑๖. องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยอ้างอิงรายละเอียดระเบียบปฏิบัติจากเอกสารแนบท้ายประกาศ “นโยบาย/ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลเมืองจันทร์ พ.ศ. ๒๕๖๓” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของหน่วยงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๒๗ ตุลาคม พ.ศ.๒๕๖๓

(นายแพทย์จิระวัตร วิเศษสังข์)
ผู้อำนวยการโรงพยาบาลเมืองจันทร์

เอกสารแนบท้ายประกาศ

นโยบาย/ระเบียบปฏิบัติ
ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
โรงพยาบาลเมืองจันทร์ พ.ศ. 2564

สารบัญ

หน้า

คำนิยาม

คำนิยามที่ใช้ในระเบียบปฏิบัติฯ นี้ ประกอบด้วย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายระบบสารสนเทศของโรงพยาบาลเมืองจันทร์ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“การพิสูจน์ยืนยันตัวตน” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (username) และรหัสผ่าน (password)

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า ความมั่นคงความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลเมืองจันทร์ การป้องกันข้อมูลที่เป็นความลับ ความถูกต้อง ครบถ้วนของข้อมูล ความพร้อมใช้งานของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์อิเล็กทรอนิกส์สื่อสารพกพา

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)” หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกันทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

“ชื่อโดเมนย่อย (Sub Domain Name)” หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ "ที่อยู่ เว็บไซต์" แทนก็ได้

“ชื่อผู้ใช้งาน (Username)” หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

“ดับเบิ้ลยู พี เอ WPA (Wi-Fi Protected Access)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

“ดับเบิ้ลยู อี พี WEP (Wired Equivalent Privacy)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“โทเค็น คีย์ (Token Key)” หมายความว่า อุปกรณ์ที่ใช้เก็บข้อมูลรูปแบบหนึ่ง ที่ใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งานเพื่อแสดงว่าเป็นบุคคลนั้นจริง ให้เข้าถึงฐานข้อมูลสารสนเทศของหน่วยงานได้ อุปกรณ์สามารถใช้งานได้ผ่านพอร์ต USB ของเครื่องคอมพิวเตอร์ ลักษณะภายนอกคล้ายกับ Thump drive แต่ไม่ใช่ Thumb drive โดยผู้ใช้งานจะต้องมีอุปกรณ์ Token Key และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตน

“บัญชีผู้ใช้บริการ (Account)” หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

“บิตทอร์เรนต์ (BitTorrent)” หมายความว่า เป็นการสื่อสารที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์ด้วยกันโดยตรง ผ่านเครือข่ายอินเทอร์เน็ต

“โปรแกรมประสงค์ร้าย (Malware)” หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาให้มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือพิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

“ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของโรงพยาบาลเมืองจันทร์ รวมถึงผู้รับบริการผู้ใช้งานอื่นๆ ทั่วไปที่โรงพยาบาลเมืองจันทร์อนุญาตให้ใช้เครือข่ายคอมพิวเตอร์ของโรงพยาบาลเมืองจันทร์ได้

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลเมืองจันทร์ หรือหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน หรือผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

“ผู้บริหาร” หมายความว่า ผู้อำนวยการโรงพยาบาลเมืองจันทร์

“แผนผังระบบเครือข่าย (Network Diagram)” หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

“ไฟร์วอลล์ (Firewall)” หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูล และทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์ ซอฟต์แวร์ในการรักษาความปลอดภัย

“แม็ค แอดเดรส MAC Address (Media Access Control Address)” หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และระเบียบปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

“ระบบแลน LAN (Local Area Network)” และ **“ระบบอินทราเน็ต (Intranet)”** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

“รหัสผ่าน (Password)” หมายความว่า ตัวอักษร อักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“เลขที่อยู่ไอพี (IP Address)” หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข 4 ส่วนหรือ 6 ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

“ลงบันทึกเข้า (Login)” หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (username) และรหัสผ่าน (password) ให้ถูกต้อง

“ลงบันทึกออก (Logout)” หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

“วี พี เอ็น VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะ แล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“เว็บเซอร์ฟเวอร์ (Web Server)” หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บเพจต่างๆ

“ศูนย์ฯ” หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษาพัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และระบบเครือข่าย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“สารสนเทศ (Information)” หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลเมืองจันทร์

“สินทรัพย์” หมายความว่า ข้อมูล ระบบข้อมูล สินทรัพย์ด้านเทคโนโลยีสารสนเทศ และการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ซอฟต์แวร์โปรแกรมประยุกต์ที่หน่วยงานพัฒนาขึ้น รวมทั้งสิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

“สื่อบันทึกพกพา” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Thumb Drive หรือ External Hard disk เป็นต้น

“หน่วยงาน” หมายความว่า โรงพยาบาลเมืองจันทร์

“หน่วยงานภายนอก” หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“อัพเดท (Update)” หมายความว่า ปรับให้เป็นปัจจุบัน ปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

“อุปกรณ์จัดเส้นทาง (Router)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“เอสเอสไอดี SSID (Service Set Identifier) ” หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่

ส่วนที่ 1

นโยบาย/ระเบียบปฏิบัติการควบคุมการเข้าถึงการใช้งานระบบสารสนเทศและการสื่อสาร

สารสนเทศสำนักงาน ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานของหน่วยงาน จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ทีมดูแลระบบสารสนเทศได้ตระหนักถึงความสำคัญของ ระบบฐานข้อมูลและสารสนเทศของหน่วยงาน ซึ่งอาจมีปัจจัยจากภายนอก และปัจจัยภายในมากระทบให้ข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้ จึงมีการกำหนดนโยบาย/ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดังต่อไปนี้

1.1 โรงพยาบาลเมืองจันทร์ ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางอินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งกฎหมาย ประกอบอื่นๆ ที่เกี่ยวข้อง

1.2 โรงพยาบาลเมืองจันทร์ ไม่สนับสนุนหรือยินยอมให้เจ้าหน้าที่ของโรงพยาบาลเมืองจันทร์กระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

1.3 ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายถือเป็นทรัพย์สินของโรงพยาบาลเมืองจันทร์ ห้ามผู้ไม่ได้รับการอนุญาตหรือผู้ที่ไม่เกี่ยวข้องใช้งานโดยมิได้รับอนุญาต หากผู้ใดกระทำการใดๆ เป็นการบุกรุกเขตหวงห้ามหรือพยายามบุกรุก เข้าสู่ระบบเครือข่าย ถือเป็นการละเมิดตามกฎหมาย ต้องได้รับโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ. 2560 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ทั้งกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

1.4 สิทธิในการเข้าถึงการใช้สารสนเทศ เป็นไปตามบทบาทหน้าที่ที่เกี่ยวข้องหรือได้รับมอบหมายจากผู้บังคับบัญชา ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องกับสารสนเทศส่วนที่ไม่เกี่ยวข้องกับตนเข้าใช้งาน

1.5 การยืมทรัพย์สินสารสนเทศจะต้องทำตามขั้นตอนการยืมและเมื่อสิ้นสุดการใช้งานหรือสิ้นสุดสัญญาหรือสิ้นสุดข้อตกลงการจ้าง จะต้องคืนทรัพย์สินตามขั้นตอนการคืนทรัพย์สิน

1.6 การทำลายอุปกรณ์หรือสื่อบันทึกข้อมูลสารสนเทศ ต้องทำตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ.2561

1.7 เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สำคัญของโรงพยาบาลเมืองจันทร์ จะต้องมีการกำหนดรหัสผ่าน (Password) ที่มีความยาวอย่างน้อย 6 ตัวอักษรและต้องมีอักขระปนเพื่อควบคุมการเข้าถึงและเพื่อป้องกันการเข้าถึงข้อมูลสำนักงานโดยไม่ได้รับอนุญาต

1. วัตถุประสงค์

เพื่อให้ผู้รับผิดชอบ และผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานได้รับรู้เข้าใจ นโยบายในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของโรงพยาบาลเมืองจันทร์ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

2. ผู้รับผิดชอบ

2.1 ผู้บังคับบัญชา

2.2 ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

2.2.1 ผู้ดูแลระบบเครือข่าย (System Network)

2.2.2 ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

2.2.3 ผู้ดูแลระบบ (System Administrator)

2.2.4 ผู้พัฒนาระบบ (System Developer)

2.2.5 ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

2.2.6 เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

2.3 เจ้าหน้าที่ประจำโครงการของหน่วยงาน

2.4 ผู้ใช้งาน

3. แนวนโยบาย/ระเบียบปฏิบัติ

โรงพยาบาลเมืองจันทร์มีแนวนโยบาย/ระเบียบปฏิบัติด้านต่าง ๆ ดังต่อไปนี้

3.1 การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

3.1.1 แนวนโยบาย

(1) ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(2) มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(3) มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

(4) มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งาน ให้ตรงตามความรับผิดชอบโดยสามารถตรวจสอบสิทธิได้

(5) การเข้าถึงระบบด้วยการ Remote User ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบจากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโรงพยาบาลเมืองจันทร์ เท่านั้น

(6) ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆ ในทางที่ผิดตามประกาศของโรงพยาบาลเมืองจันทร์

(7) การควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานได้จัดแบ่งประเภทของข้อมูลออกเป็นสองประเภท คือ

(7.1) ข้อมูลสารสนเทศด้านการบริหารราชการ ได้แก่ ข้อมูลการบริหารทรัพยากร

บุคคล ข้อมูล ข้อมูลนโยบายและแผน ข้อมูลตรวจสอบ

(7.2) ข้อมูลสารสนเทศด้านการสนับสนุน ได้แก่ ข้อมูลงานสารบรรณ ข้อมูลข่าวสารประชาสัมพันธ์ กฎหมาย ระเบียบ ประกาศ สถิติ

(8) ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบสารสนเทศ นั้น ๆ ด้วย

(9) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(10) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(10.1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

(10.2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

(10.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์ อักษร และได้รับการพิจารณาอนุญาตจากผู้บริหาร ผู้บังคับบัญชา หรือผู้ดูแลระบบที่ได้รับมอบหมาย

3.1.2 ระเบียบปฏิบัติ

หน่วยงานได้กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ การจัดแบ่งระดับการเข้าถึงข้อมูล สิทธิ เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

(1) การจัดแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

(2) การจัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ ระดับความสำคัญมากที่สุด ระดับความสำคัญปานกลาง ระดับความสำคัญน้อย

(3) การจัดแบ่งลำดับขั้นความลับของข้อมูล ได้แก่

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความ

เสียหาย

- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(4) การจัดแบ่งระดับขั้นการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ได้แก่

- ระดับขั้นสำหรับผู้บริหาร หมายความว่า ผู้อำนวยการโรงพยาบาลเมืองจันทร์
- ระดับขั้นสำหรับผู้ใช้งานทั่วไป หมายความว่า บุคลากรในโรงพยาบาลเมืองจันทร์
- ระดับขั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบดูแลในระบบงานนั้นๆ

(5) การกำหนดเวลาที่สามารถเข้าถึงได้ ตลอดเวลา 24 ชั่วโมง 7 วัน

(6) การกำหนดช่องทางการเข้าถึง ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากหน่วยงาน โดยมีการกำหนดบัญชีผู้ใช้งานตามระดับการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูล และสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายอินเตอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(7) กำหนดเงื่อนไขในการระงับหรือยกเลิกสิทธิของผู้ใช้งานในการใช้งานระบบสารสนเทศในแต่ละประเภทของข้อมูล

(8) ผู้ดูแลระบบต้องมีการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยของโรงพยาบาลเมืองจันทร์

3.1.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(2.2) ผู้ดูแลระบบ (System Administrator)

(2.3) ผู้พัฒนาระบบ (System Developer)

(2.4) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(3) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

3.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.2.1 แนวนโยบาย

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตจากหน่วยงานเจ้าของระบบและได้ผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลเมืองจันทร์ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต จะต้องประกอบด้วย

(1) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (user access) ประกอบด้วย

(1.1) มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

(1.2) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (user registration) ประกอบด้วย

(2.1) ต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานระบบตามความเหมาะสมในแต่ละระบบงาน ที่ได้รับอยู่ในความรับผิดชอบของโรงพยาบาลเมืองจันทร์

(2.2) ต้องจัดทำบัญชีผู้ใช้งานระบบ อย่างน้อยต้องประกอบด้วย

- รายชื่อผู้ขออนุญาตเข้าใช้งานระบบ
- รายชื่อผู้ได้รับการอนุมัติเข้าใช้งานระบบ
- กำหนดสิทธิการเข้าใช้งานข้อมูล
- ผู้อนุมัติ หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานระบบ

(2.3) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชา หรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

(2.4) ต้องกำหนดหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(2.5) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบหรือความต้องการของโรงพยาบาลเมืองจันทร์

(3) การบริหารจัดการสิทธิของผู้ใช้งาน ประกอบด้วย

(3.1) มีการแสดงรายละเอียดที่เกี่ยวกับการควบคุม และจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ซึ่งหมายรวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงข้อมูลสารสนเทศ

(3.2) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

(3.3) ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่าย ระบบงาน และระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน ประกอบด้วย

(4.1) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัยอย่างรัดกุม

(4.2) มีการกำหนดให้เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น และไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

(4.3) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(4.4) ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผล

ต่อความปลอดภัยของระบบ

(4.5) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิด จะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2440

(4.6) มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

(4.7) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

(5) การทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน ประกอบด้วย

(5.1) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอ โดยผู้ดูแลระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง เป็นต้น

