การจัดประชุมเสนอผลงานวิจัยระดับบัณฑิตศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 4
The 4th STOU Graduate Research Conference

การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด

The Development of Information Security Management for Access Control Based on ISO/IEC 27001:2013 for Klongyai Hospital Trat Province

รุ่งอรุณ นิรันต์เรือง (Rungarun Nirunruang)* วิภา เจริญภัณฑารักษ์ (Vipa Jaroenpuntaruk)**

บทคัดย่อ

โครงการที่นำเสนอ มีวัตถุประสงค์ (1) เพื่อพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐานISO/IEC 27001:2013 (2) เพื่อพัฒนาข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013

วิธีดำเนินการ(1) ศึกษารายละเอียดและข้อกำหนดความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 (2) ศึกษารายละเอียดและแนวทางการบริหารจัดการความเสี่ยง (3) รวบรวมข้อมูลโครงสร้างองค์กร,ระบบสารสนเทศและปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ (4) วิเคราะห์และประเมินความเสี่ยงด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ก่อนการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 (5) พัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐานISO/IEC 27001:2013 (6) วิเคราะห์และประเมินความเสี่ยงด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ หลังการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

ผลการดำเนินงาน เมื่อได้ศึกษาระบบสารสนเทศของโรงพยาบาล วิเคราะห์และประเมินความเสี่ยงก่อนการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ผลการประเมินความเสี่ยงก่อนการพัฒนา พบความเสี่ยงระดับสูงจำนวน 3 หัวข้อ ระดับกลางจำนวน 8 หัวข้อและระดับต่ำจำนวน 3 หัวข้อส่วนขั้นตอนการพัฒนาแนวทางและข้อกำหนดและผลการประเมินความเสี่ยงหลังการพัฒนา อยู่ระหว่างดำเนินงาน ซึ่งคาดว่าการประเมินความเสี่ยงหลังการพัฒนา จะไม่พบความเสี่ยงในระดับสูง ส่วนความเสี่ยงในระดับกลางและระดับต่ำจะลดลง การดำเนินงานจะแล้วเสร็จภายในเดือนตุลาคม 2557

ข้อสรุปในการดำเนินงานคือ ควรพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมทุกด้านตามกรอบมาตรฐานISO/IEC 27001:2013 การพัฒนาต้องได้รับความร่วมมือจากผู้ใช้งานและผู้ที่เกี่ยวข้องและควรมีการทบทวนและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อปรับปรุงแนวทางในการปฏิบัติงานต่อไป

คำสำคัญ ความมั่นคงปลอดภัยสารสนเทศ การควบคุมการเข้าถึง ISO/IEC 27001:2013

* นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต (แผน ข) แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช email address : chang_lolay@hotmail.com

**รองศาสตราจารย์ สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช email address :vipastou@gmail.com

Abstract

The objectives of this project were: (1) to develop procedures of information security management for access control based on ISO/IEC 27001:2013 for Klongyai hospital (2) to develop regulations of information security management for access control based on ISO/IEC 27001:2013 for Klongyai hospital.

The project has been performed as followings : (1) studying in details of information security management for access control of ISO/IEC 27001:2013 standard (2) studying in details of risk management (3) gathering information of Klongyai hospital, which are included of organization structure, existing information technology environment, and problems of information security management for access control (4) analysing problems and assess risks of Klongyai hospital regarding to information security management for access control before improvement based on ISO/IEC 27001:2013 (5) developing procedures and regulations of information security management for access control based on ISO/IEC 27001:2013 for Klongyai hospital (6) analysing results and re-assess risks of Klongyai hospital regarding to information security management for access control after improvement based on ISO/IEC 27001:2013.

The results of the project showed that after gathering information of Klongyai hospital, the results of problem analysis and risk assessment of Klongyai hospital had been done before improving information security management for access control based on ISO/IEC 27001:2013 standard. It is found that there were 3 high risk items, 8 medium risk items, and 3 low risk items. Since the project is in process of procedures and regulations of information security management for access control based on ISO/IEC 27001:2013 development, so the expected results and risks after their improvement should lead to higher security management and risk items reduction within October 2014.

In conclusion, information security management for access control based on ISO/IEC 27001:2013 should be established completely, authorized persons should be aware in information technology security policy, and the risks and policies should be reviewed and re-assesses continuously.

