การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด

นายรุ่งอรุณ นิรันต์เรือง

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2560

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

Mr. Rungarun Nirunruang

An Independent Study Submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Information and Communication Technology
School of Science and Technology
Sukhothai Thammathirat Open University
2017

หัวข้อการศึกษาค้นคว้าอิสระ การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ
ด้านการควบคุมการเข้าถึงระบบสารสนเทศ
ตามมาตรฐาน ISO/IEC 27001:2013
สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด

ชื่อและนามสกุล นายรุ่งอรุณ นิรันต์เรือง

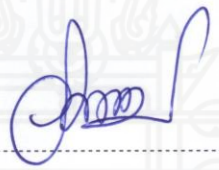
แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

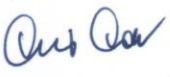
การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 25 มกราคม 2561

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ



..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์)

..... กรรมการ
(อาจารย์ ดร. ดวงดาว วิชาดากุล)



.....
(รองศาสตราจารย์ผกามาศ ผจญแกล้ว)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ชื่อการศึกษาค้นคว้าอิสระ การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด

ผู้ศึกษา นายรุ่งอรุณ นิรันต์เรือง **รหัสนักศึกษา** 2559600115

ปริญญา วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

ปีการศึกษา 2560

บทคัดย่อ

การศึกษาที่นำเสนอ มีวัตถุประสงค์ (1) เพื่อพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ จังหวัดตราด ตามมาตรฐาน ISO/IEC 27001:2013 และ(2) เพื่อพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013

วิธีดำเนินการมีดังนี้ (1) ศึกษารายละเอียดด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013 (2) รวบรวมและศึกษาข้อมูลโรงพยาบาลคลองใหญ่ประกอบด้วยโครงสร้างองค์กร เทคโนโลยีสารสนเทศในปัจจุบัน สภาพแวดล้อมและวิเคราะห์ปัญหาด้านการควบคุมการเข้าถึงระบบ ตามข้อกำหนด ISO/IEC 27001:2013 (3) พัฒนานโยบายแนวทางด้านการควบคุมการเข้าถึงระบบสารสนเทศ (4) พัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบตามมาตรฐาน ISO/IEC 27001:2013 และ (5) สรุปผลการดำเนินงาน

ผลการดำเนินงานพบว่า โรงพยาบาลคลองใหญ่มี (1) แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 :2013 และ (2) ระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบสำหรับใช้งานในองค์กรที่พัฒนาขึ้น เมื่อทำการทดสอบการใช้งานระบบพบว่า โรงพยาบาลคลองใหญ่มีความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศในภาพรวมร้อยละ 30.36 ข้อเสนอแนะสำหรับการพัฒนาครั้งนี้คือ (1) ผู้พัฒนาควรมีความรู้ความเข้าใจเกี่ยวกับข้อกำหนดและขั้นตอนการพัฒนา (2) ทำการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมทุกองค์ประกอบตามข้อกำหนด ISO/IEC 27001:2013 และ(3) ปรับปรุงนโยบายให้มีความทันสมัยตามการพัฒนาของเทคโนโลยีสารสนเทศ

คำสำคัญ: ความมั่นคงปลอดภัยสารสนเทศ, การควบคุมการเข้าถึง, ISO/IEC 27001:2013

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

Author: Mr.Rungarun Nirunruang; **ID:** 2559600115;

Degree: Master of Science Program (Information and Communication Technology);

Independent Study advisor: Dr.Vipa Jaroenpuntaruk, Associate Professor;

Academic year: 2017

Abstract

The objectives of this independent study were: (1) to develop procedures of information security management for access control based on ISO/IEC 27001:2013 for Klongyai hospital Trat Province, and (2) to develop assessment system for access control based on ISO/IEC 27001:2013.

The study was performed as followings: (1) studying the details of ISO/IEC 27001:2013 standard, (2) gathering information of Klongyai hospital including analyzing organization structure, existing information technology environment and problems of access control, (3) developing procedures and regulations of information security management for access control based on ISO/IEC 27001:2013, (4) developing information security management system for access control assessment, and (5) summarizing of operating results.

The results showed that (1) procedures and regulations for access control based on ISO/IEC 27001:2013, and (2) information security assessment system for availability of access control. According to system implementation, the overall result of access control availability in Klongyai hospital were 30.36 percent. The suggestions for this study were (1) the developer should have the knowledge and understanding of the development procedure, (2) developing procedures and regulations of information security management on every regulations of ISO/IEC 27001:2013, and (3) update procedures of information security management of information technology.

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

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระฉบับนี้ สำเร็จลุล่วงได้ด้วยความกรุณาเป็นอย่างยิ่งจาก รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช ที่ได้กรุณาให้คำแนะนำและติดตามการศึกษาค้นคว้าอิสระในครั้งนี้อย่างใกล้ชิดตลอดมา นับตั้งแต่เริ่มต้นจนกระทั่งสำเร็จเรียบร้อยสมบูรณ์ ผู้ศึกษารู้สึกซาบซึ้งในความกรุณาของท่านเป็นอย่างยิ่ง ขอขอบพระคุณ อาจารย์ ดร.ดวงดาว วิชาดากุล จากคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่กรุณาให้คำชี้แนะแนวทาง ในการปรับปรุงเนื้อหาการศึกษาค้นคว้าอิสระ ให้สมบูรณ์มากยิ่งขึ้น นอกจากนี้ผู้ศึกษาขอขอบพระคุณคณาจารย์แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช เพื่อนนักศึกษา และผู้มีส่วนเกี่ยวข้องในการศึกษาค้นคว้าอิสระครั้งนี้ทุกท่าน ที่ได้กรุณาให้การสนับสนุน ช่วยเหลือ และให้กำลังใจตลอดมา

รุ่งอรุณ นิรันต์เรือง

มกราคม 2561

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบัน การให้บริการของโรงพยาบาลในประเทศไทย มีการนำเทคโนโลยีสารสนเทศเข้ามามีส่วนร่วมในกระบวนการทำงาน เพื่อให้เกิดการบริการที่มีประสิทธิภาพและรวดเร็วมากขึ้น เห็นได้จากการที่โรงพยาบาลหลายแห่งทั้งภาครัฐและเอกชน ได้นำเทคโนโลยีทางการแพทย์ เช่น โปรแกรมการรักษา โปรแกรมการบริหารจัดการภายในโรงพยาบาล เอ็กซเรย์คอมพิวเตอร์ เอ็ม อาร์ ไอ การตรวจคลื่นไฟฟ้าหัวใจและการตรวจวิเคราะห์ทางห้องปฏิบัติการ เข้ามามีส่วนในการให้บริการ ทั้งกระบวนการรักษาและระบบงานอื่นๆ โดยเทคโนโลยีเหล่านี้มีการทำงานเชื่อมต่อกับเครื่องคอมพิวเตอร์และมีการเชื่อมโยงผ่านเครือข่าย โดยข้อมูลต่างๆได้ถูกจัดเก็บในฐานข้อมูลของโรงพยาบาลทั้งสิ้น การนำเทคโนโลยีสารสนเทศทางการแพทย์เหล่านี้เข้ามาใช้งาน ข้อมูลผู้ป่วยหรือข้อมูลอื่นๆ อาจเกิดความเสี่ยงต่อการถูกเปิดเผย เปลี่ยนแปลงหรือสูญหายได้ หากขาดการจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ดีพอ อันอาจส่งผลกระทบต่อตัวผู้ป่วยและผู้ใช้งานระบบ เช่น แพทย์ พยาบาล หรือเจ้าหน้าที่ผู้เกี่ยวข้องอื่นๆ ทำให้กระบวนการรักษาเกิดความผิดพลาดได้ ดังนั้นการจัดการให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศภายในโรงพยาบาลที่มีการใช้เทคโนโลยีสารสนเทศทางการแพทย์ จึงเป็นสิ่งสำคัญและจำเป็นอย่างยิ่ง

โรงพยาบาลคลองใหญ่ จังหวัดตราด มีการนำเทคโนโลยีสารสนเทศ เข้ามามีส่วนในกระบวนการรักษาพยาบาลและการจัดการภายในต่างๆ โดยอุปกรณ์ด้านเทคโนโลยี ทั้งซอฟท์แวร์และฮาร์แวร์ ทำงานผ่านเครือข่ายอินเตอร์เนตและอินตราเนต โดยเชื่อมโยงเครือข่ายผ่านผู้ให้บริการ ข้อมูลทั้งหมดจะถูกจัดเก็บในฐานข้อมูลของโรงพยาบาล ให้การบริการที่มีประสิทธิภาพ สะดวกรวดเร็วและได้มาตรฐาน ตามการรับรองคุณภาพมาตรฐานโรงพยาบาลหรือ Hospital Accreditation (HA) ซึ่งเป็นมาตรฐานที่กระทรวงสาธารณสุขมีนโยบาย ให้ทุกโรงพยาบาลในสังกัดทั่วประเทศ ได้รับการรับรองตามมาตรฐาน โดยมาตรฐานดังกล่าวมีข้อกำหนดเกี่ยวกับการจัดการระบบสารสนเทศและการจัดการเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยไว้ด้วย ซึ่งสภาพองค์กรด้านสารสนเทศในปัจจุบัน นโยบายและมาตรฐานความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล โดยเฉพาะด้านการควบคุมการเข้าถึง (Access Control) ระบบสารสนเทศในโรงพยาบาล พบว่ามีความเสี่ยงหลายอย่าง เช่น ขาดนโยบายด้านการเข้าถึงที่ครอบคลุม การขาด

แนวทางปฏิบัติที่ดี ในการเข้าถึงระบบสารสนเทศ เป็นต้น ซึ่งอาจเกิดความไม่ปลอดภัยต่อระบบสารสนเทศของโรงพยาบาล อันอาจส่งผลกระทบโดยตรงต่อตัวผู้ป่วย ผู้ใช้งานระบบ เช่น แพทย์ พยาบาล หรือเจ้าหน้าที่ผู้เกี่ยวข้องอื่นๆ และที่สำคัญคือ การรักษาพยาบาลอาจเกิดความผิดพลาด ส่งผลต่อชีวิตผู้ป่วยและผลเสียหายต่อโรงพยาบาลด้านอื่นๆ ตามมาได้

มาตรฐาน ISO/IEC 27001:2013 พัฒนาขึ้นโดย ISO (International Organization for Standardization) เป็นมาตรฐานสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System, ISMS) เพื่อสร้างประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศ รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยต่อผู้รับบริการ ผู้ให้บริการและระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องด้วย

ดังนั้น ผู้ศึกษาจึงได้ดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยพัฒนาด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ในโรงพยาบาลคลองใหญ่ จังหวัดตราด เพื่อเป็นแนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ และเป็นต้นแบบในการพัฒนาความมั่นคงปลอดภัยสารสนเทศด้านอื่นให้ครอบคลุม เพื่อให้ระบบสารสนเทศของหน่วยงานมีความมั่นคงปลอดภัยเพิ่มขึ้น

2. วัตถุประสงค์ของการศึกษา

2.1 เพื่อพัฒนานโยบายและแนวทาง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013

2.2 เพื่อพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013

3. ขอบเขตการศึกษา รูปแบบและวิธีการศึกษา

3.1 ศึกษารายละเอียดมาตรฐาน ทำการศึกษารายละเอียดมาตรฐาน ISO/IEC 27001:2013 ด้านการควบคุมการเข้าถึงระบบสารสนเทศ

3.2 พัฒนานโยบายและแนวทาง ทำการพัฒนานโยบายด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามแนวทาง ISO/IEC 27001:2013 ดังนี้

3.2.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

1) นโยบายควบคุมการเข้าถึง (Access Control Policy)

2) การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

3.2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

1) การลงทะเบียนและถอดถอนสิทธิ (User Registration and Deregistration

2) การจัดการสิทธิการเข้าถึง (User Access Provisioning)

3) การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Management of Secret Authentication Information of Users)

5) การทบทวนสิทธิการเข้าถึง (Review of User Access Rights)

6) การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

3.2.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of Secret Authentication Information)

3.2.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

1) การจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Restriction)

2) ขั้นตอนการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

3) ระบบบริหารจัดการรหัสผ่าน (Password Management System

4) การใช้โปรแกรมอรรถประโยชน์ (User of Privileged Utility Programs)

5) การเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to Program Source Code)

3.3 พัฒนาระบบ ทำการพัฒนาประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013

3.4 สรุปผลการดำเนินงาน ทำการสรุปผลการดำเนินการ

4. ประโยชน์ที่คาดว่าจะได้รับ

4.1 ได้นโยบายและแนวทาง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามแนวทาง ISO/IEC 27001:2013 สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด

4.2 ได้ระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามแนวทาง ISO/IEC 27001:2013 เพื่อเป็นต้นแบบสำหรับใช้งานในโรงพยาบาลคลอง-ใหญ่ จังหวัดตราด

4.3 โรงพยาบาลคลองใหญ่มีระบบสารสนเทศที่มั่นคงปลอดภัยมากขึ้น

4.4 เป็นต้นแบบสำหรับโรงพยาบาลชุมชนหรือองค์กรที่มีบริบทใกล้เคียงกัน

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

1. มาตรฐาน ISO/IEC 27001:2013

เป็นมาตรฐานสากลด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งกำหนดความต้องการเกี่ยวกับการจัดทำระบบให้มีความมั่นคงปลอดภัย เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้มีประสิทธิภาพต่อการดำเนินงานขององค์กร สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (2556) ได้แสดงข้อกำหนดตามมาตรฐาน ISO/IEC 27001:2013 ไว้ดังนี้

1.1 ข้อกำหนดองค์กร

1.1.1 การทำความเข้าใจองค์กรและบริบทองค์กร

องค์กรต้องกำหนดประเด็นภายในและภายนอกองค์กร ที่เกี่ยวข้องกับจุดประสงค์ ขององค์กรและที่ส่งผลต่อการบรรลุผลลัพธ์ ตามเป้ามายของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

1.1.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง ดังนี้ คือ

1) ผู้เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

2) ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของผู้ที่เกี่ยวข้อง

1.1.3 การกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ควรกำหนดกรอบและการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อระบุขอบเขตการดำเนินการ โดยกำหนดเป็นลายลักษณ์อักษรดังนี้

1) ประเด็นภายในและภายนอกองค์กร อ้างอิงจากข้อ 1.1.1

2) ความต้องการ อ้างอิงจาก ข้อ 1.1.2

3) การเชื่อมโยงและการสัมพันธ์กันของกิจกรรม โดยกิจกรรมอาจดำเนินงานเองหรือโดยองค์กรอื่น

1.1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ควรกำหนดระบบบริหาร บำรุงรักษา และปรับปรุงการจัดการความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องตามมาตรฐาน

1.2 ภาวะผู้นำ

1.2.1 การให้ความสำคัญของผู้นำ

ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำ และให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

1) ให้นโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ มีการกำหนดขึ้นมาและสอดคล้องกับกลยุทธ์ขององค์กร

2) รวมความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร

3) จัดการทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการดำเนินการ

4) สื่อสารความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผล และของการดำเนินการ ตามความต้องการที่กำหนดไว้

5) ทำให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามต้องการ

6) สนับสนุนและสั่งการบุคลากร เพื่อนำสู่ผลสำเร็จของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7) ส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง

8) สนับสนุนบทบาทการบริหารอื่นๆ ภายใต้ขอบเขตความรับผิดชอบ

1.2.2 นโยบาย

ผู้บริหารต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ

1) เหมาะสมต่อจุดประสงค์ขององค์กร

2) รวมวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศไว้ด้วย ตามข้อ 3.3.2 หรือกำหนดกรอบการปฏิบัติสำหรับการกำหนดวัตถุประสงค์ดังกล่าว

3) รวมการให้ความสำคัญของผู้บริหารในการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

4) นโยบายความมั่นคงปลอดภัยสารสนเทศ สามารถเข้าถึงได้ จัดทำเป็นลายลักษณ์อักษร

5) มีการสื่อสารให้ทราบภายในองค์กร

6) สามารถเข้าถึงได้โดยผู้ที่เกี่ยวข้องตามความเหมาะสม

1.2.3 บทบาท หน้าที่ ความรับผิดชอบและอำนาจหน้าที่

ผู้บริหารระดับสูง ต้องทำให้หน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มีการมอบหมายและสื่อสารให้ได้รับทราบกัน เพื่อ

1) ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับข้อกำหนดของเอกสารมาตรฐาน

2) ให้มีการรายงานประสิทธิภาพและประสิทธิผล ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

1.3 การวางแผน

1.3.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส

1) ภาพรวม

เมื่อดำเนินการวางแผนแล้ว องค์กรต้องพิจารณาประเด็นภายในและภายนอก ที่อ้างอิง ในข้อ ***1.1.1*** และความต้องการที่อ้างอิงในข้อ ***1.1.2*** และต้องกำหนดความเสี่ยงและโอกาสที่จำเป็นต้องจัดการเพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ บรรลุผลลัพธ์ตามที่ต้องการ

(1) ป้องกันหรือลดผลที่ไม่พึงปรารถนา

(2) ให้บรรลุการปรับปรุงอย่างต่อเนื่อง

(3) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส โดย

ก. รวมการดำเนินการดังกล่าวเข้ากับกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและนำสู่การปฏิบัติ

ข. ประเมินผลสัมฤทธิ์ของการดำเนินงานดังกล่าว

2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรควรกำหนดและประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศโดยต้อง

(1) กำหนดและปรับปรุงเกณฑ์ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งต้องรวมถึง

ก. เกณฑ์การยอมรับความเสี่ยง

ข. เกณฑ์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(2) การประเมินความเสี่ยงด้าน ความมั่นคงปลอดภัยสารสนเทศ ต้องได้ผลการประเมินที่สอดคล้อง ถูกต้อง และเปรียบเทียบได้

(3) ระบุความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ

ก. ประยุกต์กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องและความพร้อมของสารสนเทศ

ข. ระบุผู้เป็นเจ้าของความเสี่ยง

(4) วิเคราะห์ความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศ

ก. ประเมินผลที่เป็นไปได้ที่จะเกิดขึ้น

ข. ประเมินโอกาส ที่อาจเกิดขึ้นจริงตามความเสี่ยงที่ระบุไว้

ค. กำหนดระดับความเสี่ยง

ง. เปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดไว้ในข้อ ***1.3.1*** *2)*

จ. จัดลำดับความเสี่ยงที่ทำการวิเคราะห์ เพื่อจัดการตามความเหมาะสม

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับ กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษร

3) การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องกำหนดและประยุกต์กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาจากผลการประเมินความเสี่ยง

(1) กำหนดมาตรการทั้งหมดเพื่อดำเนินการตามที่กำหนด.

(2) องค์กรสามารถออกแบบมาตรการได้ตามที่ต้องการ หรือโดยอ้างอิงจากแหล่งก็ได้

(3) เปรียบเทียบมาตรการที่กำหนดไว้ในข้อ ***1.3.1*** *3)* กับมาตรการใน Annex A และตรวจสอบความสมบูรณ์ครบถ้วน

ข้อสังเกต 1 Annex A ประกอบด้วยรายการทั้งหมดของวัตถุประสงค์ของมาตรการและตัวมาตรการของมาตรฐานฉบับนี้ ขอให้ผู้ใช้งานมาตรฐานฉบับนี้อ้างอิงไปยัง Annex A เพื่อให้มั่นใจว่าไม่มีมาตรการใดที่ถูกมองข้ามไป

ข้อสังเกต 2 Annex A วัตถุประสงค์ของมาตรการถูกรวมไว้กับมาตรการที่เลือก วัตถุประสงค์ของมาตรการใน Annex A ไม่ครอบคลุมทั้งหมดอาจต้องมีมาตรการและวัตถุประสงค์เพิ่มเติม

(4) จัดทำเอกสารแสดงการใช้มาตรการ SoA (Statement of Applicability) ซึ่งประกอบด้วยมาตรการที่จำเป็น (ดูข้อ ***1.3.1*** *3)*) และคำอธิบายเหตุผลของการใช้มาตรการ

(5) จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(6) ขอการรับรองจากผู้เป็นเจ้าของความเสี่ยง สำหรับแผนการจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศและการยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เหลือ

องค์กรต้องจัดเก็บสารสนเทศที่เกี่ยวข้องกับกระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษร

1.3.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์

องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในกระบวนการทำงานและระดับที่เกี่ยวข้อง วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศประกอบด้วย

1) สอดคล้องกับความมั่นคงปลอดภัยสารสนเทศ

2) สามารถประเมินได้ (ถ้าสามารถปฏิบัติได้)

3) *พิจารณาผลประเมินและการจัดการความเสี่ยง* นำความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ผลการประเมินและการจัดการความเสี่ยงมาพิจารณาด้วย ดังนี้คือ

(1) สื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ

(2) ปรับปรุงตามความเหมาะสม

องค์กรต้องจัดเก็บสารสนเทศสำหรับวัตถุประสงค์ ด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างเป็นลายลักษณ์อักษรและเมื่อวางแผนวิธีการที่จะบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรต้องกำหนด

1) การดำเนินการ

2) ทรัพยากร

3) ผู้รับผิดชอบ

4) ระยะเวลา

5) วิธีประเมินผล

1.4 การสนับสนุน

1.4.1 ทรัพยากร

องค์กรต้องกำหนดทรัพยากรที่จำเป็นในการลงมือปฏิบัติ การบำรุงรักษา และการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

1.4.2 สมรรถนะ

1) กำหนดมรรถนะของบุคลากรขององค์กร ซึ่งส่งผลต่อประสิทธิภาพในการปฏิบัติงาน ด้านความมั่นคงปลอดภัยสารสนเทศ

2) ส่งเสริมให้บุคลากรมีความสามารถ โดยให้ความรู้ การฝึกอบรม หรือจากประสบการณ์การทำงาน

3) ดำเนินการเพื่อให้ได้สมรรถนะที่จำเป็น และประเมินสัมฤทธิ์ผลของการดำเนินการ

4) จัดเก็บสารสนเทศที่เหมาะสมเป็นลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานแสดง

5) การดำเนินการตามความเหมาะสม อาจหมายถึงการฝึกอบรม การเป็นพี่เลี้ยง การมอบหมายงานให้ผู้อื่น การจ้างหรือการทำสัญญากับบุคลากรที่มีความสามารถ

1.4.3 การสร้างความตระหนัก

บุคลากรในองค์กร ต้องตระหนักถึง

1) นโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

2) การมีส่วนในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงข้อดีของการปรับปรุงประสิทธิภาพในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ

3) ผลกระทบของการไม่ปฏิบัติตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.4.4 การสื่อสารให้ทราบ

องค์กรควรกำหนดความจำเป็นสำหรับการสื่อสารทั้งภายในและภายนอกองค์กรที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้ คือ

1) ต้องสื่อสารอะไรบ้าง

2) ต้องสื่อสารเมื่อไหร่

3) ต้องสื่อสารให้ใครทราบ

4) ผู้สื่อสารเป็นใคร

5) กระบวนการสื่อสาร

1.4.5 สารสนเทศที่เป็นลายลักษณ์อักษร

1) ภาพรวม

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ต้องรวมถึงสารสนเทศที่เป็นลายลักษณ์อักษร ดังนี้

(1) สารสนเทศที่เป็นลายลักษณ์อักษร กำหนดโดยองค์กรและความจำเป็นสำหรับประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อสังเกต สารสนเทศที่เป็นลายลักษณ์อักษร เกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ แตกต่างกันในแต่ละองค์กรเนื่องจาก

(2) ขนาดขององค์กร ประเภทกิจกรรม กระบวนการ ผลิตภัณฑ์ และบริการขององค์กร

(3) ความซับซ้อนของกระบวนการและความเชื่อมโยงระหว่างกระบวนการ

(4) ความสามารถของบุคลากร

2) การสร้างและปรับปรุง

เมื่อมีการสร้างและปรับปรุงสารสนเทศที่เป็นลายลักษณ์อักษร องค์กรต้องกำหนด

(1) ชื่อเอกสารและรายละเอียดต่างๆ

(2) รูปแบบภาษา เวอร์ชั่น กราฟฟิกและสื่อสำหรับ

(3) ความเหมาะสมในการทบทวนการอนุมัติเอกสาร

3) การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร

ต้องมีการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและตามมาตรฐานและต้องมีการควบคุมเพื่อ

(1) ให้สารสนเทศสามารถเข้าถึงได้เหมาะสม สำหรับการใช้งาน

(2) สารสนเทศได้รับการปกป้อง จากการสูญเสียความลับ การใช้งานที่ไม่เหมาะสม หรือการสูญเสียความถูกต้องสมบูรณ์

(3) การควบคุมสารสนเทศที่เป็นลายลักษณ์อักษร องค์ต้องระบุกิจกรรมดังนี้

(4) การแจกจ่าย การเข้าถึง การนำขึ้นมาใช้ และการใช้งาน

(5) การจัดเก็บและการรักษาไว้ รวมถึงการรักษาไว้ให้สามารถใช้งาน การควบคุมการเปลี่ยนแปลง เช่น การควบคุมเวอร์ชัน

(6) การจัดเก็บ ระยะเวลาจัดเก็บ และระยะเวลาในการทำลาย สารสนเทศที่มาจากแหล่งภายนอกที่ ต้องมีการควบคุมและระบุตามความเป็นจริง

ข้อสังเกตการเข้าถึงสารสนเทศ อาจหมายรวมถึง การตัดสินใจเกี่ยวกับการอนุญาตให้ดูสารสนเทศ หรือการอนุญาตและการให้อำนาจในการดูแลและเปลี่ยนแปลงสารสนเทศได้ด้วย