(5.2) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในหน่วยงาน

(5.3) การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(5.4) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

3.2.2 ระเบียบปฏิบัติ

(1) การลงทะเบียนผู้ใช้งาน (user registration) มีดังนี้

(1.1) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ

(1.2) อบรมหรือจัดทำคู่มือการใช้งานระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบสารสนเทศทราบ

(1.3) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบงานสารสนเทศลงในแบบฟอร์มและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(1.4) ผู้บังคับบัญชา หรือผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายพิจารณาคำขอลงทะเบียนอนุมัติกำหนดระดับการเข้าใช้งาน สารสนเทศเท่าที่จำเป็นในแต่ละระบบงาน และทำการบันทึกจัดเก็บข้อมูล การขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(1.5) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล และไม่ซ้ำซ้อนกัน

(1.6) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(1.7) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(1.8) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

หรือความต้องการของโรงพยาบาลเมืองจันทร์ให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(1.9) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(1.10) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งาน แต่ละรายในระบบเมื่อได้รับรายงาน บัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่ง หรือย้ายหน่วยงาน

(2) การบริหารจัดการสิทธิของผู้ใช้งาน ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการดังนี้

(2.1) ผู้ดูแลระบบแสดงกระบวนการในการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(2.2) ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งานระบบเท่านั้น

(2.3) ผู้บังคับบัญชามอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบ หรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้

(2.4) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(2.5) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจหน้าที่ หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(2.6) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

(3) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน มีดังนี้

(3.1) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ 6 ตัว (ต้องมีตัวอักษรภาษาอังกฤษ ตัวพิมพ์ใหญ่ และตัวเลข ผสมกัน)

(3.2) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ตัวเลขเรียง 0-9 เบอร์โทรศัพท์ ชื่อบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(3.3) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(3.4) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(3.5) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยง การใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(3.6) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(3.7) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(3.8) ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

(3.9) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้

ถูกต้องก่อนที่ จะอนุญาตให้เปลี่ยนรหัสใหม่

(3.10) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(3.11) ไม่อนุญาตให้เจ้าหน้าที่ หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

(3.12) ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(4) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน มีดังนี้

(4.1) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

(4.2) ปรับปรุงบัญชีผู้ใช้งาน และบันทึกการเปลี่ยนแปลงสิทธิบัญชีผู้ใช้งาน

(4.3) การทบทวนสิทธิการเข้าใช้งานในกรณีไม่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ที่ไม่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ หรือผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับ ว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(4.4) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

3.2.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(2.2) ผู้ดูแลระบบ (System Administrator)

(2.3) ผู้พัฒนาระบบ (System Developer)

(2.4) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(3) ผู้ใช้งาน

3.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

3.3.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานทุกคนในโรงพยาบาลเมืองจันทร์ และผู้ดูแลระบบครอบคลุมเรื่องต่าง ๆ ดังนี้

(1) ต้องกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อกำหนดแนวทางในการป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงระบบและอุปกรณ์ต่าง ๆ ของหน่วยงานในขณะที่ไม่มีผู้ดูแลควรมี ดังนี้

(2.1) มีมาตรการป้องกันดูแลอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(2.2) สร้างให้ทุกคนต้องตระหนัก และเอาใจใส่ต่อการป้องกัน และดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหาย สูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(2.3) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้งเสมอ

(2.4) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอ หลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(2.5) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่มีการดูแลชั่วคราว

(2.6) ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบ หรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศ

(3) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ ควรมีดังนี้

(3.1) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของโรงพยาบาลเมืองจันทร์ ผู้ใช้งานมีหน้าที่ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้อง ให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

(3.2) ห้ามไม่ให้เคลื่อนย้าย เปลี่ยนแปลง แก้ไข เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่อยู่ภายใต้การดูแลของโรงพยาบาลเมืองจันทร์ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

(3.3) เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช่ของโรงพยาบาลเมืองจันทร์ หากมีความจำเป็นต้องใช้งาน ให้แจ้งเจ้าหน้าที่สารสนเทศและใช้ชื่อผู้ใช้ (User ID) และรหัสผ่าน (Password) ของเจ้าของเครื่อง

(3.4) ห้ามติดตั้ง อัพเดทระบบปฏิบัติการ และโปรแกรมป้องกันไวรัส หรือชุดคำสั่งไม่พึงประสงค์ใดลงบนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลโรงพยาบาลเมืองจันทร์ โดยไม่ได้รับอนุญาตหากมีความจำเป็นจะต้องแจ้งเจ้าหน้าผู้รับผิดชอบสนเทศ

(3.5) เมื่อใช้งานคอมพิวเตอร์เสร็จแล้วให้ทำการปิดเครื่องปิดหน้าจอและเครื่องทุกครั้ง

(3.6) เมื่อพบปัญหาหรือมีข้อสงสัยในการใช้งานด้านฮาร์ดแวร์/ซอฟแวร์ ให้ติดต่อแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

(3.7) เครื่องคอมพิวเตอร์สำนักงานฯ จะต้องมีการกำหนดหมายเลขไอพีแอดเดรส โดยเจ้าหน้าผู้รับผิดชอบสารสนเทศ หากมีเหตุขัดข้องให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ ยกเว้นที่ใช้งานระบบเครือข่ายไร้สาย

(3.8) มีมาตรการการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศจากผู้ไม่มีส่วนเกี่ยวข้อง

(3.9) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึกข้อมูลเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้มีความเหมาะสม ไม่ให้ได้รับความเสี่ยง

(3.10) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์ ระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

(3.11) บุคลากรของโรงพยาบาลเมืองจันทร์ทุกคน อนุญาตให้เข้าใช้พื้นที่ และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(3.12) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.13) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.14) ต้องจัดเก็บบันทึกเหตุการณ์ การเข้า-ออก พื้นที่ของโรงพยาบาลเมืองจันทร์ อย่างสม่ำเสมอ

(3.15) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(3.16) บุคคลภายนอกหรือเจ้าหน้าที่บริษัท ที่เกี่ยวข้องกับโครงการต่างๆ ของโรงพยาบาลเมืองจันทร์ จะต้องขออนุญาตเพื่อเข้าใช้พื้นที่ และใช้อุปกรณ์ต่าง ๆ ของโรงพยาบาลเมืองจันทร์ และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหาร หรือผู้ที่ได้รับมอบอำนาจก่อนเข้าพื้นที่เท่านั้น

(3.17) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น ชื่อผู้ใช้งานและรหัสผ่าน

(3.18) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(4) ข้อมูลสารสนเทศใดที่เป็นความลับ ผู้ดูแลระบบอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2444

(5) กำหนดให้ต้องบันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลา อย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

3.3.2 ระเบียบปฏิบัติ

(1) วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password use) มีข้อปฏิบัติ ดังนี้

(1.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(1.2) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ 6 ตัว (ต้องมีตัวอักษรภาษาอังกฤษ ตัวพิมพ์ใหญ่ และตัวเลข ผสมกัน)

(1.3) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ตัวเลขเรียง 0-9 เบอร์โทรศัพท์ ชื่อบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(1.4) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(1.5) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(1.6) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(1.7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(1.8) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(1.9) ต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอทุก 3 ถึง 6 เดือน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(1.10) หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน หรือรหัสผ่านเดิมสำหรับระบบงานอื่นๆ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ มีข้อปฏิบัติ ดังนี้

(2.1) ผู้ดูแลระบบ หรือผู้รับผิดชอบกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ระบบคอมพิวเตอร์ และระบบสารสนเทศที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึง โดยไม่ได้รับอนุญาต

(2.2) สร้างให้ทุกคนต้องตระหนัก และเอาใจใส่ต่อการป้องกัน และดูแลอุปกรณ์คอมพิวเตอร์ และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(2.3) เจ้าพนักงานเครื่องคอมพิวเตอร์ หรือผู้รับผิดชอบจะต้องมีมาตรการป้องกันระบบคอมพิวเตอร์และอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(2.4) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(2.5) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอ หลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(2.6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดย ไม่ได้ดูแลชั่วคราว

(3) การควบคุมทรัพย์สินและการใช้งานระบบ มีข้อปฏิบัติ ดังนี้

(3.1) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(3.2) บุคลากรของโรงพยาบาลเมืองจันทร์ทุกคน อนุญาตให้เข้าใช้พื้นที่ และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(3.3) บุคลากรจะต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.4) ต้องบำรุงรักษาการบันทึกเหตุการณ์ และการตรวจสอบระบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.5) ต้องจัดเก็บบันทึกเหตุการณ์ การเข้า-ออก พื้นที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

(3.6) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(3.7) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของโรงพยาบาลเมืองจันทร์จะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมายอำนาจ ก่อนเข้าพื้นที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

(3.8) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(3.9) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับ

ระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(3.10) ผู้ดูแลระบบ หรือผู้รับผิดชอบจัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งระบุผู้รับผิดชอบเมื่อต้องให้บริการระบบเครือข่ายคอมพิวเตอร์

(3.11) ผู้ใช้งานระบบและเครื่องคอมพิวเตอร์ ต้องลงทะเบียนการใช้งานทุกครั้งเพื่อเป็นการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง

(3.12) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ต้องกำหนดมาตรการการป้องกัน ดังนี้

- ให้ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ต้องลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทั้งโดยไม่มีผู้ดูแล
- ต้องจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอทุกครั้งเมื่อไม่ได้ใช้งาน

(3.13) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการ รักษาความลับทางราชการ พ.ศ. 2544 โดยผู้ใช้งานต้องทำการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

3.3.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบเครือข่าย (System Network)

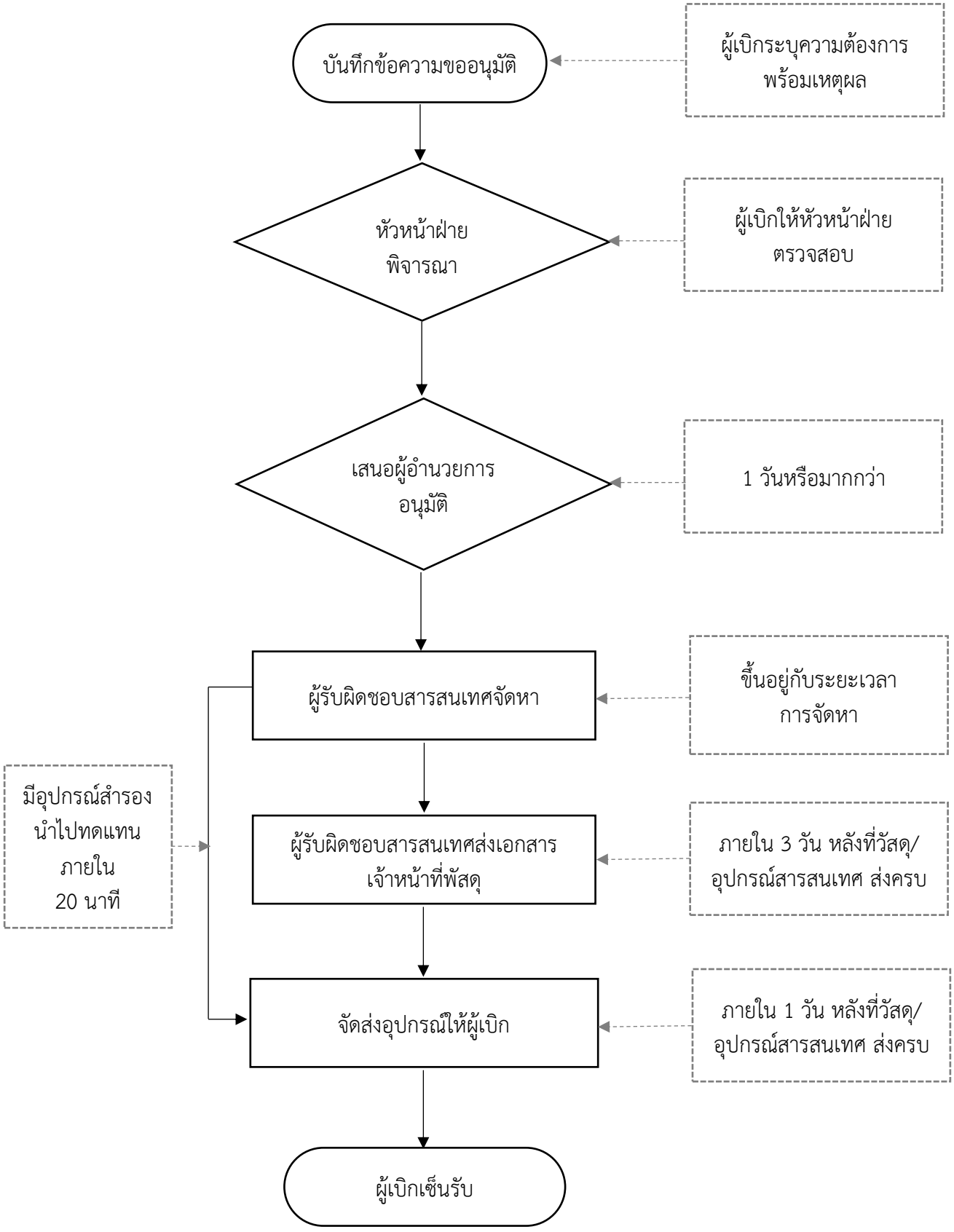
(2.2) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(2.3) ผู้ดูแลระบบ (System Administrator)