Keywords: Information Security, Access Control, ISO/IEC 27001:2013

บทนำ

ปัจจุบัน การให้บริการด้านการรักษาพยาบาลในประเทศไทย มีการนำเทคโนโลยีสารสนเทศเข้ามามีส่วนในกระบวนการทำงานเพื่อการบริการที่มีประสิทธิภาพและรวดเร็วมากขึ้น เห็นได้จากการที่โรงพยาบาลหลายแห่งทั้งภาครัฐและเอกชน ได้นำเทคโนโลยีทางการแพทย์ เช่น เอ็กซเรย์คอมพิวเตอร์ เอ็มอาร์ไอ เครื่องตรวจคลื่นไฟฟ้าหัวใจ เครื่องตรวจวิเคราะห์ทางห้องปฏิบัติการ และโปรแกรมการรักษาพยาบาลต่างๆ เข้ามามีส่วนในการให้บริการ ทั้งกระบวนการรักษาและระบบงานอื่นๆ โดยเทคโนโลยีเหล่านี้มีการทำงานเชื่อมต่อกับเครื่องคอมพิวเตอร์และมีการเชื่อมโยงผ่านเครือข่าย โดยข้อมูลต่างๆได้ถูกจัดเก็บในฐานข้อมูลของโรงพยาบาลทั้งสิ้น การนำเทคโนโลยีด้านสารสนเทศทางการแพทย์ เหล่านี้เข้ามาใช้งาน ทำให้เกิดความเสี่ยงต่อตัวผู้รับบริการและผู้ใช้งานระบบสารสนเทศและที่สำคัญที่สุดคือ มีความเสี่ยงต่อข้อมูลด้านการรักษาพยาบาล ดังนั้นการรักษาความมั่นคงปลอดภัยสารสนเทศภายในโรงพยาบาล ที่มีการใช้เทคโนโลยีสารสนเทศด้านการแพทย์จึงเป็นสิ่งสำคัญอย่างยิ่ง

ปัจจุบัน โรงพยาบาลคลองใหญ่ จังหวัดตราด มีการนำเทคโนโลยีสารสนเทศ เข้ามามีส่วนในกระบวนการรักษาพยาบาลและการจัดการภายในต่างๆ โดยอุปกรณ์ด้านเทคโนโลยี ทั้ง ซอฟต์แวร์และฮาร์ดแวร์ที่ทำงานผ่าน เครือข่าย อินเตอร์เน็ตและอินตราเน็ต โดยเชื่อมโยงเครือข่ายผ่านผู้ให้บริการ ซึ่งข้อมูลทั้งหมดจะถูกจัดเก็บในฐานข้อมูลของโรงพยาบาล เพื่อให้การบริการที่มีประสิทธิภาพ สะดวก รวดเร็วและได้มาตรฐาน ตามการรับรองคุณภาพมาตรฐานโรงพยาบาลหรือ Hospital Accreditation (HA) ซึ่งเป็นมาตรฐานที่กระทรวงสาธารณสุข มีนโยบาย ให้ทุกโรงพยาบาลในสังกัดทั่วประเทศ ได้รับการรับรอง โดยมาตรฐานดังกล่าวยัง มีข้อกำหนดเกี่ยวกับการจัดการระบบสารสนเทศและการจัดการเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัย หากโรงพยาบาลมีระบบการจัดการด้านความมั่นคงปลอดปลอดภัยของสารสนเทศดังกล่าว จะทำให้ผลการประเมินอยู่ในระดับที่ดีขึ้น

จากการรวบรวมและวิเคราะห์ปัญหาด้านความมั่นคงปลอดภัยระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ จังหวัดตราด และทำการประเมินความเสี่ยง ตามมาตรฐาน IOS/IEC 27001:2013 พบว่า โรงพยาบาลมีความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศในระดับสูงอยู่หลายด้าน โดยเฉพาะด้านการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) ซึ่งมีความเสี่ยงสูงตามมาตรฐานถึง 3 หัวข้อจากทั้งสิ้น 14 หัวข้อมาตรฐาน โดยรวมพบว่าขาดนโยบายและแนวทางการปฏิบัติด้านการควบคุมการเข้าถึงระบบสารสนเทศที่ปลอดภัยอย่างครอบคลุม อันอาจเกิดความไม่ปลอดภัยต่อระบบสารสนเทศของโรงพยาบาล ส่งผลกระทบโดยตรงต่อผู้รับบริการ ผู้ใช้งานและข้อมูลที่สำคัญได้

ดังนั้น ผู้ศึกษาจึงได้ดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด เพื่อใช้เป็นแนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ และใช้เป็นแนวทางในการพัฒนาให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ให้ครอบคลุมตามมาตรฐาน ISO/IEC 27001:2013 ต่อไป

วัตถุประสงค์ของการศึกษา

1. เพื่อพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013
2. เพื่อพัฒนาข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013

วิธีดำเนินงาน

ดำเนินงานโดยใช้ โรงพยาบาลคลองใหญ่ จังหวัดตราด ซึ่งเป็นโรงพยาบาลชุมชนขนาด 30 เตียง ในสังกัดกระทรวงสาธารณสุข เป็นโรงพยาบาลตัวอย่าง โดยมีขั้นตอนการศึกษาดังนี้