1.5 การดำเนินการ

1.5.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและควบคุม

องค์กรต้องวางแผน ลงมือปฏิบัติ และควบคุมกระบวนการ ตามที่กำหนดไว้ในข้อ ***1.3.1*** อย่างสอดคล้องกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้บรรลุวัตถุประสงค์ตามที่กำหนดไว้ในข้อ ***1.3.2***

องค์กรต้องเก็บรักษาสารสนเทศที่เป็นลายลักษณ์อักษร ในระดับที่จำเป็นเพื่อให้มั่นใจว่ากระบวนการเหล่านั้น มีการดำเนินการตามแผน

องค์กรต้องควบคุมการเปลี่ยนแปลงที่มีการวางแผนล่วงหน้า และทบทวนการเปลี่ยนแปลงที่เกิดขึ้นอย่างที่ไม่ได้ตั้งใจ เช่น การเปลี่ยนแปลงแบบฉุกเฉิน เพื่อลดผลในทางลบตามความจำเป็น

องค์ต้องทำให้มั่นใจว่ากระบวนการจ้างหน่วยงานภายนอกดำเนินการมีการระบุและควบคุมการดำเนินการ

1.5.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลง โดยนำเกณฑ์ความเสี่ยงที่กำหนดไว้ ในข้อ 3.1.2 มาพิจารณา และจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร จากผลของการประเมินความเสี่ยงด้านความมั่นปลอดภัยสารสนเทศ

1.5.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องปฏิบัติตามแผน การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและจัดเก็บสารสนเทศ ที่เป็นลานลักษณ์อักษร ซึ่งเป็นผลของการจัดการความเสี่ยงด้านความ มั่นคงปลอดภัยสารสนเทศ

1.6 การประเมินประสิทธิภาพและประสิทธิผล

1.6.1 การเฝ้าระวัง การวัดผล การวิเคราะห์และการประเมิน

องค์กรต้องประเมินประสิทธิภาพและประสิทธิผล ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามรายละเอียดดังนี้

อะไรที่จำเป็นต้องเฝ้าระวังและวัดผล

1) วิธีการในการเฝ้าระวัง วัดผล วิเคราะห์ และประเมินตามที่เหมาะสม
2) ข้อสังเกต วิธีการเลือกที่ใช้
3) เมื่อใดที่ต้องการเฝ้าระวังและวัดผลการดำเนินการ

4) ใครเป็นผู้เฝ้าระวังและวัดผล

5) เมื่อใดที่ผลจากการเฝ้าระวังและวัดผลต้องได้รับการวิเคราะห์และประเมิน

6) ใครเป็นผู้วิเคราะห์และประเมินผล

ต้องมีการจัดเก็บเอกสารที่เป็นลายลักษณ์อักษรที่เหมาะสม เพื่อใช้เป็นหลักฐานแสดงการเฝ้าระวังและวัดผล

1.6.2 การตรวจประเมินภายใน

องค์กรต้องดำเนินการตรวจประเมินภายใน ตามรอบระยะเวลาที่กำหนดไว้ โดยต้องมีความสอดคล้องกับความต้องการขององค์กรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามข้อกำหนดของมาตรฐาน

1) มีการปฏิบัติตามแนวทางอย่างเหมาะสม

2) วางแผน กำหนด ลงมือปฏิบัติ และบำรุงรักษาโปรแกรมการตรวจประเมิน รวมถึงความถี่ วิธีการ หน้าที่ความรับผิดชอบ ความต้องการในการตรวจประเมินตามแผน และการรายงานผลการตรวจประเมิน โดยนำผลการตรวจประเมินครั้งก่อนหน้า มาพิจารณาร่วมด้วย

3) กำหนดเกณฑ์การตรวจประเมินและขอบเขตของการตรวจประเมิน

4) คัดเลือกผู้ตรวจประเมิน ดำเนินการตรวจประเมินตามข้อเท็จจริงและหลักฐาน มีความเป็นกลางในการตรวจประเมิน

5) การรายงานการตรวจประเมินให้ผู้บริหารและผู้เกี่ยวข้องรับทราบ

6) จัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานโปรแกรมแสดงการตรวจประเมินและผลการตรวจประเมิน

1.6.3 การทบทวนของผู้บริหาร

ผู้บริหารระดับสูง ควรทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ขององค์กรตามรอบระยะเวลาที่กำหนดไว้ โดยพิจารณาดังนี้

1) สถานะการดำเนินการ จากผลการทบทวนครั้งก่อน

2) การเปลี่ยนแปลงภายในและภายนอกองค์กร ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในเรื่องของผลตอบกลับของประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศซึ่ง รวมถึงแนวโน้มของความไม่สอดคล้องของการดำเนินการแก้ไข ผลการเฝ้าระวังและวัดผล การตรวจประเมินและความสำเร็จตามวัตถุประสงค์ ด้านความมั่นคงปลอดภัยสารสนเทศ

3) ผลตอบกลับจากผู้ที่เกี่ยวข้อง

4) ผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง

5) แผนการปรับปรุงอย่างต่อเนื่อง

ผลการทบทวนของผู้บริหารต้องรวมการตัดสินใจเกี่ยวกับโอกาส ในการปรับปรุงอย่างต่อเนื่อง และความจำเป็นสำหรับการเปลี่ยนแปลง ต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และต้องจัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหาร

1.7 การปรับปรุง

1.7.1 ความไม่สอดคล้องและการดำเนินการแก้ไข

เมื่อมีความไม่สอดคล้องเกี่ยวดับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ควรดำเนินการดังนี้

ตอบกลับความไม่สอดคล้องตามความเหมาะสม โดยควบคุมแก้ไขความไม่สอดคล้องและจัดการกับผลที่เกิดขึ้น

1) ประเมินความจำเป็นสำหรับการดำเนินการ เพื่อแก้ไขสาเหตุ ของความไม่สอดคล้องไม่ให้เกิดขึ้นซ้ำโดย การทบทวนความไม่สอดคล้อง ระบุสาเหตุของความไม่สอดคล้องและระบุความสอดคล้องที่คล้ายกัน

2) ดำเนินการแก้ไขที่จำเป็น

3) ทบทวนประสิทธิผลผลของการดำเนินการแก้ไข

4) เปลี่ยนแปลงระบบบริหารจัดการความมั่นคงสารสนเทศ อย่างเหมาะสม

5) จัดเก็บสารสนเทศที่เป็นลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานแสดงสภาพของความไม่สอดคล้องกับการดำเนินการและผลการดำเนินการ

1.7.2 การปรับปรุงอย่างต่อเนื่อง

องค์กรต้องปรับปรุงความเหมาะสม ความเพียงพอ และความประสิทธิผลของระบบบริหารจัดการวามมั่นคงปลอดภัยอย่างต่อเนื่อง

2. ข้อกำหนดด้านการควบคุมการเข้าถึงระบบ (Access Control) ตามมาตรฐาน ISO/IEC 27001:2013

2.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

มีวัตถุประสงค์ เพื่อจัดการการเข้าถึงระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต่างๆ โดยมีข้อกำหนดถึง

2.1.1 นโยบายควบคุมการเข้าถึง (A.9.1.1 Access Control Policy)

ต้องมีการกำหนด และจัดทำเป็นลายลักษณ์อักษร ทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

2.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย (A.9.1.2 Access to Network and Network Services)

ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติให้เข้าถึงเท่านั้น

2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

มีวัตถุประสงค์ เพื่อควบคุมการเข้าถึงของผู้ใช้งาน ให้ใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตของบุคคล

2.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (A.9.2.1 User Registration and Deregistration)

ต้องมีกระบวนการขั้นตอนอย่างเป็นทางการและมีการปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง

2.2.2 การจัดการสิทธิการเข้าถึงผู้ใช้งาน (A.9.2.2 User Access Provisioning)

การจัดการสิทธิการเข้าถึงผู้ใช้งาน ต้องปฏิบัติตาม ทั้งเรื่องการให้สิทธิ การถอดถอนสิทธิ การเข้าถึงสำหรับผู้ใช้งานทุกประเภทขององค์กร

2.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (A.9.2.3 Management of Privileged Access Right)

การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดควบคุม

2.2.4 การบริการจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (A.9.2.4 Management of Secret Authentication Information of Users)

การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ที่เป็นข้อมูลลับต้องมีการควบคุมตามกระบวนการบริการจัดการที่เป็นทางการ

2.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.5 Review of User Access Rights)

เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามระยะเวลาที่กำหนด

2.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (A.9.2.6 Removal or Adjustment of Access Rights)

สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอก ต้องดำเนินการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญาหรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้อง เมื่อมีการใช้งาน

2.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

มีวัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

2.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (A.9.3.1 User of Secret Authentication Information)

ผู้ใช้งานต้องปฏิบัติตามวิธีปฏิบัติขององค์กร ในการใช้งานข้อมูลการพิสูจน์ตัวตน ซึ่งเป็นข้อมูลลับ

2.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

มีวัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

2.4.1 การจำกัดการเข้าถึงระบบสารสนเทศ (A.9.4.1 Information Access Restriction)

การเข้าถึงระบบสารสนเทศและฟังก์ชันของระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

2.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (A.9.4.2 Secure Log-on Procedures)

กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึง การเขาถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

2.4.3 ระบบบริหารจัดการระบบผ่าน (A.9.4.3 Password Management System)

ระบบบริหารจัดการระบบผ่าน ต้องมีปฏิสัมพันธ์กับผู้ใช้งานและต้องบังคับให้มีการตั้งรหัสผ่านที่มีคุณภาพ

2.4.4 การใช้โปรแกรมอรรถประโยชน์ (A.9.4.4 User of Privileged Utility Programs)

การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้งานอย่างใกล้ชิด

2.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (A.9.4.5 Access Control to Program Source Code)

ต้องมีการจำกัดและควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม

3. โปรแกรมเว็บเบส (Web Based Program)

Nopjira Suttirat (อ้างอิงจาก http://slideplayer.in.th/slide/2850745) ได้อธิบายเกี่ยวกับโปรแกรมเว็บเบสไว้ว่า เป็นโปรแกรมหรือกลุ่มของโปรแกรม ที่ได้รับการพัฒนาขึ้นมาเพื่อใช้งานในบริการ www ของระบบเครือข่ายอินเตอร์เนตหรืออินตราเนต โดยใช้โพรโตคอล TCP/IP ที่เป็นมาตรฐานสื่อสารข้อมูล โดยผู้ใช้งานสามารถติดต่อสื่อสาร ผ่านการใช้งานโปรแกรมเว็บเบส โดยมีหลักการทำงาน คือ ติดตั้งโปรแกรมหรือแอพพลิเคชั่น ไว้บนเซิรฟเวอร์เพื่อให้บริการ เมื่อต้องการใช้งานโปแกรม เพียงทำการเปิดเว็บบราวเซอร์แล้วพิมพ์ URL ของโปรแกรม ก็สามารถใช้งานโปรแกรมได้

3.1 องค์ประกอบของเว็บเบส

3.1.1 ส่วนประกอบฝั่งผู้ใช้งาน (Client side technology)

1) เว็บเบราว์เซอร์ (Web browser)

เป็นซอฟแวร์เพื่อใช้เข้าถึงแอพพลิเคชั่น โดยการใส่ URL ของโปรแกรมเว็บเบสที่ต้องการเข้าใช้งาน เว็บเบราวซ์เซอร์มีหน้าที่หลักๆ คือ รับข้อมูลและคำสั่งจากผู้ใช้งาน แปลงคำสั่งของผู้ใช้งานให้เป็น HTTP Request เพื่อส่งต่อให้เว็บเสิร์ฟเวอร์ ประมวลผล HTTP response และเรียกใช้ปลักอิน แปลงภาษา HTML, CSS, JavaScript ให้ข้อมูลแสดงผลต่อผู้ใช้งาน

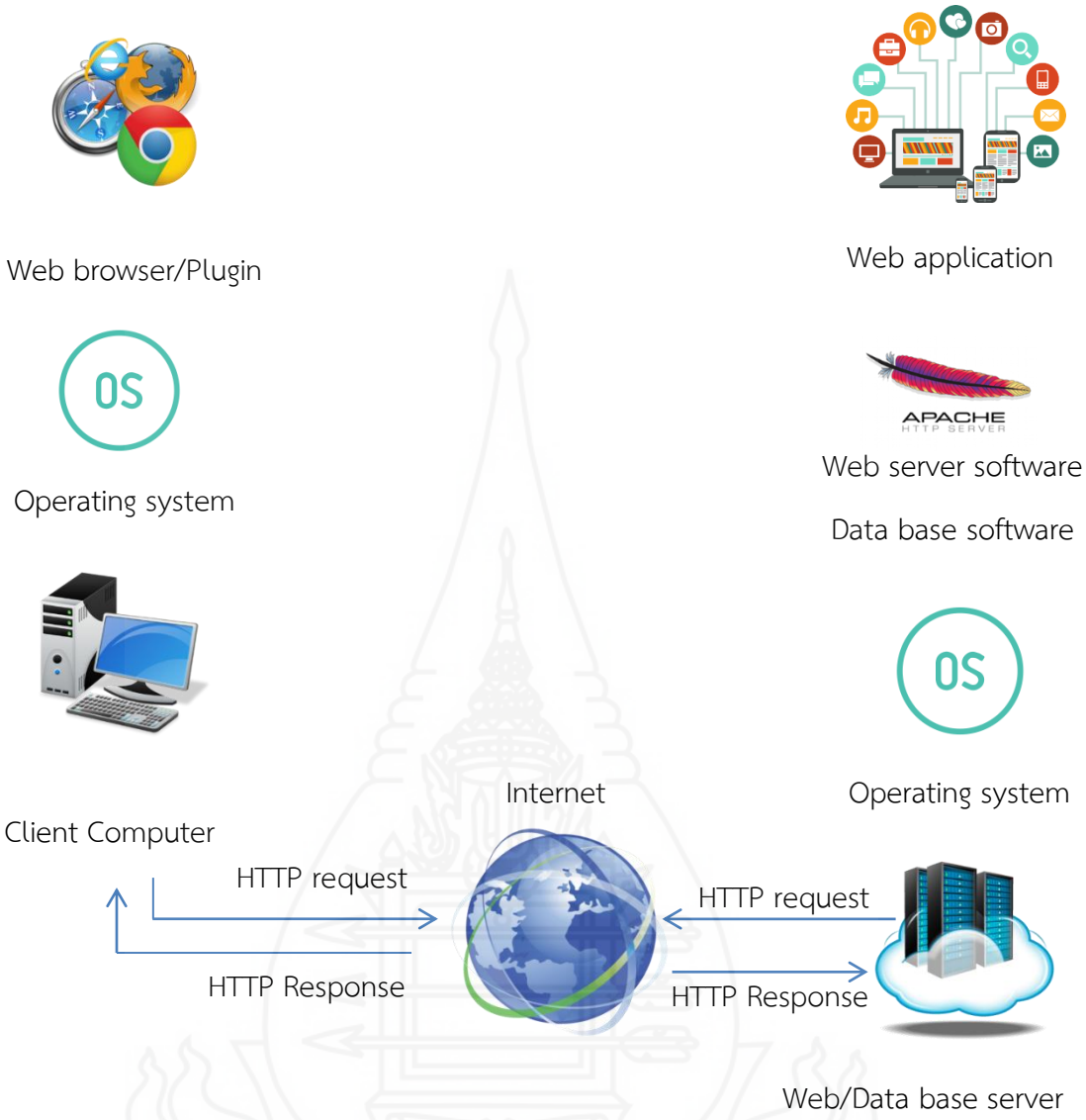
2) ส่วนต่อความสามารถเว็บและเบราว์เซอร์ (Web plugin และ Browser Add - on/Extension)

ส่วนต่อความสามารถเว็บหรือ Web plugin เป็นโปรแกรมทำงานร่วมกับเว็บเบราว์เซอร์ เช่น PDF reader, Adobe Flash, Java Applet, Silverlight เป็นต้น โดยจะถูกเบราว์เซอร์เรียกใช้ เมื่อเว็บไซต์มีเนื้อหาที่ต้องแสดงผลโดย Plugin URL ให้เป็น IP Address เพื่อค้นหาเครื่องเว็บเซิร์ฟเวอร์และสร้างการเชื่อมต่อระหว่างเครื่องผู้ใช้งานและเครื่องเซิร์ฟเวอร์

3.1.2 ส่วนประกอบฝั่งเซิร์ฟเวอร์ (Server side technology)

1) เว็บแอพพลิเคชั่น (Web Application)

ทำหน้าที่ติดต่อกับผู้ใช้งาน รับ ประมวลผลและแสดงข้อมูล ประมวลผลข้อมูลจัดการข้อมูลในฐานข้อมูล เว็บแอปพลิเคชันแบ่งเป็นสามส่วน คือ ส่วนติดต่อกับผู้ใช้งานเพื่อรับข้อมูลและแสดงผล ส่วนที่ประมวลผลการทำงาน และส่วนติดต่อและจัดการกับข้อมูลและฐานข้อมูล



ภาพที่ 2.1 องค์ประกอบของโปรแกรมเว็บเบส

2) ฟร้อนต์เอนเว็บเทคโนโลยี (Front end web technology)

ใช้สร้างส่วนติดต่อกับผู้ใช้งาน ในการสร้างเว็บแอปพลิเคชั่น เช่น HTML, CSS, และ JavaScript Front-End Web Technology ถูกจำกัดด้วยมาตรฐานของ World Wide Web Consortium (W3C) ซึ่งเป็นผู้กำหนดมาตรฐาน เพื่อให้ผู้พัฒนาเว็บเบราว์เซอร์แสดงผลข้อมูลในรูปแบบเดียวกัน

3) แบคเอนเว็บเทคโนโลยี (Back end web technology)

Back-End Web Technology เป็นส่วนประมวลผลตรรกะและการทำงานของเว็บแอปพลิเคชัน เริ่มหลังจากเว็บแอปพลิเคชั่นได้รับ HTTP request จากผู้ใช้งาน ประมวลผล และส่งข้อมูลกลับผู้ใช้งาน เทคโนโลยีที่ใช้พัฒามีความหลากหลาย เนื่องจากไม่มีข้อจำกัดจากมาตรฐานกลาง

4) เว็บเซริฟเวอร์ซอฟแวร์ (Web server software)

ทำหน้าหน้าที่ประมวลผล HTTP request ที่ได้รับและตอบกลับด้วย HTTP response ปัจจุบันมีหลายตัวที่ได้รับความนิยม เช่น Apache HTTP server และ Internet Information Service ที่ได้รับความนิยมมากที่สุดคือ Apache HTTP server โดยมักใช้งานคู่กับ PHP และ MySQL

5) ระบบปฏิบัติการ (Operating system)

มีหน้าที่จัดการทรัพยากรของเครื่องเซิร์ฟเวอร์ เนื่องจาก web application เปิดให้ผู้ใช้งานเข้าถึงได้ตลอดเวลา ระบบปฏิบัติการบนเซิร์ฟเวอร์จึงต้องมีความเสถียรและสามารถจัดการกับทรัพยากรได้อย่างมีประสิทธิภาพ

2.1 ประโยชน์ของเว็บเบส

2.1.1 ไม่จำเป็นต้องติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ส่วนตัว ทำให้ไม่เปลืองพื้นที่หน่วยความจำ

2.1.2 ผู้ดูแลระบบสามารถควบคุมและอัพเดตโปรแกรมได้ง่ายและสะดวก

2.1.3 ประหยัดค่าใช้จ่ายในการบำรุงรักษา

2.1.4 ไม่จำเป็นต้องใช้คอมพิวเตอร์เฉพาะเครื่องในการใช้งานโปแกรม

4. มาตรฐานการจัดการความมั่นคงปลอดภัยของข้อมูลผู้ป่วย พ.ศ. 2559

สำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข ได้กำหนดมาตรฐานในการจัดการความมั่นคงปลอดภัยของข้อมูลผู้ป่วยไว้ดังนี้คือ

4.1 แนวทางปฏิบัติทั่วไปสำหรับโรงพยาบาล ในการป้องกันดูแลความมั่นคงปลอดภัยสารสนเทศ

4.1.1 กำหนดและแบ่งพื้นที่จัดเก็บเวชระเบียน ทำการกำหนดพื้นที่เก็บเวชระเบียนและเครื่องแม่ข่ายคอมพิวเตอร์ให้เห็นชัดเจน ให้เป็นเขตหวงห้ามเฉพาะ ปิดหรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอ เมื่อไม่มีเจ้าหน้าที่อยู่

4.1.2 จัดให้มีสมุดทะเบียนบันทึก การเข้าออกห้องเครื่องแม่ข่ายคอมพิวเตอร์ การนำเวชระเบียนออกมาใช้และส่งเวชระเบียนกลับคืน

4.1.3 จัดให้มีระบบตรวจสอบการส่งเวชระเบียน และดำเนินการตรวจสอบทุกวัน ก่อนเวลา 16.00 น. หากพบเวชระเบียนไม่ส่งกลับ ให้ติดตามค้นหาและนำกลับคืนมาให้เสร็จสิ้นก่อนเวลา 16.30 น.

4.1.4 จัดให้มีระบบฉุกเฉินสำหรับปฏิบัติงาน เมื่อมีเหตุไฟฟ้าดับ หรือระบบคอมพิวเตอร์ ใช้งานไม่ได้ ให้มั่นใจว่าการค้นหา บันทึกและจัดเก็บข้อมูลผู้ป่วย ดำเนินไปได้อย่างครบถ้วน ถูกต้อง ไม่บกพร่อง และมีการซักซ้อมเป็นระยะๆ เช่น ทุกปี และปรับปรุงกระบวนการทำงานเมื่อระบบขัดข้องให้เหมาะสมอยู่เสมอ

4.1.5 กำหนดชั้นความลับของข้อมูลผู้ป่วย ทำการกำหนดชั้นความลับของข้อมูลของผู้ป่วยเป็นระดับ “ลับ” และดำเนินการแบบเดียวกับการรับส่ง เอกสารลับ ดังนี้

1) การทำสำเนา การพิมพ์สำเนาต้องบันทึกจำนวนชุด ชื่อ ตำแหน่งของผู้ดำเนินการ ชื่อสถานพยาบาลที่จัดทำ วันที่ เวลา ไว้ที่ต้นฉบับและฉบับสำเนาทุกฉบับ กรณีสั่งพิมพ์สำเนาออกจากระบบคอมพิวเตอร์ต้องบันทึกการสั่งพิมพ์ จำนวนชุด ชื่อ ตำแหน่งของผู้ดำเนินการ ชื่อสถานพยาบาลที่จัดทำ วันเวลาที่สั่งพิมพ์ทุกครั้ง เก็บไว้ในระบบฐานข้อมูล

2) การส่งออกเวชระเบียนหรือสำเนาเวชระเบียนออกนอกสถานพยาบาล ต้องบรรจุซองหรือภาชนะทึบแสงสองชั้น ซองชั้นในจ่าหน้าระบุเลขหนังสือนำส่ง ชื่อ ตำแหน่งผู้รับและหน่วยงานผู้ส่ง ทำเครื่องหมายแสดงชั้นความลับ ด้านหน้าและด้านหลัง ซองชั้นนอกให้จ่าหน้าระบุเลขที่หนังสือนำส่ง ชื่อ ตำแหน่งผู้รับและหน่วยงานผู้ส่ง เช่นเดียวกับซองชั้นในแต่ไม่ต้องมีเครื่องหมายแสดงชั้นความลับใดๆ การส่งออกในรูปแบบไฟล์อิเล็กทรอนิกส์ ต้องเข้ารหัส มิให้ผู้ที่ไม่มีสิทธิ์สามารถเปิดไฟล์ดูได้

3) การจัดเก็บเวชระเบียน ต้องจัดเก็บไว้ตลอดไป หากผู้ป่วยเสียชีวิตให้แยกเวชระเบียนออกมาเก็บไว้ในสถานที่เก็บเวชระเบียนผู้เสียชีวิต หากเสียชีวิตผิดธรรมชาติให้เก็บรักษาไว้ไม่ต่ำกว่า 20 ปี หากมิใช่การเสียชีวิตผิดธรรมชาติให้เก็บรักษาไว้ไม่ต่ำกว่า 10 ปี อาจพิจารณาทำลายเวชระเบียนหากพื้นที่จัดเก็บไม่พอ โดยใช้เครื่องทำลายเอกสารตัดเป็นชิ้นเล็กๆ

4.1.6 จัดให้มีกระบวนการพิจารณาความเหมาะสม ในการนำข้อมูลของผู้ป่วยที่สามารถระบุตัวบุคคลได้ เช่น มีชื่อหรือเลขประจำตัวผู้ป่วย ไปใช้ประโยชน์อย่างอื่น เช่น การวิจัย ให้เป็นไปตามกฎหมายและไม่ละเมิดสิทธิของผู้ป่วย

4.1.7 จัดให้มีระบบยินยอมให้ใช้ข้อมูลผู้ป่วย ให้ผู้ป่วยได้อ่านทำความเข้าใจและอนุญาตให้โรงพยาบาลใช้ข้อมูลเพื่อประโยชน์ในการรักษา

4.2 แนวทางปฏิบัติทั่วไปสำหรับเจ้าหน้าที่ทุกคน ที่มีโอกาสเข้าถึงข้อมูลผู้ป่วยของโรงพยาบาล

4.2.1 เจ้าหน้าที่ทุกคนมีหน้าที่ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ ของข้อมูล ตลอดจนเอกสารเวชระเบียนของผู้ป่วย

4.2.2 ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลในเวชระเบียนและ ในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ

4.2.3 การแก้ไขข้อมูลผู้ป่วยให้ดำเนินการได้ ตามระเบียบปฏิบัติว่าด้วยการแก้ไขข้อมูลโดยเคร่งครัด เช่น หากเขียนผิดห้ามใช้ปากการะบายสีทึบทับข้อความจนไม่เห็นข้อความเดิม ห้ามใช้น้ำยาลบคำผิดในเวชระเบียนผู้ป่วย การแก้ไขทำได้โดยการลากเส้นทับข้อความเดิมเพียงเส้นเดียว แล้วเขียนข้อความที่แก้ไขไว้ใกล้กับข้อความเดิม พร้อมลงนามกำกับ และวันเวลาที่แก้ไข สำหรับการแก้ไขข้อมูลในระบบคอมพิวเตอร์ ห้ามลบข้อมูลเดิมทิ้ง แต่ให้ทำเครื่องหมายว่ามีการแก้ไขแล้วเชื่อมโยงข้อมูลที่เพิ่มเติมแก้ไข ให้รู้ว่าข้อความใหม่ใช้แทนข้อความเดิมอย่างไร

4.2.4 การส่งข้อมูลผู้ป่วย ให้กับบุคลากรภายในสถานพยาบาลเดียวกัน ให้ดำเนินการตามระเบียบโดยเคร่งครัด

4.2.5 ห้ามส่งข้อมูลผู้ป่วยโดยใช้ช่องทางที่ไม่เหมาะสม เช่น ทาง LINE หรือ Social Media

4.2.6 ตั้งรหัสผ่านในการเข้าใช้งาน ระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยาก ตรงตามระเบียบของสถานพยาบาล ปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัด ไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ

4.2.7 ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอก ทุกกรณี สำหรับการเปิดไฟล์งานจากหน่วยงานภายใน ให้ตรวจหาไวรัสทุกครั้ง

4.2.8 ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูล เช่น CD-ROM, USB Drive, External Hard Disk อุปกรณ์เครือข่าย เช่น Hub, Switch, Wi-Fi Router มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของโรงพยาบาลที่ใช้ฐานข้อมูลผู้ป่วย เว้นแต่ได้รับอนุญาตจากผู้อำนวยการ

4.2.9 ห้ามใช้คอมพิวเตอร์ของโรงพยาบาล ที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วยในการติดต่อกับอินเทอร์เนตทุกกรณี ยกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะ ที่ต้องเชื่อมต่ออินเทอร์เนต พร้อมกันกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วย ซึ่งได้รับอนุญาตจากผู้อำนวยการ

5. งานวิจัยที่เกี่ยวข้อง

ผู้ศึกษาได้ทำการศึกษาค้นคว้าและพบผลงานศึกษาและวิจัยที่เกี่ยวข้องดังนี้ คือ

เดชาวัต นิชาญานันท์ (2555) ทำการศึกษาและพัฒนาการจัดการนโยบายความปลอดภัยมั่นคงระบบสารสนเทศ สำหรับโรงพยาบาลสินแพทย์ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย โดยใช้แนวทางของ ISO/IEC 27001 ในการจัดทำนโยบายและข้อกำหนดในการปฏิบัติงานของเจ้าหน้าที่ ส่งผลให้ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลดลง ระบบสารสนเทศมีความมั่งคงปลอดภัยมากขึ้น การดำเนินธุรกิจทาง โรงพยาบาลเป็นไปอย่างราบรื่น และเป็นที่ยอมรับและไว้วางใจของผู้รับบริการ

เฉลิม สุวรรณะ (2554) ทำการศึกษาความมั่นคงปลอดภัยสารสนเทศของศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ซึ่งมีการมีการนำเทคโนโลยีสารสนเทศเข้ามาใช้งานเพื่อเพิ่มประสิทธิภาพการทำงาน พบความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศหลายด้าน เช่น ระบบเครือข่ายขององค์กรถูกโจมตี การใช้เทคโนโลยีสารสนเทศไม่เหมาะสม ทำให้องค์กรมีความเสี่ยงและได้รับความเสียหาย จึงได้จัดทำนโยบายและข้อกำหนดการปฏิบัติงาน โดยอ้างอิงตามมาตรฐานสากล ISO/IEC 27001 เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยมากขึ้น เมื่อนำนโยบายและแนวทางมาใช้งานในศูนย์การแพทย์ พบว่าหน่วยงานมีความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ลดลง

ไพศาล จันทร์เลื่อน (2557) ทำการศึกษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสน - เทศ ของศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร โดยใช้มาตรฐาน ISO/IEC 27001 ในการเป็นแนวทางการศึกษา พบว่าหน่วยงานมีความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยเฉพาะการขาดนโยบายและแนวทางการปฏิบัติงาน จึงได้พัฒนาร่างนโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานสำหรับผู้ดูแลระบบและผู้เกี่ยวข้อง โดยใช้มาตรฐาน ISO/IEC 27001 เป็นแนวทางในการพัฒนานโยบายและแนวทางปฏิบัติ พบว่าหน่วยงานมีความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ลดลง

บทที่ 3
วิธีการดำเนินงาน

ผู้ศึกษาได้พัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ โดยดำเนินการพัฒนาเฉพาะด้านการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) เนื่องจากมีความสำคัญโดยตรงต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเลือกใช้มาตรฐาน ISO/IEC 27001 : 2013 เป็นแนวทางในการพัฒนา และใช้โรงพยาบาลคลองใหญ่ จังหวัดตราด เป็นกรณีศึกษาเป้าหมาย เนื่องจากพบปัญหาและความเสี่ยงด้านการควบคุมการเข้าถึงระบบสารสนเทศ โดยมีวิธีการดำเนินงานดังนี้

ภาพที่ 3.1 ขั้นตอนการดำเนินการ

1. ศึกษามาตรฐานและทฤษฎีที่เกี่ยวข้อง

ศึกษารายละเอียดและข้อกำหนดความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013 จากเว็บไซต์ บริษัททีเน็ต (อ้างอิงจาก http://www. tnetsecurity.com/content_audit/27001-2013.pdf) ตามข้อกำหนดดังนี้

1.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

มีวัตถุประสงค์ เพื่อจัดการการเข้าถึงระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต่างๆ ประกอบด้วยข้อกำหนด 2 ข้อ คือ A.9.1.1 Access Control Policy และ A.9.1.2 Access to networks and network services

1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

มีวัตถุประสงค์ เพื่อควบคุมการเข้าถึงของผู้ใช้งาน เฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตของบุคคล ประกอบด้วยข้อกำหนด 6 ข้อ คือ A.9.2.1 User Registration and Deregistration, A.9.2.2 User Access Provisioning, A.9.2.3 Management of Privileged Access Right, A.9.2.4 Management of Secret Authentication Information of Users, A.9.2.5 Review of User Access Rights และ A.9.2.6 Removal or Adjustment of Access Rights

1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

มีวัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน ประกอบด้วยข้อกำหนด 11 ข้อ คือ A.9.3.1 User of Secret Authentication Information

1.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

มีวัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ประกอบด้วยข้อกำหนด 5 ข้อ คือ A.9.4.1 Information Access Restriction, A.9.4.2 Secure Log-on Procedures, A.9.4.3 Password Management System, A.9.4.4 User of Privileged Utility Programs และ A.9.4.5 Access Control to Program Source Code

2. ศึกษาองค์กร ระบบสารสนเทศและวิเคราะห์ปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ทำการศึกษาข้อมูลองค์กร ระบบสารสนเทศ และวิเคราะห์ปัญหาการควบคุมเข้าถึงระบบสารสนเทศของโรงพยาบาลคลองใหญ่ ดังนี้

2.1 ข้อมูลพื้นฐานทั่วไปของโรงพยาบาล

โรงพยาบาลคลองใหญ่ เป็นโรงพยาบาล ในสังกัดสำนักงานสาธารณสุขจังหวัดตราดกระทรวงสาธารณสุข เป็นโรงพยาบาลชายแดนไทย - กัมพูชา เป็นโรงพยาบาลชุมชนขนาด 30 เตียง ผู้รับ บริการส่วนใหญ่ เป็นประชาชนพื้นที่ในเขตอำเภอคลองใหญ่ ทั้งชาวไทยและชาว ต่างชาติ โดยให้บริการส่งเสริม ป้องกัน รักษาและฟื้นฟูโรค

ตั้งอยู่ที่ 1 หมู่ 9 ตำบลคลองใหญ่ อำเภอคลองใหญ่ จังหวัดตราด 23110 เป็นโรงพยาบาลชุมชนระดับทุติยภูมิ สังกัดสำนักปลัดกระทรวงกระทรวงสาธารณสุขสำนักงานสาธารณสุขจังหวัดตราด จำนวนเตียงขออนุญาต 30 เตียง ให้บริการจริง 36 เตียง อัตราครองเตียงในปีงบประมาณ 2560 เท่ากับ 56% มีหน่วยบริการปฐมภูมิในเครือข่าย จำนวน 4 แห่งคือ โรงพยาบาลส่งเสริมสุขภาพตำบลบ้านไม้รูด โรงพยาบาลส่งเสริมสุขภาพบ้านห้วงโสม โรงพยาบาลส่งเสริมสุขภาพบ้านคลองมะขามและโรงพยาบาลส่งเสริมสุขภาพบ้านหาดเล็ก

วิสัยทัศน์ขององค์กรคือ เครือข่ายแห่งคุณภาพชั้นนำด้านการสร้างสุขภาพระหว่างชายแดนไทย – กัมพูชา

2.2 ข้อมูลด้านเทคโนโลยีสารสนเทศขององค์กร

ระบบสารสนเทศโรงพยาบาลคลองใหญ่ อยู่ภายใต้ความรับผิดชอบของศูนย์คอมพิวเตอร์ประจำโรงพยาบาล เป็นหน่วยงานดูแลระบบและพัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อตอบสนองความต้องการของผู้บริหาร ผู้ให้บริการและผู้รับบริการ ดูแลระบบคอมพิวเตอร์ทั้งด้าน Hardware Software และฐานข้อมูล ให้ระบบสามารถทำงานได้ตลอด 24 ชั่วโมง มีเครื่องคอมพิวเตอร์ที่ใช้ในโรงพยาบาล 72 เครื่อง โดย มีวัตถุประสงค์เพื่อตอบสนองความต้องการของหน่วยงานในโรงพยาบาลให้ได้ข้อมูลถูกต้องทันเวลา พิทักษ์สิทธิ และสามารถนำไปใช้ประโยชน์ได้จริง

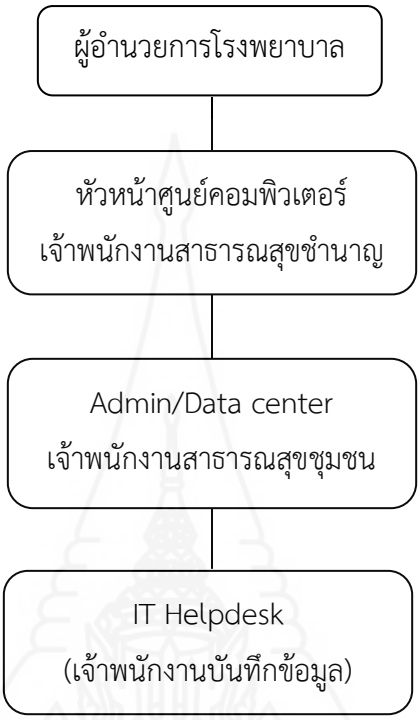
มีการนำข้อมูลที่ได้มาใช้ในการวางแผนการดำเนินงาน การแก้ปัญหาต่าง ๆ เพิ่มช่องทางการสื่อสารและการเรียนรู้ภายในองค์กร โดยด้านโครงสร้างพื้นฐานมีการเชื่อมโยงเครือข่าย LAN ครอบคลุมหน่วยงานทั้งโรงพยาบาล มีการแบ่งระบบเครือข่ายออกเป็น 2 ระบบ คือ ระบบเครือข่ายการให้บริการผู้ป่วย HosXp และระบบเครือข่าย Internet

2.1.1 โครงสร้างการบริหารงานศูนย์คอมพิวเตอร์

ศูนย์คอมพิวเตอร์โรงพยาบาลคลองใหญ่ ประกอบด้วยเจ้าหน้าที่ประจำศูนย์ 3 คน ตำแหน่งเจ้าพนักงานสาธารณสุขชุมชน จำนวน 2 คน และเจ้าหน้าที่บันทึกข้อมูล จำนวน 1 คน โดยไม่มีผู้รับผิดชอบงานที่จบการศึกษาด้านเทคโนโลยีสารสนเทศโดยตรง ผู้รับผิดชอบเป็นผู้มีความสนใจในระบบเทคโนโลยีสารสนเทศ มีประสบการณ์ทำงานและผ่านการอบรมด้านเทคโนโลยีสารสนเทศ

โครงสร้างการบริหารงานศูนย์คอมพิวเตอร์

โรงพยาบาลคลองใหญ่



ภาพที่ 3.2 โครงสร้างการบริหารงานศูนย์คอมพิวเตอร์

2.1.2 โครงสร้างด้าน Hardware

1) เครื่องแม่ข่ายหลัก (Server) สำหรับโปรแกรม HOS-xP จำนวน 1 เครื่อง

2) เครื่องแม่ข่าย Webpage และสำรองข้อมูลจาก Server จำนวน 1 เครื่อง

3) เครื่องคอมพิวเตอร์ลูกข่าย จำนวน 52 เครื่อง

4) เครื่องคอมพิวเตอร์แบบพกพา จำนวน 8 เครื่อง

5) อุปกรณ์กระจายสัญญาณ (Switch Hub) จำนวน 6 เครื่อง

6) อุปกรณ์กระจายสัญญาณไร้สาย จำนวน 7 จุด

7) กล้องวงจรปิด จำนวน 30 ตัว

8) เครื่องสำรองไฟ (UPS) จำนวน 60 เครื่อง

9) เครื่องพิมพ์ จำนวน 40 เครื่อง

2.1.3 โครงสร้างด้าน Software

1) HosXP เป็นซอฟแวร์แอพพลิคชั่น เพื่อใช้งานด้านการรักษาพยาบาล และการจัดการระบบรายงาน สำหรับโรงพยาบาลและโรงพยาบาลส่งเสริมสุขภาพประจำตำบล

2) Thai Refer เป็นซอฟแวร์แอพพลิเคชั่นที่ส่งข้อมูลผ่านเครือข่ายอินเตอร์เนต ใช้สำหรับส่งข้อมูลผู้ป่วยไปยังโรงพยาบาลที่จะทำการส่งผู้ป่วยเข้ารับการรักษา

3) Mitnet เป็นซอฟแวร์แอพพลิเคชั่น เพื่อใช้งานด้านการรักษาพยาบาลและการจัดการระบบรายงาน ในปัจจุบัน เลือกใช้งานแล้วในโรงพยาบาลคลองใหญ่ แต่ยังมีการสำรองข้อมูลเดิม เพื่อเชื่อมต่อการทำงานกับโปรแกรม HosXP

4) โปรแกรมออกหนังสือรับรองการเกิด เป็นเว็บแอพพลิเคชั่นที่เชื่อมโยงข้อมูลกับกระทรวงมหาดไทย เพื่อใช้รับรองว่าเด็กเกิดในโรงพยาบาล

5) E-claim 2008 เป็นซอฟแวร์แอพพลิเคชั่นที่ใช้ส่งข้อมูลไปยังสำนักงานหลักประกันสุขภาพแห่งชาติ เพื่อเรียกเก็บเงินชดเชยในกรณีผู้รับบริการนอกเขตรับผิดชอบ มารับบริการด้วยอุบัติเหตุและฉุกเฉิน

6) NHSO client เป็นซอฟแวร์แอพพลิเคชั่นเพื่อใช้ส่งข้อมูลการรับบริการของผู้มิสิทธิ์รักษาในระบบจ่ายตรง สำหรับสิทธิ์ข้าราชการพลเรือนและองค์กรปกครองส่วนท้องถิ่น เพื่อทำการเรียกเก็บเงินชดเชย จากสำนักงานหลักประกันสุขภาพแห่งชาติ

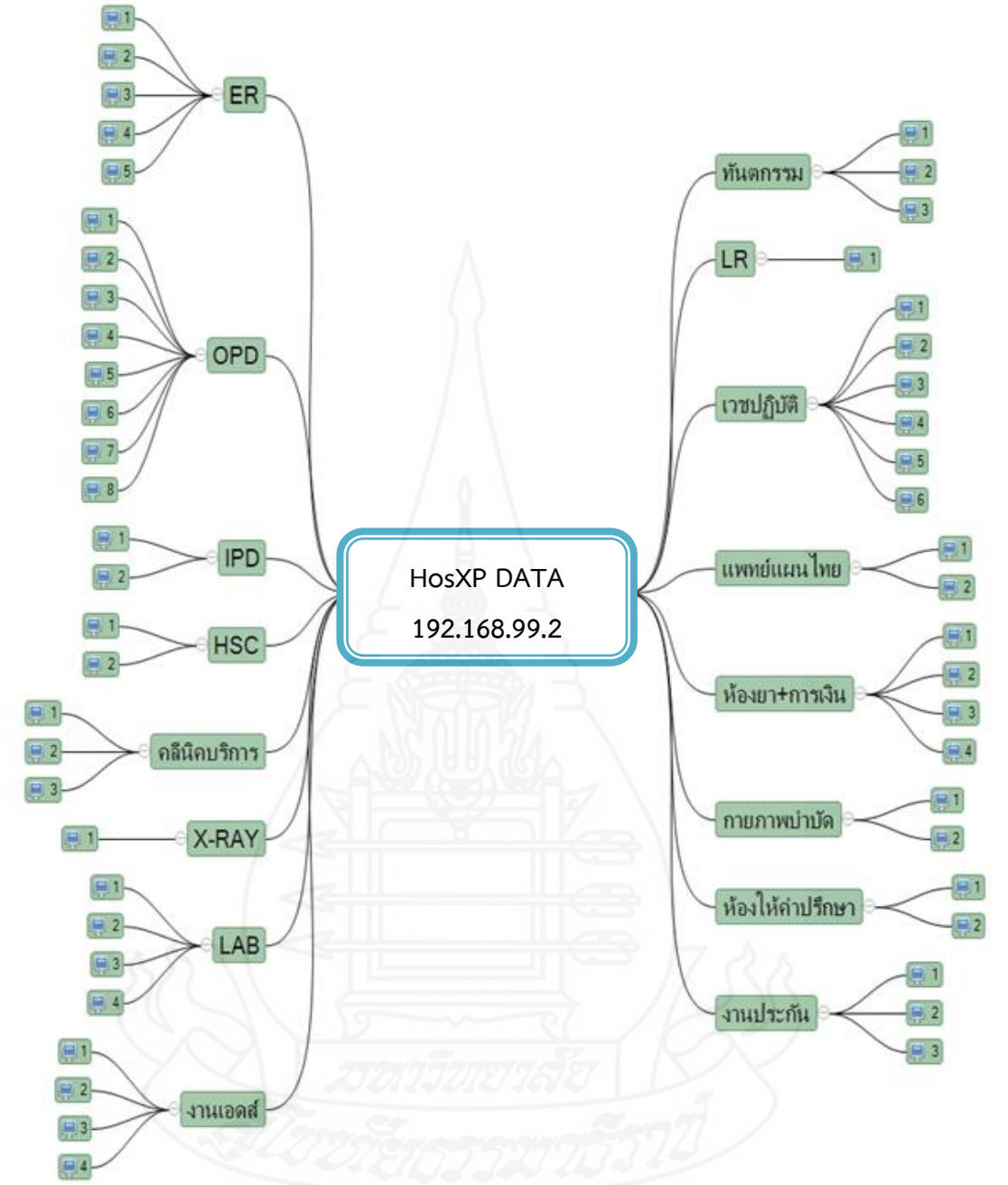
7) Ucsearch and foreigner เป็นเว็บแอพพลิเคชั่นเพื่อตรวจสอบสิทธิ์การรักษา ในระบบหลักประกันสุขภาพ โดยเชื่อมโยงฐานข้อมูลจากสำนักงานหลักประกันสุขภาพถ้วนหน้า

8) Op pp 2010 for 2556 เป็นซอฟแวร์แอพพลิเคชั่น เพื่อใช้ส่งข้อมูลด้านการส่งเสริมและป้องกันโรคของหน่วยบริการ เพื่อเรียกเก็บค่าชดเชยจากสำนักงานปลักประกันสุขภาพถ้วนหน้า

9) Welfare UC เป็นเว็บแอพพลิเคชั่น เพื่อให้หน่วยบริการใช้ขอขึ้นทะเบียนการมีสิทธิรักษาของประชาชนในระบบประกันสุขภาพถ้วนหน้าไปยังสำนักงานหลักประกันสุขภาพแห่งชาติ

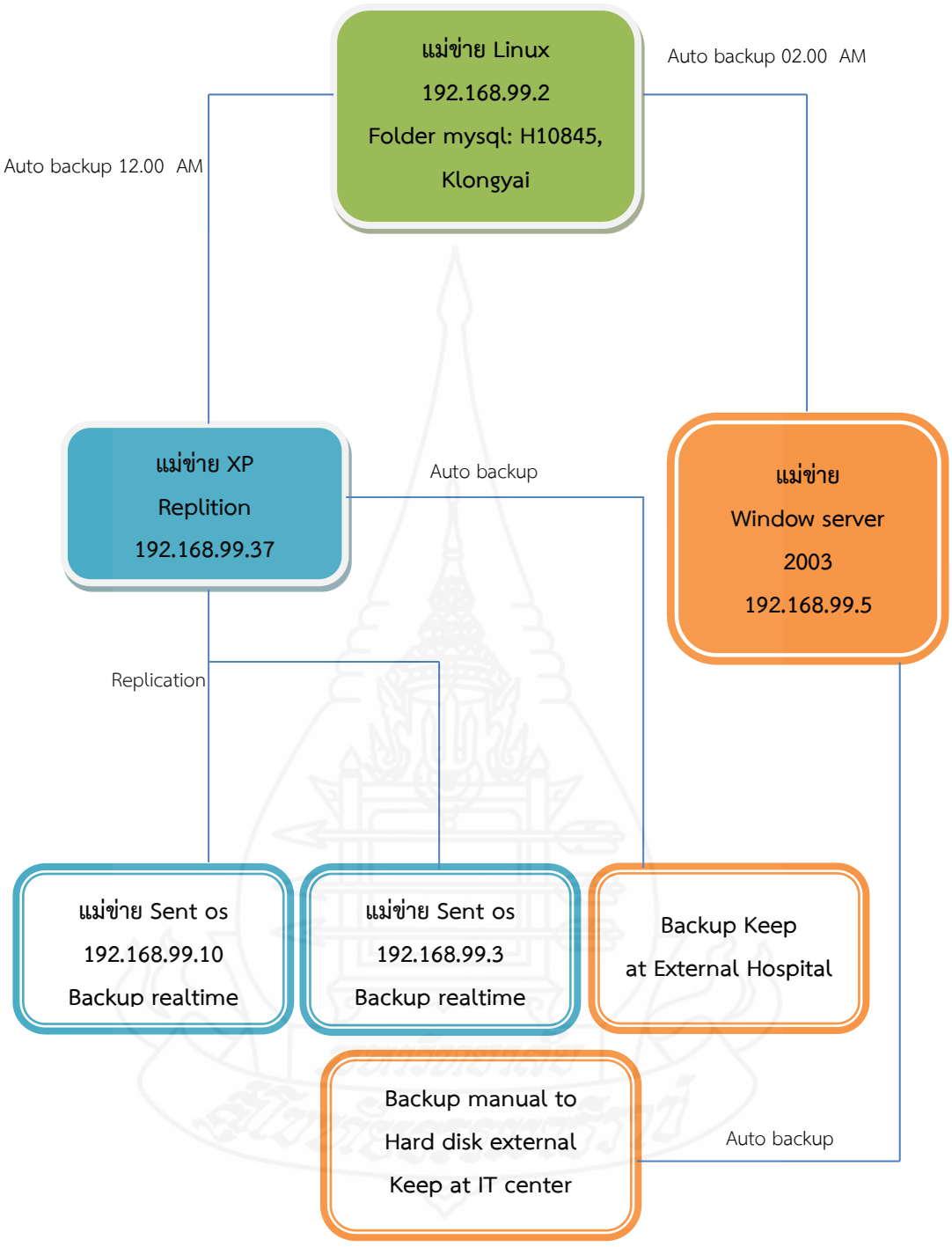
10) CSELG เป็นเว็บแอพพลิเคชัน เพื่อใช้ขึ้นทะเบียนในระบบการเบิกจ่ายเงินสวัสดิการเกี่ยวกับการรักษาพยาบาลผู้ป่วยนอกของข้าราชและผู้มีสิทธิ์จ่ายตรง

11) โปรแกรมบัตรสุขภาพบุคคลที่มีปัญหาสถานะทางสิทธิ เป็นเว็บแอพพลิเคชั่นเพื่อใช้ตรวจสอบสิทธิ์การรักษาและขึ้นทะเบียนสิทธิ์การรักษาสำหรับผู้ที่มีปัญหาด้านสัญชาติ โดยเชื่อมต่อข้อมูลจากสำนักงานหลักประกัน