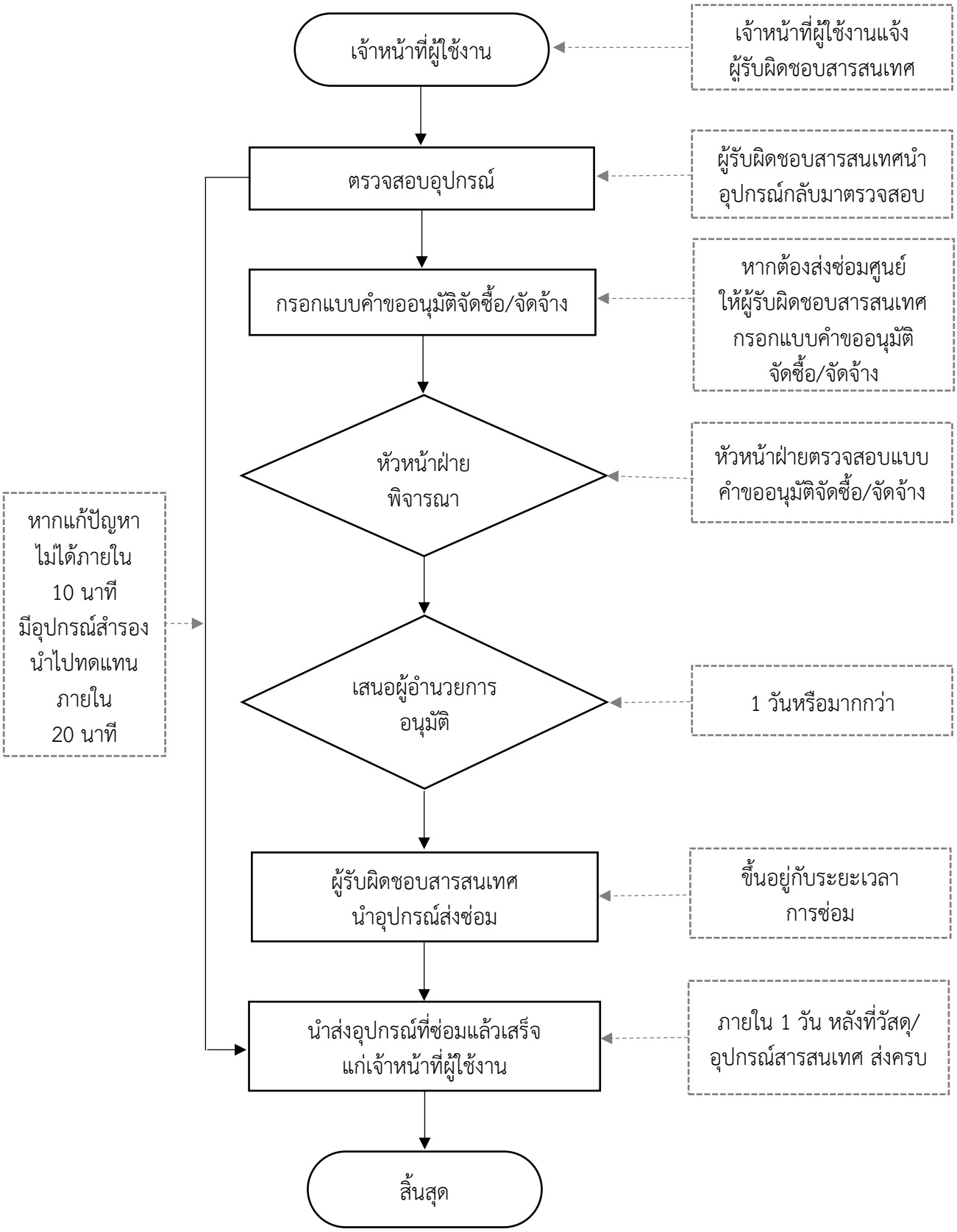
(2.4) เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

(3) ผู้ใช้งาน

3.4. Flowchart ขั้นตอนการเบิก วัสดุ/อุปกรณ์สารสนเทศ



3.5. Flowchart ขั้นตอนการขอส่งซ่อมวัสดุ/อุปกรณ์สารสนเทศ



3.6 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

3.6.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต ประกอบด้วย

(1) การกำหนดขอบเขตและสิทธิของผู้ใช้งานสามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานกำหนดเท่านั้น

(2) การกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(3) มีการทบทวนสิทธิการเข้าถึงบริการระบบเครือข่าย อย่างน้อยปีละ 1 ครั้ง และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานผู้รับผิดชอบเท่านั้น

(4) มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องมีกระบวนการในการยืนยันตัวบุคคล ก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้

(5) มีวิธีการระบุอุปกรณ์บนเครือข่าย เพื่อใช้ในการตรวจสอบการเข้าถึงอุปกรณ์บนระบบเครือข่ายของหน่วยงาน

(6) มีการกำหนดหลักเกณฑ์ในการควบคุมและการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(7) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่ายการตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึง ทางกายภาพและการเข้าถึงทางเครือข่าย

(8) ทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน

(9) มีการควบคุมการเชื่อมโยงเครือข่ายของหน่วยงานที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างกันให้มีความสอดคล้องกับหน่วยงาน

(10) มีการควบคุมการจัดเส้นทางบนเครือข่ายที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย

(11) มีการกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน

3.6.2 ระเบียบปฏิบัติ

(1) โรงพยาบาลเมืองจันทร์ จะจัดให้มีชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ให้กับเจ้าหน้าที่ ผู้มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ต เป็นรายบุคคล ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

(2) รหัสผ่านของพนักงานถือเป็นทรัพย์สินโรงพยาบาลเมืองจันทร์ ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และเจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด โรงพยาบาลเมืองจันทร์ ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน หากมีการใช้งาน ผู้ใช้ (User) และรหัสผ่าน (Password) ผู้เป็นเจ้าของมีหน้าที่ รับผิดชอบหากมีการกระทำผิด

(3) บุคคลผู้มีสิทธิใช้ข้อมูลอินเตอร์เน็ต ได้แก่ เจ้าหน้าที่โรงพยาบาลเมืองจันทร์

(4) การตั้งรหัสเข้าถึงข้อมูลอินเตอร์เน็ต จะต้องมีรหัสในการใช้งานที่มีความยาวอย่างน้อย 6 ตัวอักษรและต้องมีอักขระปน ที่ออกโดยโรงพยาบาลเมืองจันทร์

(5) การเพิ่มแก้ไขข้อมูลรหัสในการใช้งาน การเข้าใช้จะต้องแจ้งให้กับเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

(6) บุคคลภายนอกหากต้องการใช้งานอินเตอร์เน็ต จะต้องลงทะเบียนและแจ้งกับเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

(7) หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับเจ้าหน้าที่สารสนเทศเพื่อขอเลิกใช้งาน

(8) ผู้ดูแลระบบเครือข่ายจัดทำบันทึกการกำหนดขอบเขตและสิทธิของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

(9) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(10) ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (interne) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบ จากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อย ปีละ 1 ครั้ง

(11) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่าย ของหน่วยงานได้ ดังนี้

(11.1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

(11.2) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ในการเข้าใช้งาน ต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

(11.3) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

(12) การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(12.1) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน จึงจะสามารถดำเนินการได้

(12.2) ผู้ดูแลระบบเครือข่าย มีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(12.3) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

(13) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบ ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย ดังนี้

(13.1) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบ

ทั้งทางกายภาพและโดยการล๊อกอินเข้ามาใช้งาน

(13.2) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่าย ที่มีระบบควบคุมการเข้า-ออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(13.3) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(13.4) เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(13.5) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง

(13.6) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(13.7) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(13.8) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบพาเข้า

(13.9) ติดตั้งเครื่องควบคุมบันทึกการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้า-ออก และติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

(14) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบ และปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพ และการเข้าถึงทางเครือข่าย

(15) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(16) ทำการแบ่งแยกเครือข่าย สำหรับกลุ่มผู้ใช้งาน โดยแบ่ง ออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

(17) มีการควบคุมการเชื่อมโยงเครือข่ายศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับระเบียบปฏิบัติอย่างน้อย ดังนี้

(17.1) การจำกัดสิทธิการเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(17.2) มีระบบการตรวจจับผู้บุกรุกในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(17.3) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(17.4) การเข้าเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(17.5) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(17.6) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(18) มีการควบคุมการจัดเส้นทางบนเครือข่าย ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

(18.1) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

(18.2) กำหนดใหม่การแปลงหมายเลขเครือข่ายย่อย

(18.3) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

(19) ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศ และเครือข่ายของหน่วยงาน ที่ต้องผ่านการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน และต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบ เป็นลายลักษณ์อักษรเท่านั้น และผู้ใช้งานจะต้องปฏิบัติ ตามข้อกำหนดของหน่วยงานอย่างเคร่งครัด โดยดำเนินการ ดังนี้

(19.1) ผู้ดูแลระบบเครือข่ายต้องไม่เปิด port และ modem ทิ้งเอาไว้โดยไม่จำเป็น

(19.2) ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็น เท่านั้น

(19.3) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

(19.4) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (remote access) ต้องได้รับการอนุมัติจากผู้อำนวยการ ผู้บังคับบัญชา หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

3.6.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

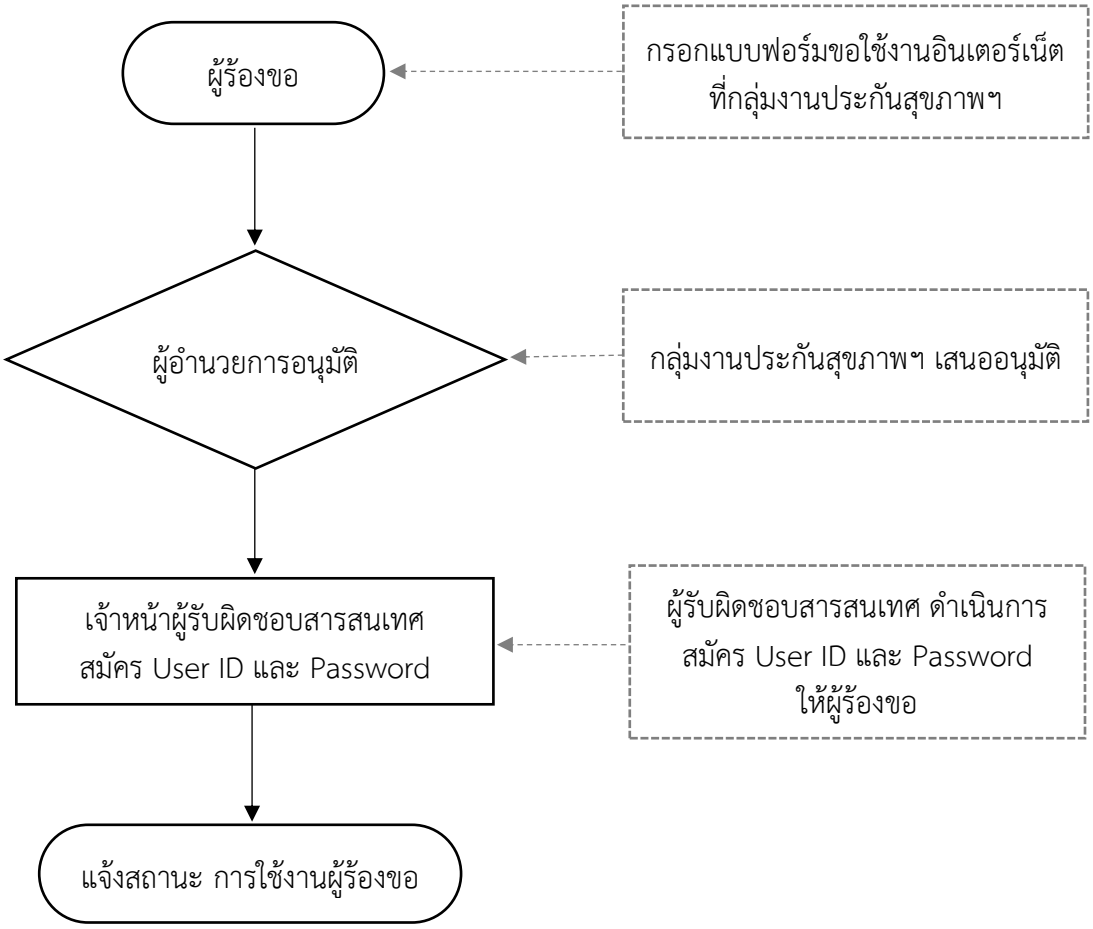
(2.1) ผู้ดูแลระบบเครือข่าย (System Network)

(2.2) ผู้ดูแลระบบ (System Administrator)