1. ศึกษารายละเอียดและข้อกำหนดความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013
2. ศึกษารายละเอียดและแนวทางการประเมินความเสี่ยง
3. ศึกษา รวบรวมข้อมูลและวิเคราะห์ปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ดังนี้
   3.1 ศึกษาข้อมูลพื้นฐานทั่วไปของโรงพยาบาล
   3.2 ศึกษาข้อมูลด้านเทคโนโลยีสารสนเทศขององค์กร เช่น โครงสร้างการบริหารงาน อุปกรณ์ และการ ควบคุมการเข้าถึงระบบสารสนเทศเดิม
   3.3 แบบบันทึกอุบัติการณ์ความเสี่ยง ด้านความความปลอดภัยสารสนเทศของโรงพยาบาล
   3.4 การสัมภาษณ์ผู้บริหารและหัวหน้าหน่วยงาน ในด้านความมั่นคงปลอดภัยสารสนเทศ โดยเฉพาะด้านการควบคุมการเข้าถึงระบบสารสนเทศ
   3.5 การสัมภาษณ์ผู้ใช้งาน ได้แก่ แพทย์ พยาบาล เภสัชกร และอื่นๆ ในด้านความมั่นคงปลอดภัยสารสนเทศ โดยเฉพาะด้านการควบคุมการเข้าถึงระบบสารสนเทศ
4. วิเคราะห์และประเมินความเสี่ยง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ก่อนการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013
5. พัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ตามมาตรฐาน ISO/IEC 27001:2013
6. วิเคราะห์และประเมินความเสี่ยง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ หลังการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

ผลการดำเนินงาน

1. ผลการศึกษารายละเอียดและข้อกำหนดความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

มาตรฐาน ISO/IEC27001 เป็นมาตรฐานสากลด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ

Annex A Control ISO/IEC 27001:2013: A.9 Access control (การควบคุมการเข้าถึง) ประกอบด้วย

1. Business requirements of access control (ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง)

A.9.1.1 Access control policy (นโยบายการควบคุมการเข้าถึง)

A.9.1.2 Access to networks and network services **(**การเข้าถึงเครือข่ายและการบริการเครือข่าย**)**

2. User access management (การบริหารจัดการการเข้าถึงของผู้ใช้งาน)

A.9.2.1 User registration and de-registration (การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน)

A.9.2.2 User access provisioning (การจัดการสิทธิการเข้าถึงของผู้ใช้งาน)

A.9.2.3 Privilege management (การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ)

A.9.2.4 Management of secret authentication information of users (การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน)

A.9.2.5 Review of user access rights (การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน)

A.9.2.6 Removal or adjustment of access rights (การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง)

3. User responsibilities (หน้าที่ความรับผิดชอบของผู้ใช้งาน)

A.9.3.1 Use of secret authentication information (การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ)

4. System and application access control (การควบคุมการเข้าถึงระบบ)

A.9.4.1 Information access restriction (การจำกัดการเข้าถึงสารสนเทศ)

A.9.4.2 Secure log-on procedures (ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย)

A.9.4.3 Password management system (ระบบบริหารจัดการรหัสผ่าน)

A.9.4.4 Use of privileged utility programs (การใช้โปรแกรมอรรถประโยชน์)

A.9.4.5 Access control to program source code (การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม)

2. ผลการศึกษารายละเอียดและแนวทางการบริหารจัดการความเสี่ยง

ความเสี่ยง (Risks) หมายถึง โอกาสที่ภัยคุกคามจะเกิดขึ้นโดยใช้ประโยชน์จากจุดอ่อน เมื่อเกิดขึ้นจะส่งผลเสียหายต่อองค์กรโดยเหตุการณ์ที่ส่งผลกระทบด้วนความมั่นคงปลอดภัย

1. การวิเคราะห์และประเมินความเสี่ยง

เป็นการพิจารณาความเสี่ยงในแง่ของโอกาสที่จะเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลกระทบ (Impact) ที่ตามมาว่ามีความรุนแรงเสียหายมากน้อยเพียงใด

เกณฑ์ที่ใช้ในการประเมินระดับโอกาสการเกิดความเสี่ยง (Likelihood) แบ่งเป็น 5 ระดับคือ

1 = โอกาสเกิดน้อยที่สุด

2 = โอกาสเกิดน้อย

3 = โอกาสเกิดปานกลาง

4 = โอกาสเกิดมาก

5 = โอกาสเกิดมากที่สุด

เกณฑ์ที่ใช้ในการประเมินระดับของผลกระทบความเสี่ยง (Impact) แบ่งเป็น 5 ระดับคือ

1 = น้อยที่สุด

2 = น้อย

3 = ปานกลาง

4 = มาก

5 = มากที่สุด

คิดค่าของระดับความเสี่ยงได้ดังนี้

ระดับความเสี่ยง (Risk Value) = ระดับโอกาสที่เกิด (likelihood) × ระดับของผลกระทบ (Impact) เมื่อได้ค่าความเสี่ยงแล้วจึงนำมาประเมินค่าความเสี่ยงตามระดับความเสี่ยง