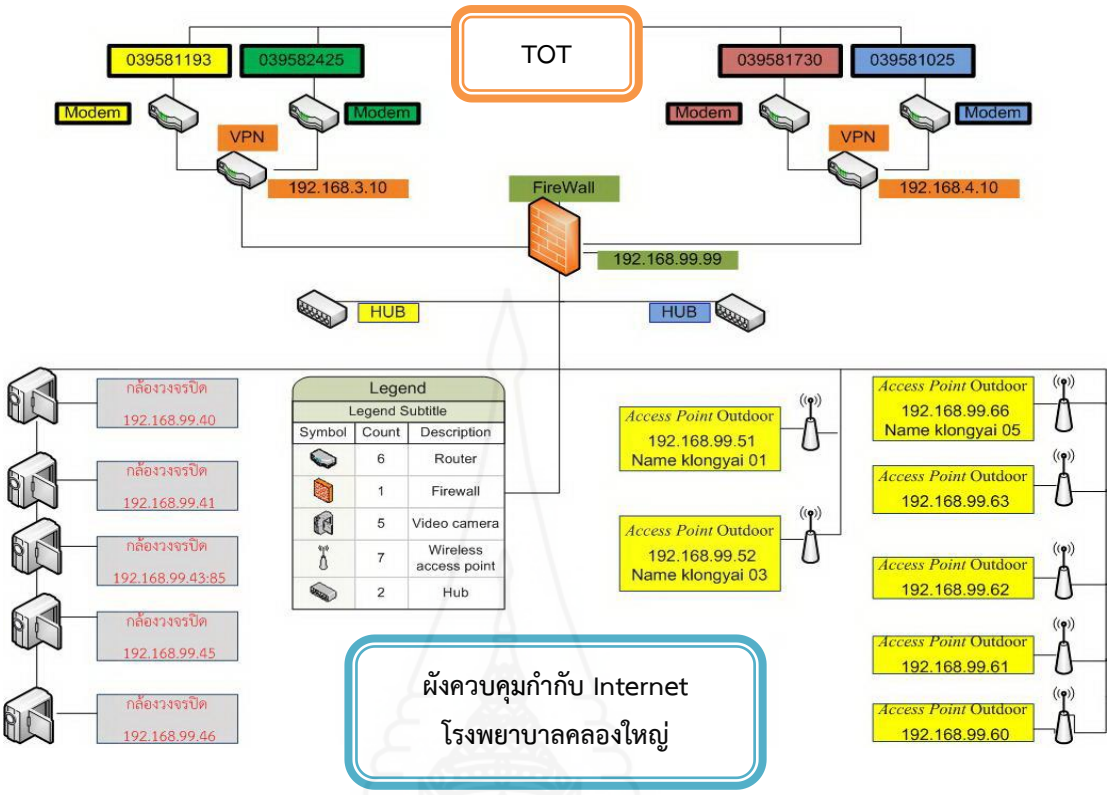
ภาพที่ 3.3 การทำงานของระบบ Hos-XP

ภาพที่ 3.3 แสดงเครือข่ายการทำงานของระบบ Hos-XP แสดงการทำงานของโปรแกรม Hos-XP ผ่านระบบ LAN ของหน่วยงานต่างๆ ภายในโรงพยาบาล



ภาพที่ 3.4 การไหลของข้อมูลและการสำรองข้อมูล

ภาพที่ 3.4 การไหลของข้อมูลและการสำรองข้อมูล แสดงการไหลของข้อมูลในเครือข่ายและ Server ที่ใช้จัดเก็บข้อมูลของโรงพยาบาล



ภาพที่ 3.5 เครือข่ายอินเตอร์เนต

ภาพที่ 3.5 เครือข่ายอินเตอร์เนต แสดงรายละเอียดเครือข่ายอินเตอร์เนตที่ใช้งานภายในโรงพยาบาล ผ่านผู้ให้บริการเครือข่าย

2.3 วิเคราะห์ปัญหาด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ทำการศึกษาสภาพองค์กร ปัญหาและความเสี่ยงความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ โดยเปรียบเทียบกับมาตรฐาน ISO/IEC 27001:2013 พบปัญหาและความเสี่ยงดังนี้

ตารางที่ 3.1 ปัญหาและความเสี่ยงด้านการควบคุมการเข้าถึงระบบขององค์กร

หัวข้อ	มาตรฐาน ISO/IEC 27001	ปัญหาที่พบ	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ
1. ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)			
1.1	นโยบายควบคุมการเข้าถึง (A.9.1.1 Access Control Policy)	- ไม่มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศจากผู้บริหาร - ไม่มีแนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศแต่ผู้ปฏิบัติงานปฏิบัติตามขอบเขตงานตนเอง	- การไม่มีนโยบายการควบคุมการเข้าถึงระบบ ทำให้ผู้ใช้งานในหน่วยงานไม่เห็นความสำคัญของการปฏิบัติตามนโยบาย หรือแนวทาง ซึ่งส่งผลกระทบต่างๆ ตามมา โดยเฉพาะข้อมูลผู้ป่วยอาจถูกล่วงละเมิด หรือระบบงานอาจถูกโจมตีจากผู้ไม่หวังดี เป็นต้น
1.2	การเข้าถึงเครือข่ายและบริการเครือข่าย (A.9.1.2 Access to Network and Network Services)	- ไม่มีนโยบายและแนวทางการเข้าถึงเครือข่ายและบริการเครือข่าย - ไม่มีแบบฟอร์มการเปลี่ยนแปลงสิทธิและยกเลิกสิทธิการใช้งาน	- การเข้าใช้งานเครือข่ายหน่วยงานโดยไม่ได้รับอนุญาตหรือมีหลักฐานการใช้งาน อาจทำให้ข้อมูลถูกทำลายหรือถูกละเมิดสิทธิได้ - เมื่อเกิดการความสูญเสียต่อข้อมูล ไม่สามารถหาผู้เข้าใช้งานที่เข้ามาละเมิดข้อมูล

หัวข้อ	มาตรฐาน ISO/IEC 27001	ปัญหาที่พบ	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)			
2.1	การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (A.9.2.1 User Registration and Deregistration)	- ไม่มีนโยบายและแนวทางการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน - ไม่มีการแสดงตารางแสดงสิทธิในการเข้าถึงระบบ - ไม่มีแนวทางการปฏิบัติการเพิกถอดลงทะเบียนสิทธิผู้ใช้งานและรายงานการเพิกถอดทะเบียนผู้ใช้งาน	- การขาดหลักฐานการลงทะเบียนผู้ใช้งานหรือถอดถอนสิทธิ ทำให้ไม่สามารถทราบประวัติการใช้งาน - การไม่มีรายงานการเพิกถอนสิทธิ์ผู้ใช้งานอาจมีการแอบเข้าใช้งานของพนักงานที่ออก
2.2	การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.2 User Access Provisioning)	- ไม่มีนโยบายและแนวทางการจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน	- ทำให้อาจมีการแอบอ้างการใช้งานจากผู้ไม่ได้รับอนุญาตใช้งาน
2.3	การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (A.9.2.3 Management of Privileged Access Right)	- ไม่มีนโยบายการบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	- ทำให้ผู้ใช้งานละเมิดสิทธิการใช้งานของผู้อื่นนอกเหนือจากสิทธิการใช้งานของตนเอง ทำให้อาจมีการเปลี่ยนแปลงข้อมูลที่สำคัญขององค์กรได้

หัวข้อ	มาตรฐาน ISO/IEC 27001	ปัญหาที่พบ	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ
2.4	การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (A.9.2.4 Management of Secret Authentication Information of Users)	-ไม่มีนโยบายการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	- ผู้ไม่ได้รับอนุญาตในการเข้าถึงข้อมูลอาจมีการแอบอ้างใช้งาน
2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.5 Review of User Access Rights)	-ไม่มีนโยบายและแนวทางการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน - ไม่มีการรายงานการสอบทานรายชื่อผู้ใช้ สิทธิการเข้าถึงของผู้ใช้งาน และตารางแสดงสิทธิในการเข้าถึง	- ผู้ที่ถูกยกเลิกสิทธิการเข้าถึงระบบงาน อาจมีการแอบอ้างเพื่อเข้าใช้งาน ทำให้เกิดความเสี่ยงต่อระบบ
2.6	การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (A.9.2.6 Removal or Adjustment of Access Rights)	- ไม่มีนโยบายและแนวทางการถอดถอนและปรับปรุงสิทธิการเข้าถึง	- ผู้ที่ถูกยกเลิกสิทธิการเข้าถึงระบบงาน อาจมีการแอบอ้างเพื่อเข้าใช้งาน ทำให้เกิดความเสี่ยงต่อระบบงาน
3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)			
3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (A.9.3.1 User of Secret Authentication Information)	- ไม่มีรายงานการถอดถอนสิทธิ - ไม่มีนโยบายการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ	- อาจเป็นช่องทางให้ผู้ประสงค์ร้ายสามารถเข้าถึงระบบงานได้ จนเกิดความเสียหายต่อระบบงาน

หัวข้อ	มาตรฐาน ISO/IEC 27001	ปัญหาที่พบ	ความเสี่ยงด้านการควบคุมการเข้าถึงระบบ
4. การควบคุมการเข้าถึงระบบ (System and Application Access Control)			
4.1	การจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Restriction)	- ไม่มีนโยบายการจำกัดการเข้าถึงระบบสารสนเทศ	- อาจเป็นช่องทางให้ผู้ประสงค์ร้ายสามารถเข้าถึงระบบงานได้
4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)	- ไม่มีนโยบายและแนวทางสำหรับการล็อกอินเข้าระบบ ที่มีความมั่นคงปลอดภัย	-การใช้งานจากที่สาธารณะต้องระมัดระวังการใช้งานรหัสผ่านและคงค้างรหัสไว้ ผู้อื่นอาจมาใช้งานต่อได้
4.3	ระบบบริหารจัดการรหัสผ่าน (Password Management System)	- ไม่มีนโยบายและแนวทางการบริหารจัดการรหัสผ่าน	-ผู้ใช้งานที่ไม่ได้รับอนุญาตอาจคาดเดารหัสผ่านได้โดยง่ายจนสามารถเข้าใช้งานระบบได้
4.4	การใช้โปรแกรมอรรถประโยชน์ (User of Privileged Utility Programs)	-ไม่มีนโยบายและแนวทางการใช้และขอติดตั้งโปรแกรมอรรถประโยชน์ -ไม่มีแบบฟอร์มขอติดตั้งโปรแกรมอรรถประโยชน์	- ผู้ใช้งานอาจมีการติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต จนอาจเกิดความเสียหายต่อระบบสารสนเทศได้
4.5	การควบคุมการเข้าถึงซอสโค้ดของโปรแกรม (Access Control to Program Source Code)	-ไม่มีนโยบายและแนวทางการควบคุมการเข้าถึงซอสโค้ดของโปรแกรม -ไม่มีแบบฟอร์มร้องขอการเปลี่ยนแปลง	- ผู้ใช้งานอาจมีการเข้าถึงซอสโคดของระบบโดยไม่ได้รับอนุญาต จนอาจเกิดความเสียหายต่อระบบสารสนเทศได้

3. การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ

เมื่อทำการศึกษาข้อมูลพื้นฐานต่างๆ ด้านข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ศึกษาองค์กร ระบบสารสนเทศภายในองค์กร ปัญหาและความเสี่ยงด้านการเข้าถึงระบบสารสนเทศ กำหนดขอบเขตในการจัดทำนโยบายและแนวทางการปฏิบัติในการเข้าถึงระบบ และพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

3.1 พัฒนานโยบายและแนวทางด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

โดยจัดทำนโยบายแนวทางการปฏิบัติงานและแบบฟอร์มเอกสารที่เกี่ยวข้อง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามแนวทางมาตรฐาน ISO/IEC 27001:2013 ตามรายละเอียด ดังนี้

3.1.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

1) นโยบายควบคุมการเข้าถึง (A.91.1 Access Control Policy)

2) การเข้าถึงเครือข่ายและบริการเครือข่าย (A.9.1.2 Access to Network and Network Services)

3.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

1) การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (A.9.2.1 User Registration and Deregistration)

2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.2 User Access Provisioning)

3) การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (A.9.2.3 Management of Privileged Access Right)

4) การบริการจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (A.9.2.4 Management of Secret Authentication Information of Users)

5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (A.9.2.5 Review of User Access Rights)

6) การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (A.9.2.6 Removal or Adjustment of Access Rights)

3.1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (A.9.3.1 User of Secret Authentication Information)

3.1.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

1) การจำกัดการเข้าถึงระบบสารสนเทศ (A.9.4.1 Information Access Restriction

2) ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (A.9.4.2 Secure Log-on Procedures)

3) ระบบบริหารจัดการระบบผ่าน (A.9.4.3 Password Management System)

4) การใช้โปรแกรมอรรถประโยชน์ (A.9.4.4 User of Privileged Utility Programs)

5) การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (A.9.4.5 Access Control to Program Source Code)

โดยจะนำเสนอรายละเอียดผลการพัฒนานโยบายและแนวทางด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ในบทที่ 4 และตัวอย่างนโยบายที่เกี่ยวข้องในภาคผนวก

3.2 พัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013

โดยกำหนดความต้องการของระบบดังนี้

3.2.1 สำหรับผู้ใช้งานทั่วไป

1) ระบบสามารถแสดงรายละเอียดตามข้อกำหนดของ ISO27001:2013 โดยแสดงรายละเอียดเฉพาะข้อกำหนดด้านการควบคุมการเข้าถึงระบบ

2) ผู้ใช้งานสามารถร้องขอการลงทะเบียน เพื่อเข้าใช้งานระบบในส่วนของผู้ใช้งานที่ต้องลงชื่อเข้าใช้งาน

3.2.2 สำหรับผู้ใช้งานที่ลงชื่อเข้าใช้งาน

1) ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบ และต้องได้รับอนุญาตจากผู้ดูแลระบบ ก่อนเข้าใช้เท่านั้น

2) ผู้เข้าใช้งานระบบที่ได้รับอนุญาตให้ใช้งาน ต้องทำการลงชื่อเข้าใช้งานระบบทุกครั้งที่ทำการใช้งาน และระบบต้องทำการออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลานานเกิน 10 นาที

3) ระบบต้องแสดงฟังก์ชันหลัก 3 ส่วนคือ Checklist, Assessment และ Download มี รายละเอียดดังนี้

(1) ฟังก์ชัน Checklist สามารถแสดงรายละเอียดตามข้อกำหนดและเอกสารที่เกี่ยวข้อง ในแต่ละข้อกำหนด ที่สอดคล้องกับการพัฒนานโยบายแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบที่ได้พัฒนาขึ้น โดยแยกแสดงผลชัดเจนตามหัวข้อหลัก

(2) ฟังก์ชัน Assessment ระบบสามารถประเมินความมั่นคงปลอดภัย ตามข้อกำหนดหลัก 4 ข้อและข้อกำหนดย่อย 14 ข้อ ดังนี้คือ

ก. Business Requirement of Access Control

ก) Access Control Policy

ข) Access to Network and Network Services

ข. User Access Management

ก) User Registration and Deregistration

ข) User Access Provisioning

ค) Management of Privileged Access Right

ง) Management of Secret Authentication Information of Users

จ) Review of User Access Rights

ฉ) Removal or Adjustment of Access Rights

ค. User Responsibilities

ก) User of Secret Authentication Information

ง. System and Application Access Control

ก) Information Access Restriction

ข) Secure Log-on Procedures

ค) Password Management System

ง) User of Privileged Utility Programs

จ) Access Control to Program Source Code

การประเมินในแต่ละข้อกำหนดย่อย ผู้ใช้งานสามารถทำการประเมินได้ง่าย โดยข้อกำหนดที่ต้องมีการแนบเอกสาร ระบบสามารถทำการแนบเอกสารและเป็นส่วนของคิดค่าคะแนนตามระดับการประเมินและเอกสาร ที่ผู้ทำการประเมินแนบไว้สามารถแสดงผลและสั่งพิมพ์ได้โดยมีระดับการประเมินดังนี้ คือ

1. มีข้อมูล/เอกสาร/ ระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัด ผลการประเมินเท่ากับ 100% และแสดงแถบสีเป็นสีเขียว

2. ระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร ผลการประเมินเท่ากับ 75% และแสดงแถบสีเป็นสีส้ม

3. กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติผลการประเมินเท่ากับ 50% แสดงแถบสีเป็นสีเหลือง

4. ไม่มีข้อมูล/ไม่มีเอกสาร/ไม่มีระเบียบปฏิบัติ ผลการประเมินเท่ากับ 25% แสดงแถบสีเป็นแดง

5. มีระเบียบปฏิบัติแต่ไม่ปฏิบัติตามผลการประเมินเท่ากับ 0% แสดงแถบสีเป็นสีดำ

เมื่อทำการประเมินครบทุกหัวข้อ ระบบสามารถแสดงการประเมินผลภาพรวมการประเมินตามหัวข้อหลักและการแสดงผลการประเมินตามข้อกำหนดย่อย ในรูปแบบแผนภูมิการแสดงผลที่เข้าใจง่ายและสามารถสั่งพิมพ์รายงานการประมวลได้

(3) ฟังก์ชัน Download ระบบสามารถแสดงรายละเอียดเอกสารตามข้อกำหนด ได้แก่ ข้อกำหนดตามเกณฑ์การประเมิน นโยบาย แนวทางการปฏิบัติและแบบฟอร์มที่เกี่ยวข้องโดยสามารถดาวน์โหลดหรือพิมพ์เอกสารที่เกี่ยวข้องเมื่อได้

3.2.3 โปรแกรมที่ใช้พัฒนา

เมื่อกำหนดความต้องการของระบบทำการพัฒนาระบบโดยใช้ โปรแกรมสร้างเว็บไซต์ Net Beam Version 8.2 โดยภาษา PHP และออกแบบโครงสร้างโปรแกรมเว็บโดย Software Bootstrap ทำการเชื่อมโยงฐานข้อมูลโดยใช้ MySql Server โดยจะนำเสนอรายละเอียดผลการพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013 ในบทที่ 4

5. สรุปผลการดำเนินงาน

ทำการสรุปผลโดยประเมินการบรรลุวัตถุประสงค์ของศึกษาตามที่ตั้งไว้ พร้อมทั้งให้ข้อเสนอแนะแนวทางและโอกาสพัฒนาในการนำนโยบายและแนวทางการควบคุมการเข้าถึงระบบ

ไปเป็นต้นแบบเพื่อพัฒนาในด้านอื่นๆ ให้ครอบคลุมทุกหัวข้อตามมาตรฐาน ISO/IEC 27001:2013 และการนำไปประยุกต์เพื่อใช้งานในโรงพยาบาลชุมชนหรือองค์กรที่มีบริบทใกล้เคียงกัน โดยจะนำเสนอรายละเอียดสรุปผลการดำเนินงานในบทที่ 5

บทที่ 4
ผลการดำเนินงาน

1. การพัฒนานโยบายและแนวทาง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

ดำเนินการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ให้สอดคล้องตามข้อกำหนดของ ISO 27001 : 2013 และบริบทขององค์กร ตามการวิเคราะห์ปัญหาด้านการควบคุมการเข้าถึงระบบดังต่อไปนี้

1.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

1.1.1 นโยบายควบคุมการเข้าถึง (Access Control Policy)

1) นโยบายควบคุมการเข้าถึงระบบสารสนเทศ
2) แนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศ

1.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

1) นโยบายการเข้าถึงเครือข่ายและบริการเครือข่าย
2) แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย
3) แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ และยกเลิกสิทธิ

1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

1.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and Deregistration)

1) นโยบายการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน
2) แนวทางการปฏิบัติการลงทะเบียนสิทธิผู้ใช้งาน
3) แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ และยกเลิกสิทธิ
4) ตารางแสดงสิทธิในการเข้าถึงระบบ
5) แนวทางการปฏิบัติการเพิกถอดลงทะเบียนสิทธิผู้ใช้งาน
6) รายงานการเพิกถอดทะเบียนผู้ใช้งาน

1.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน(User Access Provisioning)

1) นโยบายการจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน

1.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

1) นโยบายการบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ

1.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users)

1) นโยบายการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน

1.2.5 ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน(Review of User Access Rights)

1) นโยบายการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
2) แนวปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
3) รายงานการสอบทานรายชื่อผู้ใช้งาน
4) รายงานการสอบทานสิทธิการเข้าถึงของผู้ใช้งาน
5) ตารางแสดงสิทธิในการเข้าถึงระบบ

1.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

1) นโยบายการถอดถอนและปรับปรุงสิทธิการเข้าถึง
2) แนวปฏิบัติการถอดถอนและปรับปรุงสิทธิการเข้าถึง
3) รายงานการถอดถอนสิทธิ

1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of Secret Authentication Information)

1) นโยบายการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ

1.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

1.4.1 การจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Restriction)

1) นโยบายการจำกัดการเข้าถึงระบบสารสนเทศ

1.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

1) นโยบายสำหรับการล็อกอินเข้าระบบ ที่มีความมั่นคงปลอดภัย

2) แนวทางการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

1.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

1) นโยบายการบริหารจัดการรหัสผ่าน

2) แนวทางการปฏิบัติการบริหารจัดการรหัสผ่าน

1.4.4 การใช้โปรแกรมอรรถประโยชน์ (User of Privileged Utility Programs)

1) นโยบายการใช้โปรแกรมอรรถประโยชน์

2) แนวทางการปฏิบัติการขอติดตั้งโปรแกรมอรรถประโยชน์

3) แบบฟอร์มขอติดตั้งโปรแกรมอรรถประโยชน์

1.4.5 การควบคุมการเข้าถึงซอสโค้ดของโปรแกรม (Access Control to Program Source Code)

1) นโยบายการควบคุมการเข้าถึงซอสโค้ดของโปรแกรม

2) แนวทางการปฏิบัติการเข้าถึงซอสโค้ดของโปรแกรม

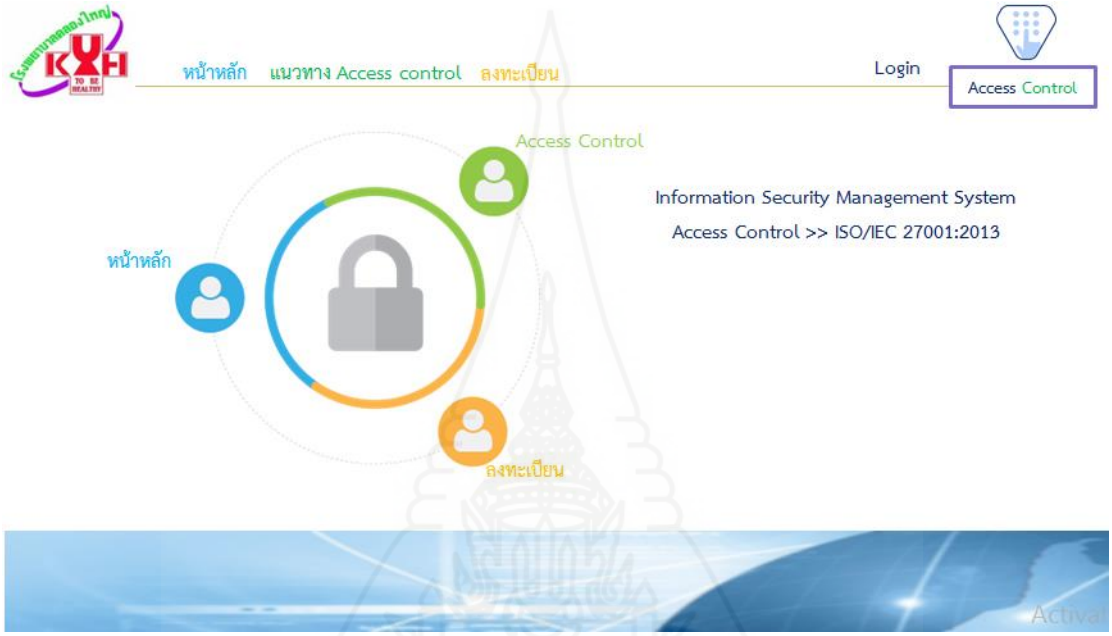
3) แบบฟอร์มร้องขอการเปลี่ยนแปลง (Change Management Form)

(มีตัวอย่างนโยบาย ตามภาคผนวก ก ตัวอย่างแนวทางการปฏิบัติงาน ตามภาคผนวก ข ตัวอย่างเอกสารที่เกี่ยวข้อง ตามภาคผนวก ค และตัวอย่างเอกสารอื่นๆ ตามภาคผนวก ง)

2. การพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001:2013

ดำเนินการพัฒนาระบบในรูปแบบโปรแกรมเว็บ โดยมีผลการพัฒนาดังนี้

2.1 สำหรับผู้ใช้งานทั่วไป



ภาพที่ 4.1 หน้าแรกของระบบ

ภาพที่ 4.1 แสดงหน้าแรกของระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบ ในส่วนของผู้ใช้งานทั่วไป ประกอบด้วยฟังก์ชันหน้าหลัก แนวทาง Access control การลงทะเบียนและ Login

ภาพที่ 4.2 ฟังก์ชันหน้าหลักของระบบ

ภาพที่ 4.2 แสดงรายละเอียดฟังก์ชันหน้าหลักของระบบ อธิบายถึงรายละเอียดขอบเขตระบบอย่างคร่าวๆ

2.1.1 ระบบสามารถแสดงรายละเอียดตามข้อกำหนดของ ISO27001:2013

โดยแสดงรายละเอียดเฉพาะข้อกำหนดและคำอธิบายคร่าวๆ ด้านการควบคุมการเข้าถึงระบบ

ภาพที่ 4.3 ฟังก์ชันแนวทาง Access control (ผู้ใช้งานทั่วไป)

ภาพที่ 4.3 แสดงฟังก์ชันแนวทาง Access control (ส่วนของผู้ใช้งานทั่วไป) ระบบจะแสดงรายละเอียดตามข้อกำหนด ISO27001:2013 ด้านการควบคุมการเข้าถึงระบบ โดยแสดงเฉพาะแนวทางหลัก และคำอธิบายคร่าวๆ ตามข้อกำหนด