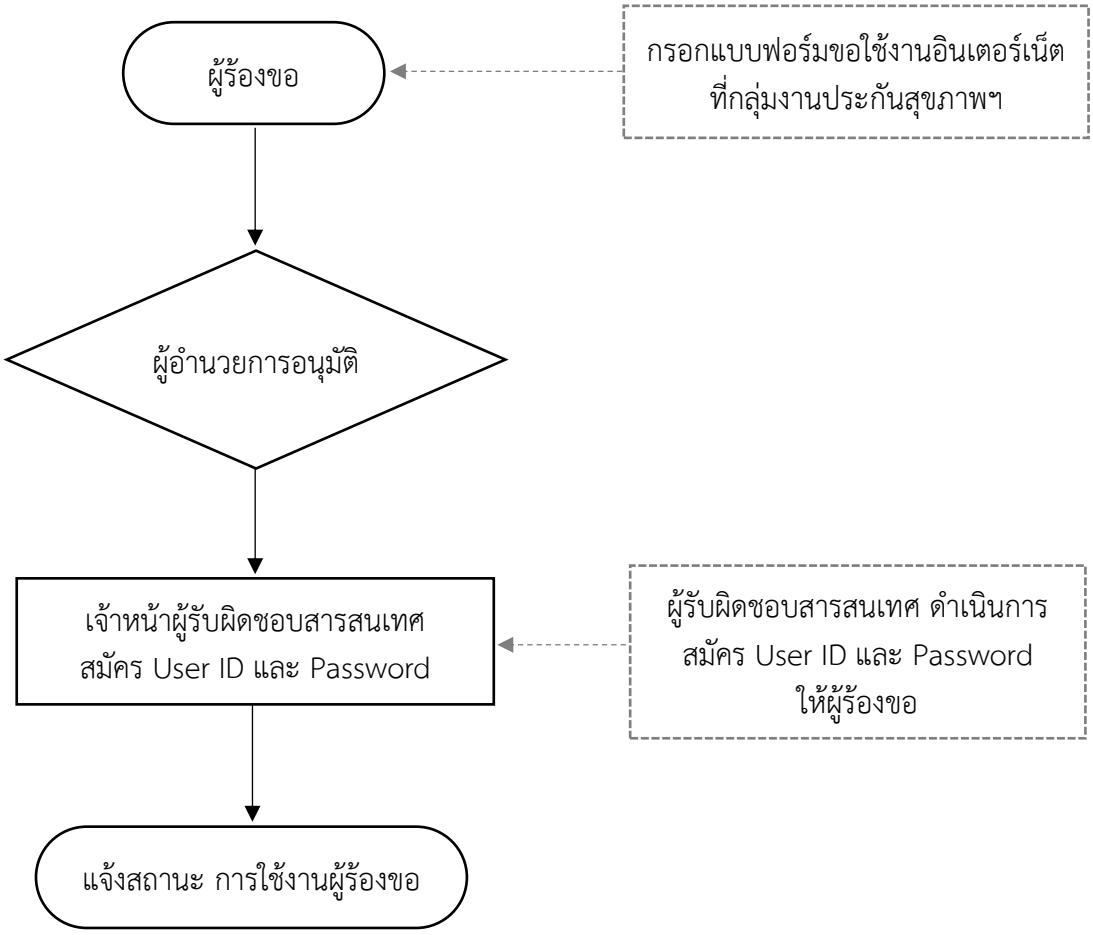
(2.3) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(3) ผู้ใช้งาน

3.7 Flowchart ขั้นตอนการขอใช้งานอินเตอร์เน็ตสำหรับบุคลากร



3.8 Flowchart ขั้นตอนการขอใช้งานอินเตอร์เน็ต สำหรับบุคคลภายนอก



3.9 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

3.9.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ควรดำเนินการดังนี้

(1) การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุมโดยการยืนยันตัวตนตามระบบรักษาความมั่นคงปลอดภัยของหน่วยงาน

(2) การระบุและยืนยันตัวตนของผู้ใช้งานต้องกำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้

(3) การระบุและยืนยันตัวตนของผู้ใช้งานสามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติมได้ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(4) การบริหารจัดการรหัสผ่านมีการแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้วให้ยกเลิกบัญชีผู้ใช้งานหรือรหัสผ่าน ที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(5) มีการจำกัดการใช้งานโปรแกรมอรรถประโยชน์ สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความ มั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้

(6) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(7) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

3.9.2 ระเบียบปฏิบัติ

(1) ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการเพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(2) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(2.1) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(2.2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(2.3) จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

(2.4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(3) การระบุและยืนยันตัวตนของผู้ใช้งาน กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้ ดังนี้

(3.1) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(3.2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นของหน่วยงานทางด้านเทคนิค

(3.3) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของหน่วยงานได้

(4) การบริหารจัดการรหัสผ่าน ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ หรือต้องทำงานในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(5) ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ ให้ดำเนินการ ดังนี้

(5.1) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติ และยังไม่ผ่านการตรวจสอบ

(5.2) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(5.3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ล้าไม่ต้องใช้งานเป็นประจำ

(5.4) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(5.5) กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(6) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 14 นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา 10 นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(7) ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(8) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(9) กำหนดระยะเวลาในการจำกัดการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลา 2 ชั่วโมง ต่อการเชื่อมต่อ 1 ครั้ง

3.9.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(2.2) ผู้ดูแลระบบ (System Administrator)

(2.3) ผู้พัฒนาระบบ (System Developer)

(2.4) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

3.10 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

3.10.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ดำเนินการดังนี้

(1) กำหนดมาตรการการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(2) การจำกัดการเข้าถึงสารสนเทศ ต้องจำกัดหรือ ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานใน การเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(3) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะได้รับการแยกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

(4) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

3.10.2 ระเบียบปฏิบัติ

(1) การจำกัดการเข้าถึงสารสนเทศ ต้องดำเนินการ ดังนี้

(1.1) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมออย่างน้อย ปีละ 1 ครั้ง

(1.2) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา 15 นาที ต้องทำการยุติการใช้งานทันที

(1.3) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทขั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทขั้นความลับ ดังนี้

- กำหนดสิทธิให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับขั้น
- กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- การนำอุปกรณ์คอมพิวเตอร์ หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

(1.4) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิ และอนุญาตในการเข้าดำเนินการและจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(2) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(2.1) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องแยกระบบซึ่งไวต่อการ

รบกวนดังกล่าวออกจากระบบอื่นๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่น ซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องเครื่องคอมพิวเตอร์แม่ข่ายกลาง ที่มีสภาพแวดล้อมเหมาะสม

(2.2) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และอื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(2.3) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

(2.4) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน ที่เกี่ยวข้องกับระบบดังกล่าว

(3) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

(3.1) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามระเบียบปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(3.2) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ ทีจะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในสำนักงาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามระเบียบปฏิบัติการควบคุมการเข้าถึง

(3.3) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัว หรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

(3.4) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

3.10.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

(2.2) ผู้ดูแลระบบ (System Administrator)

(2.3) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

3.11 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

3.11.1 แนวนโยบาย

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่ เข้ามาใช้งาน ในระบบเครือข่ายไร้สาย เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

3.11.2 ระเบียบปฏิบัติ

(1) การใช้งานเครือข่ายไร้สาย (Wireless Policy)

(1.1) โรงพยาบาลเมืองจันทร์ จะจัดให้มีชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ให้กับเจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ต เป็นรายบุคคล ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

(1.2) รหัสผ่านของพนักงานถือเป็นทรัพย์สินโรงพยาบาลเมืองจันทร์ ไม่อนุญาตให้มีการแจ้งรหัสผ่าน ที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และเจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด โรงพยาบาลเมืองจันทร์ ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน หากมีการใช้งาน ผู้ใช้ (User) และรหัสผ่าน (Password) ผู้เป็นเจ้าของมีหน้าที่ รับผิดชอบหากมีการกระทำผิด

(1.3) บุคคลผู้มีสิทธิใช้ข้อมูลเครือข่ายไร้สาย ได้แก่ เจ้าหน้าที่โรงพยาบาลเมืองจันทร์ และบุคคลภายนอกที่มีชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ที่โรงพยาบาลเมืองจันทร์ออกให้

(1.4) การตั้งรหัสเข้าถึงข้อมูลเครือข่ายไร้สาย จะต้องมีรหัสในการใช้งานที่มีความยาวอย่างน้อย 6 ตัวอักษรและต้องมีอักขระปน ที่ออกโดยโรงพยาบาลเมืองจันทร์

(1.5) การเพิ่มแก้ไขข้อมูลรหัสในการใช้งาน การเข้าใช้จะต้องแจ้งให้กับเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

(1.6) บุคคลภายนอกหากต้องการใช้งานอินเตอร์เน็ตและเครือข่ายไร้สาย จะต้องลงทะเบียนและแจ้งกับเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

(1.7) หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับเจ้าหน้าที่สารสนเทศเพื่อขอเลิกใช้งาน

(1.8) การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

(1.9) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

(1.10) ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ , wireless routers, wireless USB client หรือ wireless card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้อำนวยการ ผู้บังคับบัญชา หรือผู้รับผิดชอบของหน่วยงาน

(1.11) การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้นๆ ก่อนเข้าใช้งานเครือข่ายของหน่วยงาน

(2) การใช้งานระบบไฟร์วอลล์ (Fire wall) และระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

(2.1) มีการระบุขอบเขต (Trust Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, โซนการเชื่อมต่อภายนอกเครือข่ายภายในองค์กร และโซน remote access และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

(2.2) มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มี

การเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

(2.3) มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

(2.4) มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

(3) การใช้งานเครือข่าย (Internet Security Policy)

(3.1) มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(3.2) มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.3) มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.4) มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

(3.5) จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

(4) การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่าย

(4.1) ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่ายอื่นนอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

(4.2) ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กรต้องได้รับอนุญาตจากผู้ดูแลระบบ

(5) ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

(5.1) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับ อนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(5.2) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(5.3) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(5.4) ควรทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ มาใช้งาน

3.11.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย ประกอบด้วย

(2.1) ผู้ดูแลระบบเครือข่าย (System Network)

(2.2) ผู้ดูแลระบบ (System Administrator)

(2.3) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

3.12 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsource Access Control)

3.12.1 แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก ควรประกอบด้วย

(1) บุคคลภายนอกที่ต้องการสิทธิ ในการเข้าใช้งานระบบของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อขออนุมัติจากผู้อำนวยการ ผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมาย

(2) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(3) สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษา ความพร้อมที่จะให้บริการ

(4) ผู้ให้บริการหน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบผู้ให้บริการได้อย่างเข้มงวดและให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

3.12.2 ระเบียบปฏิบัติ

(1) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและกำหนดมาตรการรองรับ หรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

(2) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการ ผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

(3) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

(3.1) เหตุผลในการขอใช้

(3.2) ระยะเวลาในการใช้

(3.3) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(3.4) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(3.5) กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล

(4) หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้อง

จัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(5) หน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(6) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษาความพร้อมที่จะให้บริการ

(7) องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(8) ต้องกำหนดให้หน่วยงานภายนอก หรือผู้ให้บริการจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของหน่วยงานภายนอก หรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

3.12.3 ผู้รับผิดชอบ

(1) ผู้บังคับบัญชา

(2) ผู้ดูแลระบบที่ได้รับมอบหมาย

(2.1) ผู้ดูแลระบบเครือข่าย (System Network)

(2.2) ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

(2.3) เจ้าหน้าที่ประจำโครงการของหน่วยงาน

ส่วนที่ 2

นโยบาย/ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

1. ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

1.1 ศูนย์กลางข้อมูลและระบบเครือข่าย ผู้ดูแลระบบเครือข่าย ผู้ดูแลข้อมูลสารสนเทศ มีหน้าที่ปฏิบัติดังนี้

1.1.1 ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งาน ได้แก่ ข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสารภายใน ระบบเครือข่ายสื่อสารภายนอก ห้องควบคุมการปฏิบัติงาน พื้นที่จัดเก็บอุปกรณ์ต่างๆ พื้นที่จัดเก็บเอกสาร สื่อบันทึก เป็นต้น จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

1.1.2 ให้ศูนย์เป็นผู้กำหนดสิทธิ และลำดับขั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสาร

1.1.3 ให้ศูนย์กำหนดมาตรการควบคุมการเข้าออกพื้นที่ของศูนย์ทั้งหมด และกำหนดพื้นที่ที่มีความเสี่ยง ห้ามมิให้บุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าถึงได้

1.1.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาเชื่อมต่อกับระบบเครือข่ายภายในหน่วยงาน จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

1.1.5 มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง เครื่องดับเพลิง ระบบปรับอากาศควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบ ระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ

1.2 การติดตั้งระบบสายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security) ผู้ดูแลระบบเครือข่าย มีหน้าที่ปฏิบัติดังนี้

1.2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

1.2.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

1.2.3 ให้เดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

1.2.4 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

1.2.5 วางแผนการใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิมกับข้อมูลที่มีความสำคัญ

1.3 การบำรุงรักษาอุปกรณ์ (Equipment maintenance) มีหน้าที่ปฏิบัติดังนี้

1.3.1 ผู้ดูแลทรัพย์สินกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่หน่วยงานกำหนด

1.3.2 ผู้ใช้งานปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่กำหนด

1.3.3 ผู้ดูแลทรัพย์สิน ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

1.3.4 ผู้ดูแลทรัพย์สิน จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ

1.4 การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property) ผู้ดูแลทรัพย์สินหรือผู้ได้รับมอบหมายจากผู้บริหาร มีหน้าที่ปฏิบัติดังนี้

1.4.1 ผู้บริหารมอบอำนาจ หรือกำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน

1.4.2 หากมีความจำเป็นต้องนำเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ของโรงพยาบาลเมืองจันทร์ ไปใช้นอกสถานที่ เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ดูแลและรักษาหากมีข้อสงสัยหรือเหตุขัดข้องให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

1.4.3 กำหนดมาตรการความปลอดภัยและผู้รับผิดชอบเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน

1.4.4 ควบคุมดูแลให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน และต้องได้รับอนุญาตจากผู้มีอำนาจ เท่านั้น

1.4.5 กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน

1.4.6 บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน พร้อมทั้งมีการบันทึกผู้รับผิดชอบในการดูแลรักษาทรัพย์สินหรืออุปกรณ์นอกพื้นที่