ระดับความเสี่ยง 1 – 8 ความเสี่ยงระดับต่ำ (Low) ควรตรวจสอบแผนงาน

ระดับความเสี่ยง 9 – 16 ความเสี่ยงระดับกลาง (Medium) ควรมีการแก้ไข

ระดับความเสี่ยง 17 – 25 ความเสี่ยงระดับสูง (High) ต้องแก้ไขอย่างเร่งด่วน

2. การควบคุมและแก้ไขความเสี่ยง (Risk Treatment)

การควบคุมและแก้ไขความเสี่ยงตามมาตรฐาน ISO 27001

1. การลดความเสี่ยง (Risk Reduction) คือ การพิจารณาหาวิธีในการควบคุมและแก้ไขความเสี่ยงให้ลดลงอยู่ในระดับที่องค์กรสามารถยอมรับได้

2. การยอมรับความเสี่ยง (Risk Acceptance) คือ การที่องค์กรพิจารณาแล้วพบว่าการดำเนินการแก้ไขและการควบคุมความเสี่ยงนั้นไม่เหมาะสม ไม่สามารถกระทำได้ในทางปฏิบัติหรือไม่คุ้มค่า เช่น ค่าใช้จ่ายในการดำเนินการแก้ไข มีมูลค่าสูงกว่ามูลค่าของข้อมูล ทั้งนี้ขึ้นอยู่กับดุลยพินิจของผู้บริหาร

3.การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยง โดยยกเลิกกระบวนการทำงานหรือทรัพย์สินที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำเมื่อการแก้ไขความเสี่ยงด้วยวิธีการอื่นไม่คุ้มกับผลประโยชน์ที่ได้จากการทำงาน ด้วยกระบวนการหรือทรัพย์สินนั้นๆ

4.การโอนความเสี่ยง (Risk Transfer) คือการพิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย เป็นต้น

3. ผลการรวบรวมข้อมูลโครงสร้างองค์กร,ระบบสารสนเทศและปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่

ข้อมูลทั่วไป

โรงพยาบาลคลองใหญ่ ตั้งอยู่ที่ 1 หมู่ 9 ตำบลคลองใหญ่ อำเภอคลองใหญ่ จังหวัดตราด เป็นโรงพยาบาลชุมชนในสังกัดสำนักงานปลัดกระทรวงกระทรวงสาธารณสุข สำนักงานสาธารณสุขจังหวัดตราด มีเจ้าหน้าที่ทั้งสิ้น 125 คน

ระบบสารสนเทศภายในองค์กร

ระบบสารสนเทศโรงพยาบาลคลองใหญ่ อยู่ภายใต้ความรับผิดชอบของศูนย์คอมพิวเตอร์ประจำโรงพยาบาล เป็นหน่วยงานดูแลระบบและพัฒนาระบบเทคโนโลยีสารสนเทศ มีเจ้าหน้าที่ปฏิบัติงาน 3 คน มีเครื่องคอมพิวเตอร์ที่ใช้ในโรงพยาบาล 72 เครื่องและอุปกรณ์พื้นฐานด้านเทคโนโลยีสารสนเทศอื่นๆ ที่จำเป็น ประกอบด้วยอุปกรณ์ด้านฮาร์ดแวร์ ซอฟต์แวร์ ที่ทำงานผ่านระบบเครือข่ายอินเตอร์เน็ตและอินตราเน็ต โดยข้อมูลถูกจัดเก็บในฐานข้อมูลกลาง ระบบสามารถทำงานได้ตลอด 24 ชั่วโมง เพื่อตอบสนองความต้องการของผู้บริหาร เจ้าหน้าที่และผู้รับบริการ ให้ได้ข้อมูลที่ถูกต้องทันเวลาและพึงพอใจ

ปัญหาความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ดำเนินการศึกษา โดยเปรียบเทียบความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามกรอบมาตรฐาน IS0/IEC 27001:2013 กับสภาพระบบสารสนเทศของโรงพยาบาลในปัจจุบัน พบว่าโรงพยาบาลคลองใหญ่ มีปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศดังนี้ (ตารางที่ 1)

ตารางที่ 1 ปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาล

มาตรฐาน	ปัญหาที่พบ
1.ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง	
A.9.1.1 นโยบายการควบคุมการเข้าถึง	ไม่มีนโยบายด้านการควบคุมการเข้าถึงระบบสารสนเทศ ที่เป็นลายลักษณ์อักษรและการกำหนดการทบทวนความต้องการของผู้ใช้งาน
A.9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย	ไม่มีข้อกำหนดวิธีปฏิบัติการกำหนดสิทธิ์ของผู้ใช้งาน มีเพียงการกำหนดสิทธิการเข้าถึงในทางปฏิบัติ
2.การบริหารจัดการการเข้าถึงของผู้ใช้งาน	
A.9.2.1 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน	ไม่มีข้อกำหนดวิธีปฏิบัติการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน ที่เป็นลายลักษณ์อักษร
A.9.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน	ไม่มีข้อกำหนดวิธีปฏิบัติกระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งาน
A.9.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	ไม่มีข้อกำหนดวิธีปฏิบัติ การให้สิทธิ การใช้สิทธิ การจำกัดและควบคุมการเข้าถึงตามระดับสิทธิ
A.9.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	ไม่มีข้อกำหนดวิธีปฏิบัติ การมอบข้อมูลการพิสูจน์ตัวตนและกระบวนการบริหารเพื่อควบคุมข้อมูลของผู้ใช้งาน