2.1.2 ผู้ใช้งานสามารถร้องขอการลงทะเบียน เพื่อเข้าใช้งานระบบในฟังก์ชันอื่น

ภาพที่ 4.4 ฟังก์ชันลงทะเบียนใช้งาน

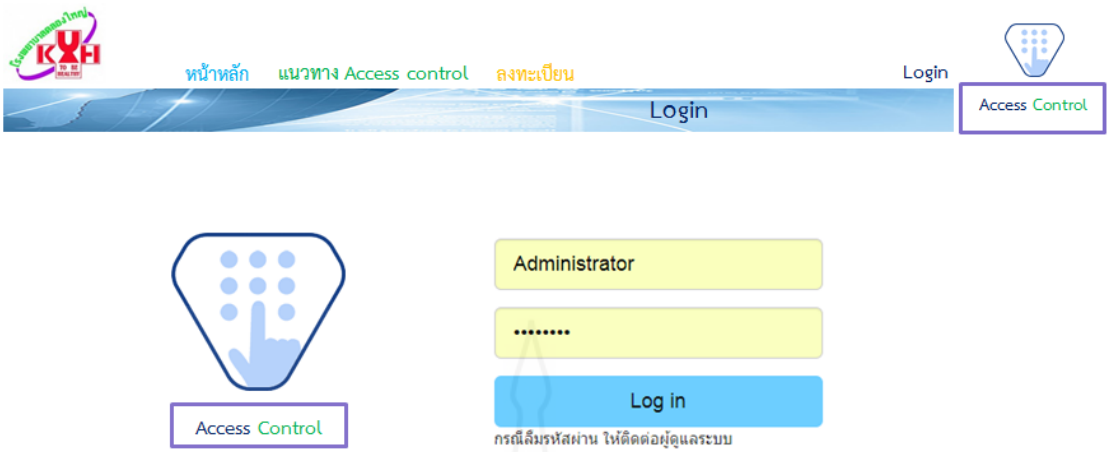
ภาพที่ 4.4 แสดงฟังก์ชันลงทะเบียน ผู้ใช้งานที่ต้องการทำการประเมินความพร้อมด้านการควบคุมการเข้าถึงระบบ หรือต้องการใช้งานฟังก์ชันอื่นๆ ต้องทำการลงทะเบียน และได้รับอนุญาตจากผู้ดูแลระบบเพื่อเข้าใช้งานระบบ

2.2 สำหรับผู้ใช้งานที่ลงชื่อเข้าใช้งาน

ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบ และต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้เท่านั้น

2.2.1 การเข้าระบบเพื่อใช้งาน

ผู้เข้าใช้งานระบบที่ได้รับอนุญาตให้ใช้งาน ต้องทำการลงชื่อเข้าใช้งานระบบทุกครั้งที่เข้าใช้งาน และระบบจะทำการออกจากระบบอัตโนมัติ เมื่อไม่มีการใช้งานเป็นระยะเวลานานเกิน 10 นาที



ภาพที่ 4.5 ฟังก์ชัน Login

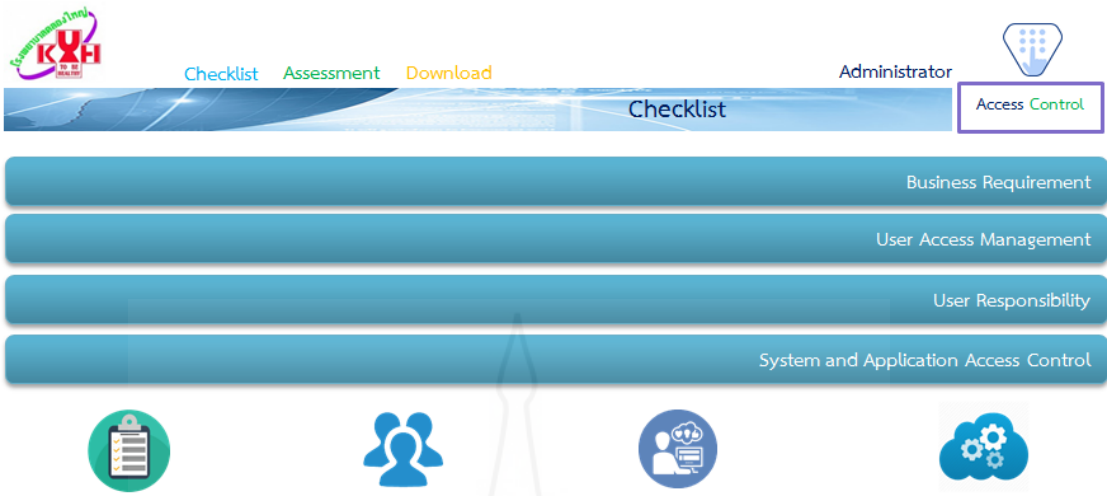
ภาพที่ 4.5 ฟังก์ชัน Login ผู้ใช้งานต้องทำการลงทะเบียนเพื่อสมัครเข้าใช้งานระบบ และต้องทำการลงชื่อเข้าใช้งานระบบทุกครั้งที่ทำการใช้งาน โดยระบบจะทำการออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลานานเกิน 10 นาที

2.2.2 ฟังก์ชันการใช้งาน

ระบบแสดงฟังก์ชันหลัก 3 ส่วน ดังนี้ คือ

1) ฟังก์ชัน Checklist

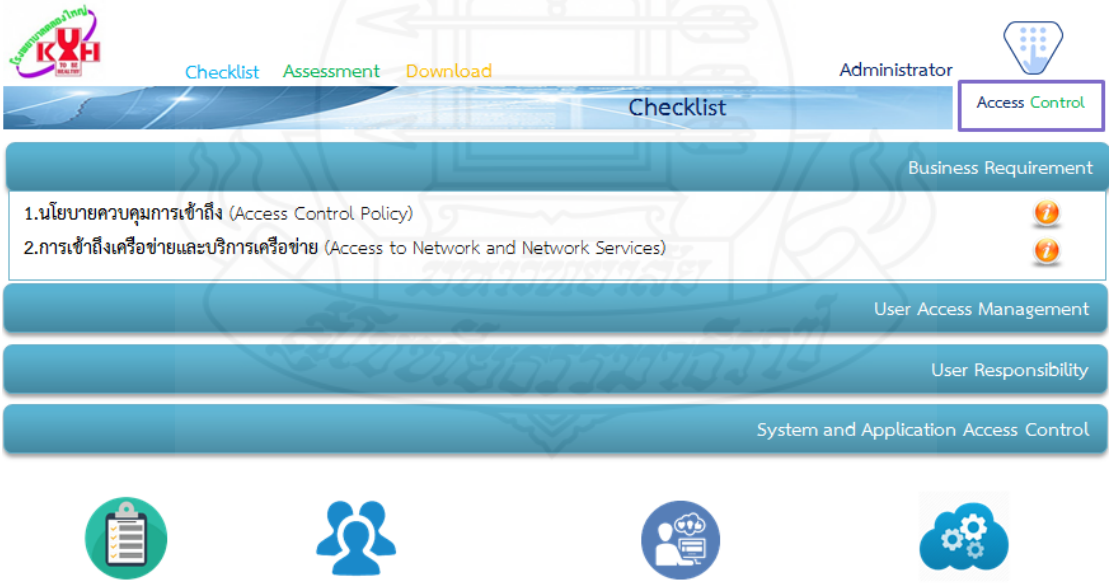
แสดงรายละเอียด ตามข้อกำหนดและเอกสารที่เกี่ยวข้อง ในแต่ละข้อกำหนด ที่สอดคล้องกับการพัฒนานโยบายแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ที่ได้พัฒนาขึ้น (รายละเอียดตามบทที่ 4 ข้อ 1) โดยแยกแสดงผลตามหัวข้อหลัก



ภาพที่ 4.6 ฟังก์ชัน Checklist

ภาพที่ 4.6 ฟังก์ชัน Checklist จะแสดงข้อกำหนดหลักทั้ง 4 ข้อ คือ Business Requirement, User Access Management, User Responsibilities, User of Secret Authentication Information และ System and Application Access Control โดยมี รายละเอียดดังนี้

(1) ฟังก์ชัน Checklist ของข้อกำหนดด้าน Business Requirement



ภาพที่ 4.7 ฟังก์ชัน Checklist ข้อกำหนดหลัก Business Requirement

ภาพที่ 4.7 แสดงฟังก์ชัน Checklist หัวข้อ Business Requirement เมื่อทำการกดเลือกที่ข้อกำหนด Business Requirement ระบบจะแสดงข้อกำหนดย่อย 2 หัวข้อคือ Access Control Policy และ Access to Network and Network Services และเมื่อทำการเลือกที่สัญลักษณ์  ระบบจะแสดงกล่องข้อความที่แสดงรายละเอียดของมาตรฐาน รวมถึงข้อกำหนดเอกสารที่ควรมีในแต่ละข้อกำหนดย่อย ดังตัวอย่างในภาพที่ 4.8 ตัวอย่างกล่องข้อความแสดงรายละเอียดข้อกำหนดย่อย

นโยบายควบคุมการเข้าถึง (Access Control Policy)

นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

ควรประกอบด้วยเอกสารดังนี้

1. นโยบายควบคุมการเข้าถึงระบบสารสนเทศ
2. แนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบสารสนเทศ

ภาพที่ 4.8 กล่องข้อความรายละเอียดข้อกำหนดย่อย

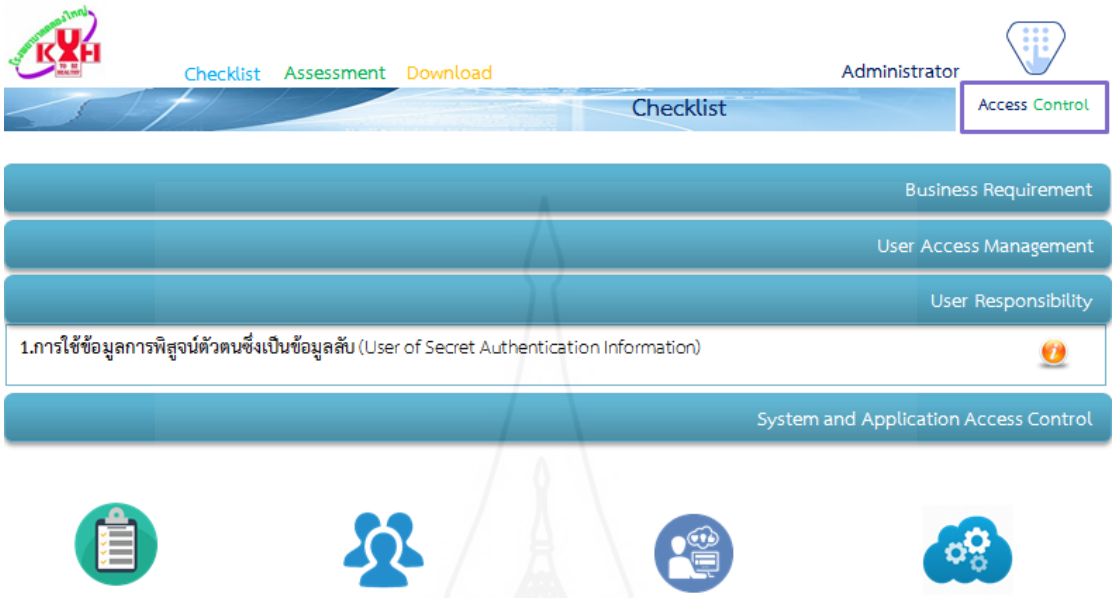
ภาพที่ 4.8 ภาพแสดงกล่องข้อความรายละเอียดข้อกำหนดย่อย แสดงรายละเอียดข้อกำหนดย่อย ของมาตรฐาน รวมถึงข้อกำหนดเอกสารที่ควรมีในข้อกำหนดย่อย (Access Control Policy)

(2) ฟังก์ชัน Checklist ของข้อกำหนดด้าน User Access Management

ภาพที่ 4.9 ฟังก์ชัน Checklist ข้อกำหนดหลัก User Access Management

ภาพที่ 4.9 ภาพแสดงฟังก์ชัน Checklist ข้อกำหนดหลัก User Access Management เมื่อทำการเลือกที่ข้อกำหนด User Access Management ระบบจะแสดงข้อกำหนดย่อย 6 หัวข้อคือ User Registration and Deregistration, User Access Provisioning, Management of Privileged Access Right, Management of Secret, Authentication Information of Users, Review of User Access Rights และ Removal or Adjustment of Access Rights และเมื่อทำการเลือกที่สัญลักษณ์ ระบบจะแสดงกล่องข้อความที่แสดงรายละเอียดของมาตรฐาน รวมถึงข้อกำหนดเอกสารที่ควรมีในแต่ละข้อกำหนดย่อย คล้ายตัวอย่างในภาพ ที่ 4.8 กล่องข้อความรายละเอียดข้อกำหนดย่อย

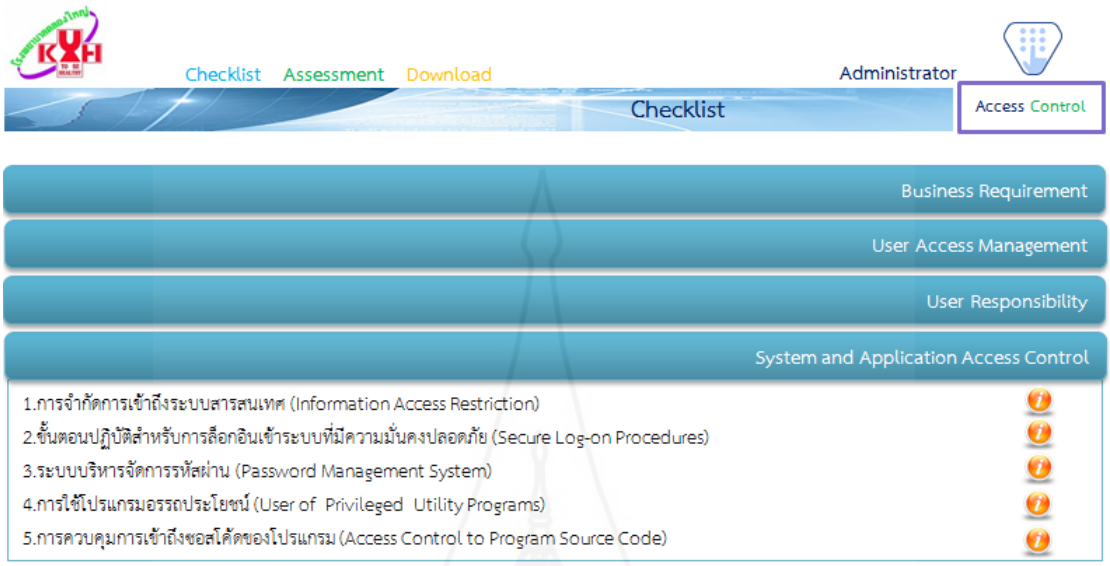
(3) ฟังก์ชัน Checklist ของข้อกำหนดด้าน User Responsibility



ภาพที่ 4.10 ฟังก์ชัน Checklist ข้อกำหนดหลัก User Responsibility

ภาพที่ 4.10 ฟังก์ชัน Checklist ข้อกำหนดหลัก User Responsibility เมื่อทำการเลือกที่ข้อกำหนด User Responsibility ระบบจะแสดงข้อกำหนดย่อย 1 หัวข้อคือ User of Secret Authentication Information และเมื่อทำการเลือกที่สัญลักษณ์ ระบบจะแสดงกล่องข้อความที่แสดงรายละเอียดของมาตรฐาน รวมถึงข้อกำหนดเอกสารที่ควรมีในข้อกำหนดย่อย คล้ายตัวอย่างในภาพที่ 4.8 ตัวอย่างกล่องข้อความรายละเอียดข้อกำหนดย่อย

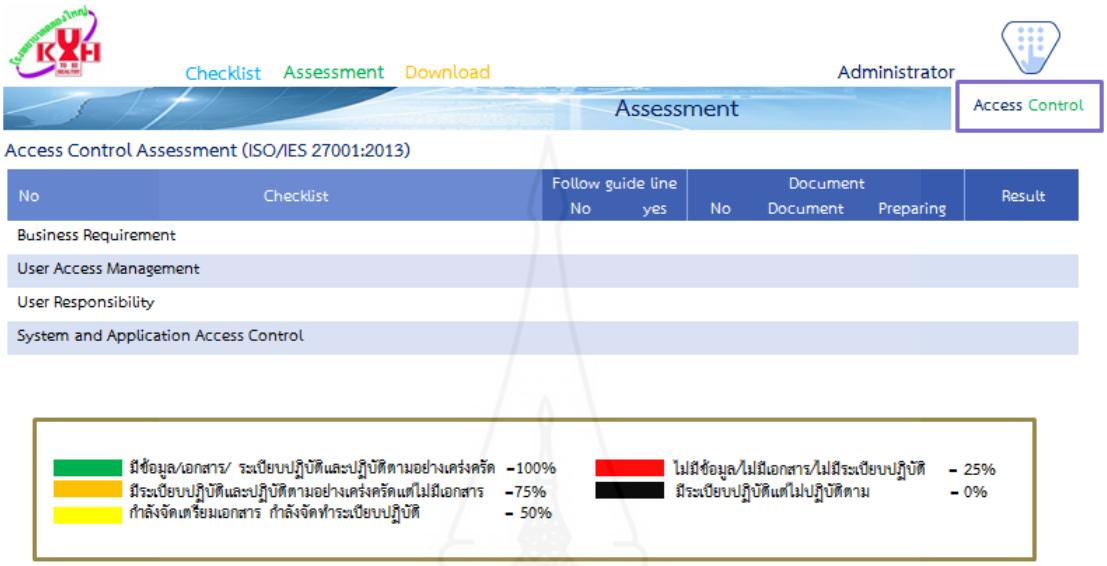
(4) ฟังก์ชัน Checklist ของข้อกำหนดด้าน System and Application Access Control



ภาพที่ 4.11 ฟังก์ชัน Checklist ข้อกำหนดหลัก System and Application Access Control

ภาพที่ 4.11 ฟังก์ชัน Checklist ข้อกำหนดหลัก System and Application Access Control เมื่อทำการเลือกที่ข้อกำหนด System and Application Access Control ระบบจะแสดงข้อกำหนดย่อย 5 หัวข้อคือ Information Access Restriction, Secure Log-on Procedures, Password Management System, User of Privileged Utility Programs, Access Control to Program Source Code และเมื่อทำการเลือกที่สัญลักษณ์ ระบบจะแสดงกล่องข้อความที่แสดงรายละเอียดของมาตรฐาน รวมถึงข้อกำหนดเอกสารที่ควรมีในข้อกำหนดย่อย คล้ายตัวอย่างในภาพ ที่ 4.8 กล่องข้อความรายละเอียดข้อกำหนดย่อย

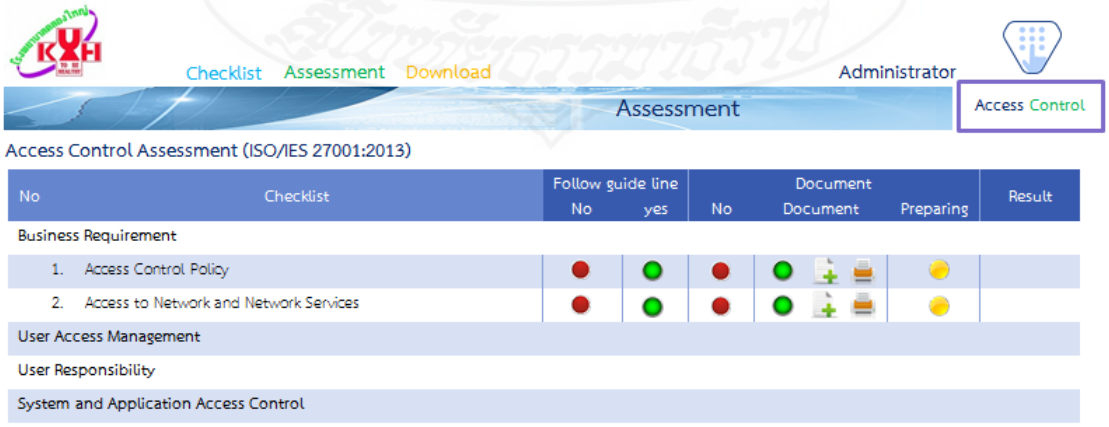
2) ฟังก์ชัน Assessment ระบบสามารถประเมินความมั่นคงปลอดภัย ตามข้อกำหนดหลัก 4 ข้อ และข้อกำหนดย่อย 14 ข้อ



ภาพที่ 4.12 ฟังก์ชัน Assessment

ภาพที่ 4.12 ฟังก์ชัน Assessment เป็นหน้าฟังก์ชันเพื่อประเมินความพร้อม ความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบ โดยประเมินตามข้อกำหนด 4 ข้อหลักและ 14 ข้อย่อยตามมาตรฐาน ISO/IEC 27001:2013 คือข้อกำหนดด้าน Business Requirement of Access Control, User Access Management, User Responsibilities และ System and Application Access Control

(1) การประเมินข้อกำหนด Business Requirement of Access Control



ภาพที่ 4.13 ฟังก์ชัน Assessment ข้อกำหนด Business Requirement

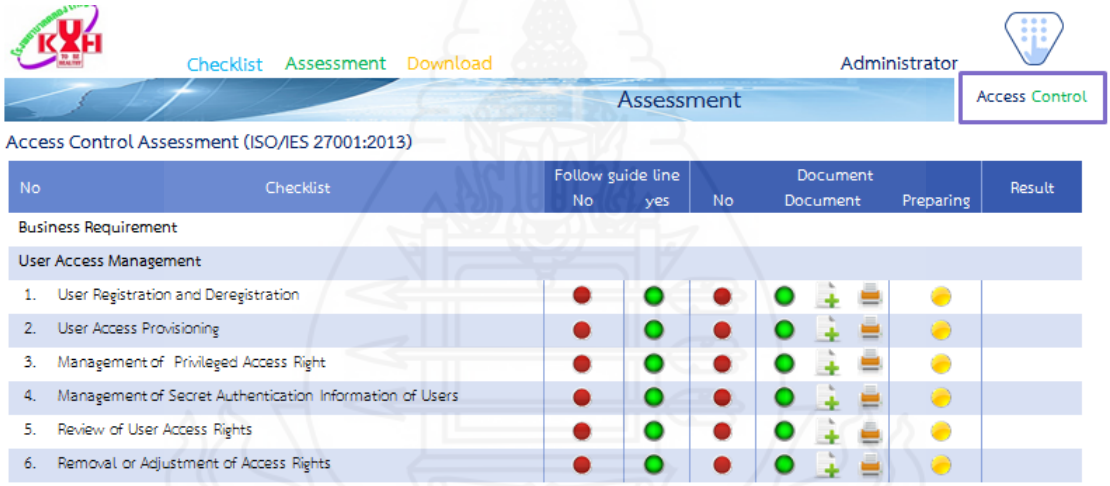
ภาพที่ 4.13 ฟังก์ชัน Assessment ข้อกำหนด Business Requirement แสดงรายละเอียดการประเมินข้อกำหนดด้าน Business Requirement ซึ่งประกอบด้วยข้อกำหนดย่อยด้าน Access Control Policy และ Access to Network and Network Services โดยผู้ประเมินต้องทำการประเมินใน 2 ส่วนคือ

1. Follow guide line หากไม่มีการปฏิบัติตามแนวทาง ให้เลือก no หากมีการปฏิบัติตามแนวทางใดๆ ให้เลือก yes

2. Document หากไม่มีเอกสารใด ให้เลือก no หากมีนโยบาย แนวทางการปฏิบัติงานหรือแบบฟอร์มที่เกี่ยวข้อง ให้เลือก yes พร้อมแนบเอกสาร โดยระบบสามารถสั่งพิมพ์เอกสารที่แนบได้ในฟังก์ชั่นนี้ หากอยู่ระหว่างการจัดเตรียมเอกสารให้เลือก prepare

เมื่อทำการประเมินครบทั้ง 2 ส่วน ระบบจะทำการประเมินและแสดงผลตามระดับสีในช่อง Result

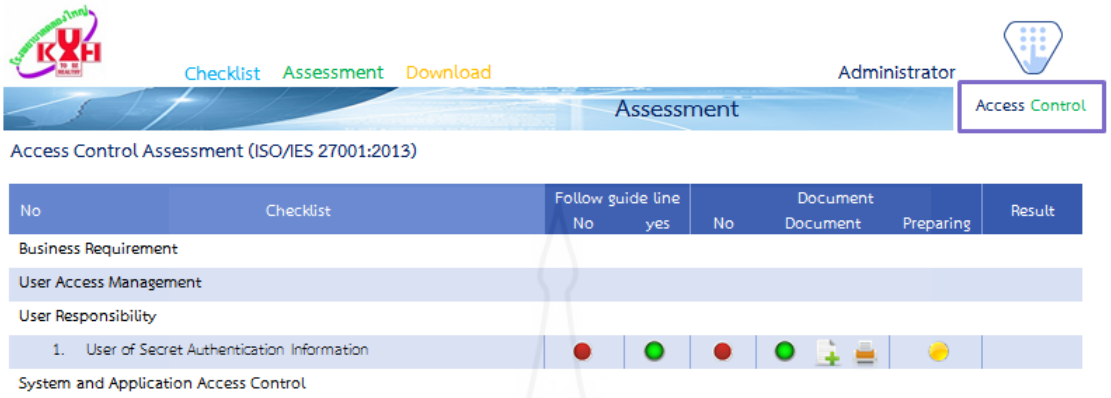
(2) การประเมินข้อกำหนด User Access Management



ภาพที่ 4.14 ฟังก์ชัน Assessment ข้อกำหนด User Access Management

ภาพที่ 4.14 ฟังก์ชัน Assessment ข้อกำหนด User Access Management แสดงรายละเอียด การประเมินข้อกำหนดด้าน User Access Management ซึ่งประกอบด้วยข้อกำหนดย่อยด้าน User Registration and Deregistration, User Access Provisioning, Management of Privileged Access Right, Management of Secret Authentication Information of Users, Review of User Access Rights, Removal or Adjustment of Access Rights โดยผู้ประเมินต้องทำการประเมินเช่นเดียวกับข้อกำหนด Business Requirement