1.4.7 เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบจำนวนทรัพย์สินกับเอกสารการชำรุดเสียหายของทรัพย์สินด้วยทุกครั้ง

1.4.8 บุคลากรที่มีส่วนเกี่ยวข้องทุกคนต้องไม่ทิ้งอุปกรณ์ หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะโดยไม่มีผู้รับผิดชอบ

1.4.9 เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

1.5 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment) ผู้ดูแลทรัพย์สินมีหน้าที่ปฏิบัติดังนี้

1.5.1 ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

1.5.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

1.5.3 เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล ดังนี้

(1) คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ให้อยู่ในกลุ่มเอกสารลับ

(2) ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการ ดังนี้

- ประเภท Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- ประเภทกระดาษ ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ประเภทแผ่น CD/DVD ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น
- ประเภทเทป ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ประเภทฮาร์ดดิสก์ ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมตตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิม เป็นจำนวนหลายรอบ)

1.6 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศผู้ดูแลระบบ ผู้ดูแลข้อมูลและเจ้าหน้าที่ที่เกี่ยวข้อง มีหน้าที่ปฏิบัติดังนี้

1.6.1 จัดแบ่งหมวดหมู่ประเภทของเอกสารและจัดหาสถานที่จัดเก็บเอกสารที่เหมาะสม

1.6.2 จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัยตามที่กำหนด

1.6.3 ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

1.6.4 ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึง หรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

1.7 สิทธิการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (Logfile)

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ ไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลเท่าที่จำเป็นเพื่อสามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่การบริการสิ้นสุดลง ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ต้องระวางโทษปรับ ไม่เกิน 500,000 บาท มีผลบังคับใช้ในวันที่ 27 ตุลาคม 2564 โรงพยาบาลเมืองจันทร์ มีการกำหนดระเบียบและสิทธิการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ ต้องปฏิบัติดังนี้

1.7.1 โรงพยาบาลเมืองจันทร์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ 90 วัน ตามกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนด ให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

1.7.2 ข้อมูลการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นความลับและบุคคลทั่วไปไม่มีสิทธิ์ในการเข้าถึงข้อมูลยกเว้น ในทางการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) พนักงานเจ้าหน้าที่มีอำนาจด้านการสืบสวนสอบสวนเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(4) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิด และสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์

2. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

2.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ผู้ดูแลเครือข่ายและผู้ดูแลระบบ มีหน้าที่ปฏิบัติดังนี้

2.1.1 ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความ เสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

2.1.2 จัดเก็บบันทึกการติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ

2.1.3 ไม่ควรติดตั้งซอร์สโค้ด และคอมไพเลอร์ ของระบบงานในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

2.1.4 จัดเก็บซอร์สโค้ดและไลบรารี่ของซอฟต์แวร์ระบบ ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และกำหนดลำดับขั้นของสิทธิการเข้าถึงข้อมูล

2.1.5 ให้มีการระบุความต้องการทางสารสนเทศ สำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

2.1.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศให้ถูกต้องตรงตามความต้องการของระบบ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ไว้ให้บริการ

2.1.7 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

2.1.8 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

2.2 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก ผู้ดูแลระบบ และผู้ดูแลข้อมูล มีหน้าที่ปฏิบัติดังนี้

2.2.1 กำกับ ควบคุม ดูแล โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างจากภายนอก

2.2.2 ระบุชื่อผู้รับผิดชอบ หน้าที่ความรับผิดชอบ โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างให้บริการจากภายนอก

2.2.3 ให้กำหนดเรื่องลิขสิทธิ์ของซอฟต์แวร์ ซอร์สโค้ด และซอฟต์แวร์ที่ใช้ในการพัฒนาและติดตั้งต้องเป็นของหน่วยงานทั้งหมด

2.2.4 ศูนย์จัดหาสถานที่ที่ใช้ในการพัฒนาซอฟต์แวร์ในกรณีที่บริษัทผู้รับจ้างต้องเข้ามาดำเนินการพัฒนา และทดสอบซอฟต์แวร์ระบบในหน่วยงาน

2.2.5 กำหนดสิทธิการเข้าถึงอุปกรณ์และสารสนเทศเพื่อใช้ในการพัฒนาซอฟต์แวร์ให้กับบริษัทผู้รับจ้างได้เท่าที่จำเป็น

2.2.6 จัดเก็บบันทึกข้อมูลการเข้า – ออกพื้นที่ ของเจ้าหน้าที่หน่วยงานภายนอก และบันทึกการเข้าใช้งานระบบเครือข่ายของหน่วยงาน

2.2.7 ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

2.2.8 ผู้ดูแลระบบจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับจัดการช่องโหว่ของซอฟต์แวร์ระบบ ต้องมีรายละเอียดอย่างน้อย

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- หน่วยงานที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ชื่อผู้รับผิดชอบซอฟต์แวร์หรือระบบงาน

2.2.9 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

2.3 มีการบันทึกพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลดังนี้

2.3.1 ชื่อบัญชีผู้ใช้งาน

2.3.2 วันเวลาที่เข้า - ออกระบบ

2.3.3 เหตุการณ์สำคัญที่เกิดขึ้น

2.3.4 การเปลี่ยนคอนฟิเกกูเรชันของระบบ

2.3.5 แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

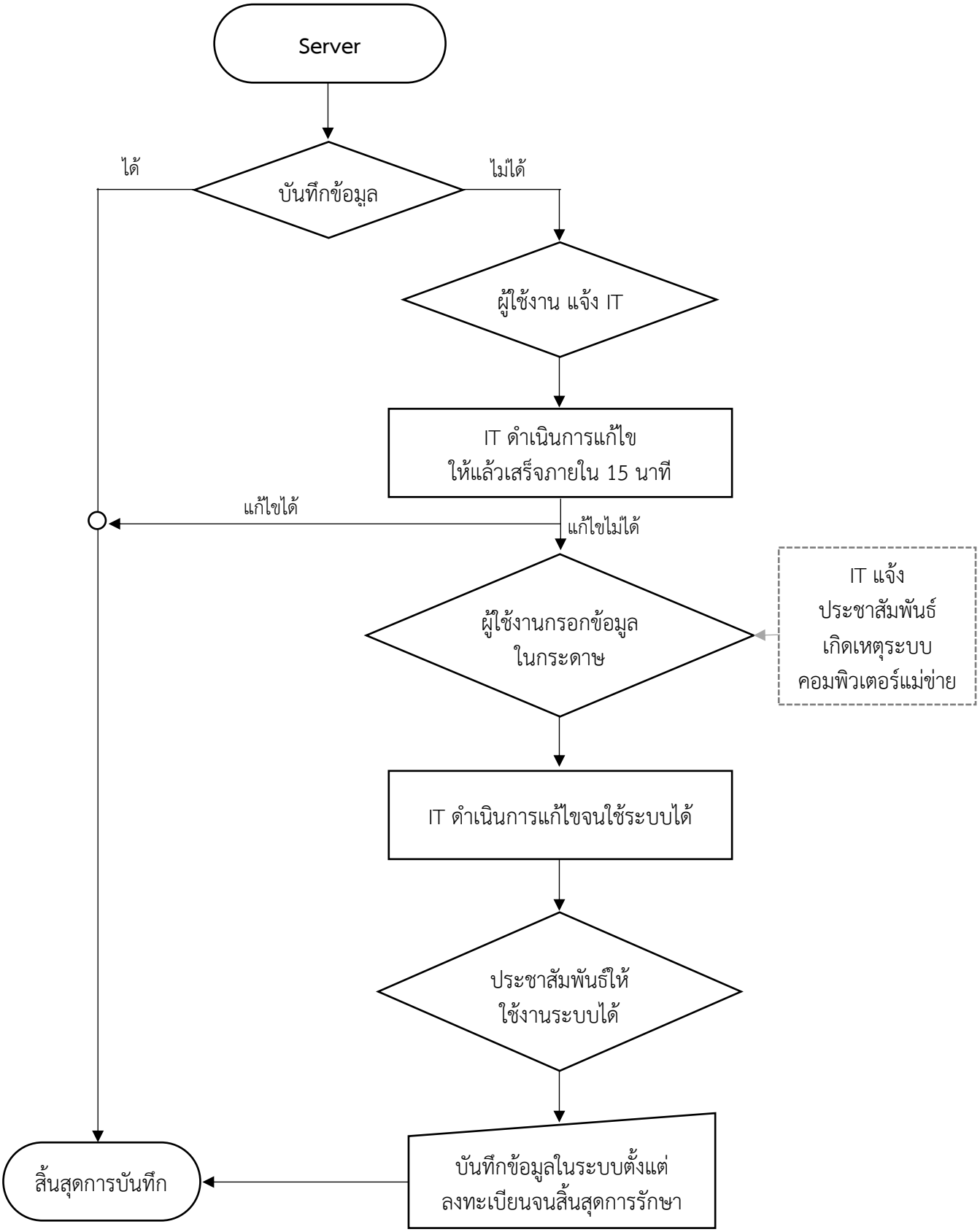
2.3.6 ไอพีแอดเดรสที่เข้าถึง

2.3.7 โพรโตคอลเครือข่ายที่ใช้

2.4 ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

2.5 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่าย และเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์การตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

3. Flowchart ขั้นตอนเมื่อเกิดเหตุระบบขัดข้อง โรงพยาบาลเมืองจันทร์



4. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์

4.1 การใช้งานทั่วไป

4.1.1 เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของโรงพยาบาลเมืองจันทร์ เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ดูแลและรักษา หากมีข้อสงสัยหรือเหตุขัดข้อง ให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

4.1.2 ห้ามไม่ให้เคลื่อนย้าย เปลี่ยนแปลง แก้ไข เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลของโรงพยาบาลเมืองจันทร์ โดยไม่ได้รับอนุญาต หากมีความจำเป็นจะต้องแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

4.1.3 หากมีความจำเป็นต้องนำเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ของโรงพยาบาลเมืองจันทร์ ไปใช้นอกสถานที่ เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ดูแลและรักษาหากมีข้อสงสัยหรือเหตุขัดข้องให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

4.1.4 เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช่ของโรงพยาบาลเมืองจันทร์ หากมีความจำเป็นต้องใช้งาน ให้แจ้งเจ้าหน้าที่สารสนเทศและใช้ชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ของเจ้าของเครื่อง

4.1.5 ห้ามติดตั้ง อัพเดทระบบปฏิบัติการ และโปรแกรมป้องกันไวรัส หรือชุดคำสั่งไม่พึงประสงค์ใดลงบนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่อยู่ภายใต้การดูแลโรงพยาบาลเมืองจันทร์ โดยไม่ได้รับอนุญาตหากมีความจำเป็นจะต้องแจ้งเจ้าหน้าผู้รับผิดชอบสนเทศ

4.1.6 เมื่อใช้งานคอมพิวเตอร์เสร็จแล้วให้ทำการปิดเครื่องปิดหน้าจอและเครื่องทุกครั้ง

4.1.7 เมื่อพบปัญหาหรือมีข้อสงสัยในการใช้งานด้านฮาร์ดแวร์/ซอฟแวร์ ให้ติดต่อแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ

4.1.8 เครื่องคอมพิวเตอร์สำนักงานฯ จะต้องมีการกำหนดหมายเลขไอพีแอดเดรส โดยเจ้าหน้าผู้รับผิดชอบสารสนเทศ หากมีเหตุขัดข้องให้รีบแจ้งเจ้าหน้าผู้รับผิดชอบสารสนเทศ ยกเว้นที่ใช้งานระบบเครือข่ายไร้สาย

4.1.9 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลและรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของหน่วยงาน

4.1.10 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

4.1.11 การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ ที่ได้รับมอบหมายให้ดูแล

4.1.12 ผู้ใช้งานจะต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงาน หรือเป็นข้อมูลส่วนบุคคล

4.1.13 ผู้ใช้งานจะต้องรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง โดยผู้ใช้งานแต่ละคนจะต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองโดยเฉพาะ ห้ามมิให้ใช้ร่วมกับผู้อื่น ห้ามมิให้ทำการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

4.1.14 ห้ามไม่ให้ผู้ใช้งานใช้โปรแกรมบางประเภท เช่น บิตทอร์เรนต์ (BitTorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาต

4.1.15 ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์

4.1.16 คอมพิวเตอร์ของผู้ใช้งานจะติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้าย ตามที่หน่วยงานได้กำหนด

4.1.17 ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในศูนย์ฯให้ตรงกันโดยให้อิงกับเวลามาตรฐานกลางของโลก เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

4.2 การใช้ตู้กระจายสัญญาณ

เนื่องจากตู้กระจายสัญญาณ ใช้สำหรับกระจายสัญญาณและนำเข้าสัญญาณเครือข่ายที่สำคัญและจัดเก็บอุปกรณ์เครือข่ายหลัก ดังนั้นเพื่อให้การเข้าใช้ตู้กระจายสัญญาณเป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัยทั้งข้อมูลและอุปกรณ์ จึงได้กำหนดสิทธิการเข้าออกห้องเซิร์ฟเวอร์ เฉพาะเจ้าหน้าผู้เกี่ยวข้องและบุคคลที่มีความจะเป็นต้องเข้าใช้ห้องเซิร์ฟเวอร์ ดังนี้

4.2.1 บุคคลผู้มีสิทธิเข้าใช้ตู้กระจายสัญญาณ ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบดูแลเครือข่ายโรงพยาบาลเมืองจันทร์