มาตรฐาน	ปัญหาที่พบ
A.9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน	ไม่มีข้อกำหนดวิธีปฏิบัติ การทบทวนสิทธิการเข้าถึงของผู้ใช้งานและไม่เคยทำการทบทวนสิทธิ
A.9.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง	ไม่มีข้อกำหนดวิธีปฏิบัติ การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง เมื่อสิ้นสุดการจ้างงาน
3.หน้าที่ความรับผิดชอบของผู้ใช้งาน	
A.9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ	ไม่มีข้อกำหนดวิธีปฏิบัติ การใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ
4.การควบคุมการเข้าถึงระบบ	
A.9.4.1 การจำกัดการเข้าถึงสารสนเทศ	ไม่มีข้อกำหนดวิธีปฏิบัติ การจำกัดการเข้าถึงระบบงานที่สอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ
A.9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	ไม่มีข้อกำหนดวิธีปฏิบัติ การล็อกอินเข้าระบบให้มีความมั่นคงปลอดภัย
A.9.4.3 ระบบบริหารจัดการรหัสผ่าน	ไม่มีข้อกำหนดวิธีปฏิบัติ การบริหารจัดการรหัสผ่านให้มีคุณภาพ
A.9.4.4 การใช้โปรแกรมอรรถประโยชน์	ไม่มีข้อกำหนดวิธีปฏิบัติ การใช้โปรแกรมอรรถประโยชน์และการควบคุมการใช้งาน
A.9.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม	ไม่มีข้อกำหนดวิธีปฏิบัติ การการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม

4. ผลการวิเคราะห์และประเมินความเสี่ยงด้านการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาลก่อนการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

ตารางที่ 2 การประเมินความเสี่ยงก่อนการพัฒนา

มาตรฐาน	การประเมินความเสี่ยง			
	โอกาส	ผลกระทบ	คะแนน	ระดับ
1.ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง				
A.9.1.1 นโยบายการควบคุมการเข้าถึง	4	5	20	สูง
A.9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย	4	5	20	สูง
2.การบริหารจัดการการเข้าถึงของผู้ใช้งาน				
A.9.2.1 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน	3	5	15	กลาง
A.9.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน	3	5	15	กลาง
A.9.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	1	5	5	ต่ำ

มาตรฐาน	การประเมินความเสี่ยง			
	โอกาส	ผลกระทบ	คะแนน	ระดับ
A.9.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	1	5	5	ต่ำ
A.9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน	4	5	20	สูง
A.9.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง	5	3	15	กลาง
3.หน้าที่ความรับผิดชอบของผู้ใช้งาน				
A.9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ	3	5	15	กลาง
4.การควบคุมการเข้าถึงระบบ				
A.9.4.1 การจำกัดการเข้าถึงสารสนเทศ	2	4	8	ต่ำ
A.9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	3	5	15	กลาง
A.9.4.3 ระบบบริหารจัดการรหัสผ่าน	3	5	15	กลาง
A.9.4.4 การใช้โปรแกรมอรรถประโยชน์	1	5	15	กลาง
A.9.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม	1	5	5	กลาง

การประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามกรอบมาตรฐาน ISO/IEC 27001:2013 ก่อนการปรับปรุงแนวทางการปฏิบัติงาน (ตารางที่ 2) ผลการประเมินความเสี่ยง พบว่าก่อนการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ มีจำนวนความเสี่ยงในระดับสูงจำนวน 3 หัวข้อ ความเสี่ยงในระดับกลาง จำนวน 8 หัวข้อและความเสี่ยงในระดับต่ำ จำนวน 3 หัวข้อ คิดเป็นร้อยละ 21.43, 57.14 และ 21.43 ของมาตรฐานด้านการควบคุมการเข้าถึงทั้งหมด โดยหัวข้อตามกรอบมาตรฐานที่มีความเสี่ยงในระดับสูง ได้แก่ นโยบายการควบคุมการเข้าถึง (A.9.1.1) การเข้าถึงเครือข่ายและการบริการเครือข่าย (A.9.1.2) และการการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.5)

5. การพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013

ตารางที่ 3 การพัฒนาการควบคุมการเข้าถึงระบบสารสนเทศ

มาตรฐาน	การพัฒนา
1.ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง	
A.9.1.1 นโยบายการควบคุมการเข้าถึง	- จัดทำนโยบายด้านการควบคุมการเข้าถึงระบบสารสนเทศที่เป็นลายลักษณ์อักษร - จัดทำข้อกำหนดวิธีปฏิบัติการทบทวนความต้องการของผู้ใช้งาน

มาตรฐาน	การพัฒนา
A.9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย	- จัดทำข้อกำหนดวิธีปฏิบัติการกำหนดสิทธิ์ผู้ใช้งานเครือข่าย
2.การบริหารจัดการการเข้าถึงของผู้ใช้งาน	
A.9.2.1 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	- จัดทำข้อกำหนดวิธีปฏิบัติการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน
A.9.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน	- จัดทำข้อกำหนดวิธีปฏิบัติกระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งาน
A.9.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	- จัดทำข้อกำหนดวิธีปฏิบัติการให้สิทธิ การใช้สิทธิ การจำกัดและควบคุมการเข้าถึงตามระดับสิทธิ
A.9.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	- จัดทำข้อกำหนดวิธีปฏิบัติการมอบข้อมูลการพิสูจน์ตัวตนและกระบวนการเพื่อควบคุมข้อมูลของผู้ใช้งาน
A.9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน	- จัดทำข้อกำหนดวิธีปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
A.9.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง	- จัดทำข้อกำหนดวิธีปฏิบัติการถอดถอนและการปรับปรุงสิทธิการเข้าถึง เมื่อสิ้นสุดการจ้างงาน
3.หน้าที่ความรับผิดชอบของผู้ใช้งาน	
A.9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ	- จัดทำข้อกำหนดวิธีปฏิบัติการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ
4.การควบคุมการเข้าถึงระบบ	
A.9.4.1 การจำกัดการเข้าถึงสารสนเทศ	- จัดทำข้อกำหนดวิธีปฏิบัติการจำกัดการเข้าถึงระบบสารสนเทศสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ
A.9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	- จัดทำข้อกำหนดวิธีปฏิบัติการล็อกอินเข้าระบบให้มีความมั่นคงปลอดภัย
A.9.4.3 ระบบบริหารจัดการรหัสผ่าน	- จัดทำข้อกำหนดวิธีปฏิบัติการบริหารจัดการรหัสผ่านให้มีคุณภาพ
A.9.4.4 การใช้โปรแกรมอรรถประโยชน์	- จัดทำข้อกำหนดวิธีปฏิบัติการใช้โปรแกรมอรรถประโยชน์และการควบคุมการใช้งาน
A.9.4.5การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม	- จัดทำข้อกำหนดวิธีปฏิบัติการการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม

หลังดำเนินการจัดทำนโยบายและแนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศดังกล่าว ได้นำเสนอต่อผู้บริหารโรงพยาบาลเพื่ออนุมัติและประกาศใช้งาน ดำเนินการชี้แจง ทำความเข้าใจกับผู้ปฏิบัติงาน และประเมินความเสี่ยงภายหลังจากมีการประกาศใช้งาน ซึ่งขั้นตอนการจัดทำนโยบายและแนวทางการปฏิบัติงานอยู่ระหว่างการจัดทำ คาดว่าจะแล้วเสร็จและประกาศใช้ภายในสิ้นเดือนกันยายน 2557

6. การวิเคราะห์และประเมินความเสี่ยงด้านการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาลหลังการพัฒนาแนวทางและข้อกำหนดด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

การประเมินความเสี่ยงหลังการประกาศใช้งาน คาดว่าจะแล้วเสร็จภายในสิ้นเดือนตุลาคม 2557 โดยคาดว่า ระดับความเสี่ยงหลังการประกาศใช้นโยบายและแนวทางการปฏิบัติงาน ด้านการควบคุมการเข้าถึงระบบสารสนเทศ จะไม่มีความเสี่ยงในระดับสูง ส่วนความเสี่ยงในระดับกลางและระดับต่ำจะลดลง