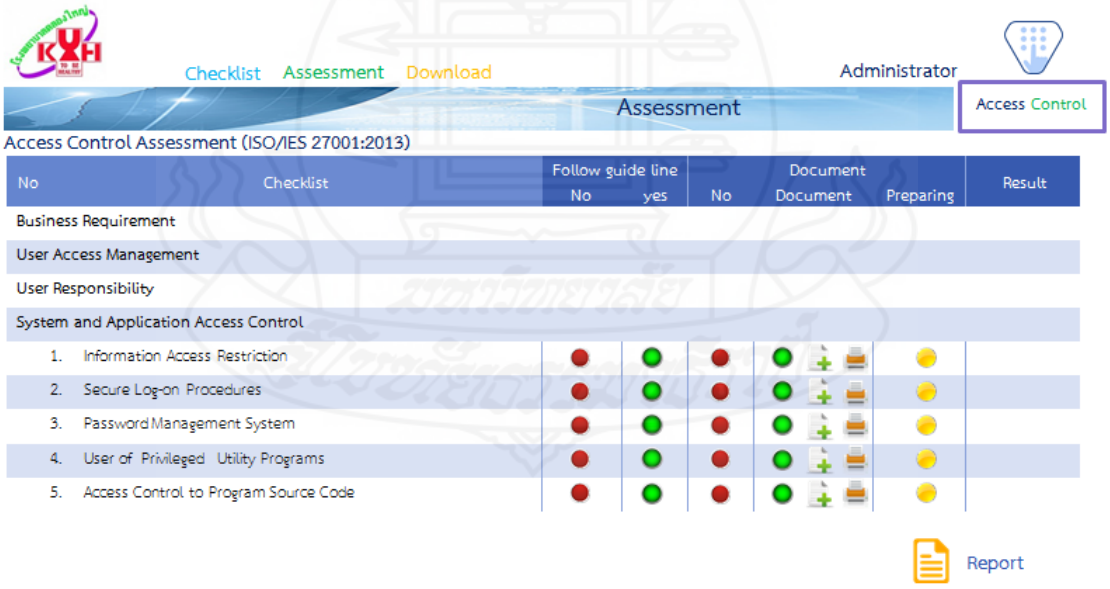
(3) การประเมินข้อกำหนด User Responsibilities



ภาพที่ 4.15 ฟังก์ชัน Assessment ข้อกำหนด User Responsibility

ภาพที่ 4.15 ฟังก์ชัน Assessment ข้อกำหนด User Responsibility แสดงรายละเอียดการประเมินข้อกำหนดด้าน User Responsibility ซึ่งประกอบด้วยข้อกำหนดย่อยด้าน User of Secret Authentication Information โดยผู้ประเมินต้องทำการประเมินเช่นเดียวกับข้อกำหนด Business Requirement

(4) การประเมินข้อกำหนด System and Application Access Control



ภาพที่ 4.16 ฟังก์ชัน Assessment ข้อกำหนด System and Application Control

ภาพที่ 4.16 ฟังก์ชัน Assessment ข้อกำหนด System and Application Control แสดงรายละเอียด การประเมินข้อกำหนดด้าน System and Application Control ซึ่งประกอบด้วย

ข้อกำหนดย่อยด้าน Information Access Restriction, Secure Log-on Procedures, Password Management System, User of Privileged Utility Programs, Access Control to Program Source Code โดยผู้ประเมินต้องทำการประเมินเช่นเดียวกับข้อกำหนด Business Requirement

การประเมินในแต่ละข้อกำหนดย่อย ผู้ใช้งานสามารถทำการประเมินได้ง่าย โดยข้อกำหนดที่ต้องมีการแนบเอกสาร ระบบสามารถทำการแนบเอกสารและเป็นส่วนของคิดค่าคะแนนตามระดับการประเมินและเอกสารที่ผู้ทำการประเมินแนบไว้สามารถแสดงผลและสั่งพิมพ์ได้โดยมีระดับการประเมินดังนี้

1. ข้อมูล/เอกสาร/ ระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัด ผลการประเมินเท่ากับ 100% และแสดงผลเป็นสีเขียว 

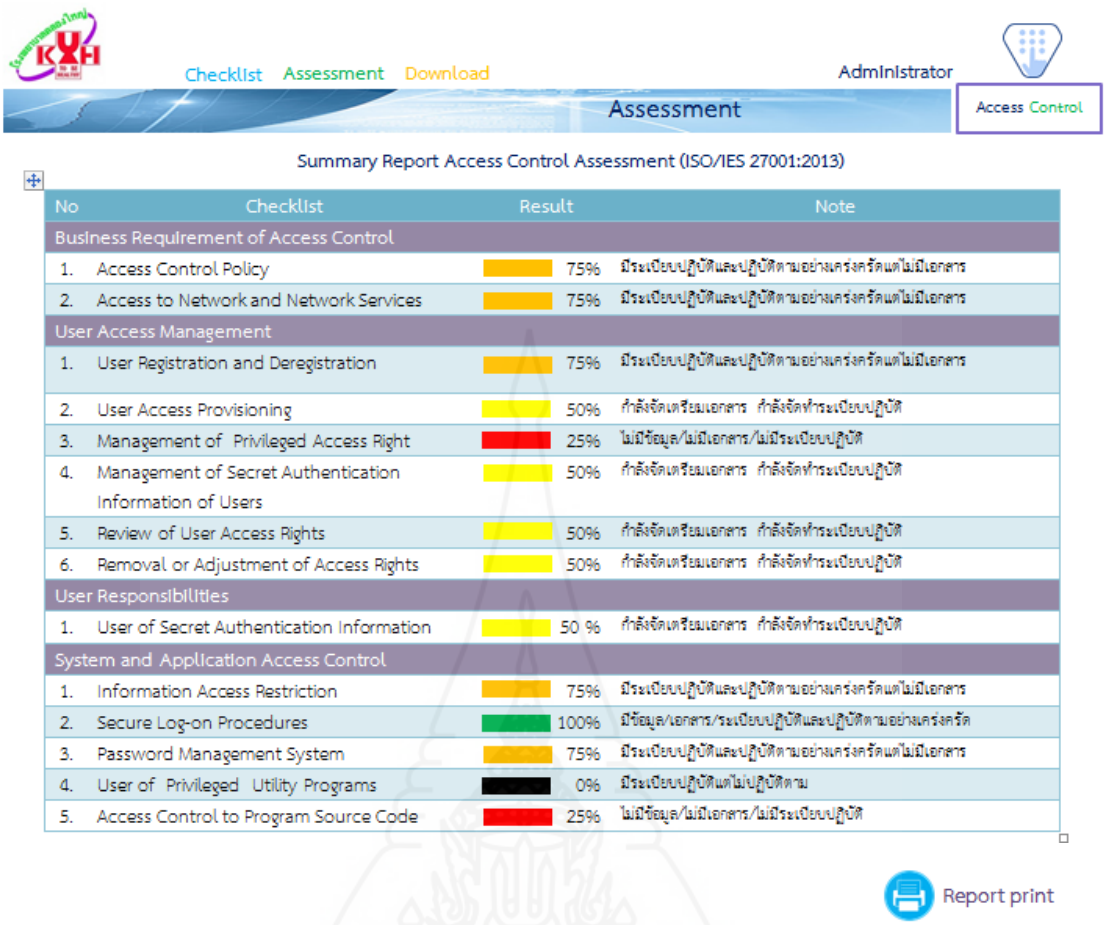
2. มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสารผลการประเมินเท่ากับ 75% และแสดงผลเป็นสีส้ม 

3. กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติผลการประเมินเท่ากับ 50% แสดงผลเป็นสีเหลือง

4. ไม่มีข้อมูล/ไม่มีเอกสาร/ไม่มีระเบียบปฏิบัติ ผลการประเมินเท่ากับ 25% แสดงผลเป็นสีแดง 

5. มีระเบียบปฏิบัติแต่ไม่ปฏิบัติตามผลการประเมินเท่ากับ 0% แสดงผลเป็นสีดำ 

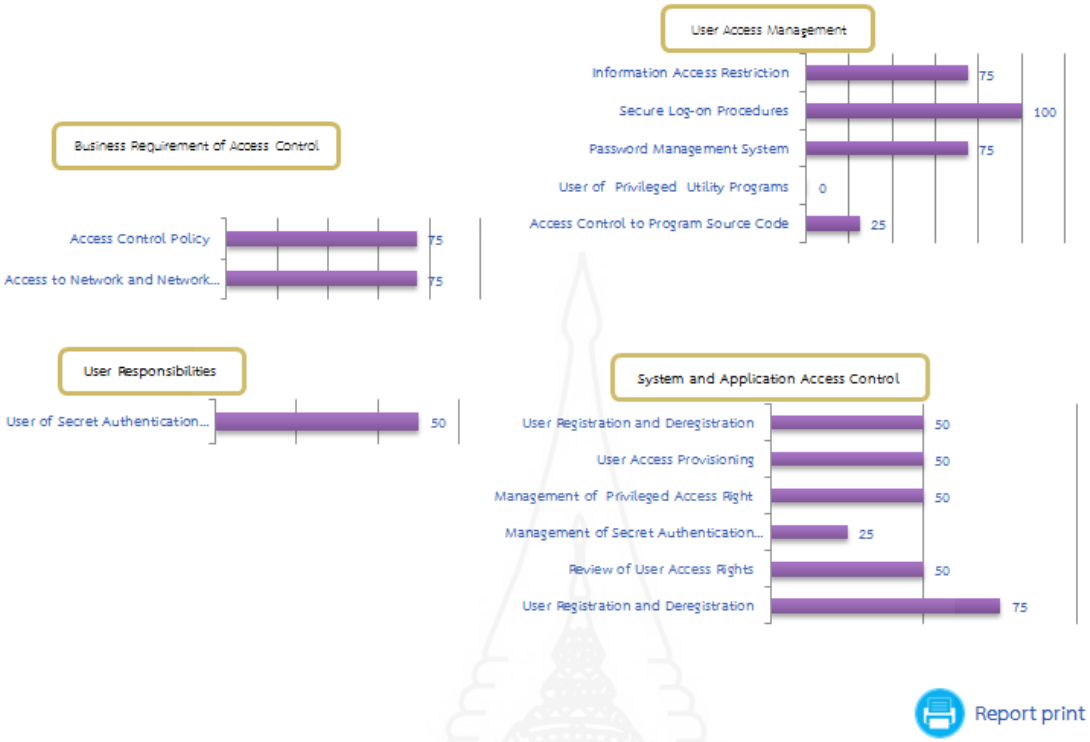
เมื่อผู้ใช้งานทำการประเมินครบทุกข้อกำหนดย่อย ระบบจะประมวลผลและแสดงผลการประเมินตามข้อกำหนดย่อย ข้อกำหนดหลัก และผลภาพรวมทั้งหมด ของความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ และการแสดงผลการประเมินตามข้อกำหนดย่อยในรูปแบบแผนภูมิการแสดงผลที่เข้าใจง่ายและสามารถสั่งพิมพ์รายงานการประมวลได้



No	Checklist	Result	Note
Business Requirement of Access Control			
1.	Access Control Policy	75%	มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร
2.	Access to Network and Network Services	75%	มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร
User Access Management			
1.	User Registration and Deregistration	75%	มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร
2.	User Access Provisioning	50%	กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติ
3.	Management of Privileged Access Right	25%	ไม่มีข้อมูล/ไม่มีเอกสาร/ไม่มีระเบียบปฏิบัติ
4.	Management of Secret Authentication Information of Users	50%	กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติ
5.	Review of User Access Rights	50%	กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติ
6.	Removal or Adjustment of Access Rights	50%	กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติ
User Responsibilities			
1.	User of Secret Authentication Information	50 %	กำลังจัดเตรียมเอกสาร กำลังจัดทำระเบียบปฏิบัติ
System and Application Access Control			
1.	Information Access Restriction	75%	มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร
2.	Secure Log-on Procedures	100%	มีข้อมูล/เอกสาร/ระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัด
3.	Password Management System	75%	มีระเบียบปฏิบัติและปฏิบัติตามอย่างเคร่งครัดแต่ไม่มีเอกสาร
4.	User of Privileged Utility Programs	0%	มีระเบียบปฏิบัติแต่ไม่ปฏิบัติตาม
5.	Access Control to Program Source Code	25%	ไม่มีข้อมูล/ไม่มีเอกสาร/ไม่มีระเบียบปฏิบัติ

ภาพที่ 4.17 ฟังก์ชัน Assessment หน้าสรุปรายงานการประเมินผล

ภาพที่ 4.17 ฟังก์ชัน Assessment หน้าสรุปรายงานการประเมินผล แสดงผลการประเมินโดยแสดงรายละเอียดตามระดับสีและเปอร์เซ็นต์ของความพร้อม และแสดงผลภาพรวมทั้งหมดของความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ โดยที่ระบบสามารถสั่งพิมพ์รายงานสรุปได้



ภาพที่ 4.18 ฟังก์ชัน Assessment หน้ากราฟสรุปผลการประเมิน

ภาพที่ 4.18 ฟังก์ชัน Assessment หน้ากราฟสรุปผลการประเมิน แสดงผลสรุปการประเมินความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ จากรายงานการประเมินผลทั้งหมดในรูปแบบแผนภูมิโดยแสดงผลการประเมินตามข้อกำหนดย่อย และสามารถสั่งพิมพ์หน้าแผนภูมิผลการประเมินได้

3) หน้า Download ระบบสามารถแสดงรายละเอียดเอกสารตามข้อกำหนด ได้แก่ ข้อกำหนดตามเกณฑ์การประเมิน นโยบาย แนวทางการปฏิบัติและแบบฟอร์มที่เกี่ยวข้องโดยสามารถดาวน์โหลดหรือพิมพ์เอกสารที่เกี่ยวข้องเมื่อได้เมื่อกำหนดความต้องการของระบบได้

ภาพที่ 4.19 ฟังก์ชันดาวน์โหลดเอกสาร

ภาพที่ 4.19 ฟังก์ชันดาวน์โหลดเอกสาร แสดงรายละเอียดข้อกำหนดหลักและผู้ใช้งานสามารถดาวน์โหลดตัวอย่างเอกสารที่เกี่ยวข้องเกี่ยวกับ นโยบายแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบ ซึ่งประกอบด้วย ตัวอย่างนโยบาย ตัวอย่างแนวทางการปฏิบัติงาน และตัวอย่างแบบฟอร์มที่เกี่ยวข้อง

บทที่ 5
อภิปรายผลและข้อเสนอแนะ

1. สรุปผลการดำเนินงาน

1.1 การพัฒนานโยบายและแนวทางด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ภายหลังการดำเนินการพัฒนานโยบายและแนวทาง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ ตามมาตรฐาน ISO/IEC 27001:2013 ทำให้ โรงพยาบาลคลองใหญ่มีนโยบายและแนวทางในการควบคุมการเข้าถึงระบบสารสนเทศ ทั้ง 4 ด้าน ที่สามารถนำไปใช้งานและเป็นต้นแบบสำหรับองค์กรที่มีบริบทใกล้เคียงกัน โดยเฉพาะโรงพยาบาลชุมชน ดังนี้คือ

1.1.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control)

1) นโยบายควบคุมการเข้าถึงระบบสารสนเทศ (Access Control Policy)

(1) นโยบายควบคุมการเข้าถึงระบบสารสนเทศ

(2) แนวทางการจัดทำนโยบายควบคุมการเข้าถึงระบบ สารสนเทศ

2) การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

(1) นโยบายการเข้าถึงเครือข่ายและบริการเครือข่าย

(2) แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

(3) แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ และยกเลิกสิทธิ

1.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

1) การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and Deregistration)

(1) นโยบายการลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน

(2) แนวทางการปฏิบัติการลงทะเบียนผู้ใช้งาน

(3) ตารางแสดงสิทธิในการเข้าถึงระบบ

(4) แนวทางการปฏิบัติการเพิกถอดการลงทะเบียนผู้ใช้งาน

(5) รายงานการเพิกถอดทะเบียนผู้ใช้งาน

2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน(User Access Provisioning)

(1) นโยบายการจัดการสิทธิการเข้าถึงของผู้ใช้งาน

3) การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

(1) นโยบายการให้และการใช้สิทธิการเข้าถึงตามระดับสิทธิ

4) การบริการจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users)

(1) นโยบายการควบคุมพิสูจน์ตัวตนของผู้ใช้งานระบบนโยบายการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน

5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน(Review of User Access Rights)

(1) นโยบายการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

(2) แนวทางการปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

(3) ตารางแสดงสิทธิในการเข้าถึงระบบงาน

(4) รายงานการสอบทานรายชื่อผู้ใช้งานระบบ

(5) รายงานการสอบทานสิทธิการเข้าถึงของผู้ใช้งาน

6) การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

(1) นโยบายการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

(2) แนวทางการปฏิบัติการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

(3) รายงานการยกเลิกสิทธิ

1.1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of Secret Authentication Information)

(1) นโยบายการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ(Use of secret Authentication information)

1.1.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

1) การจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Restriction)

(1) นโยบายการจำกัดการเข้าถึงสารสนเทศ

(2) ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

2) นโยบายการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

(1) แนวทางการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

3) ระบบบริหารจัดการระบบผ่าน (Password Management System)

(1) นโยบายการบริหารจัดการรหัสผ่าน (Password management system)

(2) แนวทางการปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management System Procedure)

4) การใช้โปรแกรมอรรถประโยชน์ (User of Privileged Utility Programs)

(1) นโยบายการใช้โปแกรมอรรถประโยชน์

(2) แนวทางการปฏิบัติการขอใช้โปรแกรมอรรถประโยชน์

(3) แบบฟอร์มขอติดตั้งโปรแกรมอรรถประโยชน์

5) การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to Program Source Code)

(1) นโยบายการควบคุมการเข้าถึงซอสโค้ดของโปรแกรม

(2) แนวทางการปฏิบัติการบริหารจัดการการเข้าถึงซอสโค้ดของโปรแกรม

(3) แบบฟอร์มร้องขอการเปลี่ยนแปลง

1.2 การพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ

การดำเนินการพัฒนาระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศด้านการควบคุมการเข้าถึงระบบ ตามมาตรฐาน ISO/IEC 27001: 2013 ที่จัดทำขึ้นเพื่อใช้งานในองค์กรและใช้เป็นต้นแบบ ดังรายละเอียดในบทที่ 4 และได้ทำการทดสอบการ โดยประเมินความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศของโรงพยาบาล ระบบสามารถใช้งานได้และสามารถประมวลผลได้ตามความต้องการ แต่มีข้อจำกัดที่ระบบเป็นการประเมินเบื้องต้น ว่าเอกสารครบตามแนวทาง

หรือไม่ ส่วนคุณภาพของเอกสาร ผู้รับผิดชอบที่ทำการตรวจสอบ ต้องมีการตรวจสอบอีกครั้งว่าคุณภาพ ครบตามแนวทางหรือไม่

เมื่อทำการทดสอบ ประเมินความมั่นคงปลอดภัยด้านการควบคุมการเข้าถึงระบบสารสนเทศ ของโรงพยาบาลคลองใหญ่ พบว่าผลการประเมินความพร้อม ด้านการควบคุมการเข้าถึงระบบอยู่ที่ ร้อยละ 30.36 โดยมีรายละเอียดตามตารางที่ 5.1 ดังนี้

ตารางที่ 5.1 ผลการทดสอบการประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
1	**ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง**	**37.50**	
1.1	นโยบายควบคุมการเข้าถึง	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
1.2	การเข้าถึงเครือข่ายและบริการเครือข่าย	50.00	ปฏิบัติตามแนวทางและอยู่ระหว่างจัดทำเอกสารเกี่ยวข้อง
2	**การบริหารจัดการการเข้าถึงของผู้ใช้งาน**	**25.00**	
2.1	การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
2.2	การจัดการสิทธิการเข้าถึงของผู้ใช้งาน	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
2.3	การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
2.4	การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
2.6	การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
3	**หน้าที่ความรับผิดชอบของผู้ใช้งาน**	**25.00**	
3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
4	**การควบคุมการเข้าถึงระบบ**	**35.00**	
4.1	การจำกัดการเข้าถึงระบบสารสนเทศ	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	50.00	ปฏิบัติตามแนวทางและอยู่ระหว่างจัดทำ

ตารางที่ 5.1 ผลการทดสอบการประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ (ต่อ)

ลำดับ	หัวข้อประเมิน	คุณภาพ (ร้อยละ)	หมายเหตุ
			เอกสารเกี่ยวข้อง
4.3	ระบบบริหารจัดการรหัสผ่าน	50.00	ปฏิบัติตามแนวทางและอยู่ระหว่างจัดทำเอกสารเกี่ยวข้อง
4.4	การใช้โปรแกรมอรรถประโยชน์	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร
4.5	การควบคุมการเข้าถึงซอสโค้ดของโปรแกรม	25.00	ไม่มีการปฏิบัติตามแนวทาง ไม่มีเอกสาร

การประเมินตนเองตามระบบดังกล่าว เมื่อระบบทำการสรุปผลเป็นรายงาน ทำให้โรงพยาบาลทราบส่วนขาดหรือส่วนที่ต้องทำการปรับปรุง เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยมากขึ้น

2. อภิปรายผลการดำเนินงาน

ผลการศึกษาค้นคว้าอิสระ “การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: สำหรับโรงพยาบาลคลองใหญ่ จังหวัดตราด” ได้เป็นไปตามที่ผู้ศึกษาได้ตั้งวัตถุประสงค์ไว้ทั้งสองประการ ประการแรก คือ โรงพยาบาลคลองใหญ่ มีนโยบายและแนวทาง ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ทั้งหมด 4 ด้าน คือ ด้านความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control) ด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ด้านหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) และด้านการควบคุมการเข้าถึงระบบ (System and Application Access Control) เป็นไปตามตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งโรงพยาบาลได้นำนโยบายและแนวทางดังกล่าวมาใช้ในองค์กร ส่งผลให้องค์กรมีความมั่นคงปลอดภัยของสารสนเทศมากขึ้น โดยนโยบายและแนวทางดังกล่าว สามารถนำไปประยุกต์ใช้ในหน่วยงาน หรือองค์กรอื่นๆ ที่มีบริบทใกล้เคียงกันได้ ประการที่สอง โรงพยาบาลคลองใหญ่ มีระบบประเมินความพร้อมความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ซึ่งระบบได้รับการพัฒนาแนวทาง ตามมาตรฐาน ISO/IEC 27001:2013 ที่ครอบคลุมทั้ง 4 ด้าน คือ ด้านความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement of Access Control) ด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ด้านหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) และด้านการควบคุมการเข้าถึงระบบ (System and Application Access Control) โดยระบบได้ถูกพัฒนาขึ้นมาในรูปแบบของเวบแอพพลิเคชัน ตามหลักการของเวบเบส

การพัฒนาตามการศึกษาดังกล่าว สอดคล้องกับผลการผลการศึกษาของ เดชาวัต นิชา-ญานันท์ (2555) ที่ทำการศึกษาและพัฒนาการจัดการนโยบายความปลอดภัยมั่นคงระบบสารสนเทศสำหรับโรงพยาบาลสินแพทย์ ตามแนวทางของ ISO/IEC 27001 ทำให้ระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัยมากขึ้น และเฉลิม สุวรรณะ (2554) ที่ทำการศึกษาความมั่นคงปลอดภัยสารสน-เทศของศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ซึ่งนำแนวทางของ ISO/IEC 27001 มาใช้พัฒนานโยบายเพื่อควบคุมการปฏิบัติงาน ทำให้หน่วยงานมีความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลดลง

การดำเนินงานทั้งหมด ส่งผลให้ระบบสารสนเทศของโรงพยาบาลคลองใหญ่ มีความมั่นคงปลอดภัยมากขึ้น ซึ่งสอดคล้องกับนโยบายของสำนักนโยบายและยุทธศาสตร์ สำนักงานปลัดกระทรวงสาธารณสุข กระทรวงสาธารณสุข ที่ได้กำหนดแนวทางปฏิบัติสำหรับโรงพยาบาล ใน

การป้องกันดูแลความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานการจัดการความมั่นคงปลอดภัยของข้อมูลผู้ป่วย พ.ศ. 2559

3. ปัญหาและข้อเสนอแนะ

3.1 สำหรับการศึกษาครั้งนี้ พบปัญหาในการกำหนดแนวทางปฏิบัติงาน เนื่องจากเป็นองค์กรของรัฐขนาดเล็ก ที่มีข้อจำกัดด้านเจ้าหน้าที่สารสนเทศที่มีจำนวนบุคลากรน้อยและไม่ตรงตำแหน่งงานรวมทั้ง เป็นองค์กรขนาดเล็กที่ยังไม่เคยมีผู้ทำการศึกษาและพัฒนาการแนวทางจัดการความมั่นคงปลอดภัยสารสนเทศ ในรูปแบบเดียวกันนี้มาก่อน จึงได้ดำเนินการพัฒนาโดยใช้แหล่งอ้างอิงที่เป็นองค์กรด้านสาธารณสุขที่มีขนาดใหญ่กว่า มีความพร้อมด้านบุคลากรและความมั่นคงปลอดภัยสารสนเทศที่เป็นระบบมากกว่า มาพัฒนาและประยุกต์ให้สอดคล้องบริบทขององค์กรให้มากที่สุด

3.2 เนื่องจากเทคโนโลยีมีการพัฒนาอย่างต่อเนื่องและรวดเร็ว ดังนั้นนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ จึงจำเป็นต้องมีการพัฒนาและปรับปรุงให้เหมาะสมอยู่ตลอดเวลาเพื่อให้ทันต่อเทคโนโลยีสารสนเทศในปัจจุบัน

3.3 ผู้จัดทำแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศ ควรมีความรู้และปฏิบัติงานเกี่ยวข้องในด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความเข้าใจในกระบวนการการรวบรวมข้อมูล การจัดทำนโยบายและแนวทางการปฏิบัติงานได้อย่างครบถ้วน

3.4 ในการศึกษาและพัฒนาครั้งต่อไป เพื่อให้ความมั่นคงปลอดภัยสารสนเทศขององค์กร มีความมั่นคงปลอดภัยมากขึ้น ควรมีการพัฒนานโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้อง ให้ครอบคลุมทุกด้าน โดยนำรูปแบบที่จัดทำขึ้นจากการศึกษาและพัฒนาครั้งนี้ ไปประยุกต์ใช้กับหลักเกณฑ์ในข้ออื่นๆ ที่เกี่ยวข้อง และดำเนินการพัฒนาระบบประเมินเพิ่มเติมให้ครบทุกองค์ประกอบ เพื่อให้องค์กรสามารถรู้ถึงสิ่งที่ต้องทำการปรับปรุง ทำให้ระบบสารสนเทศขององค์กรมีความมั่นคงปลอดภัยมากขึ้น

บรรณานุกรม

บรรณานุกรม

กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช. (2554). *แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ*. สืบค้นจาก www.dnp.go.th/isms/ISMS2557.pdf.

เฉลิม สุวรรณะ. (2554). *การรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษาศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี*. (สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมเครือข่าย ไม่ได้ตีพิมพ์). บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

เดชาวัต นิชาญานันท์. (2555). *การจัดทำนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร กรณีศึกษาสำหรับบริษัท สินแพทย์จำกัด (โรงพยาบาลสินแพทย์)*. (สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาความมั่นคงทางระบบสารสนเทศ ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

บริษัททีเน็ต จำกัด. (2555). *มาตรฐาน ISO/IEC 270001:2013*. สืบค้นจาก http://www.tnet security.com/content_audit/27001-2013.pdf.

ไพศาล จันทร์เลื่อน. (2557). *การพัฒนาความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศภายใต้มาตรฐาน ISO 27001 กรณีศึกษาศูนย์พัฒนาและบริการเทคโนโลยี สารสนเทศมหาวิทยาลัยราชภัฏพระนคร.* (สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

ภาธร เทง. (2559). *ส่วนประกอบของ Web Application (website).* สืบค้นจาก https:// blog.wisered.com/87-web-application-website.

วรรษา เปาอินทร. (2559). *มาตรฐานการจัดการความปลอดภัยของขอมูลผู่ปวย พ.ศ. 2559*. กรุงเทพฯ: สำนักกิจการโรงพิมพ องคการสงเคราะหทหารผานศึก ในพระบรมราชูปถัมภ์.

อัจฉรินทร์ พัฒนพันธ์ชัย และคณะ. (2559). *นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร.* สืบค้นจาก http://www.boi.go.th/upload/%E0A2_ ICT_(P_ IT_SP_01)_37229.pdf.

Kuo-Hsiung Liao, Hao-En Chueh. (2555). Medical Organization Information Security Management Based on ISO27001 Information Security Standard Information Management Department. *JOURNAL OF SOFTWARE*, 7(4), 792-797.

ภาคผนวก

ภาคผนวก ก

ตัวอย่างนโยบายป้องกันและรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
ด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ตัวอย่างนโยบายการเข้าถึงเครือข่ายและบริการเครือข่าย
(Access to network and network service Policy)

1.นโยบายการใช้บริการของเครือข่าย

การเชื่อมต่อทั้งจากภายในโรงพยาบาลหรือการเชื่อมต่อไปยังภายนอกโรงพยาบาล ต้องได้รับการอนุมัติจากผู้ดูแลสารสนเทศ ซึ่งผู้ดูแลสารสนเทศต้องพิจารณาหัวข้อดังต่อไปนี้ประกอบการพิจารณาอนุมัติ

- อุปกรณ์การสื่อสารเกี่ยวข้องกับการเชื่อมต่อดังกล่าว
- การจัดการและขั้นตอนการให้สิทธิในการเข้าถึงอุปกรณ์ที่เกี่ยวข้อง
- มาตรการในการควบคุมความมั่นคงปลอดภัยที่จำเป็นกับการเชื่อมต่อนั้นๆ

ผู้ดูแลสารสนเทศต้องจัดให้มีกระบวนการในการสอบทาน เพื่อให้มั่นใจว่าบริการสำหรับเครือข่ายที่ไม่ได้ใช้งานต้องถูกยกเลิกหรือระงับการใช้งาน

1.1 ผู้ดูแลสารสนเทศต้องยกเลิกการใช้งานจุดเชื่อมต่อระบบเครือข่ายภายในอาคาร บริเวณหรือสถานที่ปฏิบัติงานของโรงพยาบาล ที่ไม่ได้มีการใช้งานหรือไม่ได้มีการควบคุมความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสมเพื่อป้องกันการลักลอบใช้งานหรือเข้าถึงเครือข่ายภายในของธนาคารโดยอาศัยจุดเชื่อมต่อดังกล่าว

1.2 ผู้ใช้งานต้องไม่เชื่อมต่ออุปกรณ์คอมพิวเตอร์และอุปกรณ์การสื่อสารไปยังเครือข่ายภายนอก เพื่อให้บุคคลหรือหน่วยงานภายนอกสามารถเข้าถึงเครือข่ายภายในของโรงพยาบาลได้ ยกเว้นจะได้รับการอนุมัติจากผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศแล้ว ซึ่งการดำเนินการดังกล่าวผู้ดูแลสารสนเทศต้องพิจารณาการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการเชื่อมต่อในลักษณะดังกล่าว

1.3 ผู้ใช้งานต้องไม่ใช้อุปกรณ์คอมพิวเตอร์ของโรงพยาบาลในการบุกรุกหรือโจมตีเครือข่ายใดๆ หรือการใช้ในทางที่ผิดกฎหมาย

1.4 ผู้ใช้งานต้องไม่เปิดเผยข้อมูลโครงสร้างเครือข่ายภายในโรงพยาบาล รวมถึงรายละเอียดผังเครือข่ายคอมพิวเตอร์ เช่น เลขที่เครือข่าย รายละเอียดของอุปกรณ์การสื่อสารในเครือข่าย เป็นต้น ต่อหน่วยงานภายนอกโดยไม่ได้รับอนุญาตจากผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศ

1.5 การใช้งานอินเทอร์เน็ตของผู้ใช้งาน ต้องได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบของผู้ดูแลสารสนเทศ และต้องอยู่บนพื้นฐานของความจำเป็นในการปฏิบัติงานเท่านั้น

1.6 ผู้ใช้งานที่ได้รับอนุญาตให้เข้าถึงอินเทอร์เน็ต จากอุปกรณ์คอมพิวเตอร์ที่อยู่ภายในเครือข่ายของโรงพยาบาล ต้องใช้อินเทอร์เน็ตเพื่อการปฏิบัติงานประจำวันหรือเพื่อประโยชน์ของโรงพยาบาลเท่านั้น

1.7 ผู้ดูแลสารสนเทศต้องจัดให้มีกระบวนการในการติดตามและเฝ้าระวังกิจกรรมการใช้อินเทอร์เน็ต หรือเครือข่ายคอมพิวเตอร์ของผู้ใช้งานที่ไม่เหมาะสมหรือไม่เกี่ยวข้องกับการปฏิบัติงานและการดำเนินงานของโรงพยาบาล อันได้แก่

- การส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล์ขนาดใหญ่ไปยังผู้รับจำนวนมาก
- การส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่ หรือสแปมเมล์
- การเข้าถึงเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ภาพอนาจาร
- การเล่นเกมผ่านอินเทอร์เน็ต
- การเข้า Online Chat Room
- การหารายได้หรือผลประโยชน์ส่วนตัวหรือเพื่อธุรกิจส่วนตัว
- การใช้ประกอบหรือสนับสนุนการกระทำที่ผิดกฎหมายและ/หรือการฉ้อโกง
- การส่งข้อความหรือไฟล์ข้อมูลหรือรูปภาพที่มีเนื้อหาไม่เหมาะสม
- การจัดเก็บไฟล์ที่มีการละเมิดลิขสิทธิ์ เช่น MP3 เป็นต้น

1.8 ผู้ดูแลสารสนเทศต้องจัดให้มีการในตรวจสอบและป้องกันไวรัสคอมพิวเตอร์โดยอัตโนมัติ เมื่อมีการเข้าถึงเว็บไซต์และการดาวน์โหลดไฟล์ต่างๆ

2. **การควบคุมการเชื่อมต่อกับเครือข่ายภายนอก**

2.1 ผู้ดูแลสารสนเทศต้องจัดให้มีอุปกรณ์ป้องกันเครือข่ายสำหรับป้องกันภัยคุกคามที่อาจเกิดจากการเชื่อมต่อเครือข่ายของโรงพยาบาลกับเครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต เช่น อุปกรณ์ ไฟล์วอลล์ อุปกรณ์ดักจับหรือป้องกันผู้บุกรุก เป็นต้น โดยพิจารณาตามหลักความเสี่ยง (Risk Based Approach)

2.2 ผู้ดูแลสารสนเทศมีหน้าที่กำหนดและบริหารจัดการค่าคอนฟิกูเรชั่นและค่าความปลอดภัยด้านเทคนิคให้สอดคล้องกับความต้องการในการดำเนินงานและมีการปรับปรุงค่าความปลอดภัยต่างๆ ให้สอดคล้องกับภัยคุกคามหรือช่องโหว่ที่มีการเปลี่ยนแปลง

2.3 การเชื่อมต่อเครือข่ายของโรงพยาบาลไปยังหน่วยงานภายนอก จะต้องมีการประเมินความเสี่ยงและผลกระทบจากการเชื่อมต่อดังกล่าวเพื่อพิจารณาหามาตรการควบคุมที่เหมาะสม และการเชื่อมต่อดังกล่าวต้องได้รับการอนุมัติจากผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศ

2.4 ในการเชื่อมต่อกับระบบเครือข่ายภายนอกองค์กร ผู้ดูแลสารสนเทศต้องจัดให้มีการปิดบังเลขที่เครือข่ายภายในเพื่อป้องกันไม่ให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องรับทราบข้อมูลสำคัญดังกล่าว

2.5 ผู้ดูแลสารสนเทศต้องจัดให้มีการพิสูจน์ตัวตนของผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศหรือระบบเครือข่ายของโรงพยาบาลสำหรับระบบสารสนเทศที่มีความสำคัญ ผู้ดูแลสารสนเทศสามารถพิจารณาใช้อุปกรณ์ควบคุมความมั่นคงปลอดภัยเพิ่มเติมในขั้นตอนของการพิสูจน์ตัวตน ก่อนเข้าสู่เครือข่ายของธนาคาร เช่น สมาร์ทการ์ด)Smart Card(หรือ โทเค็น)Token) เป็นต้น โดยควรพิจารณาเลือกใช้อุปกรณ์ที่ปลอดภัยตามมาตรฐานสากล

2.6 ผู้ดูแลสารสนเทศต้องจัดการป้องกันมิให้อุปกรณ์คอมพิวเตอร์และอุปกรณ์การสื่อสารรับคำสั่งใดๆ จากเครือข่ายภายนอกโดยปราศจากการพิสูจน์ตัวตนผู้ใช้งานที่ถูกต้อง

2.7 ผู้ดูแลสารสนเทศต้องไม่อนุญาตให้มีการบริหารจัดการเครือข่ายจากระยะไกล (Remote Administration) และต้องควบคุมไม่ให้ผู้ใช้งานเชื่อมต่ออุปกรณ์คอมพิวเตอร์กับเครือข่ายภายนอกผ่านโมเด็มในขณะที่มีการเชื่อมต่ออุปกรณ์ดังกล่าวกับเครือข่ายภายในของโรงพยาบาล ในกรณีที่มีความจำเป็น กิจกรรมดังกล่าวต้องได้รับอนุมัติจากผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศก่อน และต้องจัดให้มีการควบคุมที่ปลอดภัยดังต่อไปนี้

- การเลือกใช้วิธีการพิสูจน์ตัวตนผู้ใช้งานที่รัดกุมและปลอดภัย เช่น การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่แตกต่างกันในหลายระดับชั้น การใช้อุปกรณ์ตรวจสอบตัวตนอื่นเพิ่มเติมจากรหัสผ่านสำหรับกรณีที่มีการเชื่อมต่อกับเครือข่ายที่สำคัญ เป็นต้น
- เจ้าหน้าที่ดูแลระบบต้องกำหนดรหัสผ่านที่เข้มงวดและยากแก่การเดา และเปลี่ยนรหัสผ่านทันทีเมื่อมีการเชื่อมต่อแบบระยะไกลแล้วเสร็จ
- การเข้ารหัสข้อมูลสำคัญก่อนส่งผ่านการเชื่อมต่อดังกล่าว
- การจัดเก็บบันทึกเพื่อการตรวจสอบ (Audit Log) ของกิจกรรมต่างๆ ที่เกิดขึ้น
- การจำกัดช่วงเวลาในการเชื่อมต่อและการใช้งาน
- การใช้เทคนิคของเครือข่ายส่วนตัวเสมือน (Virtual Private Network - VPN)

3.การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย

3.1 ผู้ดูแลสารสนเทศควรใช้หมายเลขระบุอุปกรณ์เพื่อบ่งชี้ว่าอุปกรณ์นี้ได้รับอนุญาตให้เชื่อมต่อเข้าหรือไปที่เครือข่ายหนึ่งหรือไม่ เช่น การใช้ MAC Address เป็นต้น

3.2 ในกรณีที่มีเครือข่ายมากกว่าหนึ่งเครือข่ายที่อุปกรณ์นั้นสามารถเชื่อมต่อเข้าไปได้ หมายเลขระบุอุปกรณ์ควรบ่งชี้ว่าเครือข่ายใดที่อุปกรณ์นั้นสามารถเชื่อมต่อเข้าไปได้และเครือข่ายใดที่ไม่สามารถเชื่อมต่อเข้าไปได้

3.3 ผู้ดูแลสารสนเทศต้องจัดให้มีความมั่นคงปลอดภัยทางกายภาพเพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์

4.การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

4.1 ผู้ดูแลสารสนเทศต้องควบคุมการเข้าถึงทางกายภาพต่อพอร์ตของอุปกรณ์เครือข่าย ที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันที่ตัวอุปกรณ์

4.2 ต้องกำหนดขั้นตอนปฏิบัติเพื่อขออนุมัติจากผู้มีอำนาจก่อนอนุญาตให้ผู้ให้บริการภายนอกเข้าดำเนินการบำรุงรักษา หรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

4.3 ผู้ดูแลสารสนเทศต้องยกเลิก หรือปิดพอร์ต ยกเลิกหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

5.การแบ่งแยกเครือข่าย

5.1 ผู้ดูแลสารสนเทศต้องจัดแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

5.2 ผู้ดูแลสารสนเทศต้องควบคุมการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเหล่านั้น เช่น เครือข่ายย่อยแต่ละเครือข่ายจะอยู่ในบริเวณหรือสถานที่ที่สามารถควบคุมการเข้าถึงทางกายภาพได้ เป็นต้น

5.3 ผู้ดูแลสารสนเทศต้องจัดแบ่งเครือข่ายออกเป็นเครือข่ายภายในและเครือข่ายภายนอก

5.4 ผู้ดูแลสารสนเทศต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับแต่ละเครือข่ายย่อยเหล่านั้น เช่น ใช้ไฟร์วอลล์กั้นทางเข้าเครือข่ายที่มีระบบงานสำคัญอยู่ในนั้น เป็นต้น

5.5 ผู้ดูแลสารสนเทศต้องประเมินความเสี่ยง เพื่อกำหนดการจัดแบ่งเครือข่ายที่เหมาะสม และจำแนกระบบที่สำคัญ เพื่อกำหนดมาตรการการรักษาความมั่นคงปลอดภัยสำหรับแต่ละเครือข่ายย่อย

5.6 ผู้ดูแลสารสนเทศต้องสร้างเกตเวย์เพื่อกั้นหรือแบ่งเครือข่ายออกเป็นส่วนๆ และควบคุมการเข้าถึงของผู้ใช้งานรวมทั้งควบคุมการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น

5.7 ผู้ดูแลสารสนเทศต้องใช้เกตเวย์ เช่น ไฟร์วอลล์ เพื่อกรองหรือจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อยต่างๆ

5.8 ผู้ดูแลสารสนเทศต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายย่อยภายในองค์กรโดยไม่ได้รับอนุญาต เช่น จากผู้ไม่ประสงค์ดี เป็นต้น

5.9 ผู้ดูแลสารสนเทศต้องปรับแต่งเกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายให้สอดคล้องกับนโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศและนโยบายการใช้บริการเครือข่ายของโรงพยาบาล

5.10ผู้ดูแลสารสนเทศต้องแบ่งแยกเครือข่ายให้สอดคล้องกับนโยบายการใช้บริการเครือข่ายขององค์กร

5.11ผู้ดูแลสารสนเทศต้องแบ่งแยกเครือข่ายให้สอดคล้องกับความต้องการในการเข้าถึงเครือข่าย เช่น ของผู้ใช้งานในกลุ่มต่างๆ หรือของผู้บริหาร เป็นต้น

5.12ผู้ดูแลสารสนเทศต้องพิจารณาคุณค่าและชั้นความลับของข้อมูลที่ใช้งานในเครือข่ายก่อนที่จะตัดสินใจแบ่งเครือข่ายออกเป็นส่วนๆ

5.13ผู้ดูแลสารสนเทศต้องพิจารณาว่าส่วนใดของเครือข่ายที่สามารถจัดให้อยู่ในวงเดียวกันได้ก่อนที่จะตัดสินใจแบ่งเครือข่ายออกเป็นส่วนๆ

5.14ผู้ดูแลสารสนเทศต้องพิจารณาแยกวงของเครือข่ายไร้สายออกจากเครือข่ายภายในองค์กรอื่น

5.15 ผู้ดูแลสารสนเทศต้องประเมินความเสี่ยงและกำหนดมาตรการป้องกันที่เหมาะสมก่อนแบ่งแยก

วงเครือข่ายไร้สาย เช่น การกำหนดมาตรการการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย ด้วยวิธีการที่มีการเข้ารหัสข้อมูล เป็นต้น

6.การควบคุมการเชื่อมต่อทางเครือข่าย

6.1 ผู้ดูแลสารสนเทศต้องกำหนดและปรับปรุงสิทธิในการเข้าถึงเครือข่ายของผู้ใช้งานให้มีความทันสมัย เช่น สิทธิ ในการเข้าถึงหรือใช้งานบริการเครือข่ายต่างๆ และสิทธิในการเข้าถึงเครือข่ายของผู้ใช้งานควรมีความสอดคล้องกับนโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

6.2 ผู้ดูแลสารสนเทศต้องจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน เพื่อกรองข้อมูลจราจรในเครือข่ายให้เป็นไปตามนโยบายหรือ ระเบียบ ข้อบังคับที่กำหนดไว้ เช่น นโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

6.3 ผู้ดูแลสารสนเทศต้องจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานดังนี้

- ระบบงานที่ใช้ในการส่งข้อความ (Messaging applications) เช่น ระบบงานอีเมล์, Live Messaging
- ระบบงานสำหรับการโอนย้ายไฟล์
- ระบบงานต่างๆ สำหรับใช้งานภายในองค์กร

6.4 ผู้ดูแลสารสนเทศต้องจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งานเท่านั้น

7. การควบคุมการกำหนดเส้นทางบนเครือข่าย

7.1 ผู้ดูแลสารสนเทศต้องกำหนดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อทางเครือข่ายและการไหลของข้อมูลผ่านเครือข่ายสอดคล้องกับนโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

7.2 ผู้ดูแลสารสนเทศต้องใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบไอพีแอดเดรส (IP Address) ของทั้งต้นทางและปลายทาง และควบคุมการไหลของข้อมูลผ่านเครือข่าย เช่น จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

8.การควบคุมด้านเครือข่าย

8.1 ผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศต้องกำหนดกิจกรรมการควบคุมเพื่อให้มั่นใจว่าเครือข่ายและโครงสร้างพื้นฐานด้านเครือข่ายของโรงพยาบาล ได้รับการบริหารจัดการความมั่นคงปลอดภัยอย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยงและวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่เจ้าของสารสนเทศกำหนด ซึ่งประกอบด้วยกิจกรรมการควบคุมดังต่อไปนี้

- การกำหนดหน้าที่ความรับผิดชอบในการดูแลเครือข่าย และการจำกัดสิทธิในการเข้าใช้งาน การบริหารจัดการหรือการเชื่อมต่อกับเครือข่ายของโรงพยาบาล โดยต้องพิจารณาตามหลัก ความจำเป็นในการปฏิบัติงาน (Need-to-do Basis) และ

หลักการแบ่งแยกหน้าที่ (Segregation of Duty) โดยควรแยกหน้าที่ความรับผิดชอบออกจากการบริหารและดูแลระบบสารสนเทศอย่างชัดเจน

- การจัดให้มีการป้องกันทางกายภาพในการเข้าถึงอุปกรณ์การติดต่อสื่อสารหรืออุปกรณ์ป้องกันเครือข่ายเพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
- การจัดให้มีอุปกรณ์ป้องกันเครือข่ายเพื่อกลั่นกรองข้อมูลที่รับส่งโดยอาศัยกฎเกณฑ์ต่างๆ ที่ได้กำหนดไว้ล่วงหน้า เช่น การใช้ระบบกลั่นกรอง (Filtering) บนเกตเวย์ (Gateway) หรือการกำหนดกฎการตรวจสอบข้อมูลบนไฟร์วอลล์ (Firewall Rule base) เป็นต้น
- การจัดทำคู่มือปฏิบัติงานสำหรับการจัดการและบริหารอุปกรณ์การติดต่อสื่อสารและอุปกรณ์ป้องกันเครือข่าย
- การจัดให้มีการจัดการเพื่อความพร้อมใช้ของการให้บริการด้านเครือข่าย เช่น การเฝ้าระวัง การทดสอบ และควบคุมการใช้งานทั้งฮาร์ดแวร์และซอฟต์แวร์ของเครือข่าย การวิเคราะห์ Traffic บนเครือข่ายอย่างต่อเนื่อง เป็นต้น
- การพิจารณานำซอฟต์แวร์ที่เหมาะสมมาช่วยบริหารจัดการเครือข่าย เช่น การตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์การติดต่อสื่อสาร การแจ้งเตือนเมื่อพบความผิดปกติกับอุปกรณ์หรือเครือข่าย และการจัดทำทะเบียนรายการอุปกรณ์การติดต่อสื่อสาร (Inventory) เป็นต้น
- การพิจารณานำระบบการตรวจจับและ/หรือป้องกันผู้บุกรุก (Intrusion Detection System – IDS) / Intrusion Prevention System – IPS) มาช่วยในการตรวจจับและ/หรือป้องกันไม่ให้ ผู้บุกรุกเข้ามาทำความเสียหายต่อระบบเครือข่ายของธนาคาร เช่น ระบบการตรวจจับผู้บุกรุกในระดับเครือข่าย (Network-based) และในระดับเครื่องแม่ข่าย (Host-based) เป็นต้น รวมทั้งการติดตามและสอบทานผลที่ได้จากระบบดังกล่าวอย่างสม่ำเสมอเพื่อหาแนวทางแก้ไขและป้องกันเหตุการณ์ละเมิดความมั่นคงปลอดภัยได้อย่างทันท่วงที โดยการพิจารณานำระบบดังกล่าวมาใช้ต้องคำนึงถึงระดับความเสี่ยงและผลกระทบต่อระบบเครือข่ายของโรงพยาบาล
- การตรวจสอบการเชื่อมต่อเครือข่ายผ่านสายโทรศัพท์หรือผ่านเครือข่ายแบบไร้สายเพื่อตรวจหาการเชื่อมต่อโดยไม่ได้รับอนุญาต โดยตรวจสอบอย่างน้อยทุก 6 เดือน
- การปรับปรุงผังเครือข่าย (Network Diagram) ของโรงพยาบาลให้ถูกต้องเป็นปัจจุบันอยู่เสมอ นอกจากนั้นผังเครือข่ายทางกายภาพต้องมีรายละเอียดทรัพย์สินของอุปกรณ์เครือข่ายที่ชัดเจน
- การไม่ส่งข้อมูลสำคัญผ่านบริการเครือข่าย (Network Service) ที่ไม่มีการเข้ารหัส (เช่น Telnet , FTP)

- การกำหนดให้อุปกรณ์การติดต่อสื่อสารที่ทำหน้าที่กลั่นกรองข้อมูลต้องปฏิเสธการเชื่อมต่อจากภายนอกที่ทำเสมือนว่ามาจากภายในองค์กร (IP Spoofing) มิให้เข้ามาในเครือข่ายของโรงพยาบาล

8.2 เมื่อมีการเปลี่ยนแปลงระบบเครือข่ายเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบจะต้องขออนุมัติจากผู้บริหารของหน่วยงานผู้ดูแลสารสนเทศก่อนที่จะเปลี่ยนแปลงใดๆ เพื่อป้องกันไม่ให้เกิดผลกระทบกับการดำเนินงานและต้องปฏิบัติตามมาตรฐานการปฏิบัติงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการการเปลี่ยนแปลง

9. **ความมั่นคงปลอดภัยของบริการด้านเครือข่าย**

9.1 เจ้าของสารสนเทศต้องแจ้งความต้องการให้ผู้ดูแลสารสนเทศทราบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศเมื่อมีการจัดซื้ออุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์การสื่อสาร และอุปกรณ์ป้องกันความมั่นคงปลอดภัยด้านเครือข่ายของธนาคาร และเมื่อมีการทำสัญญาใช้บริการด้านเครือข่ายต่างๆ กับหน่วยงานภายนอก

9.2 ผู้ดูแลสารสนเทศต้องกำหนดมาตรฐานของรูปแบบการสื่อสาร (Network Protocol) และบริการเครือข่าย (Network Service) ที่ได้รับอนุญาตของโรงพยาบาลในการติดต่อสื่อสารภายในและกับเครือข่ายของหน่วยงานภายนอก

9.3 เจ้าของสารสนเทศ (หรือผู้ดูแลสารสนเทศ ในกรณีที่ได้รับมอบหมาย)ต้องจัดให้มีการทำสัญญาการให้บริการด้านเครือข่ายกับหน่วยงานภายนอก โดยมีการกำหนดข้อตกลงของระดับการให้บริการ (Service Level Agreement - SLA) และข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศให้ชัดเจน

ชื่อเอกสาร	เลขที่เอกสาร	ปรับปรุงครั้งที่	วันที่ออกเอกสาร
นโยบายการเข้าถึงเครือข่ายและบริการเครือข่าย	KYH-IM-AC-01-03	จัดทำครั้งแรก	10 ตุลาคม 2560

ผู้จัดทำเอกสาร	ผู้เห็นชอบเอกสาร	ผู้อนุมัติ
..... (.....) ตำแหน่ง.....	คณะกรรมการสารสนเทศ	..... (.....) ตำแหน่ง.....