4.2.2 บุคคลภายนอกที่จะขอเข้าใช้ตู้กระจายสัญญาณ เช่น ติดตั้งและซ่อมบำรุงรักษาอุปกรณ์ต่างๆ ภายในห้องเซิร์ฟเวอร์และต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

4.2.3 วันและเวลาการใช้ตู้กระจายสัญญาณ วันและเวลาราชการที่มีการทำงานตามปกติคือ 08.00 น. –16.00 น. ยกเว้นวันหยุดราชการ

4.2.4 กรณีที่มีเหตุฉุกเฉินที่จะเข้าใช้ตู้กระจายสัญญาณ ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบสารสนเทศ

4.3 การสำรองข้อมูลและการกู้คืน

4.3.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น Usb drive, CD, DVD, External Hard Disk, ระบบคลาวด์ เป็นต้น

4.3.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

4.3.3 การสำรองข้อมูลการทำงานเบื้องต้น อื่นๆ เช่น ข้อมูลการทำงานส่วนตัว ฯลฯ เป็นหน้าที่ของเจ้าของข้อมูลนั้นๆ ในการเก็บข้อมูลสำรองผ่านอุปกรณ์การเก็บข้อมูลสำรอง เช่น Usb drive, CD, DVD, External Hard Disk, ระบบคลาวด์ เป็นต้น

4.3.4 ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

4.4 การยืม-คืน วัสดุ/อุปกรณ์สารสนเทศ

4.4.1 เจ้าหน้าที่ผู้เบิก กรอกรายละเอียด ในทะเบียนคุมการยืม-คืน วัสดุ/อุปกรณ์/ครุภัณฑ์สำนักงาน

4.4.2 ผู้รับผิดชอบสารสนเทศ เซ็นจ่าย วัสดุ/อุปกรณ์สารสนเทศ พร้อมตรวจเช็คความเรียบร้อย

4.4.3 เจ้าหน้าที่ผู้เบิก เซ็นรับ วัสดุ/อุปกรณ์สารสนเทศ พร้อมตรวจเช็คความเรียบร้อยอุปกรณ์ก่อนนำไปใช้

4.4.4 เจ้าหน้าที่ผู้เบิก นำวัสดุ/อุปกรณ์สารสนเทศ มาคืนผู้รับผิดชอบสารสนเทศ พร้อมเซ็นคืน

4.5 การเผยแพร่ข้อมูล (เว็บไซต์)

4.5.1 ผู้ใช้ร้องขอ ต้องส่งไฟล์เอกสารที่เป็นต้นฉบับ คู่กับไฟล์ .pdf เสมอ ให้เจ้าหน้าที่สารสนเทศ

4.5.2 เจ้าหน้าที่สารสนเทศ ดำเนินการลงข้อมูลบนเว็บไซต์

5. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูล แต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

5.2 เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของของสิทธิ ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.3 วิธีในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล หรือใช้การพิสูจน์ตัวตนด้วย Token Key

5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

5.5 มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

6.1 การใช้งานสำหรับผู้ใช้งาน

6.1.1 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่ผิดกฎระเบียบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

6.1.2 E-mail จะถูกเก็บเป็นความลับ ห้ามผู้ใดพยายามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิใน E-mail ดังกล่าว

6.1.3 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายลูกโซ่ ข่มขู่ ลามก อนาจาร หรือไม่สุภาพ

6.1.4 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายกระจาย โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลเมืองจันทร์

6.1.5 การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

6.1.5 หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 หรือผิดต่อกฎระเบียบของโรงพยาบาลเมืองจันทร์ ให้แจ้งต่อผู้บังคับบัญชาโดยตรงหรือผู้รับผิดชอบสารสนเทศ

6.1.5 ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (Spam e-mail)

6.2 แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (system administrator)

6.2.1 กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของผู้ใช้งาน

6.2.2 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (password) ผิดพลาดได้ไม่เกิน 5 ครั้ง

6.2.3 มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

6.2.4 มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งานที่ได้กำหนดไว้อย่างเคร่งครัด

7. การใช้งานระบบอินเทอร์เน็ต (internet)

6.1 การควบคุมการใช้งาน (Access Control Policy)

6.1.1 ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์ หรือระบบเครือข่ายของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

6.1.2 มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

6.1.3 มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

6.1.4 มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

6.1.5 การเข้าถึงระบบด้วย Remote User ต้องได้รับการอนุญาตจากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลเมืองจันทร์

6.1.6 ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆ ในทางที่ผิด

6.1.7 ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบด้วย

6.2 การใช้และการเปลี่ยนรหัสผ่าน สำหรับใช้ในการเข้าถึงฐานข้อมูลของเจ้าหน้าที่ ต้องปฏิบัติดังนี้

6.2.1 การกำหนดให้รหัสผ่านควรมีมากกว่าหรือเท่ากับ 6 ตัวอักษร (ต้องมีตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่ และตัวเลข ผสมกัน)

6.2.2 ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ตัวเลขเรียง 0-9 เบอร์โทรศัพท์ ชื่อบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

6.2.3 ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ ที่ง่ายต่อการสังเกตของบุคคลอื่น

6.2.4 ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันที สำหรับการเข้าใช้งานครั้งแรก

6.2.5 ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

6.2.6 ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

6.2.7 เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น

6.2.8 ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

6.3 การใช้งานเครือข่ายไร้สาย (Wireless Policy) ปฏิบัติดังนี้

6.3.1 การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

6.3.2 เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

6.3.3 ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็น access point, wireless routers, wireless USB client, หรือ wireless card ภายในโรงพยาบาล ยกเว้นจะได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ

6.3.4 การเข้าถึงระบบเครือข่ายไร้สาย (wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบและมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายขององค์กร

6.4 การใช้งานระบบไฟร์วอลล์ และระบบ IDS/IPS ปฏิบัติดังนี้

6.4.1 มีการระบุขอบเขตของเครือข่าย เช่น เครือข่าย Internet, web servers, remote access

โซนการเชื่อมต่อภายนอกในองค์กร และโซนภายในเครือข่าย และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

6.4.2 มีการควบคุมระบบ firewall เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

6.4.3 มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

6.4.4 มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

6.5 การใช้งานเครือข่าย (Internet Security Policy) ปฏิบัติดังนี้

6.5.1 มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

6.5.2 มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

6.5.3 มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลา พร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

6.5.4 มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

6.5.5 จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

6.6 ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่น นอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

6.7 ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

6.8 การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล หรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2440

6.9 ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

6.10 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

6.11 ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

8. การดูแลรักษาคอมพิวเตอร์และสารสนเทศ

คอมพิวเตอร์เมื่อใช้ไประยะหนึ่งจะมีการเสื่อมชำรุดไปตามสภาพระยะเวลาที่ใช้งาน ผู้ใช้คอมพิวเตอร์จึงควรเอาใจใส่ ดูแลและบำรุงรักษาอย่างเหมาะสมสม่ำเสมอเพื่อเพิ่มอายุการใช้งานของเครื่องคอมพิวเตอร์ ซึ่งจะช่วยให้สามารถประหยัดงบประมาณในการซ่อมบำรุงหรือการเปลี่ยนอุปกรณ์

8.1 วิธีการใช้งานคอมพิวเตอร์ตั้งโต๊ะและคอมพิวเตอร์พกพา เบื้องต้น

8.1.1 การเปิดเครื่องคอมพิวเตอร์

(1) เสียบปลั๊กไฟทุกเส้นที่ต่อจากเครื่องคอมพิวเตอร์

(2) กดปุ่ม Power เพื่อเปิดเครื่อง จะมีไฟติดที่เครื่องและแป้นพิมพ์

(3) เปิดสวิตช์จอภาพ จะมีตัวอักษรขึ้นบนจอภาพ และเริ่มเข้าสู่โปรแกรม

(4) ใช้เมาส์คลิกที่ปุ่ม Start จะปรากฏกลุ่มงานให้เลือกใช้
(5) ใช้เมาส์คลิกที่โปรแกรม (Programs) จะปรากฏแถบรายชื่อโปรแกรมต่าง ๆ ให้เลือก
(6) คลิกชื่อโปรแกรมที่ต้องการใช้งาน โปรแกรมงานก็จะถูกเปิดขึ้นทันที

8.1.2 การปิดเครื่องคอมพิวเตอร์
(1) คลิกที่ปุ่มปิดโปรแกรม (Close) X
(2) คลิกที่ปุ่ม Start
(3) เลือก Shut down
(4) เลือกตัวเลือกที่ต้องการ
(5) เลือกปุ่ม OK แล้วเครื่องจะถูกปิดลง
(6) ถอดปลั๊กไฟทุกเส้นที่ต่อจากเครื่องคอมพิวเตอร์

8.2 วิธีการใช้งานอุปกรณ์เก็บบันทึกข้อมูล USB Flash Drive

USB Flash Drive เป็นอุปกรณ์ที่ใช้เก็บข้อมูลที่ได้รับความนิยมอย่างมากในปัจจุบัน เนื่องจากมีความจุสูง และมีขนาดเล็กพกพาได้ง่าย ขั้นตอนการใช้งาน USB Flash Drive ดังนี้

8.2.1 เสียบอุปกรณ์ USB Flash Drive ใส่ในช่อง USB Port
8.2.2 สังเกตตรง Task Bar (ด้านมุมขวาล่างของหน้าจอ) จะมีชื่อ USB Flash Drive ที่เสียบปรากฏ
8.2.3 เมื่อเปิดไอคอน My Computer หรือ This PC จะปรากฏไดร์ฟ เพิ่มขึ้นมาให้ใช้งาน
8.2.4 หลังจากใช้งานเสร็จ ให้ทำการยกเลิกใช้งาน โดยสังเกตตรง Task Bar (ด้านมุมขวาล่างของหน้าจอ) ลากเมาส์ไปชี้ที่ไอคอนรูป Flash Drive จะมีคำว่า Safely Remove Hardware and Eject Mediaให้คลิกขวา 1 ครั้ง จะมีเมนูขึ้นมา ให้คลิกซ้ายเลือกคำสั่ง safely remove USB หรือ Eject Cruzer Blade ที่ต้องการเลิกใช้งาน
8.2.5 จะมีกล่องข้อความขึ้นมาบอกว่าตอนนี้สามารถถอดอุปกรณ์ USB Flash Drive ออกได้อย่างปลอดภัยแล้ว จึงค่อยถอดอุปกรณ์ออก

8.3 การบำรุงรักษาตัวเครื่องทั่วๆ ไป
8.3.1 เครื่องจ่ายไฟสำรอง (UPS) หากมีงบประมาณเพียงพอควรติดตั้งร่วมกับตัวเครื่องคอมพิวเตอร์ด้วย เพราะ UPS จะช่วยป้องกัน และแก้ปัญหาทางไฟฟ้าไม่ว่าจะเป็นไฟตก ไฟเกิน หรือไฟกระชากอันเป็นสาเหตุที่จะทำให้เกิดความเสียหายของข้อมูล และชิ้นส่วน อื่นๆ
8.3.2 การติดตั้งตัวเครื่องคอมพิวเตอร์ ควรติดตั้งในห้องที่มีเครื่องปรับอากาศหรือถ้ามีไม่มีเครื่องปรับอากาศ ควรเลือกห้องที่ปลอดฝุ่นมากที่สุดและการติดตั้งตัวเครื่องควรจากผนังพอสมควร เพื่อการระบายความร้อนที่ดี
8.3.3 การต่อสาย Cable ระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์ต่างๆ เช่น Printer Modem Fax หรือส่วนอื่นๆ จะต้องกระทำเมื่อ power off เท่านั้น
8.3.4 อย่าปิด – เปิดเครื่องบ่อยๆ เกินความจำเป็น เพราะจะทำให้เกิดความเสียหายแก่โปรแกรมที่กำลังทำงานอยู่
8.3.5 ไม่เคลื่อนย้ายเครื่องคอมพิวเตอร์ขณะที่เครื่องทำงานอยู่ เพราะจะทำให้อุปกรณ์บางตัวเกิดความเสียหายได้
8.3.6 อย่าเปิดฝาเครื่องขณะใช้งานอยู่ ถ้าต้องการเปิดต้อง Power off และถอดปลั๊กไฟก่อน
8.3.7 ควรศึกษาจากคู่มือก่อน หรือการอบรมการใช้งาน Software ก่อนการใช้งาน

8.3.8 ตัวภายนอกของเครื่องคอมพิวเตอร์ส่วนใหญ่เป็นส่วนประกอบของเหล็กกับพลาสติกเมื่อใช้นานๆ จะมีฝุ่นและคราบรอยนิ้วมือมาติดทำให้ดูไม่สวยงาม และถ้าปล่อยไว้นานๆ จะทำความสะอาดยาก จึงควรทำความสะอาดบ่อยๆ อย่างน้อย 1-2 เดือนต่อครั้งโดยใช้ผ้าเช็ดที่ตัวเครื่อง หรือใช้น้ำยาทำความสะอาดเครื่องคอมพิวเตอร์โดยเฉพาะ และที่สำคัญคือควรใช้ผ้าคลุมเครื่องให้เรียบร้อย หลังเลิกใช้งานทุกครั้ง เพื่อป้องกันฝุ่นผงต่างๆ

8.4 การบำรุงรักษา Hard Disk

ฮาร์ดดิสก์เป็นอุปกรณ์ที่มีอายุยืนมาก ยากจะบำรุงรักษาด้วยตัวเอง ผู้ใช้คอมพิวเตอร์จึงควรระมัดระวังไม่ให้เกิดความเสียหายซึ่งควรปฏิบัติดังต่อไปนี้