สรุปผลการศึกษา

การดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ในโรงพยาบาลคลองใหญ่ จังหวัดตราด หลังทำการศึกษาข้อมูลด้านรายละเอียดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ โดยทำการศึกษาข้อมูลพื้นฐาน ระบบสารสนเทศ สภาพปัญหาความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศของโรงพยาบาล และนำบริบทต่างๆ มาทำการประเมินความเสี่ยง ความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ก่อนดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัย ด้านการเข้าถึงระบบสารสนเทศ ผลการประเมินความเสี่ยงพบความเสี่ยงในระดับสูงดังนี้ คือ (A.9.1.1) นโยบายการควบคุมการเข้าถึง คือ การไม่มีนโยบายด้านการควบคุมการเข้าถึงระบบสารสนเทศที่เป็นลายลักษณ์อักษรและการกำหนดการทบทวนความต้องการของผู้ใช้งาน (A.9.1.2) การเข้าถึงเครือข่ายและการบริการเครือข่าย คือไม่มีข้อกำหนดวิธีปฏิบัติการกำหนดสิทธิ์ผู้ใช้งานเครือข่าย มีเพียงการกำหนดสิทธิการเข้าถึงในทางปฏิบัติ และ (A.9.2.5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน คือไม่มีข้อกำหนดวิธีปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งานและไม่เคยทำการทบทวนสิทธิ ซึ่งความเสี่ยงระดับสูงดังกล่าวจำเป็นต้องดำเนินการแก้ไขโดยเร่งด่วน พบความเสี่ยงในระดับกลาง คือ การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (A.9.2.1) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.2) การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (A.9.2.6) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (A.9.3.1) ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (A.9.4.2) ระบบบริหารจัดการรหัสผ่าน (A.9.4.3) การใช้โปรแกรมอรรถประโยชน์ (A.9.4.4) การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (A.9.4.5) ซึ่งเป็นความเสี่ยงในระดับที่ควรมีการแก้ไข เพื่อไม่ให้ลุกลามเป็นความเสี่ยงระดับสูง และพบความเสี่ยงในระดับต่ำ คือ การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (A.9.2.3) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (A.9.2.4) การจำกัดการเข้าถึงสารสนเทศ (A.9.4.1) ซึ่งต้องมีการตรวจสอบแผนงานและควบคุมไม่ให้เกิดความเสี่ยงในระดับที่สูงขึ้น

หลังจากได้ดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ โดยการจัดทำนโยบายและแนวทางการปฏิบัติ ประกาศใช้ในหน่วยงาน ดำเนินการประเมินความเสี่ยงหลังการใช้นโยบายและแนวทางการปฏิบัติ โดยขั้นตอนการจัดทำนโยบายและแนวทางการปฏิบัติ และขั้นตอนการประเมินความเสี่ยง หลังการพัฒนาอยู่ระหว่างการดำเนินงาน ซึ่งคาดว่าความเสี่ยงมีแนวโน้มลดลง

นอกจากนี้การศึกษายังพบว่า มาตรฐานความมั่นคงปลอดภัยสารสนเทศ ตามกรอบมาตรฐาน ISO/IEC 27001:2013 หลายด้านที่ยังไม่มีการจัดทำเป็นนโยบายและแนวทางปฏิบัติ ซึ่งได้นำเสนอผู้บริหารโรงพยาบาลและจัดทำแผนการจัดทำนโยบายและแนวทางการปฏิบัติเพื่อให้ครอบคลุมตามมาตรฐาน ISO/IEC 27001 : 2013 (ตารางที่ 4) ทั้งนี้เพื่อให้เกิดความปลอดภัยสูงสุดต่อระบบสารสนเทศของโรงพยาบาล อย่างครอบคลุม

ตารางที่ 4 แผนการจัดทำนโยบายและแนวทางปฏิบัติตามมาตรฐาน ISO/IEC 27001:2013

ลำดับ	การพัฒนาตามมาตรฐาน	ระยะเวลา											
		ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย	พ.ค.	มิ.ย.	ก.ย.	ส.ค.	ก.ย.
1	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)												
2	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)												
3	ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)												
4	การบริหารจัดการทรัพย์สิน (Asset Management)												
5	การเข้ารหัสข้อมูล (Cryptography)												
6	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)												
7	ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)												
8	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)												
9	การจัดหา การพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)												
10	ความสัมพันธ์กับผู้ใช้บริการภายนอก (Suppliers Relationships)												

ข้อเสนอแนะ

การที่กระทรวงสาธารณสุขพยายามผลักดันให้โรงพยาบาลในสังกัดทุกแห่ง ต้องผ่านการรับรองคุณภาพมาตรฐานโรงพยาบาลหรือ Hospital Accreditation ซึ่งมีเกณฑ์การประเมินด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ ทำให้ทุกโรงพยาบาลหันมาเห็นความสำคัญของการจัดการด้านความมั่นคงปลอดภัยสารสนเทศมากขึ้น จากการดำเนินโครงการการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด มีข้อเสนอแนะเพื่อให้เกิดประโยชน์กับองค์กรโดยเฉพาะโรงพยาบาลชุมชน ดังนี้คือ

1. แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ที่จัดทำขึ้นเป็นแนวทางที่สามารถปฏิบัติตามและเหมาะสำหรับโรงพยาบาลชุมชนหรือองค์กรที่มีองค์ประกอบด้านสารสนเทศ สภาพปัญหาความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศที่ใกล้เคียงกัน

2. แนวทางการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศองค์กร ควรทำการศึกษาข้อมูลพื้นฐาน ด้านโครงสร้างทั่วไป โครงสร้างระบบสารสนเทศ สภาพปัญหาด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร และทำความเข้าใจข้อกำหนดตามกรอบมาตรฐานISO/IEC 27001: 2013 ที่เลือกใช้ เพื่อการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมในทุกด้าน