ภาคผนวก ข

ตัวอย่างแนวทางการปฏิบัติงาน ด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ตัวอย่างแนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

(Network Services Request Procedure)

สารบัญ

1.บทนำ

แนวทางการปฏิบัติงานการขอใช้บริการเครือข่ายฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทาง และแสดงให้เห็นถึงขั้นตอนในการปฏิบัติงานที่เกี่ยวกับการขอใช้บริการเครือข่าย เพื่อกำหนดแนวทางในการควบคุมการเข้าถึงสารสนเทศให้เหมาะสมกับข้อกำหนดความต้องการสำหรับการควบคุมการเข้าถึง

2.วัตถุประสงค์

แนวทางการปฏิบัติงานการขอใช้บริการเครือข่ายฉบับนี้ จัดทำขึ้นเพื่ออธิบายรายละเอียดของการขอใช้บริการเครือข่าย โดยแสดงให้เห็นความจำเป็นในการจัดการและควบคุมการเข้าถึงสารสนเทศเครือข่ายการสื่อสารโทรคมนาคม ความสัมพันธ์ของผู้ดำเนินการและบทบาทหน้าที่ความรับผิดชอบในแต่ละขั้นตอนเพื่อให้สอดคล้องกับนโยบายด้านการควบคุมการเข้าถึงระบบสารสนเทศ ด้านความต้องการการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

3.ขอบเขต

แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย ครอบคลุมถึงขั้นตอนการขอใช้บริการเครือข่ายและขั้นตอนการเปลี่ยนแปลงการใช้บริการเครือข่าย

4.หน่วยงานที่เกี่ยวข้องและหน้าที่ความรับผิดชอบ

รายละเอียดในหัวข้อนี้ จะกล่าวถึงหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับ แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

4.1 ผู้ร้องขอ

บุคคลหรือหน่วยงานภายในโรงพยาบาล ซึ่งเป็นผู้ที่มีความประสงค์จะขอเปลี่ยนแปลงสิทธิการใช้งานบริการเครือข่าย โดยผู้ร้องขอมีบทบาทและหน้าที่ความรับผิดชอบดังต่อไปนี้

- กรอกแบบฟอร์มเพื่อขอใช้บริการเครือข่าย
- กรอกแบบฟอร์มเพื่อขอเปลี่ยนแปลงการใช้บริการเครือข่าย

4.2 ผู้บังคับบัญชาของผู้ร้องขอ

ผู้บังคับบัญชาของผู้ร้องขอ มีบทบาทและหน้าที่ความรับผิดชอบดังต่อไปนี้

- พิจารณาการขอใช้บริการเครือข่าย
- ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ
- ลงนามอนุมัติ
- พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย

4.3 ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ

ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ มีบทบาทและหน้าที่ความรับผิดชอบดังต่อไปนี้

- พิจารณาการขอใช้บริการเครือข่าย
- ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ
- ลงนามอนุมัติ
- พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย

4.4 ผู้ดูแลสารสนเทศ

ผู้ดูแลสารสนเทศ มีบทบาทและหน้าที่ความรับผิดชอบดังต่อไปนี้

- สร้างบัญชีผู้ใช้งานและรหัสผ่านสำหรับใช้งานเครือข่ายในระบบ
- ลงนามผู้ดำเนินการ
- จัดเก็บเอกสาร
- เปลี่ยนแปลงสิทธิการใช้เครือข่ายในระบบ

4.5 IT Helpdesk

IT Helpdesk มีบทบาทและหน้าที่ความรับผิดชอบดังต่อไปนี้

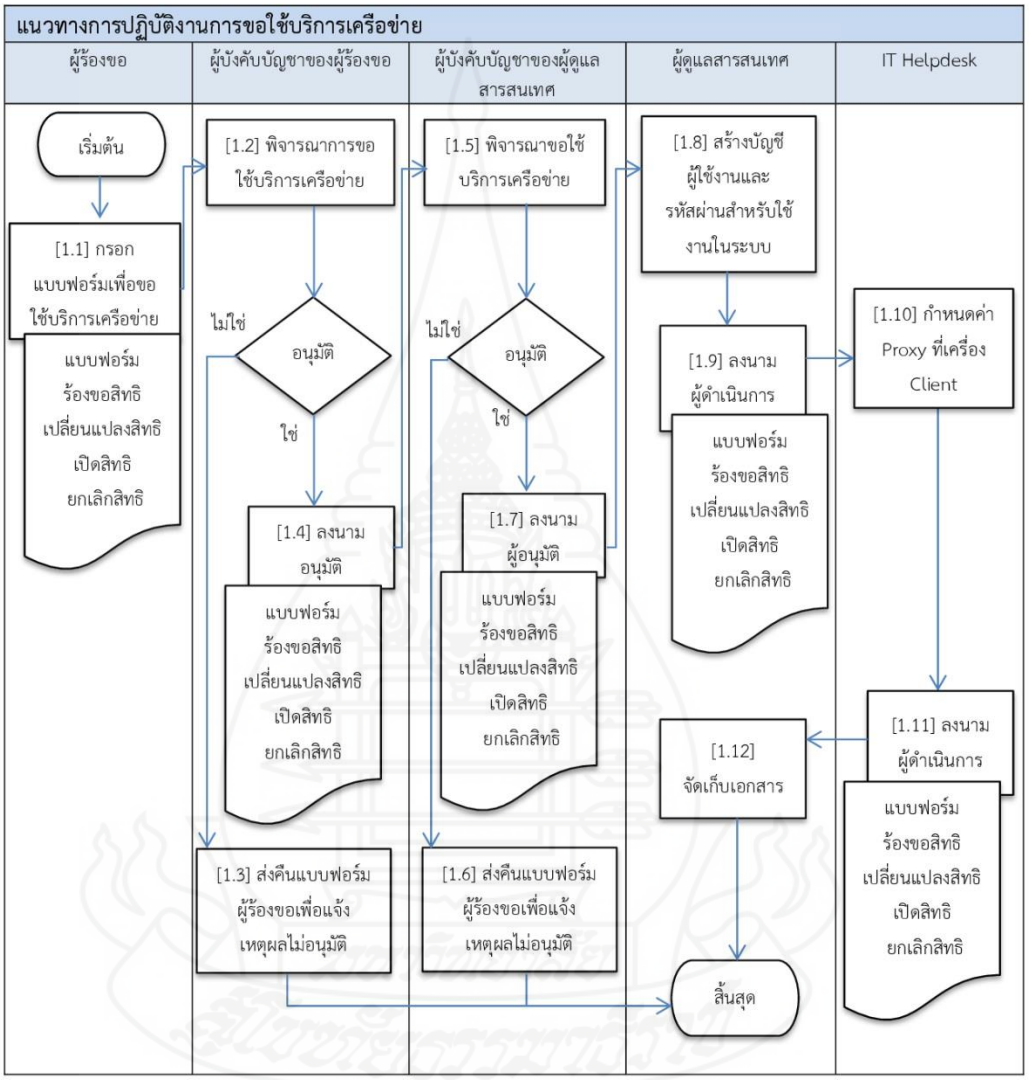
- กำหนดค่า Proxy Server ที่เครื่อง Client
- ลงนามผู้ดำเนินการ
- เปลี่ยนค่า IP Address ที่เครื่อง Client

5.รายละเอียดขั้นตอนแนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

ภาพรวมขั้นตอนแนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

รายละเอียดในส่วนนี้จะแสดงให้เห็นถึงภาพรวมของขั้นตอน แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย

5.1 การขอใช้บริการเครือข่าย

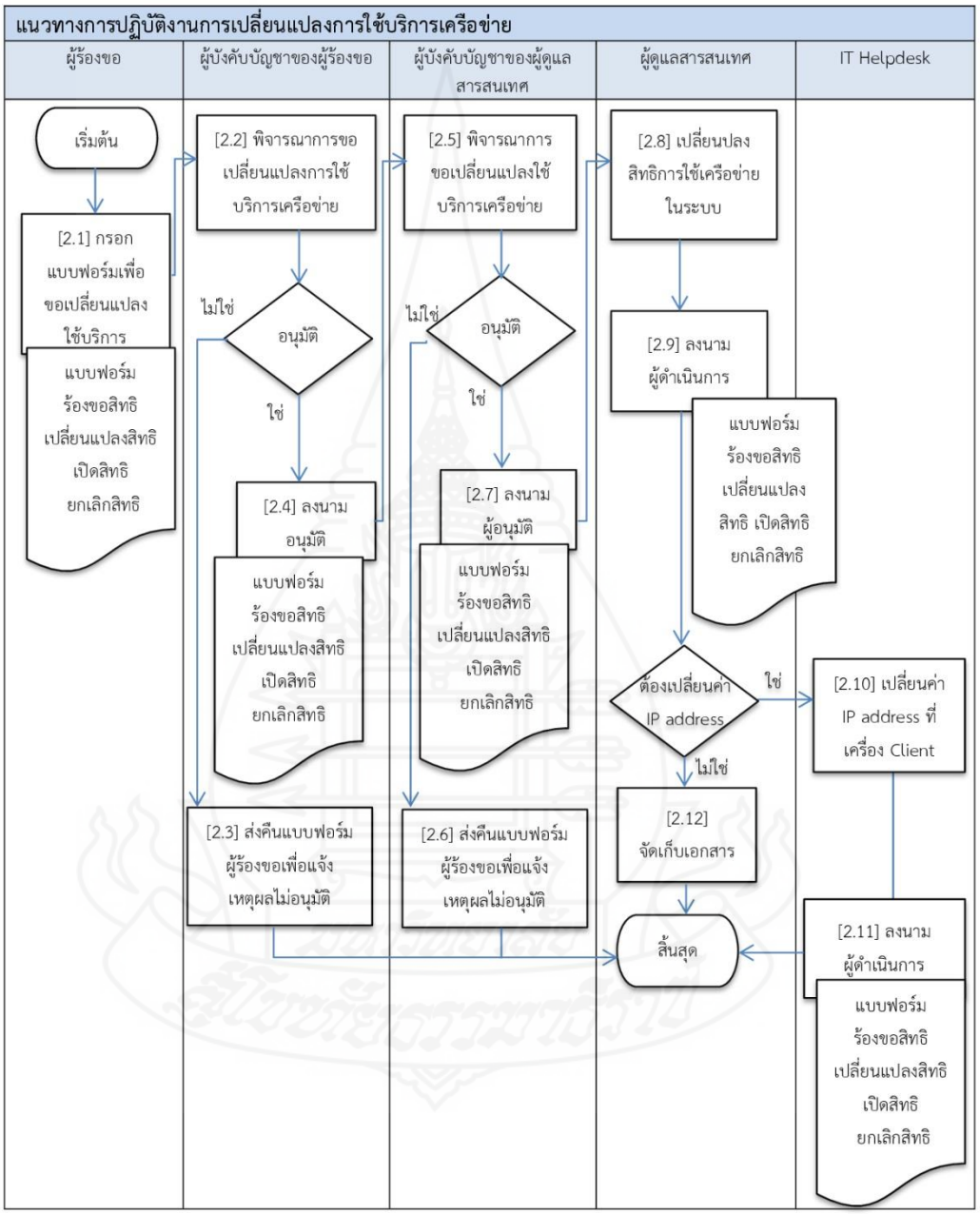


เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[1.1]	ผู้ร้องขอ	กรอกแบบฟอร์ม เพื่อขอใช้บริการ เครือข่าย	ความต้องการขอใช้ บริการ เครือข่าย	ผู้ร้องขอกรอกแบบฟอร์มเพื่อขอใช้บริการ เครือข่าย แล้วส่งให้ ผู้บังคับบัญชาของผู้ร้องขอ พิจารณา [1.2]	แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[1.2]	ผู้บังคับบัญชา ของผู้ร้องขอ	พิจารณาการขอใช้ บริการเครือข่าย	แบบฟอร์มร้องขอ สิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ	พิจารณาการขอใช้ บริการเครือข่าย - กรณีอนุมัติ ให้ลงนาม อนุมัติ [1.4] - กรณีไม่อนุมัติ ให้ส่ง แบบฟอร์มคืนผู้ร้องขอ เพื่อแจ้งเหตุผลที่ไม่ อนุมัติ[1.3]	แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิด สิทธิ ยกเลิก สิทธิ
[1.3]	ผู้บังคับบัญชา ของผู้ร้องขอ	ส่งแบบฟอร์มคืนผู้ร้อง ขอเพื่อแจ้งเหตุผลที่ไม่ อนุมัติ	แบบฟอร์มร้องขอ สิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ผู้บังคับบัญชาของผู้ร้องขอส่ง แบบฟอร์มคืนผู้ร้องขอชี้แจง เหตุผลที่ไม่อนุมัติ และสิ้นสุด ขั้นตอนการปฏิบัติงาน	แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิด สิทธิ ยกเลิก สิทธิ
[1.4]	ผู้บังคับบัญชา ของผู้ร้องขอ	ลงนามอนุมัติ	แบบฟอร์มร้องขอ สิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ลงนามอนุมัติลงในแบบฟอร์ม แล้วส่งให้ผู้บังคับบัญชาของ ผู้ดูแลสารสนเทศพิจารณา [1.5]	แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[1.5]	ผู้บังคับบัญชา ของผู้ดูแล สารสนเทศ	พิจารณาการขอใช้ บริการเครือข่าย	แบบฟอร์มร้องขอ สิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ	พิจารณาการขอใช้ บริการเครือข่าย - กรณีอนุมัติ ให้ลงนาม อนุมัติ [1.7] - กรณีไม่อนุมัติ ให้ส่ง แบบฟอร์มคืนผู้ร้องขอ เพื่อแจ้งเหตุผลที่ไม่ อนุมัติ[1.6]	แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ

เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[1.6]	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ	ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศส่งแบบฟอร์มคืนผู้ร้องขอชี้แจงเหตุผลที่ไม่อนุมัติ และสิ้นสุดขั้นตอนการปฏิบัติงาน	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[1.7]	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ	ลงนามอนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ลงนามอนุมัติลงในแบบฟอร์มแล้วส่งให้ผู้ดูแลสารสนเทศ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[1.8]	ผู้ดูแลสารสนเทศ	สร้างบัญชีผู้ใช้งานและรหัสผ่านสำหรับใช้งานเครือข่ายในระบบ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	สร้างบัญชีผู้ใช้งานและรหัสผ่านสำหรับใช้งานเครือข่ายในระบบให้แก่ผู้ร้องขอ	บัญชีผู้ใช้งานและรหัสผ่านสำหรับใช้งานเครือข่ายระบบ
[1.9]	ผู้ดูแลสารสนเทศ	ลงนามผู้ดำเนินการ	การเปิดให้บริการเครือข่าย	ผู้ดูแลสารสนเทศลงนามผู้ดำเนินการ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[1.10]	IT Helpdesk	กำหนดค่า Proxy Server ที่เครื่อง Client	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	กำหนดค่า Proxy Server ที่เครื่อง Client	การกำหนดค่า Proxy Server
[1.11]	IT Helpdesk	ลงนามผู้ดำเนินการ	การกำหนดค่า Proxy Server	IT Helpdesk ลงนามผู้ดำเนินการ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ

เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[1.12]	ผู้ดูแล สารสนเทศ	จัดเก็บเอกสาร	แบบฟอร์มร้องขอ สิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ผู้ดูแลสารสนเทศจัดเก็บ เอกสาร และสิ้นสุดขั้นตอน การปฏิบัติงาน	แฟ้ม แบบฟอร์ม ร้องขอสิทธิ เปลี่ยนแปลง สิทธิ เปิดสิทธิ ยกเลิกสิทธิ

5.2 การเปลี่ยนแปลงการใช้บริการเครือข่าย



เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[2.1]	ผู้ร้องขอ	กรอกแบบฟอร์มเพื่อขอเปลี่ยนแปลงการใช้บริการเครือข่าย	ความต้องการเปลี่ยนแปลงการใช้บริการเครือข่าย	ผู้ร้องขอกรอกแบบฟอร์มเพื่อขอเปลี่ยนแปลงการใช้บริการเครือข่าย แล้วส่งให้ผู้บังคับบัญชาของผู้ร้องขอพิจารณา [2.2]	แบบฟอร์มร้องขอสิทธิเปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ
[2.2]	ผู้บังคับบัญชาของผู้ร้องขอ	พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ	พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย - กรณีอนุมัติ ให้ลงนามอนุมัติ [2.4] - กรณีไม่อนุมัติ ให้ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ [2.3]	แบบฟอร์มร้องขอสิทธิเปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ
[2.3]	ผู้บังคับบัญชาของผู้ร้องขอ	ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ	ผู้บังคับบัญชาของผู้ร้องขอส่งแบบฟอร์มคืนผู้ร้องขอชี้แจงเหตุผลที่ไม่อนุมัติ และสิ้นสุดขั้นตอนการปฏิบัติงาน	แบบฟอร์มร้องขอสิทธิเปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ
[2.4]	ผู้บังคับบัญชาของผู้ร้องขอ	ลงนามอนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ	ลงนามอนุมัติลงในแบบฟอร์ม แล้วส่งให้ผู้บังคับบัญชาของผู้ดูแลสารสนเทศพิจารณา [2.5]	แบบฟอร์มร้องขอสิทธิเปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ
[2.5]	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ	พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ	พิจารณาการขอเปลี่ยนแปลงการใช้บริการเครือข่าย - กรณีอนุมัติ ให้ลงนามอนุมัติ [2.7] - กรณีไม่อนุมัติ ให้ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ[2.6]	แบบฟอร์มร้องขอสิทธิเปลี่ยนแปลงสิทธิ เปิดสิทธิยกเลิกสิทธิ

เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[2.6]	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ	ส่งแบบฟอร์มคืนผู้ร้องขอเพื่อแจ้งเหตุผลที่ไม่อนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศส่งแบบฟอร์มคืนผู้ร้องขอชี้แจงเหตุผลที่ไม่อนุมัติ และสิ้นสุดขั้นตอนการปฏิบัติงาน	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[2.7]	ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ	ลงนามอนุมัติ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ลงนามอนุมัติลงในแบบฟอร์ม แล้วส่งให้ผู้ดูแลสารสนเทศ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[2.8]	ผู้ดูแลสารสนเทศ	เปลี่ยนแปลงสิทธิการใช้เครือข่ายในระบบ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	เปลี่ยนแปลงสิทธิการใช้เครือข่ายในระบบให้แก่ผู้ร้องขอ	การเปลี่ยนแปลงสิทธิการใช้เครือข่าย
[2.9]	ผู้ดูแลสารสนเทศ	ลงนามผู้ดำเนินการ	การเปลี่ยนแปลงสิทธิการใช้เครือข่าย	ผู้ดูแลสารสนเทศลงนามผู้ดำเนินการ และพิจารณาว่าต้องเปลี่ยนค่า IP Address หรือไม่ กรณีต้องเปลี่ยน IP Address ให้ IT Helpdesk เปลี่ยนค่า IP Address ที่เครื่อง Client [2.10] กรณีต้องไม่เปลี่ยน IP Address ให้จัดเก็บเอกสาร [2.12]	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ
[2.10]	IT Helpdesk	เปลี่ยนค่า IP Address ที่เครื่อง Client	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	เปลี่ยนค่า IP Address ที่เครื่อง Client	การเปลี่ยนค่า IP Address
[2.11]	IT Helpdesk	ลงนามผู้ดำเนินการ	การเปลี่ยนค่า IP Address	IT Helpdesk ลงนามผู้ดำเนินการ	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ

เลขที่	ผู้ดำเนินการ	คำอธิบายการทำงาน	สิ่งที่นำเข้า	รายละเอียด	ผลลัพธ์
[2.12]	ผู้ดูแลสารสนเทศ	จัดเก็บเอกสาร	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ	ผู้ดูแลสารสนเทศจัดเก็บเอกสาร และสิ้นสุดขั้นตอนการปฏิบัติงาน	แฟ้มแบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ ยกเลิกสิทธิ

6. เอกสารที่เกี่ยวข้อง

รหัสอ้างอิง	ชื่อเอกสาร
KYH-IM-AC-02-03	แบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ และยกเลิกสิทธิ

ชื่อเอกสาร	เลขที่เอกสาร	ปรับปรุงครั้งที่	วันที่ออกเอกสาร
แนวทางการปฏิบัติงานการขอใช้บริการเครือข่าย	KYH-IM-AC-01-04	จัดทำครั้งแรก	10 ตุลาคม 2560

ผู้จัดทำเอกสาร	ผู้เห็นชอบเอกสาร	ผู้อนุมัติ
..... (.....) ตำแหน่ง.....	คณะกรรมการสารสนเทศ	..... (.....) ตำแหน่ง.....

ภาคผนวก ค

ตัวอย่างแบบฟอร์มที่เกี่ยวข้องด้านการควบคุมการเข้าถึงระบบสารสนเทศ

ตัวอย่างแบบฟอร์มร้องขอสิทธิ เปลี่ยนแปลงสิทธิ เปิดสิทธิ และยกเลิกสิทธิ
สำหรับการใช้งานบริการเครือข่าย โรงพยาบาลคลองใหญ่

เลขที่: .....
วันที่: .....

ส่วนที่ ๑ ผู้ร้องขอ			
รายละเอียดผู้ร้องขอ	หมายเลขบัตรประชาชน ..... คำนำหน้าชื่อ (Title Name) : ☐ นาย /Mr. ☐ นาง / Mrs. ☐ น.ส. /Ms. ☐ อื่นๆ/ Other..... ชื่อ/นามสกุล ภาษาไทย (Thai Name):..... ชื่อ/นามสกุล ภาษาอังกฤษ (Eng. Name):..... ตำแหน่ง: ..... ระดับ: ..... ฝ่าย/สาขา..... ส่วน: ..... หมายเลขติดต่อ: ..... อีเมล์:		
วัตถุประสงค์	☐ เพิ่มรหัสผู้ใช้ ☐ เพิ่มสิทธิผู้ใช้ ☐ ลดสิทธิผู้ใช้ ☐ ขอเปิดสิทธิ ☐ ขอยกเลิกสิทธิ ☐ ลบรหัสผู้ใช้		
ประเภท	☐ E-mail Account ☐ Intranet ☐ Wireless ☐ Internet	รายละเอียด	
ระยะเวลา	ตั้งแต่วันที่ ..... ถึง ..... ตั้งแต่ช่วงเวลา ..... ถึง		
ส่วนที่ ๒ ผู้บังคับบัญชาของผู้ร้องขอ			
ผู้มีอำนาจอนุมัติ	☐ อนุมัติ ☐ ไม่อนุมัติ	ลงนาม .....วันที่ ...../...../.....	
ความเห็น:			
ส่วนที่ ๓ ผู้บังคับบัญชาของผู้ดูแลสารสนเทศ			
ผู้มีอำนาจอนุมัติ	☐ อนุมัติ ☐ ไม่อนุมัติ	ลงนาม .....วันที่ ...../...../.....	
ความเห็น:			

ส่วนที่ ๔ ผู้ดูแลสารสนเทศ	
ผลการดำเนินงาน	E-mail Account + Password Slip ..... Network ID + Password Slip ..... Wireless: Physical Address ..... IP Address ..... หมาย ..... เหตุ .... ลงนาม ..... วันที่ ...../...../.....
ส่วนที่ ๕ IT Helpdesk	
ผลการดำเนินงาน	☐ เสร็จสมบูรณ์ ☐ ยังไม่แล้วเสร็จ หมาย ..... เหตุ .... ลงนาม ..... วันที่ ...../...../.....

ภาคผนวก ง

ตัวอย่างโนยาย แนวทางการปฏิบัติงานและแบบฟอร์มที่เกี่ยวข้อง
ด้านการควบคุมการเข้าถึงระบบสารสนเทศ

สามารถดูตัวอย่างนโยบาย แนวทางปฏิบัติงานและแบบฟอร์มที่เกี่ยวข้องในด้านอื่นๆ ได้ที่ https://goo.gl/1VyjeL หรือที่คิวอาร์โค้ด

ภาพที่ 4.20 คิวอาร์โค้ดเพื่อเข้าถึงตัวอย่างนโยบาย
แนวทางการปฏิบัติงานและแบบฟอร์มที่เกี่ยวข้อง

ประวัติผู้ศึกษา

ชื่อ-สกุล	นายรุ่งอรุณ นิรันต์เรือง
วัน เดือน ปีเกิด	19 ตุลาคม 2522
สถานที่เกิด	อำเภอคลองใหญ่ จังหวัดตราด
ประวัติการศึกษา	พย.บ. วิทยาลัยพยาบาลพระปกเกล้าจันทบุรี พ.ศ.2545
	นศ.บ. มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ.2550
สถานที่ทำงาน	โรงพยาบาลคลองใหญ่ อำเภอคลองใหญ่ จังหวัดตราด
ตำแหน่ง	พยาบาลวิชาชีพชำนาญการ กลุ่มการพยาบาล