8.4.1 การติดตั้งเครื่องคอมพิวเตอร์ ควรติดตั้งเครื่องคอมพิวเตอร์โดยให้ด้านหลังของตัวเครื่องคอมพิวเตอร์ห่างจากฝาผนังไม่น้อยกว่า 3 นิ้ว เพื่อการระบายความร้อนเป็นปกติ ไม่ทำให้เครื่องร้อนได้

8.4.2 ควรเลือกใช้โต๊ะทำงานที่แข็งแรงป้องกันการโยกไปมา เพราะจะทำให้หัวอ่านของฮาร์ดดิสก์ถูกกระทบกระเทือนได้

8.4.3 ควรมีการตรวจสอบสถานภาพของ Hard Disk ด้วยโปรแกรม Utility ต่างๆว่ายังสามารถใช้งานได้ครบ 100 % หรือมีส่วนใดของ Hard Disk ที่ใช้งานไม่ได้

8.5 การบำรุงรักษา Disk Drive

ช่องอ่านดิสก์เมื่อทำงานไปนานๆ หัวอ่านแผ่นดิสก์อาจจะเสื่อมสภาพได้ หัวอ่านดิสก์เกิดความสกปรก เนื่องจากมีฝุ่นละอองเข้าไปเกาะที่หัวอ่าน หรือเกิดจากความสกปรกของแผ่นดิสก์ที่มีฝุ่นหรือคราบไขมันจากมือ ผลที่เกิดขึ้นทำให้การบันทึกหรืออ่านข้อมูลจากแผ่นดิสก์ ไม่สามารถดำเนินการได้ การดูแลรักษา Disk Drive ควรปฏิบัติดังนี้

8.5.1 เลือกใช้แผ่นดิสก์ที่สะอาดคือไม่มีคราบฝุ่น ไขมัน หรือรอยขูดขีดใดๆ

8.5.2 ใช้น้ำยาล้างหัวอ่านดิสก์ทุกๆเดือน

8.5.3 หลีกเลี่ยงการใช้แผ่นดิสก์เก่าที่เก็บไว้นานๆ เพราะจะทำให้หัวอ่าน Disk Drive สกปรกได้ง่าย

8.5.4 ก่อนนำแผ่นดิสก์ออกจากช่องอ่าน Disk Drive ควรจะให้ไฟสัญญาณที่ Disk Drive ดับก่อน เพื่อป้องกันหัวอ่านชำรุด

8.6 การบำรุงรักษาจอภาพ (Monitor)

ในส่วนของจอภาพนั้นอาจเสียหายได้ เช่น ภาพอาการเลื่อนไหล ภาพล้ม ภาพเต้นหรือไม่มีภาพ ซึ่งความเสียหายดังกล่าวจะต้องให้ช่างเท่านั้นเป็นผู้แก้ไข ผู้ใช้คอมพิวเตอร์ควรระมัดระวังโดยปฏิบัติ ดังนี้

8.6.1 อย่าให้วัตถุหรือน้ำไปกระทบหน้าจอคอมพิวเตอร์

8.6.2 ควรเปิดจอก่อนที่จะเปิดเครื่องคอมพิวเตอร์

8.6.3 ไม่ควรปิดๆ เปิดๆ เครื่องติดๆ กัน เมื่อปิดเครื่องแล้วทิ้งระยะไว้เล็กน้อยก่อนเปิดใหม่

8.6.4 ควรปรับความสว่างของจอภาพให้เหมาะสมกับสภาพของห้องทำงาน เพราะถ้าสว่างมากเกินไปย่อมทำให้จอภาพอายุสั้นลง

8.6.5 อย่าเปิดฝาหลังจอภาพซ่อมเอง เพราะจะเป็นอันตรายจากกระแสไฟฟ้าแรงสูง

8.6.6 เมื่อมีการเปิดจอภาพทิ้งไว้นานๆ ควรจะมีการเรียกโปรแกรมถนอมจอภาพ (Screen Sever) ขึ้นมาทำงานเพื่อยืดอายุการใช้งานของจอภาพ

8.7 สิ่งที่ไม่ควรใช้ทำความสะอาดคอมพิวเตอร์

8.7.1 ไม่ควรทำความสะอาดเครื่องคอมพิวเตอร์ในขณะที่เครื่องยังเปิดอยู่ ถ้าคุณจะทำความสะอาดควรปิดเครื่องทิ้งไว้ 5 นาที ก่อนลงมือทำความสะอาด

8.7.2 อย่าใช้ผ้าเปียก ผ้าชุ่มน้ำ เช็ดคอมพิวเตอร์อย่างเด็ดขาด ควรใช้ผ้าแห้ง

8.7.3 อย่าใช้สบู่ น้ำยาทำความสะอาดใด ๆ กับคอมพิวเตอร์ เพราะจะทำให้ระบบของเครื่องเกิดความเสียหาย

8.7.4 ไม่ควรฉีดสเปรย์ใด ๆ ไปที่คอมพิวเตอร์ แป้นพิมพ์ และอุปกรณ์ต่าง ๆ

8.7.5 ไม่ควรใช้เครื่องดูดฝุ่นกับคอมพิวเตอร์ และอุปกรณ์ประกอบอื่น ๆ

8.7.6 ถ้าคุณจำเป็นต้องทำความสะอาดเครื่องคอมพิวเตอร์ โปรดใช้อุปกรณ์ทำความสะอาด ที่คู่มือแนะนำไว้เท่านั้น

8.7.7 ไม่ควรดื่มน้ำชา กาแฟ เครื่องดื่มต่าง ๆ ในขณะที่ใช้คอมพิวเตอร์

8.7.8 ไม่ควรกินของคบเคี้ยวหรืออาหารใด ๆ ขณะทำงานด้วยเครื่องคอมพิวเตอร์

8.8 การบำรุงรักษา เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer)

8.8.1 วางไว้ในที่สะอาด คอยดูแลไม่ให้ฝุ่นเกาะ หรือหาผ้าคลุมมาคลุมไว้ ถ้าฝุ่นละอองเข้าไปในเครื่องพิมพ์มาก อาจจะทำให้เครื่องพิมพ์ขัดข้องได้

8.8.2 หมั่นใช้งานเครื่องพิมพ์ สั่งพิมพ์อยู่ตลอดเพื่อป้องกันไม่ให้ หัวพิมพ์ตัน ควรใช้ 2-3 ต่อสัปดาห์ ถ้าทำทุกวัน วันละแผ่นสองแผ่นได้ยิ่งดี

8.8.3 เปิด-ปิดเครื่องตามขั้นตอน การปิดเครื่องพิมพ์ด้วยสวิตช์ จะทำให้เครื่องทำความสะอาดหัวพิมพ์ และเก็บตลับหมึกเข้าที่อัตโนมัติก่อนการตัดไฟ

8.8.4 ใช้หมึกที่มีคุณภาพ หมึกไม่มีคุณภาพอาจทำให้หัวพิมพ์ตันได้ง่าย ซึ่งมีผลต่อตัวเครื่องพิมพ์ด้วย

8.8.5 เติมหมึกเมื่อมีการแจ้งเตือน หลายคนมักฝืนที่จะใช้เครื่องพิมพ์งานต่อ จนทำให้หัวพิมพ์มีความร้อนเพิ่มขึ้น และเครื่องพังในที่สุด

8.9 การบำรุงรักษา เครื่องพิมพ์เลเซอร์ (Laser Printer)

เป็นเครื่องพิมพ์ที่มีประสิทธิภาพสูงสามารถพิมพ์ภาพได้คมชัดมาก มีความละเอียด สวยงามแต่ราคาค่อนข้างสูง ผู้ใช้คอมพิวเตอร์จึงควรระมัดระวังในการใช้งาน แม้ว่าโอกาสจะเสียหายมีน้อยก็ตาม ข้อควรปฏิบัติดังนี้

8.9.1 เลือกใช้กระดาษให้เหมาะกับเครื่องพิมพ์ หากใช้กระดาษที่หนาเกินไป จะทำให้กระดาษติดเครื่องพิมพ์ได้

8.9.2 ควรกรีดกระดาษให้ดี อย่าให้กระดาษติดกัน เพราะอาจจะเป็นสาเหตุหนึ่งที่ทำให้กระดาษติดในตัวเครื่องพิมพ์ได้

8.9.3 ใส่กระดาษแต่พอเหมาะ ไม่มากหรือน้อยเกินไป เพราะอาจเกิดปัญหากระดาษติด

8.9.4 การพิมพ์ลงในแผ่นใส ต้องเลือกใช้แผ่นใสที่ใช้ถ่ายเอกสารได้เท่านั้น หากใช้แผ่นใสแบบธรรมดาซึ่งไม่สามารถทนความร้อนได้ อาจจะหลอมละลายติดเครื่องพิมพ์ทำให้ เกิดความเสียหาย

8.9.5 คลุมผ้ากันฝุ่น หลังการใช้งานเสร็จทุกครั้ง ควรมีผ้าคลุมตัวเครื่องเพื่อป้องกันฝุ่น หรือแมลงเข้าไปอาศัยในเครื่อง

8.9.6 ใช้หมึกที่มีคุณภาพ หมึกไม่มีคุณภาพอาจทำให้หัวพิมพ์ตันได้ง่าย ซึ่งมีผลต่อตัวเครื่องพิมพ์ด้วย

8.10 การบำรุงรักษา เครื่องพิมพ์ดอตแมทริกซ์ (Dot Matrix Printer)

8.10.1 การทดสอบหรือการสั่งพิมพ์เครื่องพิมพ์ควรตรวจสอบการใส่ผ้าหมึก กระดาษว่าเรียบร้อยหรือไม่เพื่อเป็นการถนอมหัวเข็ม

8.10.2 การใส่กระดาษควรใส่ให้ถูกวิธี เช่น การโหลดกระดาษแบบอัตโนมัติ หรือการโหลดกระดาษโดยการกดเครื่องพิมพ์โหลดไม่ควรใช้ลูกบิดของเครื่องพิมพ์อาจจะทำให้เฟืองหรือลูกบิดชำรุดได้

8.10.3 ควรใช้กระดาษที่มีคุณภาพ เช่น กระดาษต่อเนื่องหรือกระดาษถ่ายเอกสารเพราะ หากเป็นกระดาษคุณภาพไม่ดีอาจจะทำให้หัวเข็มชำรุดเร็วขึ้น

8.10.4 ก่อนการสั่งการเครื่องพิมพ์ทุกครั้งพิมพ์ทุกครั้งควรตรวจสอบอุปกรณ์ว่าอยู่ในสภาพเรียบร้อยทุกชิ้นสวนหรือไม่โดยเฉพาะฝาครอบของเครื่องส่วนมากไม่ชอบปิดอาจจะทำให้ฝุ่นละอองหรือเศษวัสดุเข้าไปติดในเครื่องพิมพ์ได้โดยง่าย

8.10.5 เครื่องพิมพ์ประเภทนี้จะมีคันโยกสำหรับความหนาของกระดาษควรตรวจสอบความถูกต้องก่อนสั่งพิมพ์ทุกครั้ง

8.10.6 ควรถอดชิ้นส่วนในการเป่าฝุ่นละอองบ้าง ทีสำคัญช่วงขั้นตอนการถอดชิ้นส่วนควรจำวิธีการประกอบคืนด้วย

8.10.7 ฝาเครื่องควรเช็ดทำความสะอาดด้วยน้ำยาคอมพิวเตอร์อย่างน้อยสัปดาห์ละครั้งถ้าเป็นไปได้ควรทำเป็นประจำทุกวัน

ส่วนที่ 3

นโยบาย/ระเบียบปฏิบัติระบบสำรองของสารสนเทศ

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

2. ผู้รับผิดชอบ

2.1 ผู้บังคับบัญชา
2.2 ผู้ดูแลระบบที่ได้รับมอบหมาย
2.3 ผู้ดูแลระบบสารสนเทศ
2.4 ผู้ใช้งาน

3. แนวนโยบาย

3.1 ต้องจัดทำแผนและระบบสำรองสำหรับระบบสารสนเทศ เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน
3.2 การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
3.3 การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ
3.4 ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
3.5 ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
3.6 มีศูนย์คอมพิวเตอร์สำรองซึ่งตั้งอยู่ในสภาพที่ปลอดภัยพร้อมระบบคอมพิวเตอร์ เพื่อสนับสนุนการฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน
3.7 ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

4. ระเบียบปฏิบัติ

4.1 พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูลและกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง
4.2 ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามสำดับความสำคัญของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานมากไปหาน้อย
4.3 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
4.4 ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

4.5 มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลา ที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

4.6 ให้ใช้ข้อมูลทันสมัยที่สุด ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ

4.7 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปี ละ 1 ครั้ง

4.8 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

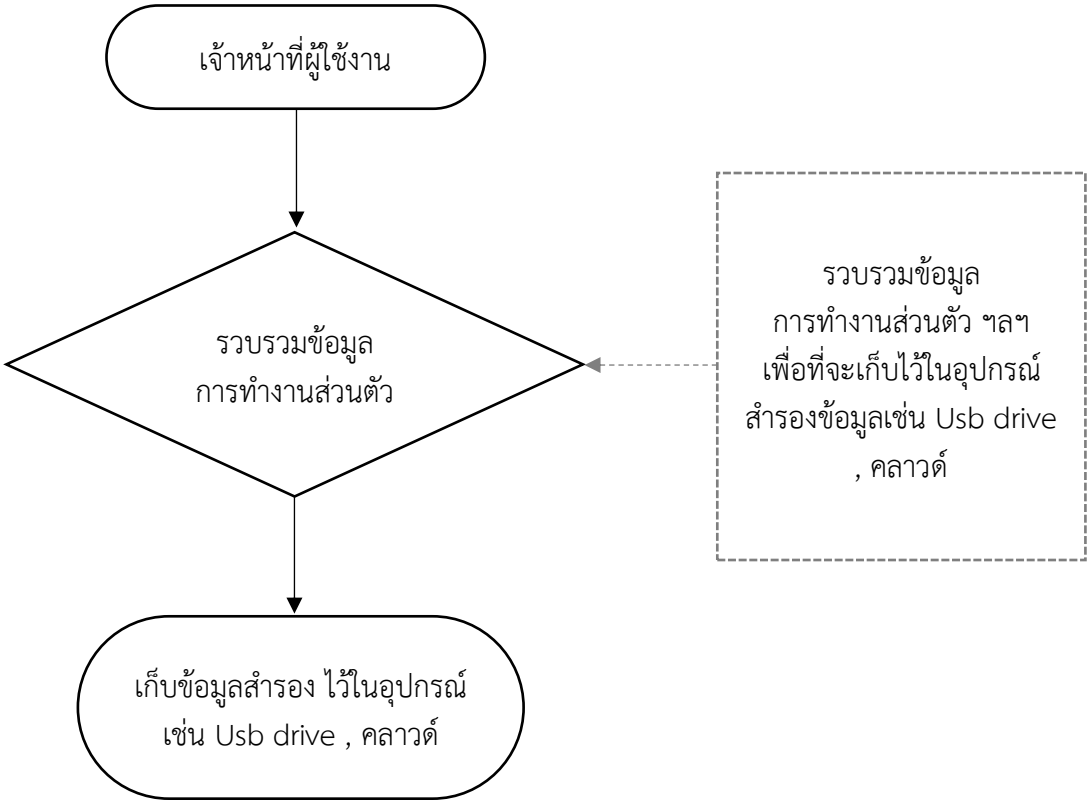
4.9 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาทราบโดยด่วน

4.10 กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

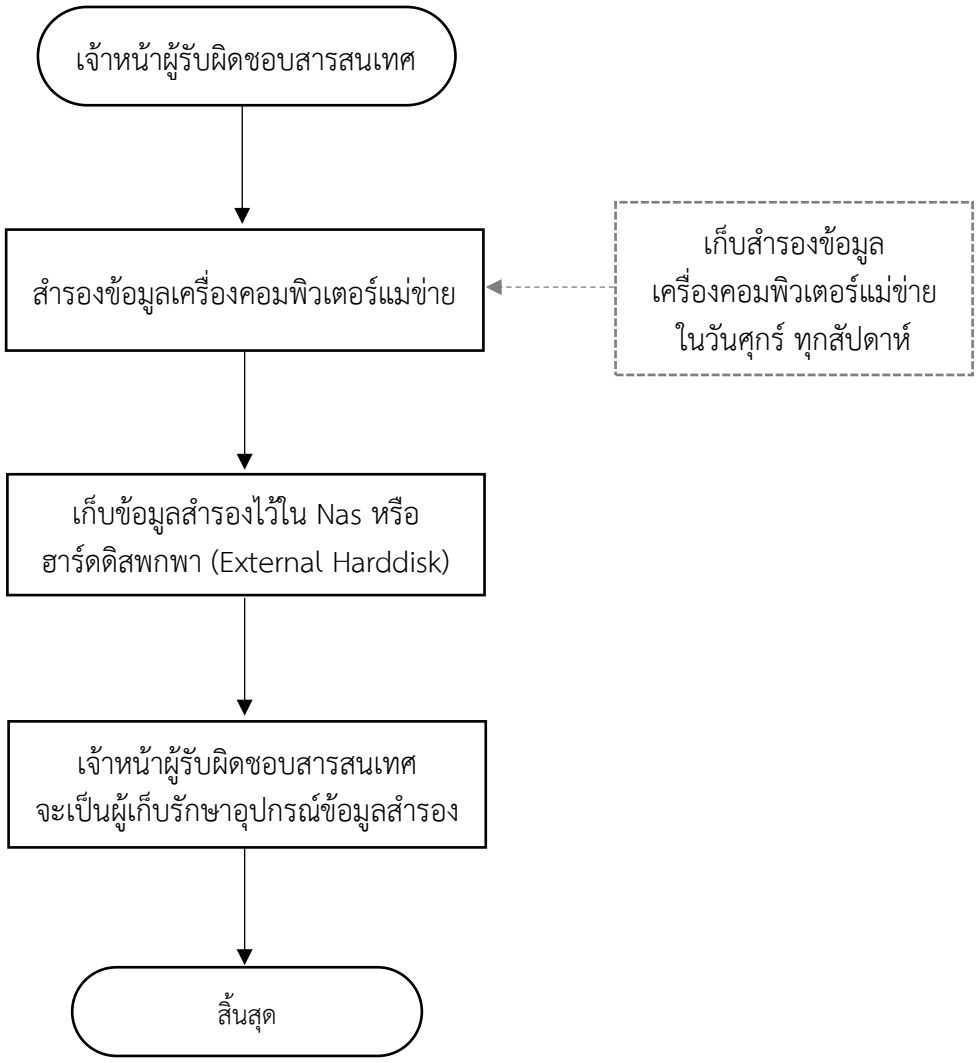
4.11 กำหนดให้ผู้ดูแลระบบ ต้องสำรองข้อมูลที่สำคัญ ได้แก่ ข้อมูลและค่า Configure ของ Database Server, Web Server, Mail Server และ Firewall Server เป็นประจำอย่างน้อย 3 เดือนครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

4.12 การสำรองข้อมูลการทำงานเบื้องต้น อื่นๆ เช่น ข้อมูลการทำงานส่วนตัว ฯลฯ เป็นหน้าที่ของเจ้าของข้อมูลนั้นๆ ในการเก็บข้อมูลสำรองผ่านอุปกรณ์การเก็บข้อมูลสำรอง เช่น Usb drive , ระบบคลาวด์

5. Flowchart ขั้นตอนการสำรองข้อมูลสารสนเทศ ของแต่ละกลุ่ม/ฝ่าย โรงพยาบาลเมืองจันทร์



6. Flowchart ขั้นตอนการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย โรงพยาบาลเมืองจันทร์



ส่วนที่ 4

นโยบาย/ระเบียบปฏิบัติการประเมินความเสี่ยง

1. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยง และป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

2. ผู้รับผิดชอบ

2.1 ผู้บังคับบัญชา

2.2 ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

2.3 ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวนโยบาย

3.1 ต้องมีการจัดแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

3.2 ต้องมีผู้ตรวจสอบภายในของหน่วยงาน ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

3.3 ต้องมีการรายงานผลการบริหารความเสี่ยงด้านระบบสารสนเทศให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

4. ระเบียบปฏิบัติ

4.1 ระบุความเสี่ยง และผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน เพื่อการประเมินความเสี่ยงนั้น ควรประกอบด้วย

4.1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

4.1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

4.1.3 ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

4.1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

4.1.5 ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

4.2 มีการกำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความ เสี่ยงนั้น

4.3 การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

4.3.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

4.3.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

4.3.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

4.4 กำหนดให้กลุ่มตรวจสอบภายในของโรงพยาบาลเมืองจันทร์มีหน้าที่ในการตรวจสอบ และประเมินความเสี่ยง และจัดทำรายงานพร้อมข้อเสนอแนะ อย่างน้อยปีละ 1 ครั้ง

4.5 มีการทบทวนนโยบาย และมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

4.6 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง และป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

4.7 ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

4.8 ควรกำหนดให้แยกเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 5

นโยบาย/ระเบียบปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

1. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารของโรงพยาบาลเมืองจันทร์ มีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและน่าเชื่อถือจึงกำหนดนโยบาย/ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยของโรงพยาบาลเมืองจันทร์ เพื่อให้เจ้าหน้าที่ของโรงพยาบาลเมืองจันทร์ทุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ และตั้งใจปฏิบัติอย่างเคร่งครัด ตามแนวทางดังนี้

2. ผู้รับผิดชอบ

2.1 ผู้บังคับบัญชา

2.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

3. แนวนโยบาย

3.1 จัดทำระเบียบปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.2 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้อง เมื่อมีการเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

4. ระเบียบปฏิบัติ

4.1 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

4.2 ติดตาม ตรวจสอบการดำเนินงาน ปรับปรุงแนวนโยบาย และระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคล ให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี รวมทั้งการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

4.3 จัดทำระเบียบปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคลของโรงพยาบาลเมืองจันทร์ เพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคลให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้

4.4 แจ้งหรือจัดให้มีประกาศแนวนโยบาย และข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศโรงพยาบาลเมืองจันทร์ ให้แก่บุคลากรและบุคคลที่เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจและปฏิบัติตามนโยบายและข้อปฏิบัติได้

4.5 จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

4.6 จัดฝึกอบรมระเบียบปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของ หน่วยงาน

4.7 ระดมการมีส่วนร่วมด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ 6

การกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัย

เพื่อสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินและอุปกรณ์ของโรงพยาบาลเมืองจันทร์ ซึ่งมีความสำคัญและคุณค่า ผู้บริหารจะให้การสนับสนุนในการกำหนดมาตรการป้องกัน ได้แก่ นโยบายความ มั่นคงปลอดภัย ขั้นตอนปฏิบัติ และเอกสารสนับสนุนอื่นๆรวมทั้งกระบวนการในการทบทวนมาตรการดังกล่าว เพื่อให้สามารถปรับปรุงหรือแก้ไขข้อบกพร่องหรือปัญหาทางด้านความมั่งคงปลอดภัยได้อย่างมีประสิทธิภาพ หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

1. ผู้บริหาร (CEO)

1.1 กำกับให้มีการกำหนด จัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัยอยู่เสมอ

1.2 กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ผู้ใดฝ่าฝืนหรือละเลยการปฏิบัติตามแนวทางนโยบาย และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.3 มอบหมาย อำนาจ หน้าที่ให้ผู้ดูแล ควบคุมและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

2. ผู้บังคับบัญชา (IT Director)

2.1 กำหนดให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)

2.2 กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

2.3 กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของโรงพยาบาล

2.4 จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

3. ผู้ดูแลระบบงานคอมพิวเตอร์ (Application Administrator)

3.1 กำหนดมาตรการควบคุม กำหนดสิทธิการใช้งานระบบงานต่าง ๆ ของหน่วยงาน

3.2 ควบคุม การบริหารจัดการใช้งานระบบงานหรือแอปพลิเคชันของหน่วยงาน

4. ผู้ดูแลระบบคอมพิวเตอร์ (System Administrator)

4.1 ดูแลบัญชีผู้ใช้ กำหนดสิทธิ และทบทวนสิทธิการใช้งานของผู้ใช้ระบบ

4.2 บริหารจัดการเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายให้มีความมั่งคงปลอดภัย และสามารถใช้งานได้ตลอดเวลา

4.3 ทำการสำรองข้อมูลและตรวจสอบข้อมูลที่สำรองไว้

5. ผู้พัฒนาระบบ (System Developer)

5.1 พัฒนาระบบโดยคำนึงถึงความถูกต้องของข้อมูลนำเข้า ข้อมูลที่อยู่ในระหว่างการประมวลผล และข้อมูลนำออก

5.2 ทำการทดสอบระบบหรือแอปพลิเคชันก่อนเริ่มต้นการใช้งานจริง

5.3 จัดทำคู่มือการใช้งาน คู่มือสำหรับระบบ และหรือคู่มือสำหรับการดำเนินงาน

5.4 จัดอบรมการใช้งานระบบหรือแอปพลิเคชันให้กับผู้ใช้งานที่เกี่ยวข้อง

6. ผู้ดูแลระบบเครือข่าย (System Network)

6.1 บันทึกเหตุการณ์ ตรวจสอบการเข้าถึงระบบเครือข่ายของหน่วยงาน

6.2 ควบคุมดูแลระบบเครือข่ายสื่อสารให้สามารถใช้งานได้ตลอดเวลา

6.3 ควบคุมการดำเนินการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นแนวทางตามที่พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2440 ได้กำหนดไว้

7. ผู้ดูแลระบบความมั่นคงปลอดภัย (Security Administrator)

7.1 ร่วมกับเจ้าของระบบหรือแอปพลิเคชันเพื่อกำหนด Security requirements สำหรับระบบหรือแอปพลิเคชัน

7.2 กำหนดมาตรการควบคุม กำหนดสิทธิการใช้ระบบเครือข่ายสื่อสารของหน่วยงาน

7.3 ตรวจสอบป้องกันการบุกรุกจู่โจมจากผู้ไม่ประสงค์ดี

8. เจ้าหน้าที่สนับสนุนและให้ความช่วยเหลือ (Help Desk)

8.1 ช่วยเหลือและประสานงานกับเจ้าหน้าที่ผู้ใช้งานของโรงพยาบาลเมืองจันทร์ ในการแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์

8.2 ทำหน้าที่รับมือกับเหตุการณ์ความมั่งคงปลอดภัย ตามที่ได้รับรายงานโดยปฏิบัติตามขั้นตอนอย่างเคร่งครัด

8.3 บันทึกข้อมูลปัญหาการใช้งานเครื่องคอมพิวเตอร์ และข้อมูลเหตุการณ์ความมั่งคงปลอดภัย

9. ผู้ใช้งาน (End User)

9.1 ปฏิบัติตามนโยบายฉบับนี้โดยเคร่งครัด