3. เครื่องมือที่ได้จากการจัดทำโครงการนี้ ครอบคลุมเฉพาะด้านการควบคุมการเข้าถึงระบบสารสนเทศเท่านั้น ควรดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ให้ครอบคลุมตามกรอบมาตรฐาน เพื่อให้เกิดความมั่นคงปลอดภัยต่อองค์กรมากที่สุด

4. ในการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ขั้นตอนการดำเนินการจัดทำนโยบายและข้อกำหนดวิธีปฏิบัติ จำเป็นต้องได้รับความเห็นชอบจากผู้บริหาร และได้รับความร่วมมือจากผู้ใช้งานและผู้ที่เกี่ยวข้องทุกคน โดยหลังจากประกาศใช้นโยบายและข้อกำหนดวิธีปฏิบัติ ผู้จัดทำจำเป็นต้องมีการชี้แจงและทำความเข้าใจกับผู้ที่เกี่ยวข้องทั้งหมดในการปฏิบัติตามนโยบายและข้อกำหนด เพื่อให้ทุกคนในหน่วยงานตระหนักถึงความสำคัญ และสามารถปฏิบัติตามได้

5. ภายหลังการนำแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศมาใช้งาน ควรมีการทบทวนและประเมินความเสี่ยง อย่างสม่ำเสมอเพื่อใช้เป็นข้อมูลในการปรับปรุงแนวทางการปฏิบัติ ให้เกิดความปลอดภัยต่อสารสนเทศองค์กรต่อไป

เอกสารอ้างอิง

กระทรวงสาธารณสุข,ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. (2556). แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของกระทรวงสาธารณสุข. สืบค้นเมื่อ 30 มิถุนายน 2557 จาก http://ict.moph.go.th /project /eva/securepolicy.htm

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2550).คู่มือการรักษาความมั่นคงปลอดภัย ICTกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. สืบค้นเมื่อ 30 มิถุนายน 2557 จาก http://www.portal.mot.go.th/e_logistics/content%5Cpublic_document %5CICT%20security%20manual.pdf .

เฉลิมสุวรรณะ. (2554). *การรักษาความมั่นคงปลอดภัยสารสนเทศกรณีศึกษาศูนย์การแพทย์สมเด็จพระเทพรัตน-ราชสุดาฯ สยามบรมราชกุมารี*. (สารนิพนธ์ วิทยาศาสตรมหาบัณฑิต). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

บริษัททีเน็ต จำกัด.ระบบ ISO/IEC 27001:2013. Retrived 31 August 2014. Fromhttp://www.tnetsecurity.com/content_audit/27001-2013.pdf

สุชาดา สิทธิ์จงสถาพร. (2556).กรณีศึกษาการป้องกันสำหรับความมั่นคงปลอดภัย สารสนเทศสำหรับองค์กร. ใน *เอกสารการสอนชุดวิชาการบริหารความมั่นคงปลอดภัยสารสนเทศ* (หน่วยที่ 15 หน้า 20-42). นนทบุรี: สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช.สืบค้นจาก http://www.stou.ac.th/ Website/Subbj /fileUpload/99411-15-1.pdf

สุชาดา สิทธิ์จงสถาพร. (2556) นโยบายและมาตรฐานความมั่นคงปลอดภัยสารสนเทศ.*ในเอกสารการสอนชุดวิชาการบริหารความมั่นคงปลอดภัยสารสนเทศ* (หน่วยที่ 13 หน้า 1-48). นนทบุรี: สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช.สืบค้นจาก http://www.stou.ac.th/Website/Subbj/fileUpload/99411-13-1.pdf

สถาบันพัฒนาและรับรองคุณภาพโรงพยาบาล . (2549). มาตรฐานโรงพยาบาลและบริการสุขภาพ ฉบับเฉลิมพระเกียรติฉลองสิริราชสมบัติครบ ๖๐ ปี . สืบค้นเมื่อ 30 มิถุนายน 2557 จาก www.si.mahidol.ac.th/th/division/soqd /admin/news_files/360_18_1.pdf และhttp://www.ha.or.th.

เอกสิทธิ์ ศรีระสันต์. (2554). *การจัดทานโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรกรณีศึกษาสาหรับ กองการสื่อสารศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย*. (สารนิพนธ์ วิทยาศาสตรมหาบัณฑิต)มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

Kuo-Hsiung Liao, Hao-En Chueh. (2012). Medical Organization Information Security Management Based on ISO27001 Information Security Standard, Information Management Department, Yuanpei University, HsinChu, Taiwan.*JOURNAL OF SOFTWARE*, 7(4), 792-797. Retrieved 30 June, 2014 from From http://www.ojs.academypublisher.com/index.php/jsw/article/download/jsw0704792797/4726

BSI UK. (2013). ISO/IEC 27001 Mapping guide, United kingdom. Retrived 31 August 2014. from http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf