การพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 กรณีศึกษา เนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

นายพลภัทร สุนทรทิวากร

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2560

Development of Risk Assessment and Information Technology Access Control Security System Based on ISO/IEC 27001: 2013, A Case Study of the Thai Bar under the Royal Patronage

Mr. Phonlaphat Suntorntiwakrom

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 การพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013 กรณีศึกษาเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

ชื่อและนามสกุล นายพลภัทร สุนทรทิวากร

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 3 สิงหาคม 2561

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

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

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

.....
(รองศาสตราจารย์ผกามาศ ผจญแกล้ว)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ชื่อการศึกษาค้นคว้าอิสระ การพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013 กรณีศึกษาเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์

ผู้ศึกษา นายพลภัทร สุนทรทิวากร **รหัสนักศึกษา** 2559600107 **ปริญญา** วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร) **อาจารย์ที่ปรึกษา** รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์

ปีการศึกษา 2560

บทคัดย่อ

การศึกษาที่นำเสนอ มีวัตถุประสงค์ (1) เพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ ตามหลัก CIA Triad และ (2) เพื่อพัฒนาเว็บแอปพลิเคชันระบบการควบคุมความมั่นคงปลอดภัย ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013 ของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

วิธีดำเนินการมีดังนี้ (1) ศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013 (2) ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ตามหลัก CIA Triad โดย (2.1) ประเมินมูลค่าสินทรัพย์ (2.2) ประเมินความความเสี่ยงของสินทรัพย์ และ (3) พัฒนาเว็บแอปพลิเคชันระบบควบคุมความมั่นคงปลอดภัยด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 เครื่องมือในการวิจัย ได้แก่ (1) รายการบัญชีด้านความมั่นคงปลอดภัยอ้างอิงตามความเสี่ยงในแต่ละองค์ประกอบด้วยมาตรฐาน ISO 27001 (2) ตัวชี้วัดประสิทธิภาพ (KPI) ที่พัฒนาขึ้นเพื่อแสดงระดับความเสี่ยงโดยนำเสนอในรูปแบบของสีเขียว สีเหลือง และสีแดง ตามลำดับความเสี่ยงจากน้อยไปมาก (3) PHP เป็นภาษาโปรแกรมสำหรับการพัฒนาแอปพลิเคชัน และ (4) MySQL ใช้เป็นฐานข้อมูล

ผลการดำเนินงานพบว่า (1) สถานะความเสี่ยงของเนติบัณฑิตยสภาฯ อยู่ในระดับต่ำถึงปานกลาง และ (2) ระบบการควบคุมความมั่นคงปลอดภัยด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ที่พัฒนาขึ้น ทดสอบการใช้งานพบว่า เนติบัณฑิตยสภาฯ มีการควบคุมความมั่นคงปลอดภัย ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ ในภาพรวมอยู่ในระดับดี

คำสำคัญ ประเมินความเสี่ยง การควบคุมความมั่นคงปลอดภัย ISO/IEC 27001:2013

Independent Study title: Development of Risk Assessment and Information Technology Access Control Security System Based on ISO/IEC 27001:2013, A Case Study of the Thai Bar under the Royal Patronage
Author: Mr. Phonlaphat Suntorntiwakron; **ID:** 2559600107;
Degree: Master of Science (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 assess the information technology risk under the CIA Triad of the Thai Bar under the Royal Patronage; and (2) to develop the web application for access control security system based on ISO/IEC 27001: 2013.

The research methodology were as follows: (1) The study of the information technology security for ISO / IEC 27001:2013; (2) The assessment of the information technology risk under the CIA Triad by (2.1) assessing the assets value and (2.2) assessing risk of assets; (3) The development of a web application for access control security system based on ISO/IEC 27001:2013; Research tools were (1) a checklist of risk-based security in each component using ISO 27001; (2) the KPI to indicate level of risk in each component in green, yellow and red to represent the risk level as low, medium and high respectively; (3) PHP as a programming language for the development application; and (4) MySQL used for database.

The research results showed that (1) risk status of the Thai Bar under the Royal Patronage was between low and medium level; (2) the developed system based on ISO/IEC 27001:2013 was field trialed at the Thai Bar under the Royal Patronage. resulting the of overall security system of information technology was in good level.

Keywords: Risk assessment, Access control security system, ISO/IEC 27001: 2013

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระนี้ได้พัฒนาจนสำเร็จได้ด้วยดีและสมบูรณ์ได้รับความเมตตากรุณาอย่างยิ่งจากรองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์ อาจารย์ที่ปรึกษา สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช ที่ได้กรุณาให้คำแนะนำและติดตามการศึกษาค้นคว้าอิสระในครั้งนี้อย่างใกล้ชิดตลอดมา นับตั้งแต่เริ่มต้นจนกระทั่งสำเร็จเรียบร้อยสมบูรณ์ ผู้ศึกษาซาบซึ้งในความกรุณาของท่านเป็นอย่างยิ่ง ขอบพระคุณอาจารย์ ดร.ดวงดาว วิชาดากุล คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่กรุณาให้คำชี้แนะแนวทางในการปรับปรุงเนื้อหาการศึกษาค้นคว้าอิสระให้มีความสมบูรณ์ยิ่งขึ้น

ขอบพระคุณสาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช บิดา มารดา นางสาวอรปภา ธารณปริตรชัย เพื่อนนักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้เกี่ยวข้องในการศึกษาค้นคว้าอิสระครั้งนี้ทุกท่านที่ได้กรุณาให้การสนับสนุน ช่วยเหลือและให้กำลังใจตลอดมา

พลภัทร สุนทรทิวากร

สิงหาคม 2561

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญภาพ

บทที่ 1
บทนำ

1. ความสำคัญและความเป็นมา

ในปัจจุบัน องค์กรภาครัฐและภาคเอกชน มีการนำเทคโนโลยีสารสนเทศมาใช้เพื่อสนับสนุนกิจกรรมต่างๆ ขององค์กรมากขึ้น เพื่อใช้อำนวยความสะดวกในการปฏิบัติงานของพนักงานในองค์กร เมื่อมีการใช้ระบบเทคโนโลยีสารสนเทศแพร่หลายมากขึ้น ความเสี่ยงในการใช้งาน ซึ่งเกิดจากพนักงานขององค์กรที่ยังขาดความรู้ ความเข้าใจในระบบเทคโนโลยีสารสนเทศ หรือเกิดจากจำนวนผู้ไม่ประสงค์ดีต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น อาจส่งผลกระทบต่อการดำเนินงานและภาพลักษณ์ขององค์กร องค์กรจึงควรนำมาตรฐานการจัดการความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศมาประยุกต์ใช้ให้สอดคล้องกับการปฏิบัติงานขององค์กร เพื่อสร้างความตระหนักให้กับพนักงานในองค์กร และเป็นการบริหารจัดการความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายกับการดำเนินงานขององค์กรได้

เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ เป็นองค์กรหลักในการส่งเสริมความรู้และกำกับดูแลการประกอบอาชีพของนักกฎหมายให้มีคุณภาพกอปรด้วยจริยธรรมและเกียรติศักดิ์ตามมาตรฐานสากล มุ่งเสริมสร้างความสมานฉันท์ในหมู่นักกฎหมายและความเชื่อถือศรัทธาของประชาชนที่มีต่อวิชาชีพกฎหมายให้มั่นคงยิ่งขึ้น ทั้งจะเน้นบทบาทการให้ความช่วยเหลือทางกฎหมายแก่ประชาชน ให้เป็นที่เห็นอย่างเด่นชัด ได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในองค์กร เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน ทั้งระบบเทคโนโลยีสารสนเทศสำหรับพนักงานภายในองค์กร และระบบเทคโนโลยีสารสนเทศสำหรับให้บริการบุคคลภายนอก

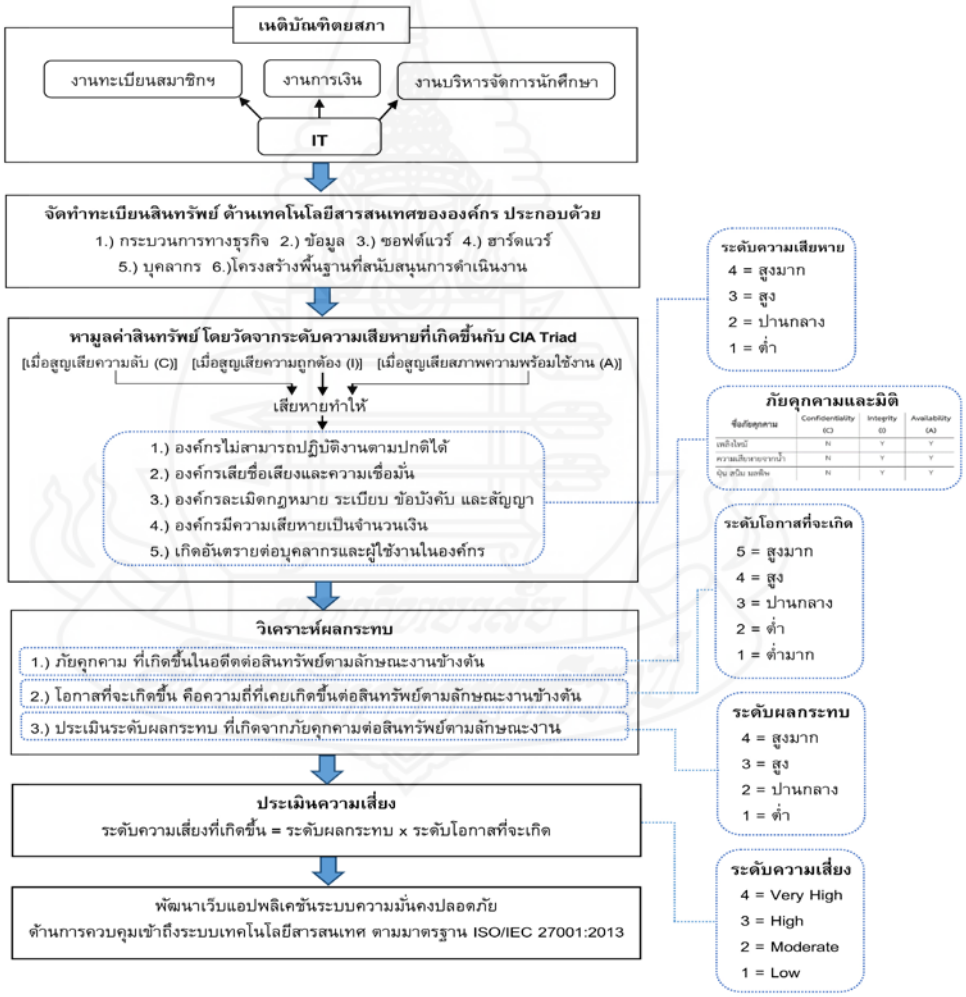
ปัจจุบันเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ มีมาตรการจัดการความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Access Control) ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2005 แต่เนื่องจากมาตรฐาน ISO/IEC 27001:2005 มีการปรับปรุงใหม่ คือ มาตรฐาน ISO/IEC 27001:2013 จึงจำเป็นต้องมีการประเมินความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศในปัจจุบันมีความสอดคล้องกับมาตรฐาน ISO/IEC 27001: 2013

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ ตามหลัก CIA Triad

2.2 เพื่อพัฒนาเว็บแอปพลิเคชัน ระบบการควบคุมความมั่นคงปลอดภัย ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

3. กรอบแนวคิดการวิจัย



ภาพที่ 1.1 กรอบแนวคิดการวิจัย

4. ขอบเขตการวิจัย

4.1 หลักการ CIA Triad ประกอบด้วย

4.1.1 Confidentiality การรักษาความลับ หมายถึง การรักษาหรือสงวนไว้ เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์จากการเข้าถึงใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

4.1.2 Integrity การรักษาความถูกต้องครบถ้วน หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ถูกต้อง ขณะที่มีการใช้งานประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหายหรือถูกทำลายโดยไม่ได้รับอนุญาต หรือโดยมิชอบ

4.1.3 Availability การรักษาสภาพพร้อมใช้งาน หมายถึง การจัดทำให้สินทรัพย์สารสนเทศสามารถทำงานเข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

4.2 กลุ่มตัวอย่างของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์ ที่ใช้ในการประเมินและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามหลัก CIA Triad โดยครอบคลุมลักษณะงาน ดังนี้

4.2.1 งานทะเบียนสมาชิกและทนายความ (กองกลาง)

4.2.2 งานการเงิน (กองคลัง)

4.2.3 งานบริหารจัดการนักศึกษา (กองบริการ)

4.3 รายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ เพื่อใช้การประเมินความเสี่ยงและการรักษาความมั่นคงปลอดภัย แบ่งออกเป็น 6 ด้าน (อ้างอิงจาก ISO/IEC27005: 2008 Annex B) คือ

4.3.1 กระบวนการทางธุรกิจ (Business processes Assets)

4.3.2 ข้อมูล (Information Assets)

4.3.3 ซอฟต์แวร์ (Software Assets)

4.3.4 ฮาร์ดแวร์ (Hardware Assets)

4.3.5 บุคลากร (People Assets) และ

4.3.6 โครงสร้างพื้นฐานที่สนับสนุนการดำเนินงาน (Infrastructure Assets)

5. วิธีการดำเนินการวิจัย

5.1 ศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2013 ผู้วิจัยจะทำการวิจัย การควบคุม (Control) ตามมาตรฐาน ISO/IEC 27001: 2013 ว่ามีการปรับเปลี่ยนการควบคุม (Control) จากเดิมอย่างไร พร้อมสรุปการควบคุม (Control) ได้มีการปรับเพิ่มขึ้นใหม่ (New Control) โดยมีรายละเอียดที่สำคัญที่จะศึกษา คือ

5.1.1 เอกสารมาตรฐานการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2013

5.1.2 เอกสารมาตรฐานการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2005

5.1.3 งานวิจัยที่เกี่ยวข้อง

5.2 ศึกษาความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบัน ผู้วิจัยทำความเข้าใจ ความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบัน โดยมีรายละเอียดที่สำคัญที่จะศึกษา คือ

5.2.1 ความสอดคล้องของความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรกับมาตรฐาน ISO/IEC 27001: 2005 และ

5.2.2 ความสอดคล้องกับกฎหมายอื่นที่เกี่ยวข้อง

5.3 ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรตามหลัก CIA Triad ประกอบไปด้วย มูลค่าของสินทรัพย์ ภัยคุกคาม ผลกระทบ โอกาสที่จะเกิดความเสี่ยง และระดับความเสี่ยง (อ้างอิงจาก ISO 31000:2009) ผู้วิจัยจะทำการประเมินและวิเคราะห์ความเสี่ยง โดยมีขั้นตอนการดำเนินงาน ดังนี้

5.3.1 ทำทะเบียนสินทรัพย์และกำหนดมูลค่าของสินทรัพย์ (Asset Identification and Valuation)

5.3.2 กำหนดภัยคุกคามต่อสินทรัพย์ (Threat Identification) (อ้างอิงรายการภัยคุกคามของ Supplement to BSI Standard 100-3, Version 2.5)

5.3.3 วิเคราะห์ผลกระทบ (Impact Analysis)

5.3.4 ระดับโอกาสที่จะเกิดขึ้น (Likelihood)

5.3.5 ประเมินระดับความเสี่ยง (Risk assessment)

5.4 พัฒนา Web Application ระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 ประกอบด้วย

5.4.1 ระบบบริหารจัดการผู้เข้าใช้งานระบบ

5.4.2 ระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 โดยจัดทำเป็นรายการเช็คลิสต์ (check list) เพื่อตรวจสอบและประเมินความพร้อมในการจัดการด้านความมั่นคงปลอดภัย และ KPI เพื่อแสดงระดับความเสี่ยง เป็นของสีเขียว เหลือง แดง ซึ่งสีเขียว หมายถึง ความเสี่ยงต่ำ เหลือง หมายถึง ความเสี่ยงปานกลาง และแดง หมายถึง ความเสี่ยงสูง

5.4.3 ระบบการออกรายงาน

6. ประโยชน์ที่คาดว่าจะได้รับ

6.1 ได้ระบบประเมินความเสี่ยง ด้านเทคโนโลยีสารสนเทศตามหลัก CIA Triad ของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

6.2 ได้เว็บแอปพลิเคชันระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013 ของเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

7. นิยามศัพท์

สินทรัพย์ (Asset) หมายถึง สิ่งใดก็ตามที่มีคุณค่าต่อองค์กร ทั้งที่จับต้องได้หรือจับต้องไม่ได้ ซึ่งหมายรวมถึงสินทรัพย์ในรูปแบบของข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์สารสนเทศ สำหรับการดำเนินงานขององค์กร ในการวิจัยนี้ สินทรัพย์ คือ (1) กระบวนการทางธุรกิจ (Business processes Assets) (2) ข้อมูล (Information Assets) (3) ซอฟต์แวร์ (Software Assets) (4) ฮาร์ดแวร์ (Hardware Assets) (5) บุคลากร (People Assets) และ (6) โครงสร้างพื้นฐานที่สนับสนุนการดำเนินงาน (Infrastructure Assets)

มูลค่าของสินทรัพย์ (Asset Value) หมายถึง ระดับความเสียหาย เมื่อสินทรัพย์ได้รับผลกระทบด้าน CIA Triad

ภัยคุกคาม (Threat) หมายถึง ภาวะที่อาจเกิดต่อสินทรัพย์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ไม่ว่าจะเป็นด้านความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์

ครบถ้วนของข้อมูล (Integrity) หรือความพร้อมให้ใช้งานของข้อมูล (Availability) หรือเรียกโดยรวมว่าผลกระทบต่อ CIA Triad

ความเสี่ยง หมายถึง ความเป็นไปได้ (Probability) ที่ภัยคุกคาม (Threat) เข้ากระทำความเสียหาย และก่อให้เกิดผลกระทบ (Impact) ต่อสินทรัพย์

ผลกระทบ (Impact) หมายถึง ความเสียหายที่เกิดขึ้นจากภัยคุกคามเป็นการพิจารณาระดับความเสียหายที่เกิดขึ้น

โอกาสที่จะเกิดขึ้น (Likelihood) หมายถึง โอกาสที่จะเกิดขึ้นที่ภัยคุกคามอาจกระทำความเสียหายต่อสินทรัพย์ได้สำเร็จ พิจารณาจากแนวโน้มการเกิดขึ้นของภัยคุกคาม ซึ่งเกิดจากแรงจูงใจและสถิติที่เคยเกิดขึ้น มีการบันทึกไว้หรือจากประสบการณ์ของเจ้าของสินทรัพย์

การควบคุม (Control) หมายถึง มาตรการควบคุมต่างๆ ที่ถูกใช้เพื่อป้องกัน และ/หรือลดความเสี่ยงต่อสินทรัพย์

บทที่ 2
ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ เป็นองค์กรหลักในการส่งเสริมความรู้และกำกับดูแล การประกอบอาชีพของนักกฎหมายให้มีคุณภาพกอปรด้วยจริยธรรมและเกียรติศักดิ์ตามมาตรฐานสากล มุ่งเสริมสร้างความสมานฉันท์ในหมู่นักกฎหมาย และความเชื่อถือศรัทธาของประชาชนที่มีต่อวิชาชีพกฎหมายให้มั่นคงยิ่งขึ้น ทั้งจะเน้นบทบาทการให้ความช่วยเหลือทางกฎหมายแก่ประชาชนให้เป็นที่เห็นอย่างเด่นชัด

ด้วยคุณลักษณะดังกล่าว เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ จึงมีการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรเพื่อเพิ่มประสิทธิภาพในการทำงานมากขึ้น ทั้งระบบเทคโนโลยีสารสนเทศสำหรับพนักงานภายในและระบบเทคโนโลยีสารสนเทศ สำหรับให้บริการบุคคลภายนอก รวมถึงระบบเครือข่าย ดังนั้น เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ จึงได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัย โดยเฉพาะด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Access Control) ซึ่งยึดหลักการของมาตรฐานการรักษาความมั่นคง ปลอดภัย ตามมาตรฐานสากลอย่างมาตรฐาน ISO/IEC 27001: 2005 และหลักการของกฎหมายอื่นที่เกี่ยวข้อง

ในประเทศไทย มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ที่กำหนดขึ้นตามกฎหมาย (พระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551) โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ ในการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ โดยยึดแนวทางของมาตรฐาน ISO/IEC 27001 จึงพัฒนาเป็นมาตรฐาน “การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555” ทางด้านกฎหมายได้มีการนำมาตรฐานมาประยุกต์ใช้ ดังนี้

1) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

2) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

3) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

ซึ่งมีการอ้างถึง หลักการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยบังคับใช้กับโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศที่สำคัญของประเทศ (Critical Infrastructure) ซึ่งเป็นการสร้างความมั่นคงปลอดภัยในภาพรวมกับการใช้งานเทคโนโลยีสารสนเทศของประเทศไทย

1. ทฤษฎีที่เกี่ยวข้อง

ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 มาตรา 3 (3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 ซึ่งมีองค์ประกอบการครอบคลุม 3 ด้าน (CIA Triad) ดังนี้

1.1 “การรักษาความลับ” (Confidentiality) หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์จากการเข้าถึงใช้หรือเปิดเผย โดยบุคคลซึ่งไม่ได้รับอนุญาต

1.2 “การรักษาความถูกต้องครบถ้วน” (Integrity) หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพถูกต้องสมบูรณ์ ขณะที่มีการใช้งานประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไขทำให้สูญหายทำให้เสียหายหรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

1.3 “การรักษาสภาพพร้อมในการใช้งาน” (Availability) หมายถึง การจัดทำให้สินทรัพย์สารสนเทศสามารถทำงานเข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ หรือที่เรียกกันว่า CIA Triad ซึ่งมีความสัมพันธ์ปรากฏดังภาพ

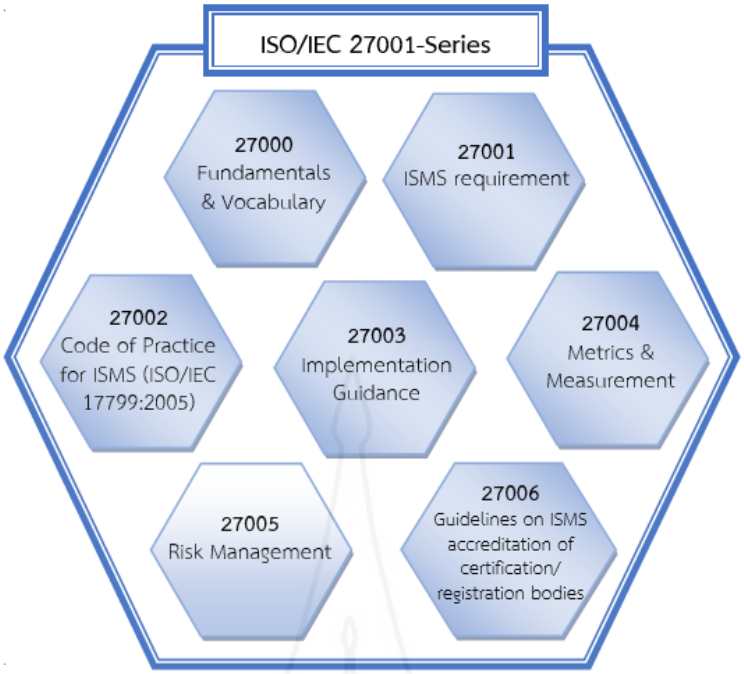
ภาพที่ 2.1 CIA Triad

2. มาตรฐาน ISO/IEC 27001

2.1 ISO ย่อมาจาก “The International Organization for Standardization” เป็นองค์กรระหว่างประเทศว่าด้วยการมาตรฐาน” ISO ก่อตั้งเมื่อปี พ.ศ.2489 (ค.ศ. 1946) สำนักงานอยู่ที่กรุงเจนิวา (Geneva) ประเทศสวิตเซอร์แลนด์ (Switzerland) เป็นองค์กรกำหนดมาตรฐานทางด้านวิทยาศาสตร์และเทคโนโลยี

2.2 IEC ย่อมาจาก “The International Electro technical Commission” เป็นองค์กรระหว่างประเทศที่ร่างมาตรฐานทางด้านไฟฟ้า อิเล็กทรอนิกส์ และเทคโนโลยี นอกจากนั้นยังดำเนินการจัดทำระบบการตรวจประเมิน โดยเน้นหนักไปในด้านมาตรฐานการจัดการข้อมูล IEC ก่อตั้งขึ้นเมื่อปี พ.ศ. 2449 (ค.ศ. 1906) และร่วมมือกับ ISO อย่างใกล้ชิด โดยมีประเทศสมาชิกเกือบทุกประเทศในโลก

2.3 มาตรฐาน ISO/IEC 27001-series หรือ ISMS Family of Standards หมายถึง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Management System (ISMS)) จัดทำขึ้นด้วยความร่วมมือขององค์กรระหว่างประเทศ ว่าด้วยการมาตรฐาน (ISO). และองค์กรระหว่างประเทศ ที่ร่างมาตรฐานทางด้านไฟฟ้า อิเล็กทรอนิกส์ และเทคโนโลยี (IEC) ซึ่งประกอบไปด้วยมาตรฐานต่างๆ ดังภาพด้านล่างนี้



ภาพที่ 2.2 เอกสารมาตรฐาน ISO/IEC 27001-Series อ้างอิง https://www.iso.org/isoiec-27001-information-security.html

2.4 ISO/IEC 27001: 2005 (Information Security Management Systems: ISMS) หมายถึง มาตรฐานที่นำมาปรับใช้ในการรักษาความมั่นคงปลอดภัยของระบบด้านเทคโนโลยีสารสนเทศ เพื่อช่วยให้องค์กรมีการจัดการความเสี่ยง ลดความรุนแรงและป้องกันไม่ให้เกิดความเสียหายต่อสินทรัพย์ขององค์กร

2.5 ISO/IEC 27002: 2005 (Code of practice for information security management) หมายถึง มาตรฐานที่นำมาประยุกต์ใช้ เพื่อเป็นแนวทางปฏิบัติที่ดีด้านเทคโนโลยีสารสนเทศ โดยอธิบายวัตถุประสงค์และวิธีการไว้อย่างละเอียด

2.6 ISO/IEC 2710001 ได้พัฒนาและปรับปรุง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้ก้าวทันเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง โดยปัจจุบันได้ออก ISO/IEC 27001: 2013 (Information Security Management Systems: ISMS) และ ISO/IEC 27002: 2013 (Code of practice for information security controls)

3. ISO/IEC27001: 2013

เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ISMS) เป็นมาตรฐานการจัดการข้อมูลที่สำคัญ เพื่อให้องค์กรสามารถดำเนินภารกิจไปอย่างต่อเนื่อง เป็นมาตรฐานที่องค์การระหว่างประเทศ คือ ISO และ IEC มาตรฐานนี้ เป็นมาตรฐานสากลและใช้กับองค์กรอย่างแพร่หลาย มุ่งเน้นในด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร โดยมีหมวดหลักทั้งหมด 10 หมวด (Clause) ซึ่งหมวดที่ 0-3 เป็นคำนิยามสำหรับการเริ่มต้นเรื่องความปลอดภัย หมวดหลักที่สำคัญของ ISO/IEC 27001:2013 อยู่ในหมวดที่ 4-10 ประกอบด้วย 4. Context of the organization, 5. Leadership, 6. Planning, 7. Support, 8. Operation, 9 . Performance evaluation และ 10.Improvement ซึ่งเนื้อหาครอบคลุม Annex A แบ่งเนื้อหาออกเป็น 14 หัวข้อหลัก (Domain) (A.5 ถึง A.18) ซึ่งแต่ละหัวข้อหลัก มีวัตถุประสงค์ที่แตกต่างกันไปรวม 35 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อ ประกอบด้วย มาตรการควบคุมความมั่นคงปลอดภัยแตกต่างกัน รวมแล้ว 114 ข้อย่อย (Control 114 items)

มาตรฐาน ISO/IEC 27001: 2013 เป็นที่นิยมและยอมรับกันอย่างแพร่หลาย เนื่องจากมีวงจรควบคุมคุณภาพ (PDCA Cycle) Plan-Do-Check-Act และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาแนวทาง กระบวนการ วิธีการ หรือมาตรการป้องกันต่างๆ ลดความเสี่ยงและรักษาสินทรัพย์ด้านเทคโนโลยีสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม

4. วงจรควบคุมคุณภาพ (PDCA Cycle)

4.1 การวางแผน (Plan) หมายถึง การวางแผนดำเนินการตามกระบวนการและขั้นตอนที่เกี่ยวข้องในระบบการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อบริหารความเสี่ยงและลดความเสี่ยง ให้สอดคล้องกับนโยบายและเป้าหมายขององค์กรโดยรวม

4.2 การปฏิบัติ (Do) หมายถึง นโยบายหรือมาตรการควบคุมการดำเนินการและการดำเนินงานในการจัดการความเสี่ยงที่ได้จากขั้นตอนแรก

4.3 การตรวจสอบ (Check) หมายถึง การตรวจสอบและประเมินความเสี่ยงเป็นประจำตามระยะเวลาที่เหมาะสม และทบทวนประสิทธิภาพของนโยบายหรือมาตรการควบคุมความมั่นคงปลอดภัยให้สอดคล้องกับการเปลี่ยนแปลงที่สำคัญของเทคโนโลยีสารสนเทศหรือการเปลี่ยนแปลงขององค์กร

4.4 การปรับปรุงแก้ไข (Act) หมายถึง มาตรการแก้ไขและป้องกันความเสี่ยงที่จะเกิดขึ้นได้อย่างเหมาะสม เพื่อปรับปรุงระบบการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

4.5 กระบวนการ (Process) หมวดหลักตามมาตรฐาน ISO/IEC27001: 2005 และกระบวนการ (Process) หมวดหลักตามมาตรฐาน ISO/IEC27001: 2013 ผ่าน PDCA Cycle ผลลัพธ์ของกระบวนการจะได้เหมือนกัน ปรากฏดังตาราง

ตารางที่ 2.1 หมวดหลักตามมาตรฐาน ISO/IEC27001: 2005 และ ISO/IEC27001: 2013 ผ่าน PDCA Cycle

ISO/IEC	**วงจรควบคุมคุณภาพ (PDCA Cycle)**			
	Plan	**Do**	**Check**	**Act**
ISO/IEC27001: 2005	Establish the ISMS	Implement and operate the ISMS	Monitor and review the ISMS	Maintain and improve the ISMS
ISO/IEC27001:2013	***Context of the organization*** ***Leadership*** ***Planning*** ***Support***	***Operation***	***Performance evaluation***	***Improvement***

5. หมวดหลักที่สำคัญของ ISO/IEC 27001:2013

5.1 ภูมิหลังขององค์กร/Context of the organization

5.1.1 เข้าใจองค์กรและภูมิหลังขององค์กร

องค์กรควรกำหนดประเด็น เกี่ยวกับปัญหาภายนอกและภายในองค์กรที่เกี่ยวข้องกับเป้าหมายขององค์กรที่ส่งผลต่อผลลัพธ์ที่ต้องการของ ISMS

หมายเหตุ: การกำหนดประเด็นดังกล่าว หมายถึงการกำหนดภูมิหลังภายนอกและภายใน ที่มีการพิจารณาในข้อ 2.3 ของมาตรฐาน ISO 31000: 2009

5.1.2 เข้าใจความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง

องค์กรต้องกำหนด:

1) กลุ่มผู้ที่เกี่ยวข้องกับ ISMS และ

2) ความต้องการของกลุ่มผู้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

หมายเหตุ: ความต้องการของกลุ่มผู้เกี่ยวข้อง อาจรวมถึงข้อกำหนดกฎหมายและข้อผูกพันตามสัญญาจ้าง

5.1.3 ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

องค์กรควรกำหนดขอบเขตและการประยุกต์ ISMS เพื่อกำหนดขอบเขตการดำเนินการ เมื่อองค์กรกำหนดขอบเขต ควรต้องพิจารณา:

1) ประเด็นภายนอกและภายในที่กล่าวถึงในข้อ 5.1.1

2) ข้อกำหนดที่กล่าวถึงในข้อ 5.1.2 และ

3) การเชื่อมโยงและการสัมพันธ์กันของกิจกรรมต่างๆ ที่ดำเนินการโดยองค์กร และองค์กรอื่นๆ

ขอบเขตการเข้าถึง ต้องทำเอกสารเป็นลายลักษณ์อักษร

5.1.4 ระบบการจัดการความมั่นคงด้านเทคโนโลยีสารสนเทศ

องค์กรต้องกำหนด ลงมือปฏิบัติ และปรับปรุง ISMS อย่างต่อเนื่องตามข้อกำหนดของมาตรฐานนี้

5.2 ความเป็นผู้นำ/Leadership

5.2.1 ความเป็นผู้นำและความมุ่งมั่น

ผู้บริหารควรแสดงให้เห็นถึงความเป็นผู้นำและความมุ่งมั่นต่อ ISMS โดย:

1) ต้องทำให้เกิดความมั่นใจว่าการกำหนดนโยบายและเป้าหมายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สอดคล้องกับทิศทางยุทธศาสตร์ขององค์กร

2) ต้องทำให้มีความมั่นใจได้ว่าข้อกำหนดของ ISMS ถูกรวมกับกระบวนการขององค์กร

3) ต้องทำให้มีความมั่นใจได้ว่ามีทรัพยากร ISMS พร้อมใช้

4) ต้องสื่อสารความสำคัญของการจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ และสอดคล้องกับข้อกำหนดของ ISMS

5) ต้องทำให้มีความมั่นใจว่า ISMS บรรลุผลตามที่เป้าหมาย

6) ให้คำปรึกษาและสนับสนุนบุคลากรเพื่อประสิทธิภาพของ ISMS

7) ส่งเสริมให้มีการพัฒนาอย่างต่อเนื่อง และ

8) สนับสนุนบทบาทการจัดการอื่นๆ ที่เกี่ยวข้อง เพื่อแสดงให้เห็นถึงความเป็นผู้นำและมีความรับผิดชอบ

5.2.2 นโยบาย

ผู้บริหารระดับสูงควรกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่ง:

1) เหมาะสมกับวัตถุประสงค์ขององค์กร

2) รวมวัตถุประสงค์ความมั่นคงด้านเทคโนโลยีสารสนเทศ (ดูในข้อ 5.4.1) หรือกำหนดวัตถุประสงค์ ความมั่นคงด้านเทคโนโลยีสารสนเทศ

3) รวมความสำคัญที่จะปฏิบัติตามข้อกำหนดด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ และ

4) รวมถึงข้อผูกพันในการปรับปรุงระบบ ISMS อย่างต่อเนื่อง ควรจัดทำเป็น:

5) ควรทำเป็นเอกสารลายลักษณ์อักษรและสามารถเข้าถึงได้

6) ควรมีการสื่อสารแจ้งเวียนภายในองค์กร และ

7) กลุ่มผู้มีส่วนได้ส่วนเสียหรือผู้เกี่ยวข้อง สามารถเข้าถึงได้ตามความเหมาะสม

5.2.3 บทบาท ความรับผิดชอบ และอำนาจหน้าที่ขององค์กร

ผู้บริหารระดับสูง ควรให้ความสำคัญกับบทบาทของความมั่นคงปลอดภัยด้านสารสนเทศ มีการมอบหมายและสื่อสารความรับผิดชอบให้รับทราบโดยทั่วกัน

ผู้บริหารระดับสูงมอบหมายความรับผิดชอบ และอำนาจหน้าที่เพื่อ:

1) ให้แน่ใจว่า ISMS สอดคล้องกับข้อกำหนดของมาตรฐานฉบับนี้ และ

2) ให้มีการรายงานประสิทธิภาพของ ISMS ให้กับผู้บริหารระดับสูง

หมายเหตุ: ผู้บริหารระดับสูงยังสามารถกำหนดความรับผิดชอบ อำนาจหน้าที่ และรายงานประสิทธิภาพ ISMS ภายในองค์กรด้วย

5.3 การวางแผน/Planning

5.3.1 การดำเนินการเพื่อแก้ไขปัญหาความเสี่ยงและโอกาสที่จะเกิดขึ้น

1) ภาพรวม

เมื่อวางแผน ISMS องค์กรควรพิจารณาประเด็นที่กล่าวถึงในข้อ 5.1.1 และ 5.1.2 ต้องระบุความเสี่ยงและโอกาสที่จะเกิดขึ้น:

(1) ตรวจสอบให้แน่ใจว่า ISMS บรรลุผลตามเป้าหมาย

(2) ป้องกันหรือลดผลกระทบ และ

(3) พัฒนาอย่างต่อเนื่อง

องค์กรควรวางแผนให้:

(4) ดำเนินการเพื่อแก้ไขความเสี่ยงเหล่านั้น

(5) วิธีการที่จะ

ก. รวมและใช้มาตรการในกระบวนการ ISMS และ

ข. ประเมินประสิทธิผลของมาตรการเหล่านี้

2) การประเมินความเสี่ยงความมั่นคงด้านเทคโนโลยีสารสนเทศ

องค์กรควรกำหนดกระบวนการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ:

(1) กำหนดและปรับปรุงเกณฑ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึง

ก. เกณฑ์ความเสี่ยงที่ยอมรับได้ และ

ข. การดำเนินการตามมาตรฐานการประเมินความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(2) สร้างความมั่นใจว่าการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสอดคล้องกันได้อย่างมีประสิทธิภาพ และสามารถเปรียบเทียบผลได้

(3) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ก. กระบวนการประเมินความปลอดภัยของสารสนเทศที่ใช้ควรระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์และสภาพพร้อมใช้งานด้านเทคโนโลยี สารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ และ

ข. ระบุบุคคลรับผิดชอบต่อความเสี่ยง

(4) วิเคราะห์ความเสี่ยงด้านความมั่นคงด้านเทคโนโลยีสารสนเทศ

ก. ผลกระทบที่อาจเกิดขึ้นจากการประเมินความเสี่ยงที่ระบุไว้ในข้อ 2)(3) เกิดขึ้น

ข. ประเมินความเสี่ยงที่ระบุไว้ในข้อ 3)(3) ความเป็นไปได้ที่จะเกิดขึ้นจริง กำหนดระดับความเสี่ยง

(5) ประเมินความเสี่ยงด้านความมั่นคงด้านเทคโนโลยีสารสนเทศ

ก. เปรียบเทียบความเสี่ยงที่วิเคราะห์เทียบกับเกณฑ์ความเสี่ยงที่กำหนด ในข้อ 2)(1) และ

ข. จัดลำดับความสำคัญของการวิเคราะห์ความเสี่ยงเพื่อการบริหารความเสี่ยงที่เหมาะสม

องค์กรควรมีสารสนเทศที่เป็นเอกสารลายลักษณ์อักษรเกี่ยวกับกระบวนการประเมินความเสี่ยงด้านความมั่นคงด้านเทคโนโลยีสารสนเทศ

3) การจัดการความเสี่ยงด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ

องค์กรควรกำหนด และใช้กระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งต้อง:

(1) กำหนดเลือกตัวเลือกการจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยที่เหมาะสมและนำผลการประเมินความเสี่ยงมาพิจารณา

(2) กำหนดตัวควบคุมทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้

หมายเหตุ: องค์กรสามารถออกแบบมาตรการควบคุมได้ตามต้องการหรือระบุโดยอ้างอิงจากแหล่งใดก็ได้

(3) เปรียบเทียบตัวควบคุมที่ระบุในข้อ 2) (2) ข้างต้นกับภาคผนวก A และยืนยันว่าไม่ได้ละเลยการควบคุมข้อใด

หมายเหตุ 1: ภาคผนวก A มีรายละเอียดเกี่ยวกับวัตถุประสงค์การควบคุม ผู้ใช้มาตรฐานนี้โปรดดูที่ภาคผนวก A เพื่อให้แน่ใจว่าจะไม่มองข้ามข้อบังคับทางกฎหมายที่สำคัญ

หมายเหตุ 2: วัตถุประสงค์การควบคุมที่ระบุไว้ในภาคผนวก A อาจยังไม่เพียงพอ ดังนั้น อาจต้องใช้วัตถุประสงค์และการควบคุมเพิ่มเติมนำมาใช้ด้วย

(4) จัดทำเอกสารแสดงการใช้การควบคุม SoA (Statement of Applicability) ซึ่งประกอบด้วยการควบคุมที่จำเป็น (ดูในข้อ 3)(2) และ (3)) ซึ่งอธิบายเหตุผลที่เกี่ยวข้องและเหตุผลในการยกเว้นจากข้อบังคับในภาคผนวก A

(5) จัดทำแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ

(6) ขอความเห็นชอบจากผู้รับผิดชอบความเสี่ยงในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการยอมรับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีอยู่

หมายเหตุ: การประเมินความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาตรฐานการประมวลผล และ ISO 31000: 2009 ให้ใช้หลักการและคำแนะนำทั่วไปประกอบกัน

5.3.2 วัตถุประสงค์การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแผนการดำเนินงาน

องค์กรควรกำหนดวัตถุประสงค์ความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศไว้ในฟังก์ชั่นงานและระดับที่เกี่ยวข้อง

วัตถุประสงค์การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศควร:

1) สอดคล้องกับนโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

2) วัดได้ (ถ้าปฏิบัติได้)

3) พิจารณาข้อกำหนดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ตลอดจนผลการประเมินความเสี่ยง

4) มีการสื่อสารให้ผู้เกี่ยวข้องได้รับทราบ และ

5) มีการปรับปรุงตามความเหมาะสม

องค์กรควรจัดทำเอกสารลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เมื่อวางแผนวิธีการที่จะบรรลุวัตถุประสงค์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ องค์กรควรตัดสินใจว่า:

6) จะทำอย่างไร

7) ต้องการทรัพยากรอะไร

8) ใครเป็นผู้รับผิดชอบ

9) ระยะเวลาดำเนินการเสร็จสิ้น และ

10) วิธีประเมินผล

5.4 การสนับสนุน/Support

5.4.1 ทรัพยากร

องค์กรควรกำหนดและจัดเตรียมการดำเนินงานการบำรุงรักษาทรัพยากรที่จำเป็นต่อการปรับปรุง ISMS อย่างต่อเนื่อง

5.4.2 สมรรถนะบุคลากร

องค์กรควร:

1) กำหนดสมรรถนะที่จะส่งผลต่อประสิทธิภาพการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและทักษะที่จำเป็น

2) ทำให้บุคลากรเหล่านี้ ได้รับการพัฒนาความสามารถได้ศึกษา ฝึกอบรม หรือถ่ายทอดความรู้จากประสบการณ์การทำงานที่ได้รับ

3) ดำเนินการตามความเหมาะสม เพื่อให้ได้มาซึ่งสมรรถนะที่จำเป็น และประเมินประสิทธิผลของการดำเนินการนั้น และ

4) เก็บสารสนเทศให้เป็นเอกสารลายลักษณ์อักษรที่เหมาะสม เพื่อเป็นหลักฐาน

หมายเหตุ: มาตรการที่บังคับใช้อาจรวมถึง การฝึกอบรม การเป็นพี่เลี้ยง หรือจ้างงานหรือทำสัญญากับบุคคลที่มีความสามารถ เป็นต้น

5.4.3 การสร้างความตระหนัก

บุคลากรที่ทำงาน ภายใต้การควบคุมดูแลขององค์กรควรตระหนักถึง:

1) นโยบายความมั่นคงด้านเทคโนโลยีสารสนเทศขององค์กร

2) การมีส่วนร่วมในประสิทธิภาพของ ISMS รวมถึงการปรับปรุงการปฏิบัติงานและสมรรถนะของตนเอง ในการบริหารจัดการความมั่นคงปลอดภัย

3) สิ่งที่เกี่ยวข้องของการไม่ปฏิบัติตามข้อกำหนดของ ISMS

5.4.4 สื่อสารให้ทราบ/Communication

องค์กรควรกำหนดความจำเป็น สำหรับการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับ ISMS รวมถึง:

1) สิ่งที่จะสื่อสาร

2) เมื่อใดที่จะต้องสื่อสาร

3) ใครบ้างที่จะสื่อสารให้ทราบ

4) ใครเป็นผู้สื่อสารออกไป และ

5) ควรมีการสื่อสารออกไปแบบไหน

5.4.5 เอกสารสารสนเทศที่เป็นลายลักษณ์อักษร/Documented Information

1) ภาพรวม

ISMS ขององค์กรควรรวมถึง:

(1) สารสนเทศที่เป็นเอกสารลายลักษณ์อักษรที่กำหนดโดยมาตรฐานฉบับนี้ และ

(2) เอกสารลายลักษณ์อักษรที่องค์กรกำหนดเอง เพื่อพิจารณาความถูกต้องของ ISMS ด้านเทคโนโลยีสารสนเทศ

หมายเหตุ: ปริมาณสารสนเทศที่เป็นเอกสารลายลักษณ์อักษรสำหรับ ISMS มีความแตกต่างกันในแต่ละองค์กร เนื่องจาก:

(1) ขนาดขององค์กรและประเภทของภารกิจ กิจกรรมกระบวนการ ผลิตภัณฑ์ และบริการ

(2) ความซับซ้อนและการเชื่อมโยงของกระบวนการ และ

(3) ความสามารถของบุคลากร

2) การสร้างและปรับปรุง

องค์กรควรตรวจสอบให้แน่ใจว่าเมื่อสร้างและปรับปรุงสารสนเทศที่มีการจัดทำเป็นเอกสารลายลักษณ์อักษร ประเด็นเหล่านี้ ให้มีความเหมาะสม:

(1) คำอธิบาย (เช่น ชื่อ, วันที่, ผู้แต่ง หรือหมายเลขอ้างอิง)

(2) รูปแบบ (เช่น ภาษาเวอร์ชั่นซอฟต์แวร์ แผนภูมิ) และสื่อ (เช่นกระดาษ อิเล็กทรอนิกส์) และ

(3) ทบทวน และอนุมัติความเหมาะสมและความเพียงพอ

3) การควบคุมสารสนเทศที่เป็นเอกสารลายลักษณ์อักษร

เอกสารสารสนเทศที่จำเป็นสำหรับ ISMS ตามมาตรฐานนี้ ขึ้นอยู่กับการควบคุม เพื่อให้มั่นใจว่า:

(1) สารสนเทศมีอยู่และใช้อย่างถูกต้อง และเมื่อใดที่จำเป็น

(2) ได้รับการบำรุงรักษาอย่างเพียงพอ (ตัวอย่าง เช่น หลีกเลี่ยงการสูญเสียความลับการใช้ผิดวัตถุประสงค์ หรือความสูญเสียความถูกต้องสมบูรณ์)

ในการจัดทำเอกสารสารสนเทศ องค์กรควรระบุกิจกรรมต่อไปนี้:

(3) การแจกจ่าย การเข้าถึง การนำมาใช้และการใช้ งาน

(4) การจัดเก็บรักษาให้สามารถอ่านใช้งานได้

(5) การควบคุมการเปลี่ยนแปลง (เช่น การเปลี่ยนแปลงของเวอร์ชั่น) และ

(6) การจัดเก็บ ระยะเวลาการจัดเก็บ และการทำลายสารสนเทศของแหล่งข้อมูลภายนอกที่จำเป็นสำหรับองค์กรและการดำเนินงานของ ISMS สารสนเทศควรได้รับการควบคุมตามความเหมาะสม

หมายเหตุ: การเข้าถึงสารสนเทศรวมถึง การตัดสินใจเกี่ยวกับการอนุญาตให้ดูสารสนเทศได้เท่านั้น การอนุญาตสิทธิ์ในการเข้าถึงและเปลี่ยนแปลงเอกสาร ฯลฯ ได้ด้วย หรืออื่นๆ

5.5 การดำเนินงาน / Operation

5.5.1 การวางแผนและควบคุมการดำเนินงาน

องค์กรควรวางแผน ลงมือปฏิบัติ และควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กระบวนการ ข้อกำหนด และมาตรการที่กำหนดในข้อ 5.3.1 องค์กรควรลงมือปฏิบัติ เพื่อให้บรรลุวัตถุประสงค์ เป้าหมายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่กำหนดในข้อ 5.4.1

องค์กรควรปฏิบัติตามขั้นตอนที่จำเป็น เพื่อให้มีความมั่นใจว่ากระบวนการเหล่านั้น มีการดำเนินการตามแผน

องค์กรควรควบคุมการเปลี่ยนแปลงที่มีการวางแผนล่วงหน้า และทบทวนผลของการเปลี่ยนแปลงที่ไม่คาดคิด เพื่อลดผลกระทบตามความจำเป็น

องค์กรควรตรวจสอบให้แน่ใจว่าได้มีการกำหนดและควบคุมกระบวนการจ้างหน่วยงานภายนอกดำเนินการ มีการระบุและควบคุมการดำเนินงานเอาไว้

5.5.2 การประเมินความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

องค์กรควรดำเนินการประเมินความเสี่ยงตามรอบระยะเวลาแผนงานที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มากขึ้น พิจารณาเกณฑ์ที่กำหนดไว้ในข้อ 2) (1)

องค์กรควรเก็บรักษาเอกสาร เกี่ยวกับผลการประเมินความเสี่ยงด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ

5.5.3 การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

องค์กรควรลงมือปฏิบัติตามแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ องค์กรควรเก็บรักษาเอกสารลายลักษณ์อักษรเกี่ยวกับผลของกระบวนการความเสี่ยงความปลอดภัยด้านเทคโนโลยีสารสนเทศ

5.6 การประเมินผลการปฏิบัติงาน/Performance evaluation

5.6.1 การกำกับดูแล การวัดผลการวิเคราะห์ และการประเมินผล

องค์กรควรประเมินประสิทธิภาพของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและประสิทธิภาพของ ISMS

องค์กรต้องกำหนด:

1) สิ่งที่ต้องติดตามและวัดผล รวมถึงกระบวนการและการควบคุมความปลอดภัยด้านเทคโนโลยี สารสนเทศ

2) วิธีการในการกำกับดูแล การวัดผล การวิเคราะห์และการประเมินผลตามความเหมาะสม เพื่อให้ได้ผลที่มีประสิทธิภาพ

หมายเหตุ: วิธีการที่เลือกใช้ผลการประเมินสามารถเปรียบเทียบกันได้และสามารถทำซ้ำได้ เพื่อให้ได้ผลที่ถูกต้องและสามารถทำซ้ำได้เพื่อให้ได้ผลที่ถูกต้อง

3) เมื่อใดที่ต้องมีการติดตามและวัดผล

4) ใครเขียนกำกับดูแลและวัดผล

5) เมื่อใดผลที่ได้จากการกำกับดูแล และการวัดผลได้รับการวิเคราะห์และประเมิน และ

6) ใครควรเป็นผู้วิเคราะห์และประเมินผล

องค์กรควรเก็บรักษาสารสนเทศที่เป็นเอกสารลายลักษณ์อักษรไว้ เพื่อใช้เป็นหลักฐานแสดงการติดตามและวัดประเมินผลต่อไป

5.6.2 การตรวจสอบภายใน

องค์กรต้องดำเนินการตรวจสอบภายในตามช่วงระยะเวลาที่วางแผนไว้เพื่อให้มีสารสนเทศ สำหรับการระบุว่าระบบ ISMS:

1) สอดคล้องกับ

(1) ข้อกำหนดขององค์กรสำหรับ ISMS และ

(2) ข้อกำหนดของมาตรฐานนี้

2) มีการปฏิบัติและบำรุงรักษาที่มีประสิทธิภาพ

องค์กรควร:

3) วางแผน กำหนด ลงมือปฏิบัติ และดูแลกระบวนการตรวจสอบ ซึ่งรวมถึงความถี่ วิธีการใช้ หน้าที่ความรับผิดชอบ ความต้องการของโปรแกรม และรายงาน กระบวนการตรวจสอบ ต้องพิจารณาความสำคัญของกระบวนการที่เกี่ยวข้อง, รวมทั้งผลกาตรวจสอบก่อนหน้านี้

4) กำหนดมาตรฐานตรวจประเมินและขอบเขตการตรวจสอบแต่ละรายการ

5) การคัดเลือกผู้ตรวจประเมินและการตรวจสอบ เพื่อให้มั่นใจว่ากระบวนการมีความเป็นธรรม

6) ทบทวนให้แน่ใจว่ารายงานผลการตรวจสอบเกี่ยวข้องกับผู้บริหาร และ

7) จัดเก็บสารสนเทศที่เป็นเอกสารลายลักษณ์อักษรไว้ เพื่อเป็นหลักฐานในกระบวนการตรวจสอบและผลการตรวจสอบ

5.6.3 การทบทวนของผู้บริหาร

ผู้บริหารระดับสูงควรตรวจสอบ ISMS ขององค์กรในช่วงระยะเวลาที่กำหนดไว้ เพื่อให้มีความเหมาะสม เพียงพอและมีประสิทธิผลอย่างต่อเนื่องการทบทวนควรรวมถึงการพิจารณา:

1) สถานะของมาตรการจากการทบทวนครั้งก่อนหน้านี้

2) การเปลี่ยนแปลงที่เกี่ยวข้องกับปัญหา ISMS ทั้งภายนอกและภายใน

3) ผลตอบกลับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงแนวโน้มต่อไปนี้:

(1) การไม่ปฏิบัติตามข้อกำหนด มาตรการ และการดำเนินการแก้ไข

(2) ผลการกำกับดูแลและการวัดผล

(3) ผลการตรวจประเมิน และ

(4) ความสำเร็จของวัตถุประสงค์ความมั่นคง ปลอดภัย ด้านเทคโนโลยีสารสนเทศ

4) ผลตอบกลับจากผู้ที่เกี่ยวข้อง

5) ผลการประเมินความเสี่ยงและสถานะของแผนการบริหารความเสี่ยง และ

6) โอกาสสำหรับปรับปรุงอย่างต่อเนื่อง

ผลลัพธ์ของการทบทวนผู้บริหารระดับสูงควรรวมการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงและการเปลี่ยนแปลงต่อระบบ ISMS

องค์กรควรจัดเก็บสารสนเทศที่เป็นเอกสารลายลักษณ์อักษร เพื่อใช้เป็นหลักฐานแสดงผลการทบทวนของผู้บริหารระดับสูง

5.7 การปรับปรุง/Improvement

5.7.1 ความไม่สอดคล้องและการดำเนินการแก้ไข

เมื่อเกิดความไม่สอดคล้องขึ้น องค์กรควร:

1) ดำเนินการต่อความไม่สอดคล้องตามที่กำหนด:

(1) ใช้มาตรการในการควบคุมและดำเนินการแก้ไข

(2) จัดการกับผลที่เกิดขึ้น

2) ประเมินความจำเป็นในการใช้มาตรการ เพื่อขจัดสาเหตุของความไม่สอดคล้องเพื่อป้องกันไม่ให้เกิดซ้ำ หรือเกิดขึ้นที่อื่นโดย:

(1) ทบทวนความไม่สอดคล้อง

(2) กำหนดสาเหตุของความไม่สอดคล้อง และ

(3) การระบุว่าความไม่สอดคล้องที่คล้ายมีหรือไม่ หรืออาจเป็นไปได้ที่จะเกิดขึ้น

3) ใช้มาตรการที่จำเป็น

4) ทบทวนประสิทธิผลของการดำเนินการแก้ไขใดๆ ที่เกิดขึ้น และ

5) ถ้าจำเป็นให้ทำการเปลี่ยนแปลง ISMS ควรใช้มาตรการที่เหมาะสมกับผลกระทบของความไม่สอดคล้องที่เกิดขึ้น

องค์กรควรเก็บรักษาสารสนเทศไว้เพื่อใช้เป็นหลักฐาน แสดง:

6) ลักษณะของความไม่สอดคล้องและการดำเนินการใดๆ ที่ได้ดำเนินการภายหลังที่เกิดขึ้น และ

7) ผลของการดำเนินการแก้ไข

5.7.2 การปรับปรุงอย่างต่อเนื่อง

องค์กรควรปรับปรุง ISMS ให้เหมาะสม เพียงพอ ต่อเนื่อง และมีประสิทธิภาพ

6. เว็บแอปพลิเคชัน

เว็บแอปพลิเคชัน คือ โปรแกรมหรือกลุ่มของโปรแกรมที่ได้รับการพัฒนาขึ้นมาเพื่อใช้งานในบริการ WWW ผู้ใช้สามารถเข้าถึงได้ผ่านทางเครือข่ายอินเทอร์เน็ต ที่ใช้โปรโตคอล TCP/IP เป็นมาตรฐานในการสื่อสารข้อมูล ไม่ว่าจะอยู่ที่ไหน หรือจะเข้าใช้งานเมื่อไหร่ ก็สามารถใช้งานได้ตลอดเวลา โดยใช้เว็บเบราว์เซอร์

การพัฒนาเว็บแอปพลิเคชัน สามารถทำได้โดยการเขียนโปรแกรมในภาษาที่ถูกออกแบบมาสำหรับการพัฒนาแอปพลิเคชันบนระบบเครือข่ายอินเทอร์เน็ต เช่น Perl, PHP, ASP, JavaScript, VB Script, JSP, JAVA ฯลฯ และในแอปพลิเคชันบางชนิด จะต้องมีการติดต่อกับระบบฐานข้อมูล

AppServ คือ โปรแกรมที่รวบรวมเอา Open Source Software หลายๆ อย่างมารวมกัน โดยมีแพ็กเกจหลัก คือ Apcher, PHP, MySQL และ phpMyAdmin โปรแกรมต่างๆ ที่นำมารวบรวมไว้ทั้งนี้ ได้ทำการดาวน์โหลดจาก Official Release ทั้งสิ้น

ภาษา PHP ย่อมาจากคำว่า Hypertext Preprocessor หรือชื่อเดิม Personal Home Page คือ ภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะ Open Source ภาษา PHP ใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบ HTML โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา C ภาษา Java และภาษา Perl ภาษา PHP เป็นผลงานที่เติบโตมาจากกลุ่มของนักพัฒนาในเชิงเปิดเผยรหัสต้นฉบับ หรือ Open Source ดังนั้น PHP จึงมีการพัฒนาไปอย่างรวดเร็วและแพร่หลายโดยเฉพาะอย่างยิ่ง เมื่อใช้ร่วมกับ Apache Webserver ระบบปฏิบัติการอย่างเช่น Linux หรือ Windows เป็นต้น

MySQL คือ โปรแกรมระบบจัดการฐานข้อมูล ที่พัฒนาโดยบริษัท MySQL AB มีหน้าที่เก็บข้อมูลอย่างเป็นระบบ รองรับคำสั่ง SQL เป็นเครื่องมือสำหรับเก็บข้อมูล ที่ต้องใช้ร่วมกับเครื่องมือหรือโปรแกรมอื่นอย่างบูรณาการ เพื่อให้ได้ระบบงานที่รองรับ ความต้องการของผู้ใช้ เช่น ทำงานร่วมกับเครื่องบริการเว็บ (Web Server) เพื่อให้บริการแก่ภาษาสคริปต์ที่ทำงานฝั่งเครื่องบริการ (Server-Side Script) เช่น ภาษา PHP, ภาษา APS.net เป็นต้น โปรแกรมถูกออกแบบให้สามารถทำงานได้บนระบบปฏิบัติการที่หลากหลาย และเป็นระบบฐานข้อมูล Open Source

7. งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ทำการศึกษาค้นคว้าและพบผลงานศึกษาและวิจัยที่เกี่ยวข้อง ดังนี้

ชุลีกร นวลสมศรี (2559) ทำการวิจัยและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001: 2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อประเมินความเสี่ยง และนำเสนอแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001: 2013 ให้แก่องค์กรกรณีศึกษาเพื่อใช้เป็นแนวทางในการกำหนดนโยบาย และแนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร กรณีศึกษาให้มีมาตรฐานในระดับสากล

ณัทรัฏฐ์ มณีรัสยากร (2559) ทำการศึกษาและพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO27001 ของ บริษัท เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น จำกัด จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อการปรับปรุง พัฒนานโยบาย และแนวทางปฏิบัติ ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่องค์กร เพื่อใช้เป็นแนวทางสร้างความมั่นคง ปลอดภัย และยกระดับระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยเป็นมาตรฐานสากล โดยมีมาตรฐาน ISO/IEC 27001: 2013 เป็นเครื่องมือในการพัฒนาเพื่อให้องค์กรดำเนินงานได้อย่างมีประสิทธิภาพ

ธนวรรธน์ ว่องพิบูลย์ (2559) ทำการศึกษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงภายใต้มาตรฐาน ISO/IEC 27001: 2013 ของ บริษัท แปซิฟิค เฮลธ์แคร์ (ไทยแลนด์) จำกัด จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อจัดทำร่างนโยบายความปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงาน รวมถึงการวิเคราะห์และประเมินความเสี่ยง (Risk Management) ซึ่งจะช่วยลดผลกระทบและสามารถบริหารความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ และเป็นการเพิ่มประสิทธิภาพในการทำงานของระบบเทคโนโลยีสารสนเทศภายในองค์กรให้มีมาตรฐานเพิ่มมากขึ้น

รุ่งอรุณ นิรันต์เรือง (2560) ทำการศึกษาและพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 ของโรงพยาบาลคลองใหญ่ จังหวัดตราด จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อพัฒนานโยบายและแนวทางด้านการควบคุมการเข้าถึงระบบสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 ขององค์กรเพื่อใช้เป็นแนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ และเป็นต้นแบบในการพัฒนาความมั่นคงปลอดภัยสารสนเทศด้านอื่นให้ครอบคลุมตามมาตรฐาน ISO/IEC 27001: 2013 เพื่อให้ระบบสารสนเทศขององค์กรมีความมั่นคง ปลอดภัยเพิ่มขึ้น

สุรชาติ จันทสุวรรณ (2559) ทำการศึกษาและพัฒนาระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิต เพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย โดยมีวัตถุประสงค์เพื่อศึกษาวิธีการตรวจประเมินหน่วยงานเทคโนโลยีสารสนเทศของผู้ตรวจสอบภายใน ที่อ้างอิงมาตรฐานโคบิต 5.0 (COBIT 5.0) และเพื่อพัฒนาระบบสำหรับในการประเมินความพร้อมของหน่วยงานเทคโนโลยีสารสนเทศ เพื่อเข้าตลาดหลักทรัพย์ตลาดหลักทรัพย์ เอ็ม เอ ไอ กลุ่มอุตสาหกรรมทรัพยากรโดยใช้หลักธรรมาภิบาลไอที

อัจฉรา เวียงสิมา (2559) ทำการทบทวนและพัฒนานโยบายการบริหารจัดการความมั่นคงของระบบเทคโนโลยีสารสนเทศของบริษัท ที-เน็ต จำกัด ให้สอดคล้องกับมาตรฐาน ISO/IEC 27001: 2013 ที่ได้ปรับปรุงให้เป็นไปตามมาตรฐานสากล จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อปรับปรุงนโยบายการบริหารจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ รวมถึงให้องค์กรมีมาตรฐานและการพัฒนากระบวนการบริหารจัดการความมั่นคงทางสารสนเทศ ให้เป็นไปตามแนวทางขององค์กร โดยนำกระบวนการดังกล่าวมาพัฒนาและประยุกต์ใช้ในการดำเนินงานของแต่ละส่วนงานให้มีการปฏิบัติเป็นไปตามข้อกำหนดที่ได้กำหนดไว้ ประกอบกับส่งเสริมบุคลากรภายในองค์กรให้มีความพร้อมและปฏิบัติหน้าที่ไปในทิศทางเดียวกัน

บทที่ 3
วิธีดำเนินการวิจัย

การพัฒนาระบบประเมินความเสี่ยงและความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ เป็นกระบวนการที่มีความสำคัญในการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพราะการประเมินความเสี่ยงทำให้ทราบถึงสถานะความเสี่ยงขององค์กรใน แต่ละด้านว่าอยู่ในระดับใด และการควบคุมความมั่นคงปลอดภัยเป็นมาตรการและแนวทางในการปฏิบัติงานให้มีความปลอดภัย ซึ่งเป็นทิศทางนำไปสู่การปฏิบัติงานได้ตามเป้าหมาย และภารกิจขององค์กรที่ตั้งไว้ได้อย่างมีประสิทธิภาพ ปลอดภัย

ผู้ศึกษาได้พัฒนาระบบประเมินความเสี่ยงและการควบคุมความมั่นคงปลอดภัย เนื่องจากมีความสำคัญต่อการกำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ ผู้ศึกษาได้เลือกใช้มาตรฐาน ISO/IEC 27001: 2013 เป็นแนวทางในการพัฒนาและใช้เนติบัณฑิตยสภาในพระบรมราชูปถัมภ์ เป็นกรณีศึกษา โดยศึกษาเฉพาะความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Access Control) ควรให้สอดคล้องตามมาตรฐาน ISO/IEC 27001: 2013

1. เครื่องมือที่ใช้ในการวิจัย

1.1 แบบสัมภาษณ์เกี่ยวกับการประเมินความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013

1.2 ทะเบียนสินทรัพย์และมูลค่าของสินทรัพย์ด้านเทคโนโลยีสารสนเทศขององค์กร

1.3 ระบบความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Web Application)

2. ขั้นตอนการดำเนินการวิจัย

2.1 ศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2013

2.1.1 ศึกษาค้นคว้าเกี่ยวกับการจัดการความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (ISMS)

2.1.2 ศึกษาเปรียบเทียบความแตกต่างระหว่าง ISO/IEC 27001: 2005 และ ISO/IEC 27001: 2013

2.2 ศึกษาความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบัน

ศึกษาทำความเข้าใจมาตรการความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบันว่ามาตรการความมั่นคงปลอดภัยข้อใดสอดคล้องตามมาตรฐาน ISO/IEC 27001:2005 และกฎหมายอื่นที่เกี่ยวข้อง

2.3 ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรตามหลัก CIA Triad

ขอบเขตของการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร ครอบคลุมสินทรัพย์ด้านเทคโนโลยีสารสนเทศขององค์กร โดยแบ่งกลุ่มตามแผนกและลักษณะงาน ในการศึกษานี้ แบ่งเป็น 3 แผนกและ 3 ลักษณะงาน คือ 1) สินทรัพย์ด้านเทคโนโลยีสารสนเทศเกี่ยวกับงานทะเบียนสมาชิกและทนายความ (กองกลาง) 2) สินทรัพย์ด้านเทคโนโลยีสารสนเทศเกี่ยวกับงานการเงิน (กองคลัง) และ 3) สินทรัพย์ด้านเทคโนโลยีสารสนเทศเกี่ยวกับงานบริหารจัดการนักศึกษา (กองบริการ)

2.3.1 จัดทำทะเบียนสินทรัพย์และกำหนดค่าของสินทรัพย์จากผลกระทบหากเกิดความเสียหาย (Asset Identification and Valuation)

1) ทะเบียนสินทรัพย์แบ่งออกเป็น 6 ด้าน ดังนี้

(1) กระบวนการทางธุรกิจ (Business processes Assets)

(2) ข้อมูล (Information Assets)

(3) ซอฟต์แวร์ (Software Assets)

(4) ฮาร์ดแวร์ (Hardware Assets)

(5) บุคลากร (People Assets)

(6) โครงสร้างพื้นฐานที่สนับสนุนการดำเนินงาน (Infrastructure Assets)

2) หามูลค่าของทรัพย์สิน (Asset Value) โดยวัดจากระดับความเสียหายที่เกิดขึ้นกับความมั่นคงปลอดภัย ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมใช้งาน (Loss of Availability) ที่ส่งผลเสียหายกับองค์กร ดังนี้

(1) ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้

(2) ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น

(3) ทำให้องค์กรละเมิดกฎหมาย ระเบียบ ข้อบังคับ และสัญญา

(4) ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน

(5) ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร

ตารางที่ 3.1 ความเสียหายจากการสูญเสีย CIA Triad ส่งผลต่อองค์กร

Confidentiality (C) เมื่อสินทรัพย์สูญเสียความลับ		
	Disruption of Service (DS)	ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้
	Loss of Credibility (LC)	ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น
	Violation of Law, Regulation and Contract (VL)	ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับ และสัญญา
	Financial Loss (FL)	ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน
	Endangerment of Personal Safety (ES)	ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร
Integrity (I) เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน		
	Disruption of Service (DS)	ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้
	Loss of Credibility (LC)	ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น
	Violation of Law, Regulation and Contract (VL)	ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับ และสัญญา
	Financial Loss (FL)	ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน
	Endangerment of Personal Safety (ES)	ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร

ตารางที่ 3.1 (ต่อ)

Confidentiality (C) เมื่อสินทรัพย์สูญเสียความลับ	
Availability (A) เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน	
Disruption of Service (DS)	ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้
Loss of Credibility (LC)	ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น
Violation of Law, Regulation and Contract (VL)	ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับ และสัญญา
Financial Loss (FL)	ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน
Endangerment of Personal Safety (ES)	ทำให้เกิดอันตรายต่อบุคลากรและผู้ใช้งานในองค์กร

3) ลงข้อมูลในทะเบียนสินทรัพย์ แยกตามประเภทของสินทรัพย์ ซึ่งมีข้อมูลของสินทรัพย์ในแต่ละประเภทที่ต้องระบุ ดังนี้

(1) ระบุชื่อสินทรัพย์/ชื่อกระบวนการ

(2) ระบุรายละเอียดของสินทรัพย์/กระบวนการ

(3) ระบุผู้ดูแลสินทรัพย์/ผู้รับผิดชอบ/ผู้บังคับบัญชา

(4) ระบุรายละเอียดของกฎหมาย ระเบียบข้อบังคับและสัญญาที่เกี่ยวข้องกับสินทรัพย์

(5) ข้อมูลอื่นๆ ที่เกี่ยวข้องกับสินทรัพย์

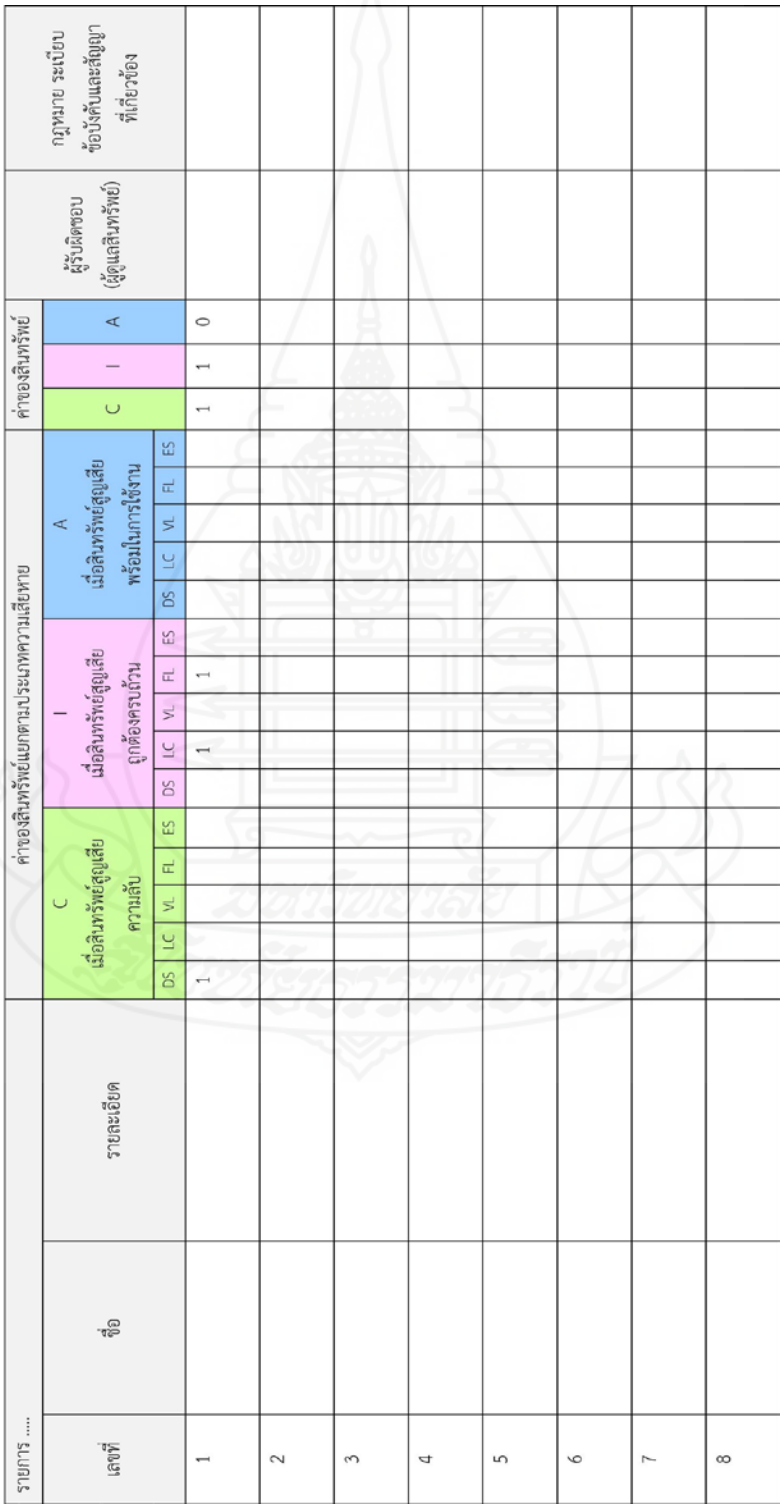
4) ประเมินค่าของสินทรัพย์แยกตามประเภทความเสียหาย โดยพิจารณาแยกตามแต่ละมิติซึ่งประกอบด้วย Confidentiality (C) Integrity (I) และ Availability (A) ตามประเภท และเกณฑ์ที่กำหนดไว้ โดยใช้ค่าของสินทรัพย์ที่มีค่าสูงสุดในแต่ละประเภทความเสียหายมาเป็นค่าของสินทรัพย์ในแต่ละมิติ ดังตารางด้านล่างนี้

ตารางที่ 3.2 ค่าของสินทรัพย์แยกตามประเภทความเสียหาย

ความเสียหาย	ค่าของสินทรัพย์			
	สูงมาก (4)	สูง (3)	ปานกลาง (2)	ต่ำ (1)
ทำให้องค์กรไม่สามารถปฏิบัติงานตามปกติได้ (Disruption of services : DS)	มีผลให้องค์กรต้องหยุดการปฏิบัติภารกิจมากกว่า 8 ชั่วโมง	มีผลให้องค์กรต้องหยุดการปฏิบัติภารกิจไม่เกิน 8 ชั่วโมง	มีผลให้องค์กรต้องหยุดการปฏิบัติภารกิจไม่เกิน 4 ชั่วโมง	มีผลให้องค์กรปฏิบัติภารกิจไม่สะดวก
ทำให้องค์กรเสียชื่อเสียงและความเชื่อมั่น (Loss of Creditability : LC)	กระทบกับภาพลักษณ์ขององค์กร ทำให้เกิดความไม่เชื่อมั่นในการทำงานขององค์กร	กระทบกับภาพลักษณ์ขององค์กร ทำให้เกิดความไม่ชื่อมั่นในการปฏิบัติงานของพนักงาน	กระทบกับภาพลักษณ์ของหน่วยงานย่อยในองค์กร	กระทบกับภาพลักษณ์ขององค์กรเล็กน้อย ไม่เป็นข่าวในสื่อ
ทำให้องค์กรละเมิดกฎหมาย ระเบียบข้อบังคับและ สัญญา (Violation Of Law, Regulation and Contract : VL)	ส่งผลให้ ต้องรับผิดชอบตามกฎหมาย ระเบียบ ข้อบังคับและสัญญา	ส่งผลให้ผู้บริหารระดับสูงรับผิดชอบตามกฎหมาย ระเบียบข้อบังคับ ระเบียบและสัญญา	ส่งผลให้เจ้าหน้าที่ที่เกี่ยวข้องต้องรับผิดชอบตามกฎหมายระเบียบ ข้อบังคับ ระเบียบและสัญญา	ส่งผลให้เจ้าหน้าที่ที่เกี่ยวข้องได้รับการตักเตือนหรือมีโทษทางวินัยเล็กน้อย
ทำให้องค์กรมีความเสียหายเป็นจำนวนเงิน (Financial Loss : FL)	มากกว่า 10 ล้านบาท	มากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท	มากกว่า 1 ล้านบาท แต่ไม่เกิน 5 ล้านบาท	น้อยกว่าล้าน 1 บาท
ทำให้เกิดอันตรายต่อบุคลากร และผู้ใช้งานในองค์กร (Endangerment Of Personal Safety : ES)	มีผู้เสียชีวิต 1 คนขึ้นไป	บาดเจ็บสาหัสจนทำให้พิการหรือทุพลภาพ	บาดเจ็บสาหัสหรือทรัพย์สินบุคลากรเสียหาย	บาดเจ็บเล็กน้อย

สรุปตามขั้นตอนที่ 2.3.1 ได้ดังตารางด้านล่างนี้ ทะเบียนสินทรัพย์ และมูลค่าของสินทรัพย์ (Asset Identification and Valuation)

ตารางที่ 3.3 เครื่องมือในการจัดทำทะเบียนสินทรัพย์และกำหนดมูลค่าของสินทรัพย์



รายการ			ค่าของสินทรัพย์ตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบ ข้อบังคับและสัญญาที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียพร้อมในการใช้งาน					C	I	A		
เลขที่	ชื่อ	รายละเอียด	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
1			1						1		1							1	1	0		
2																						
3																						
4																						
5																						
6																						
7																						
8																						

2.3.2 กำหนดภัยคุกคามต่อสินทรัพย์ (Threat Identification)

1) จัดทำรายการภัยคุกคาม (Threat List) ที่สามารถเกิดขึ้นกับสินทรัพย์ โดยใช้ข้อมูลจากภัยคุกคามที่เคยเกิดขึ้นในอดีต หรือประสบการณ์ของเจ้าของสินทรัพย์ และแหล่งข้อมูลที่น่าเชื่อถือ โดยภัยคุกคามที่นำมาพิจารณาแยกเป็นประเภทตามสาเหตุที่เกิดขึ้น เช่น ภัยคุกคามที่เกิดจากธรรมชาติ (Environmental threats), ภัยคุกคามที่เกิดจากอุบัติเหตุ (Accidental threats), ภัยคุกคามที่เกิดโดยเจตนาของมนุษย์ (Deliberate threats)

2) ประเมินภัยคุกคามแต่ละรายการว่ามีผลต่อในทุกมิติของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้แก่ การสูญเสียความลับ (C) การสูญเสียความถูกต้องครบถ้วน (I) และการสูญเสียความพร้อมในการใช้งาน (A) หากเกิดผลต่อในมิติใดให้ระบุค่า “Y” ลงในช่องของมิตินั้น หากไม่มีผลต่อมิติใดให้ระบุคำ “N” โดยอ้างอิงรายการภัยคุกคามของ Supplement to BSI Standard 100-3,Version 2.5 ซึ่งมีภัยคุกคามหลัก 46 รายการ แต่มีภัยคุกคามส่วนที่เกี่ยวข้องการศึกษาครั้งนี้มี 42 รายการ (รายละเอียดภาคผนวก ก)

ตารางที่ 3.4 รายการภัยคุกคามและมิติด้าน CIA Triad ที่เกี่ยวข้อง

ชื่อภัยคุกคาม (Threat)	Confidentiality (C)	Integrity (I)	Availability (A)
เพลิงไหม้	N	Y	Y
ความเสียหายจากน้ำ	N	Y	Y
ฝุ่น สนิม มลพิษ	N	Y	Y
ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง	N	Y	N
การปฏิเสธความรับผิดชอบ	Y	Y	N
หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	N	Y	Y
อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y
การล้วงความลับหรือข้อมูลจากระบบ	Y	N	N
ความลับถูกเปิดเผย	Y	N	N
การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y
หยุดทำงานเนื่องจากบริการพื้นฐาน (Mains supply)	N	Y	Y
การเข้าถึงสถานที่หรือบริเวณต้องห้าม	Y	Y	Y
ฯลฯ			

ที่มา: อ้างอิงรายการภัยคุกคามของ Supplement to BSI Standard 100-3,Version 2.5

2.3.3 ประเมินระดับโอกาสที่จะเกิดขึ้น (Likelihood Determination)

1) ระดับโอกาสที่จะเกิดขึ้น (Likelihood) โดยประเมินค่าโอกาสที่จะเกิดขึ้นที่ภัยคุกคามอาจกระทำความเสียหายต่อสินทรัพย์ได้สำเร็จ พิจารณาจากแนวโน้มการเกิดขึ้นของภัยคุกคาม ซึ่งเกิดจากแรงจูงใจและสถิติที่เคยเกิดขึ้นมีการบันทึกไว้หรือจากประสบการณ์ของเจ้าของสินทรัพย์ เช่น สินทรัพย์ที่มีราคาสูงและเคลื่อนย้ายง่ายจะมีแนวโน้มที่จะถูกขโมยได้มากกว่าสินทรัพย์ทั่วไป หรือภัยคุกคามประเภทภัยธรรมชาติต่างๆ จะมีแนวโน้มการเกิดต่ำเมื่อดูจากสถิติที่เคยเกิดขึ้น ถ้าแนวโน้มการเกิดของภัยคุกคามสูง โอกาสที่จะเกิดขึ้นที่ภัยคุกคามนั้นจะกระทำความเสียหายต่อสินทรัพย์ได้สำเร็จจะสูงกว่าภัยคุกคามที่มีแนวโน้มการเกิดต่ำ

2) เมื่อประเมินค่าได้แล้วทำการปรับปรุงค่าโอกาสที่จะเกิดขึ้น ให้เป็นปัจจุบัน ระดับโอกาสที่จะเกิดขึ้น แบ่งออกเป็น 5 ระดับ ตามตารางด้านล่างนี้

ตารางที่ 3.5 ระดับโอกาสที่จะเกิดขึ้น

โอกาสที่จะเกิดขึ้น	**คำอธิบายและหลักเกณฑ์**
สูงมาก (5)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูงมาก หรืออาจเกิดขึ้นได้**ทุกสัปดาห์หรือบ่อยกว่านั้น**
สูง (4)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้สูง หรืออาจเกิดขึ้นได้ประมาณ**เดือนละครั้ง**
ปานกลาง (3)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ปานกลาง หรืออาจเกิดขึ้นได้ประมาณ**ปีละครั้ง**
ต่ำ (2)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำ หรือในรอบ**สิบปีอาจเกิดขึ้นได้ 1-2 ครั้ง**
ต่ำมาก (1)	ภัยคุกคามมีโอกาสสร้างความเสียหายได้ต่ำมาก หรือในรอบ**ร้อยปีอาจเกิดขึ้นได้สักครั้ง หรือแทบเป็นไปไม่ได้ที่จะเกิดขึ้น**

2.3.4 ประเมินผลกระทบ (Impact)

ประเมินผลกระทบ (Impact) จากภัยคุกคาม **โดยพิจารณาความสัมพันธ์ของมิติของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่ได้รับความเสียหายจากภัยคุกคาม และ ค่าของสินทรัพย์ในแต่ละมิติ (ดังตารางที่ 3.2)** ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมในการใช้งาน (Loss of Availability)

2.3.5 ประเมินระดับความเสี่ยง (Risk Exposure)

1) ประเมินระดับความเสี่ยง คำนวณได้จากผลคูณของระดับของผลกระทบ (Impact) และระดับโอกาสที่จะเกิดความเสี่ยงขึ้น (Likelihood) (อ้างอิงจาก ISO 31000: 2009)

ระดับความเสี่ยง (Risk Exposure) = ระดับผลกระทบ (Impact) x ระดับโอกาสที่จะเกิด (Likelihood)

ระดับความเสี่ยง (Risk Exposure)
- **ระดับผลกระทบ (Impact)** — **หากเกิดภัยคุกคามแล้วองค์กรจะได้รับผลกระทบระดับใด**
- **ระดับโอกาสที่จะเกิดขึ้น (Likelihood)** — **ภัยคุกคามมีโอกาสเกิดขึ้นมาก น้อย บ่อยครั้งเพียงใด**

โดยพิจารณาจากผลกระทบแยกตามมิติของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งได้แก่ การสูญเสียความลับ (Loss of Confidentiality) การสูญเสียความถูกต้องครบถ้วน (Loss of Integrity) และการสูญเสียสภาพความพร้อมในการใช้งาน (Loss of Availability) และใช้ระดับความเสี่ยงที่มากที่สุดที่ประเมินได้ในแต่ละด้านเป็นความเสี่ยงของภัยคุกคามนั้นๆ ต่อสินทรัพย์การประเมินค่าระดับความเสี่ยงให้อ้างอิงจาก ตารางด้านล่างนี้

ตารางที่ 3.6 ตารางแสดงระดับความเสี่ยง (Risk Exposure level)

โอกาสที่จะเกิดขึ้น	**ระดับผลกระทบ**			
	(1) = (Low) ต่ำ	**(2) = (Medium) ปานกลาง**	**(3) = (High) สูง**	**(4) = (Very High) สูงมาก**
โอกาสเกิดสูงมาก (5)	(1) x (5) ปานกลาง	(2) x (5) สูง	(3) x (5) สูงมาก	(4) x (5) สูงมาก
โอกาสเกิดสูง (4)	(1) x (4) ปานกลาง	(2) x (4) สูง	(3) x (4) สูง	(4) x (4) สูงมาก
โอกาสเกิดปานกลาง (3)	(1) x (3) ปานกลาง	(2) x (3) ปานกลาง	(3) x (3) สูง	(4) x (3) สูง
โอกาสเกิดน้อย (2)	(1) x (2) ต่ำ	(2) x (2) ปานกลาง	(3) x (2) ปานกลาง	(4) x (2) สูง
โอกาสเกิดน้อยมาก (1)	(1) x (1) ต่ำ	(2) x (1) ต่ำ	(3) x (1) ปานกลาง	(4) x (1) ปานกลาง

2) เกณฑ์ความสามารถในการยอมรับความเสี่ยง ผลลัพธ์ในตารางข้างต้น สำหรับช่องที่ถูกแรเงาแบ่งตามสีนั้นเป็นกรณีที่ต้องนำไปดำเนินการหาวิธีแก้ไขความเสี่ยง ความหมายของความเสี่ยงในแต่ละระดับตามตารางที่ 3.6 มีความหมาย ดังนี้

ตารางที่ 3.7 ตารางแสดงเกณฑ์ความสามารถในการยอมรับความเสี่ยง

ระดับความเสี่ยง	รายละเอียดความเสี่ยง / เกณฑ์การยอมรับ
สูงมาก (VH) 13-20 คะแนน	ความเสี่ยงในระดับสูงมาก ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการทันที
สูง (H) (7-12 คะแนน)	ความเสี่ยงในระดับสูง ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
ปานกลาง (M) (3-6 คะแนน)	ความเสี่ยงในระดับปานกลาง ควรพิจารณาแก้ไขความเสี่ยง แต่หากมีเหตุจำเป็น สามารถพิจารณายอมรับความเสี่ยงได้
ต่ำ (L) (1-2 คะแนน)	ความเสี่ยงในระดับที่ต่ำ ควรพิจารณาแก้ไขความเสี่ยง แต่สามารถยอมรับได้โดยไม่ต้องดำเนินการใดๆ เพิ่มเติม

สรุปตามขั้นตอนที่ 2.3.2 – 2.3.5 ได้ดังตารางด้านล่างนี้

การประเมินความเสี่ยงของสินทรัพย์

ตารางที่ 3.8 เครื่องมือในการประเมินความเสี่ยง

No.	สินทรัพย์		ประเมินโอกาสที่จะเกิดขึ้น (จากภัยคุกคาม/จุดอ่อน)										ความเสี่ยง				
	ชื่อกระบวนการ	ประเภท	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
			C	I	A		C	I	A	C	I	A		C	I	A	
1	xxxx	Business processes	1	1	0	เพลิงไหม้	N	Y	Y		1	0	1		1	N/A	

ขั้นตอนที่ 3.2.3.2

ขั้นตอนที่ 3.2.3.3

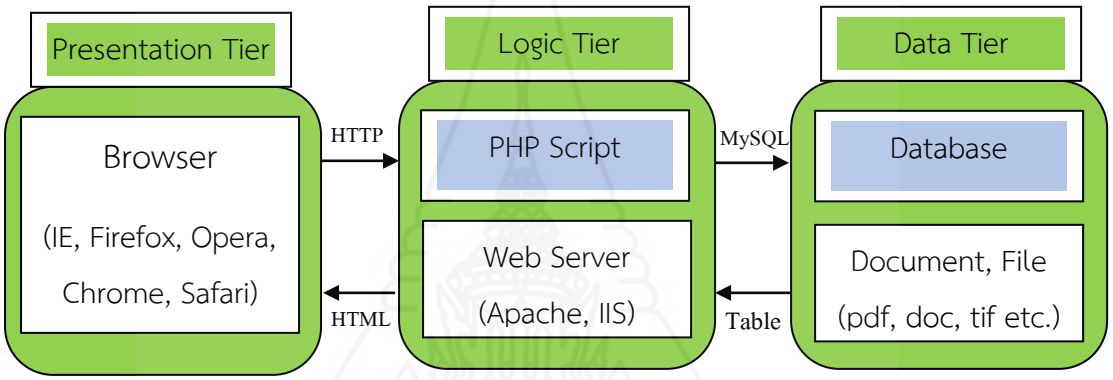
ขั้นตอนที่ 3.2.3.4

ขั้นตอนที่ 3.2.3.5

3. การพัฒนาเว็บแอปพลิเคชันระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013

3.1 แนวคิดในการออกแบบและพัฒนาระบบ

ระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 พัฒนาตามสถาปัตยกรรมเว็บแอปพลิเคชัน โดยมีการออกแบบระบบเป็น Three-Tier Architecture ประกอบไปด้วย 3 ส่วน ดังภาพด้านล่างนี้



ภาพที่ 3.1 สถาปัตยกรรมการออกแบบเว็บแอปพลิเคชัน

3.1.1 Presentation Tier คือ ส่วนของหน้าจอต่างๆ ของระบบที่ติดต่อกับผู้ใช้งาน โดยจะทำงานอยู่ที่เครื่อง Client ผ่าน Web Browser

3.1.2 Logic Tiezr คือ ส่วนที่ระบบใช้ในการควบคุมการแสดงผลของส่วน Presentation tier และรับคำสั่งการทำงานต่างๆ จากผู้ใช้งาน

1) PHP Script คือ ส่วนที่นำคำสั่งจากผู้ใช้งานที่ส่งมาจาก Presentation tier มาประมวลผล เช่น คำนวณเปรียบเทียบข้อมูลต่างๆ เพื่อใช้ในการเข้าถึงข้อมูลที่อยู่ฐานข้อมูล

2) Web Server คือ ส่วนที่ใช้สำหรับติดต่อกับฐานข้อมูล โดยจะรับคำสั่งจาก PHP Script แล้วส่งคำสั่งไปติดต่อกับData tier เมื่อได้ผลลัพธ์แล้วก็จะส่งกลับไปยัง PHP Script ต่อไป

3.1.3 Data Tier คือ ส่วนที่ใช้สำหรับเก็บข้อมูลที่เป็น Physical ของระบบ แบ่งออกเป็น

1) Database ใช้ในการเก็บ Index ของข้อมูลที่ผู้ใช้งานได้เพิ่มเข้ามาในระบบ

2) Database Server ใช้ในการเก็บไฟล์เอกสารต่างๆ ที่ผู้ใช้งานเพิ่มเข้ามาในระบบ

3.2 ภาษาและเครื่องมือที่ใช้ในการพัฒนาระบบ

3.2.1 ใช้โปรแกรมภาษา PHP ในการพัฒนาระบบซึ่งเป็นภาษาที่มีประสิทธิภาพและมีความยืดหยุ่นสูง

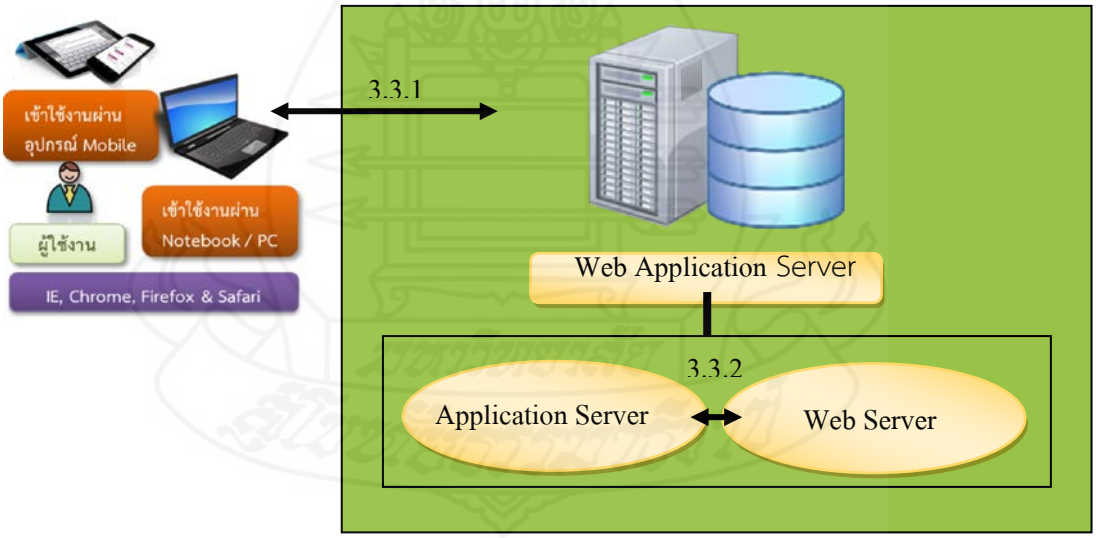
3.2.2 ใช้โปรแกรม Adobe Dreamweaver CS6 ในการออกแบบและจัดการ User Interface

3.2.3 ใช้โปรแกรม Adobe Photoshop CS5 ตกแต่งและออกแบบเว็บไซต์

3.2.4 ใช้ AppServ 8.6.0 ในการเชื่อมโยงข้อมูล

3.2.5 ใช้ My SQL เป็น Database สำหรับจัดเก็บข้อมูล

3.3 โครงสร้างการทำงานของระบบ



ภาพที่ 3.2 โครงสร้างการทำงานของระบบความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013

3.3.1 ผู้ใช้งานสามารถใช้งานผ่าน Web Brower เช่น IE, Firefox, Opera, Chrome และ Safari โดยเป็นการใช้งานในส่วนของ Web Server

3.3.2 เมื่อระบบต้องการใช้การประมวลผลข้อมูลจากฐานข้อมูลโดยเรียกใช้งานไปที่ Application Server ข้อมูลจากฐานข้อมูลก็จะทำการประมวลผลและส่งผลลัพธ์กลับไปยัง Web Server

3.4 ฟังก์ชั่นการทำงานของระบบ

3.4.1 ระบบบริหารจัดการการเข้าใช้งานสำหรับผู้ใช้งานทั่วไปและผู้ใช้งานที่ลงทะเบียนเข้าใช้งาน

3.4.2 ระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2013

3.4.3 แสดงผล และรายงานการประเมินความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน SO/IEC27001: 2013

3.4.4 แสดงรายละเอียด แนวทางมาตรการความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน SO/IEC27001: 2013

3.4.5 แสดงเอกสารและดาวน์โหลดเอกสารแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บทที่ 4
ผลการดำเนินการวิจัย

1. ข้อมูลพื้นฐานขององค์กร

เนติบัณฑิตยสภาในพระบรมราชูปถัมภ์ เป็นองค์กรอิสระที่มีฐานะเป็นนิติบุคคลตามพระราชบัญญัติเนติบัณฑิตยสภา พ.ศ.2507 ซึ่งตราขึ้นโดยจอมพล ถนอม กิตติขจร โดยมีรัฐมนตรีว่าการกระทรวงยุติธรรม เป็นสภานายกพิเศษมีอำนาจหน้าที่ควบคุมกิจการทั้งปวงของสภา และมีคณะกรรมการคณะหนึ่งเรียกว่า คณะกรรมการเนติบัณฑิตยสภามีประธานศาลฎีกาเป็นนายกเนติบัณฑิตยสภา ประธานศาลอุทธรณ์ เป็นอุปนายกคนที่ 1 และอัยการสูงสุด เป็นอุปนายกคนที่ 2 คณะกรรมการเนติบัณฑิตยสภา มาจากผู้ทรงคุณวุฒิ 4 ฝ่าย ได้แก่ ผู้ทรงคุณวุฒิฝ่ายตุลาการ ผู้ทรงคุณวุฒิฝ่ายอัยการ ผู้ทรงคุณวุฒิฝ่ายทนายความ และผู้ทรงคุณวุฒิจากกลุ่มอาชีพอื่น ฝ่ายละ 5 คน ผ่านการเลือกตั้งจากสมาชิกเนติบัณฑิตยสภา ประเภทสามัญสมาชิกทุกๆ 4 ปี

คณะกรรมการเนติบัณฑิตยสภามีอำนาจในการตราข้อบังคับเนติบัณฑิตยสภา เกี่ยวกับประเภทสมาชิก คุณสมบัติของผู้สมัครเป็นสมาชิก การเข้าเป็นสมาชิก และการขาดจากสมาชิกภาพ คณะกรรมการเนติบัณฑิตยสภาจึงออกข้อบังคับเนติบัณฑิตยสภา พ.ศ.2507 กำหนดให้สมาชิกมี 5 ประเภท คือ 1.สามัญสมาชิก 2.สมาชิกวิสามัญ 3.สมาชิกสมทบ 4.ภาคีสมาชิก (นักศึกษา) และ 5. สมาชิกกิตติมศักดิ์

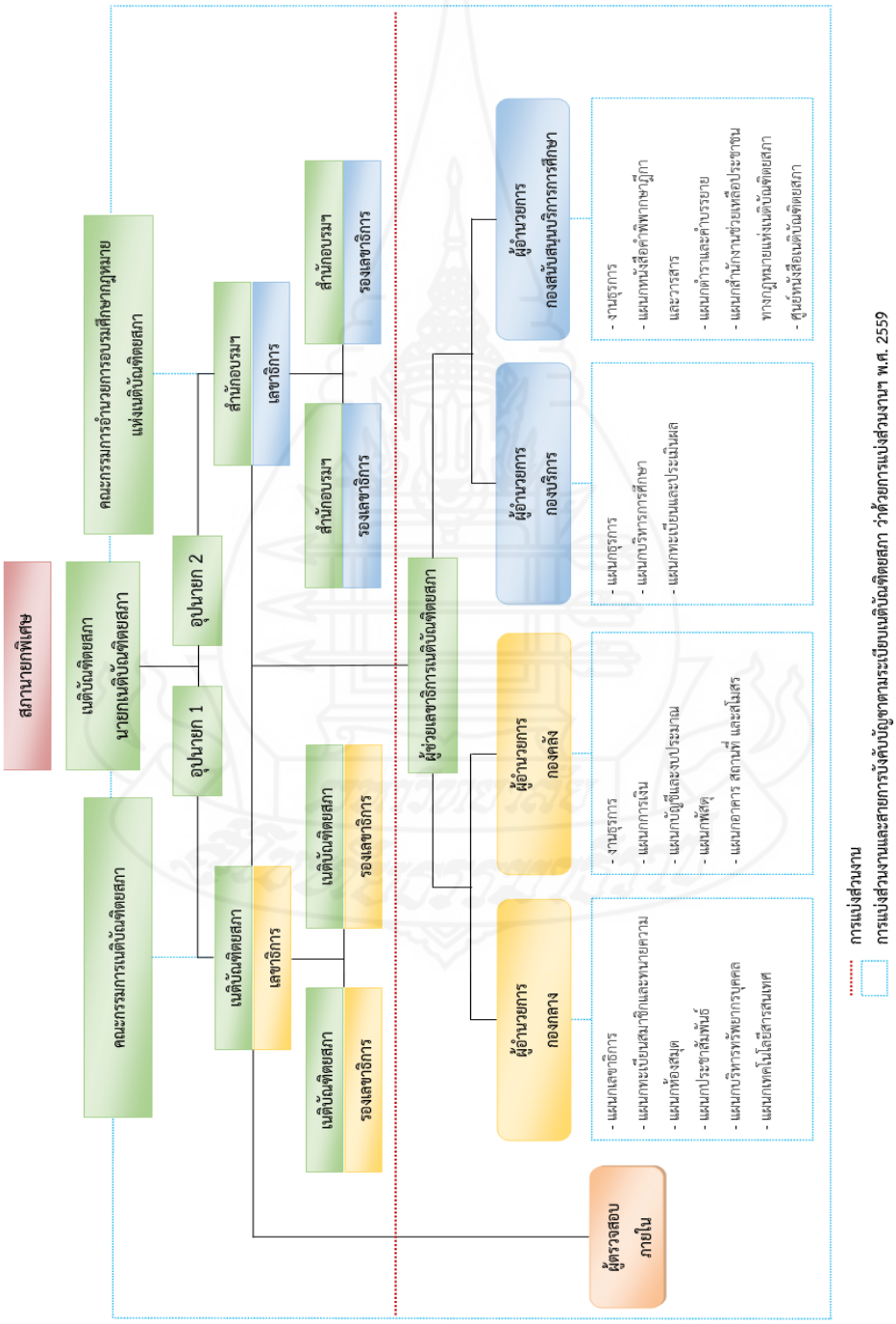
สามัญสมาชิก สมาชิกวิสามัญ และสมาชิกกิตติมศักดิ์ มีสิทธิสวมเสื้อครุยเนติบัณฑิตตามระเบียบว่าด้วยเสื้อครุยเนติบัณฑิต การเป็นสามัญสมาชิกเป็นคุณสมบัติข้อหนึ่งที่จะมีสิทธิสมัครสอบเป็นผู้ช่วยผู้พิพากษา และอัยการผู้ช่วย และการเป็นสมาชิกวิสามัญเป็นคุณสมบัติข้อหนึ่งในการขอใบอนุญาตประกอบวิชาชีพทนายความ

วิสัยทัศน์ เนติบัณฑิตยสภาจะเป็นองค์กรหลักในการส่งเสริมความรู้และกำกับดูแลการประกอบอาชีพของนักกฎหมายให้มีคุณภาพกอปรด้วยจริยธรรมและเกียรติศักดิ์ตามมาตรฐานสากล มุ่งเสริมสร้างความสมานฉันท์ในหมู่นักกฎหมายและความเชื่อถือศรัทธาของประชาชนที่มีต่อวิชาชีพกฎหมายให้มั่นคงยิ่งขึ้น ทั้งจะเน้นบทบาทการให้ความช่วยเหลือทางกฎหมายแก่ประชาชนให้เป็นที่เห็นอย่างเด่นชัด

สถานที่ตั้ง 32/2-8 หมู่ที่ 16 ถนนกาญจนาภิเษก แขวงบางระมาด เขตตลิ่งชัน กรุงเทพมหานคร 10170

2. โครงสร้างการบริหารงานเนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์

เนติบัณฑิตยสภาฯ มีโครงสร้างองค์กร แบ่งออกเป็น 4 กอง (พ.ศ. 2559) ได้แก่ กองกลาง กองคลัง กองบริการ และกองสนับสนุน โดยมีโครงสร้าง ดังภาพด้านล่างนี้

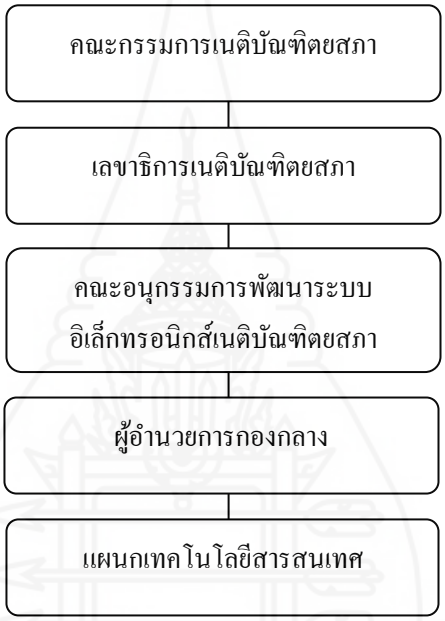


ภาพที่ 4.1 โครงสร้างการบริหารงานเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์

2.1 โครงสร้างการบริหารงานแผนกเทคโนโลยีสารสนเทศ

แผนกเทคโนโลยีสารสนเทศเนติบัณฑิตยสภาประกอบด้วยนักเทคโนโลยีสารสนเทศ 2 คน สำเร็จการศึกษาด้านเทคโนโลยีสารสนเทศ จำนวน 1 คน และสำเร็จการศึกษาทางด้านคอมพิวเตอร์ศึกษาจำนวน 1 คน

โครงสร้างการบริหารงานแผนกเทคโนโลยีสารสนเทศ
เนติบัณฑิตยสภา



ภาพที่ 4.2 โครงสร้างการบริหารงานแผนกเทคโนโลยีสารสนเทศ

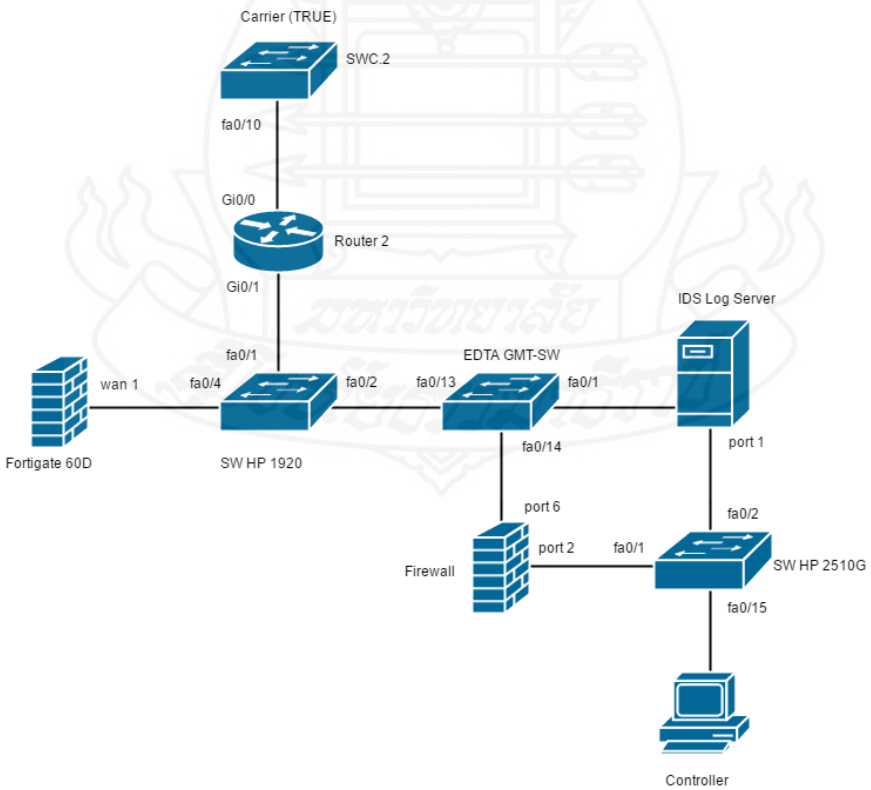
2.2 โครงสร้างพื้นฐานและทรัพยากรทางด้านเทคโนโลยีสารสนเทศ

ปัจจุบันระบบเครือข่ายภายในขององค์กรเป็นระบบเครือข่ายแบบ Fast Ethernet มีความเร็วสูงสุดที่ 100 Mbps โดยจะมีการเชื่อมต่อจากอุปกรณ์ Fast Ethernet Core Switch ที่ติดตั้งอยู่ภายในห้องส่วนงานซ่อมบำรุงระบบพลังงาน ชั้น 1 กระจายการเชื่อมต่อไปทั้ง 4ชั้น ผ่านอุปกรณ์ Fast Ethernet Distribution Switch ในแต่ละชั้น และเชื่อมต่อเข้าสู่ห้องปฏิบัติงานด้วยการพ่วงต่ออุปกรณ์ Switch หรือ Hub กันไปเป็นทอดๆ โดยอุปกรณ์ Switch ส่วนใหญ่จะติดตั้งอยู่ในพื้นที่ที่บุคคลอื่นเข้าถึงได้ และการเชื่อมต่อสายสัญญาณทั้งหมด เจ้าหน้าที่ขององค์กรเป็นผู้ติดตั้งสายสัญญาณเองในส่วนการเชื่อมต่อกับระบบเครือข่ายภายนอก

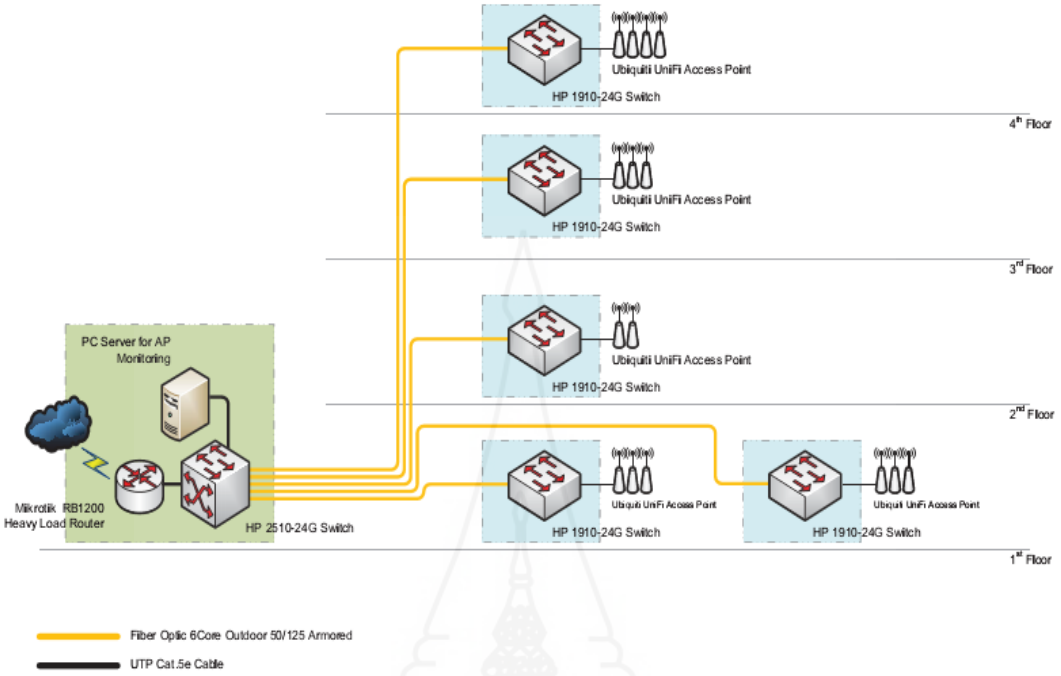
องค์กรมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตผ่านผู้ให้บริการด้วยความเร็วภายในประเทศ 100 Mbps และความเร็วภายนอกประเทศ 50 Mbps เพื่อให้บริการกับเครื่องคอมพิวเตอร์จำนวน 79 เครื่องสำหรับใช้ในการสืบค้นข้อมูล ประชาสัมพันธ์ข้อมูลต่างๆ ขององค์กรผ่านเครือข่ายอินเทอร์เน็ต

ในส่วนเครื่องแม่ข่าย (Server) ที่ให้บริการภายในองค์กรมีจำนวน 4 เครื่อง โดยแต่ละเครื่องตั้งอยู่ในแต่ละแผนกที่เป็นผู้รับผิดชอบดูแล ได้แก่ 1) ห้องควบคุมการถ่ายทอดสัญญาณ 2) แผนกทะเบียนและประเมินผล 3) แผนกห้องสมุด และ 4)แผนกทะเบียนสมาชิกและทนายความ ซึ่งการควบคุมการเข้าถึงยังไม่รัดกุม และเครื่องแม่ข่ายดังกล่าวติดตั้งอยู่ในสภาพแวดล้อมที่ไม่เหมาะสม ในส่วนเครื่องแม่ข่ายที่ให้บริการภายนอกมีจำนวน 2 เครื่อง ติดตั้งอยู่ที่บริษัทอินเทอร์เน็ต (ประเทศไทย) จำกัด (มหาชน) เป็นเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ขององค์กร และเครื่องแม่ข่ายที่ให้บริการถ่ายทอดสัญญาณการเรียนการสอนผ่านระบบอินเทอร์เน็ต โดยผู้ดูแลจะทำการส่งข้อมูลที่ต้องการถ่ายทอดผ่านระบบอินเทอร์เน็ตเข้าสู่เครื่องแม่ข่ายทุกครั้งที่มีการถ่ายทอดสัญญาณ

ในด้านการบริหารจัดการการใช้งานระบบเครือข่ายและคอมพิวเตอร์ปัจจุบัน องค์กรมีแผนกเทคโนโลยีสารสนเทศ (จัดตั้งเมื่อ พ.ศ.2559) ดูแลระบบเครือข่ายและคอมพิวเตอร์โดยตรง มีนโยบายด้านเทคโนโลยีสารสนเทศเกี่ยวกับการควบคุมการเข้าระบบเครือข่าย และคอมพิวเตอร์



ภาพที่ 4.3 ผังเครือข่ายอินเทอร์เน็ต



ภาพที่ 4.4 ผังเครือข่ายไร้สาย

2.3 ระบบเทคโนโลยีสารสนเทศภายในองค์กร

ตารางที่ 4.1 สรุประบบเทคโนโลยีสารสนเทศภายในองค์กร

กองกลาง		
แผนก	**ระบบเทคโนโลยีสารสนเทศ**	**รายละเอียด**
1. แผนกเลขาธิการ	ไม่มี	ปฏิบัติงานทางด้านธุรการให้ฝ่ายบริหารขององค์กร บันทึก จัดทำรายงาน เอกสาร หนังสือราชการใน Ms. Word และ Ms. Excel
2. แผนกทะเบียนสมาชิกและทนายความ	ระบบฐานข้อมูลทะเบียนสมาชิก	• พัฒนาเองโดย Microsoft Access 2010 • จ้างบริษัทพัฒนา (โปรแกรม TYPO (MySQL))
	ระบบขอหนังสือรับรองการเป็นสมาชิกออนไลน์	• บันทึกข้อตกลง (MOU) ระหว่างเนติบัณฑิตยสภา กับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สพธอ.

ตารางที่ 4.1 (ต่อ)

แผนก	ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
3. แผนกห้องสมุด	ระบบห้องสมุดอัตโนมัติ ELIB	• เป็นระบบเพื่อทำ Catalog ของหนังสือและเอกสารภายในห้องสมุด ใช้เพื่อให้เจ้าหน้าที่จัดเก็บข้อมูลหนังสือและสืบค้นหนังสือได้ • ปัจจุบันระบบการยืม–คืน ใช้บัตรยืมกระดาษ • บัตรสำหรับการเข้าใช้ห้องสมุดใช้บัตรที่สามารถระบุตัวตนได้ (มีรูปและเลขบัตรประชาชน)
4. แผนกประชาสัมพันธ์	ไม่มี	ปฏิบัติงานประชาสัมพันธ์และเผยแพร่งานนิทรรศการ จัดทำสื่อสิ่งพิมพ์ จุลสาร เป็นการจ้างบริษัทเอกชนรับเหมาจัดทำงานอื่นๆ ใน Ms. Word และ Ms. Excel
5. แผนกทรัพยากรบุคคล	ไม่มี	ปฏิบัติงาน HR ขององค์กรมีการบันทึกข้อมูลส่วนบุคคลของพนักงาน ตำแหน่ง วันที่บรรจุ คุณวุฒิทางการศึกษา ผลการประเมินผลงาน การทำเงินเดือน ใน Ms. Word และ Ms. Excel ทำการสำรวจเพื่อปรับปรุงข้อมูลทุกครึ่งปีงบประมาณ
6. แผนกเทคโนโลยีสารสนเทศ	เว็บไซต์เพื่อให้ข้อมูลประชาสัมพันธ์และสามารถพิมพ์แบบฟอร์มต่างๆ	เดิมมีการแยกเป็น 2 เว็บไซต์ คือ เว็บไซต์เนติบัณฑิตยสภาและเว็บไซต์สำหรับสำนักอบรมฯ ปัจจุบันมีการรวมทั้งสองเว็บไซต์เข้าด้วยกันในเบื้องต้น เป็นเว็บไซต์เดียว ที่ URL http://www.thethaibar.or.th
	ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ZANE Firewall	กำกับ ดูแล ควบคุมการใช้งานเครือข่ายไร้สาย Wi-Fi ของผู้บริหาร พนักงาน นักศึกษา และสมาชิกเนติบัณฑิตยสภา

ตารางที่ 4.1 (ต่อ)

แผนก	ระบบเทคโนโลยีสารสนเทศ	รายละเอียด
<u>กองคลัง</u>		
1. แผนกการเงิน	ระบบการออกหนังสือรับรองภาษี	เป็นซอฟต์แวร์ที่พัฒนาโดยกรมสรรพากร
	ระบบพิมพ์ใบเสร็จ	อยู่ระหว่างการดำเนินการพัฒนา
2. แผนกบัญชีและงบประมาณ	ไม่มี	มีการทำบัญชีด้วยการบันทึกด้วยมือทั้งกระบวนงาน และสำหรับค่าธรรมเนียมการศึกษาจะมีการส่งสรุปทุกวันมาจากธนาคาร แล้วทำการลงบันทึกด้วยมือ และใน Ms. Word และ Ms. Excel
3. แผนกพัสดุ	ไม่มี	มีการบันทึกหมายเลขครุภัณฑ์ใน Ms. Excel และมีการสำรวจครุภัณฑ์เพื่อปรับปรุงข้อมูลทุกปี
4. แผนกอาคาร สถานที่และสโมสร	ไม่มี	เป็นแผนกที่มีหน้าที่ความรับผิดชอบเกี่ยวกับการดูแลอาคาร สถานที่ สโมสร ดูแลและซ่อมระบบโทรศัพท์ ทำรายการใน Ms. Word และ Ms. Excel
<u>กองบริการ สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา</u>		
สำหรับกองบริการฯ มีการจัดทำระบบเพื่อบูรณาการงานของแต่ละแผนกเข้ารวมกัน ทั้ง 3 แผนก คือ - แผนกธุรการ - แผนกบริหารการศึกษา - แผนกทะเบียนและประเมินผล	ระบบบริหารจัดการฐานข้อมูลทะเบียนนักศึกษา	ระบบประกอบไปด้วย 4 ระบบย่อยได้แก่ • ระบบข้อมูลพื้นฐานและระบบรักษาความปลอดภัย • ระบบการสมัครเรียนและลงทะเบียนเรียน • ระบบการสมัครนักศึกษาใหม่และออกบัตรนักศึกษา • ระบบการสมัครสอบและระบบการจัดการฐานข้อมูลผู้สมัครสอบและผู้สอบไล่ได้ ทั้งนี้สามารถพิมพ์ใบสมัครไปชำระเงินที่ธนาคารกรุงไทย ธนาคารออมสิน ธนาคารกรุงศรีอยุธยา และเคาน์เตอร์เซอร์วิส ได้
	ระบบการถ่ายทอดสด (VDO Streaming)	มีการถ่ายทอดสดไปยังศูนย์ทั่วประเทศ มีการให้ user name และ password แก่ศูนย์ที่มีการร้องขอใช้บริการถ่ายทอดสด

ตารางที่ 4.1 (ต่อ)

กองสนับสนุน สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา		
แผนก	**ระบบเทคโนโลยีสารสนเทศ**	**รายละเอียด**
1. แผนกหนังสือคำพิพากษาฎีกาและวารสาร	ไม่มี	มีหน้าทีในการดูแลการจัดพิมพ์และจำหน่ายหนังสือคำพิพากษาฎีกาและวารสาร การรับจองและจัดส่ง
2. แผนกตำราและคำบรรยาย	ไม่มี	มีหน้าที่ในการดูแลการจัดพิมพ์และจำหน่ายหนังสือตำราและคำบรรยาย รับจองหนังสือและรับชำระเงินค่าจองฯ การส่งเงินให้กองคลัง
3. สำนักงานช่วยเหลือประชาชนทางกฎหมายแห่งเนติบัณฑิตยสภา	ระบบฐานข้อมูลการดำเนินงานช่วยเหลือประชาชนทางกฎหมายและเก็บสำนวนทางคดี	จ้างบริษัทเอกชนพัฒนา (โปรแกรม Typo)
4. ศูนย์หนังสือเนติบัณฑิตยสภา	ระบบการขายหนังสือสำเร็จรูปสำหรับรับระบบสต็อกสินค้า ข้อมูลรายการหนังสือเข้า-ออก	จ้างบริษัทเอกชนพัฒนา (โปรแกรม POS)

3. มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2013

ความแตกต่างระหว่าง ISO/IEC 27001:2005 และ ISO/IEC 27001:2013 (รายละเอียดภาคผนวก ข) ISO/IEC 27001:2005 มี 11 หัวข้อหลัก (Domain) ตัวควบคุม 133 มาตรการ (Control) และ ISO/IEC 27001:2013 มี 14 หัวข้อหลัก (Domain) การปรับลดตัวควบคุม เป็น 114 มาตรการ (Control) (รายละเอียดผนวก ค)

3.1 14 หัวข้อหลัก (Domain) ตามมาตรฐาน ISO/IEC 27001:2013 มีดังนี้

ตารางที่ 4.2 รายการ 14 หัวข้อหลัก (Domain) ตามมาตรฐาน ISO/IEC 27001:2013

14 Domain ตามมาตรฐาน ISO/IEC27001:2013			
A.5	**1**	Information security policies	นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
A.6	**2**	Organization of information security	โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
A.7	**3**	Human resource security	ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล
A.8	**4**	Asset management	การบริหารจัดการสินทรัพย์
A.9	**5**	Access control	การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
A.10	**6**	Cryptography	การเข้ารหัสข้อมูล
A.11	**7**	Physical and environmental security	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
A.12	**8**	Operations Security	ความปลอดภัยในการปฏิบัติงาน
A.13	**9**	Communications security	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
A.14	**10**	System acquisition, development and maintenance	การจัดหาระบบ การพัฒนา และการบำรุงรักษาระบบ
A.15	**11**	Supplier relationships	ความสัมพันธ์กับผู้ให้บริการภายนอก
A.16	**12**	Information security incident management	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
A.17	**13**	Information security aspects of business continuity management	ประเด็นความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
A.18	**14**	Compliance	ความสอดคล้อง

3.2 มาตรการควบคุมความมั่นคงปลอดภัย (Control) ตามมาตรฐาน ISO/IEC 27001:2013 มีการปรับเพิ่มขึ้น 8 มาตรการควบคุม ดังตารางด้านล่างนี้

ตารางที่ 4.3 มาตรการควบคุมตามมาตรฐาน ISO/IEC 27001:2013 ที่ปรับเพิ่มขึ้นใหม่

New Control			
A.6 Organization of information security	1	A.6.1 **A.6.1.5**	Internal organization **Information security in project management**
A.14 System acquisition, development and maintenance	2	A.14.2 **A.14.2.1**	Security in development and support processes **Secure development policy**
	3	**A.14.2.5**	**Secure system engineering ring principles**
	4	**A.14.2.6**	**Secure development environment**
	5	**A.14.2.8**	**System security testing**
A.15 Supplier relationships	6	A.15.1 **A.15.1.3**	Information security in supplier relationship **Information and communication technology supply chain**
A.16 Information security incident management	7	A.16.1 **A.16.1.4**	Management of information security incidents and improvements **Assessment of and decision on information security events**
A.17 Information security aspects of business continuity management	8	A.17.2 **A.17.2.1**	Redundancies **Availability of information processing facilities**

4. ความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กร

ผลการศึกษาความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบันมีความสอดคล้องกับมาตรฐาน ISO/IEC27001:2005 และกฎหมายอื่นที่เกี่ยวข้อง สรุปได้ ดังตารางด้านล่างนี้ (รายละเอียดผนวก ง)

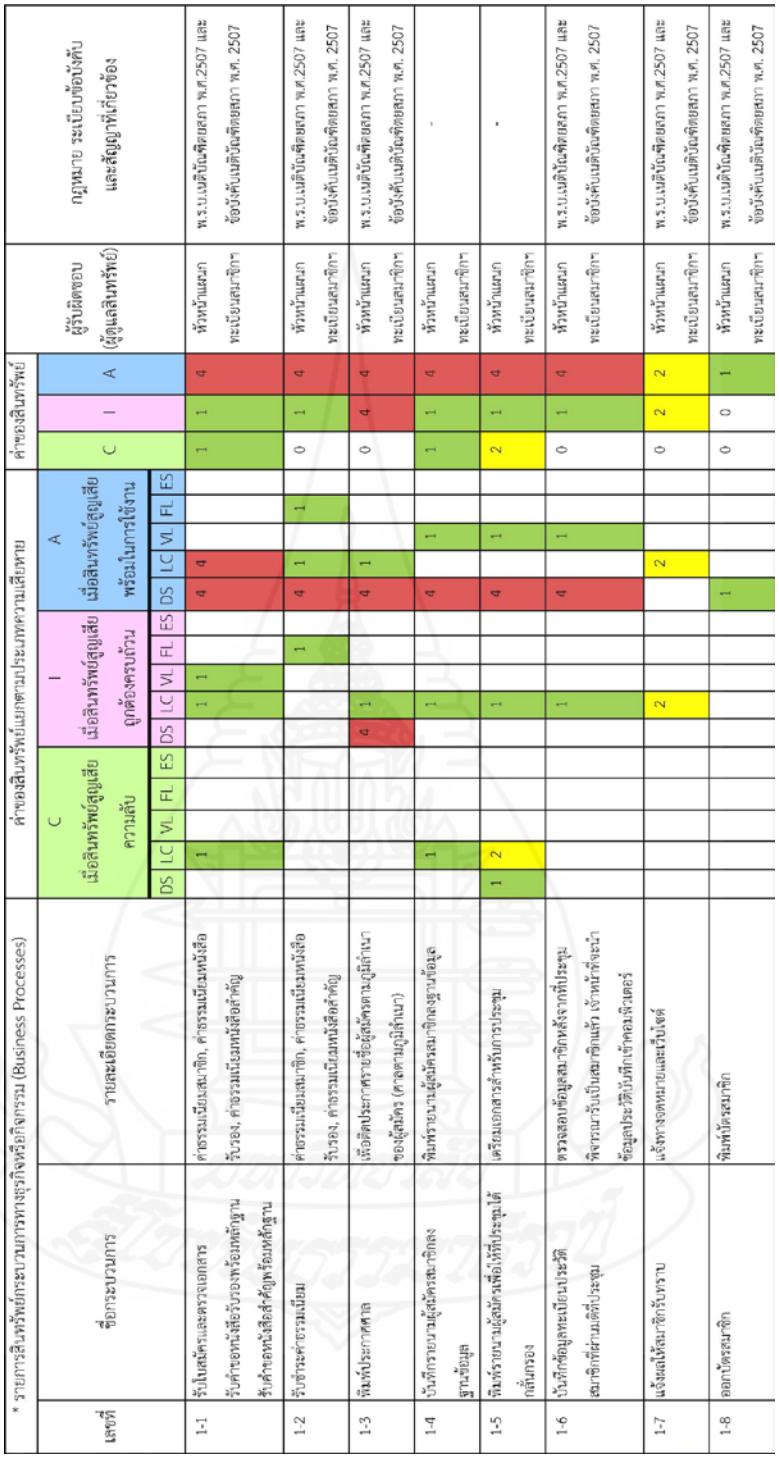
ตารางที่ 4.4 ความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กรในปัจจุบัน

	ISO/IEC27001:2005	กฎหมายอื่นที่เกี่ยวข้อง	
ความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศของเนติบัณฑิตยสภา	✓ สอดคล้องตามมาตรฐาน ISO/IEC 27001:2005	พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

5. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

5.1 การจัดทำทะเบียนสินทรัพย์ และกำหนดมูลค่าของสินทรัพย์ (Asset Identification and Valuation)

โดยใช้เครื่องมือในบทที่ 3 ตามภาพที่ 3.3 ได้ผลลัพธ์ดังตัวอย่างตามตารางด้านล่างนี้ (รายละเอียดผนวก จ)

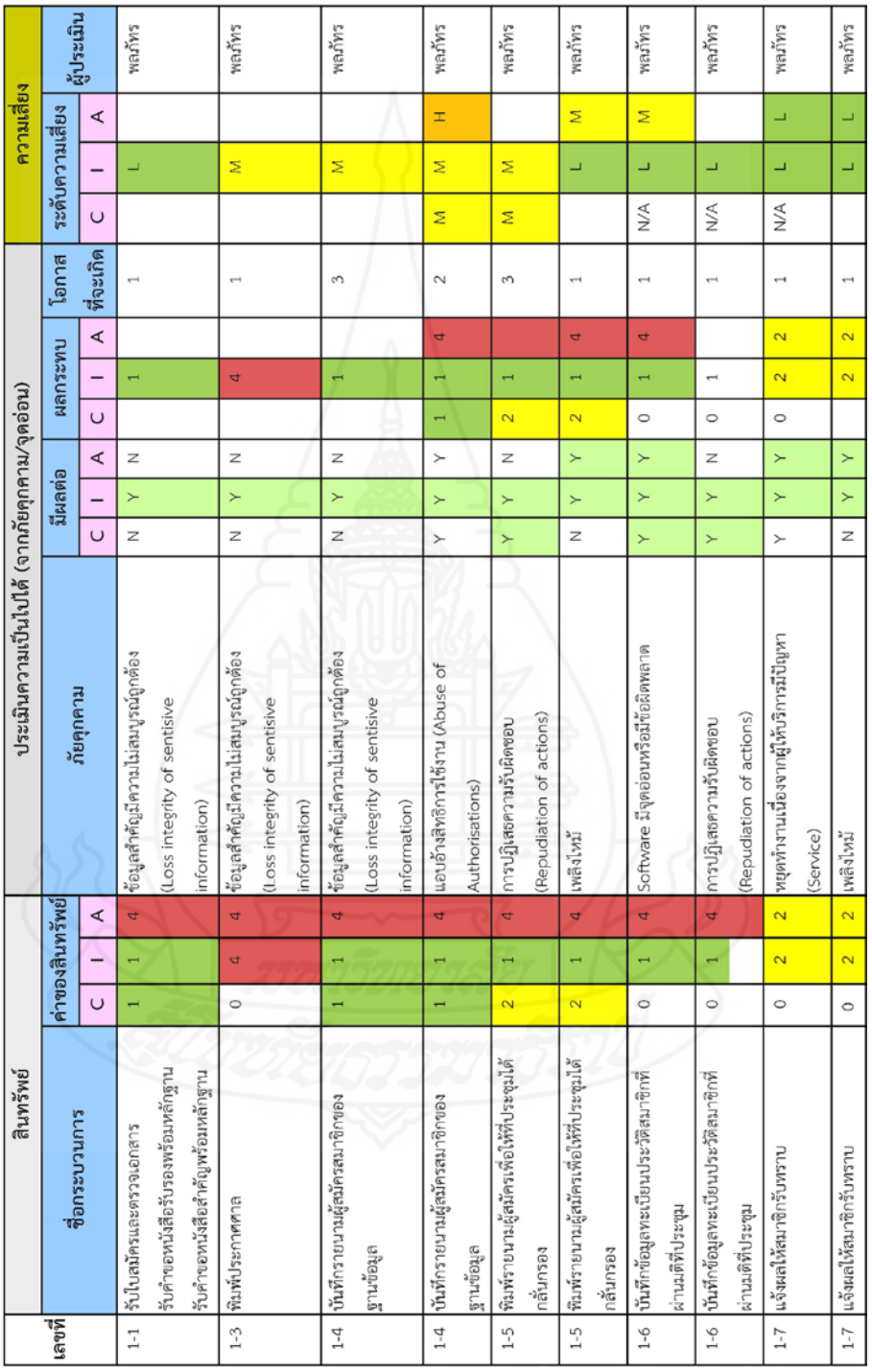


* รายการสินทรัพย์กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)			ค่าของสินทรัพย์ในแง่มุมความประสงค์ความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ						I เมื่อสินทรัพย์สูญเสียถูกต้องครบถ้วน						A เมื่อสินทรัพย์สูญเสียพร้อมในการใช้งาน						C	I	A		
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS					
1-1	รับใบสั่งและตรวจเอกสารรับคำขอหนังสือรับรองพร้อมหลักฐานสั่งคำขอหนังสือสำคัญพร้อมหลักฐาน	ค่าธรรมเนียมสมาชิก, ค่าธรรมเนียมหนังสือรับรอง, ค่าธรรมเนียมหนังสือสำคัญ		1					1	1			4	4					1	1	4	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507
1-2	รับชำระค่าธรรมเนียม	ค่าธรรมเนียมสมาชิก, ค่าธรรมเนียมหนังสือรับรอง, ค่าธรรมเนียมหนังสือสำคัญ									1		4	1		1			0	1	4	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507
1-3	พิมพ์ประกาศนียบัตร	เลือกดีดประกาศรายชื่อผู้สมัครตามภูมิลำเนาของผู้สมัคร (ตามตามภูมิลำเนา)						4	1				4	1					0	4	4	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507
1-4	บันทึกรายงานผู้สมัครสมาชิกลงฐานข้อมูล	พิมพ์รายงานผู้สมัครสมาชิกลงฐานข้อมูล		1					1				4		1				1	1	4	หัวหน้างานทะเบียนสมาชิก	-
1-5	พิมพ์รายงานผู้สมัครเพื่อให้ที่ประชุมได้กลั่นกรอง	เตรียมเอกสารสำหรับการประชุม	1	2					1				4		1				2	1	4	หัวหน้างานทะเบียนสมาชิก	-
1-6	บันทึกข้อมูลหลังเปิดประชุมใช้สมาชิกที่เข้าประชุม	ตรวจสอบข้อมูลสมาชิกหลังจากที่ประชุมพิจารณาว่าเป็นสมาชิกแล้ว เจ้าหน้าที่จะนำข้อมูลประวัติบันทึกเข้าคอมพิวเตอร์							1				4		1				0	1	4	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507
1-7	แจ้งผลให้สมาชิกรับทราบ	แจ้งทางจดหมายและเว็บไซต์							2					2					0	2	2	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507
1-8	ออกบัตรสมาชิก	พิมพ์บัตรสมาชิก											1						0	0	1	หัวหน้างานทะเบียนสมาชิก	พ.ร.บ.เมล็ดพืชพันธุ์ พ.ศ.2507 และข้อบังคับเมล็ดพืชพันธุ์ พ.ศ. 2507

ตารางที่ 4.5 ทะเบียนสินทรัพย์และมูลค่าของสินทรัพย์ (Asset Identification and Valuation)

5.2 ผลการประเมินความเสี่ยงของสินทรัพย์ (Asset Risk Assessment)

โดยใช้เครื่องมือในบทที่ 3 ตามภาพที่ 3.8 ได้ผลลัพธ์ดังตัวอย่างตามตารางด้านล่างนี้ (รายละเอียดผนวก ฉ)



เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม/จุดอ่อน)									ความเสี่ยง				
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-1	รับใบสมัครและตรวจเอกสาร รับคำขอหนังสือรับรองพร้อมหลักฐาน รับคำขอหนังสือสำคัญพร้อมหลักฐาน	1	1	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		1		1		L		พลภัทร
1-3	พิมพ์ประกาศศาล	0	4	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		4		1		M		พลภัทร
1-4	บันทึกรายงานผู้สมัครสมาชิกของฐานข้อมูล	1	1	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		1		3		M		พลภัทร
1-4	บันทึกรายงานผู้สมัครสมาชิกของฐานข้อมูล	1	1	4	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	1	1	4	2	M	M	H	พลภัทร
1-5	พิมพ์รายงานผู้สมัครเพื่อให้ที่ประชุมได้กลั่นกรอง	2	1	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	1		3	M	M		พลภัทร
1-5	พิมพ์รายงานผู้สมัครเพื่อให้ที่ประชุมได้กลั่นกรอง	2	1	4	เพลิงไหม้	N	Y	Y	2	1	4	1		L	M	พลภัทร
1-6	บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ผ่านมติที่ประชุม	0	1	4	Software มีจุดอ่อนหรือมีข้อผิดพลาด	Y	Y	Y	0	1	4	1	N/A	L	M	พลภัทร
1-6	บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ผ่านมติที่ประชุม	0	1	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	1		1	N/A	L		พลภัทร
1-7	แจ้งผลให้สมาชิกรับทราบ	0	2	2	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา (Service)	Y	Y	Y	0	2	2	1	N/A	L	L	พลภัทร
1-7	แจ้งผลให้สมาชิกรับทราบ	0	2	2	เพลิงไหม้	N	Y	Y		2	2	1		L	L	พลภัทร

ตารางที่ 4.6 การประเมินความเสี่ยงของสินทรัพย์ (Asset Risk Assessment)

6. พัฒนาเว็บแอปพลิเคชันระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

ฟังก์ชั่นการทำงานของระบบ

6.1 ระบบบริหารจัดการการเข้าใช้งาน

6.1.1 สำหรับผู้ใช้งานทั่วไป

1) ระบบสามารถแสดงรายละเอียดมาตรการควบคุมตามมาตรฐาน ISO/IEC 27001:2013 Annex A (A.5 – A.18) (Control 114 items)

2) ระบบสามารถดาวน์โหลดข้อมูล เกี่ยวกับวัตถุประสงค์นโยบายแนวปฏิบัติและกฎหมายข้อบังคับของรัฐที่เกี่ยวข้อง

3) ผู้ใช้งานทั่วไปสามารถร้องขอการลงทะเบียน เพื่อเข้าใช้งานระบบเฉพาะผู้ที่ได้ทำการลงทะเบียนแล้ว

6.1.2 สำหรับผู้ใช้งานที่ลงชื่อเข้าใช้งาน

1) ผู้ใช้งานต้องทำการลงทะเบียนเพื่อเข้าใช้งานระบบและต้องได้รับการอนุญาตจากผู้ดูแลระบบหรือผู้มีอำนาจอนุญาตก่อนเข้าใช้งาน

2) ผู้ที่ได้รับอนุญาตต้องลงชื่อเข้าใช้ระบบทุกครั้งที่ทำการใช้งานและออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลาเกิน 15 นาที

6.2 ระบบการควบคุมความมั่นคงปลอดภัย สำหรับผู้ใช้งานที่ลงทะเบียนเข้าใช้งานระบบแสดงหน้าหลัก 3 ส่วนคือ Control List, Assessment of Control และ Download

6.2.1 หน้า Control List

ระบบแสดงรายละเอียด ตามมาตรการควบคุมและเอกสารที่เกี่ยวข้องที่สอดคล้องกับมาตรฐานISO/IEC 27001: 2013 โดยแบ่งหัวข้อการแสดงผลอย่างชัดเจนตามมาตรการควบคุมหลัก 14 หัวข้อ (A.5 ถึง A.18)

6.2.2 หน้า Assessment of Control

ระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 มีมาตรการควบคุมหลัก 4 ข้อและมาตรการควบคุมย่อย 14 ข้อ โดยผู้ใช้งานสามารถทำการ Checklistรายการสินทรัพย์ (กระบวนการทางธุรกิจ, ข้อมูล, ซอฟต์แวร์, ฮาร์ดแวร์, บุคลากร และโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร) และระดับความเสี่ยงที่ได้จากการประเมิน ความเสี่ยง (Low, Moderate, High และ Very High) ซึ่งการควบคุมที่มี

เอกสารระบุมาตรการควบคุมพร้อมแนวปฏิบัติ(ระบบสามารถแนบเอกสารได้) และพนักงานปฏิบัติตามมาตรการเป็นส่วนของการคิดค่าคะแนนตามระดับความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ

6.2.3 เกณฑ์ประเมินความสอดคล้องความมั่นคงปลอดภัยมี 4 ระดับ

ในแต่ละมาตรการควบคุมย่อย ผู้ใช้สามารถทำประเมินได้โดยง่ายโดยคิดจากระดับความเสี่ยง (Low, Moderate, High และ Very High) การมีเอกสารระบุมาตรการควบคุมพร้อมแนวปฏิบัติแนบ และพนักงานในองค์กรปฏิบัติตามมาตรการ เกณฑ์ควบคุมมี 4 ระดับ ดังนี้

1) ระดับความเสี่ยงสูงมาก (VH = Very High)

(1) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และพนักงานปฏิบัติตามมาตรการ ผลการควบคุม 100% แสดงสีเขียว

(2) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และ พนักงานไม่ปฏิบัติตามมาตรการ ผลการควบคุม 20% แสดงสีเหลือง

(3) ปัจจุบันองค์กรไม่มีมาตรการควบคุม การควบคุม 0% แสดงสีแดง

2) ระดับความเสี่ยงสูง (H = High)

(1) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และ พนักงานปฏิบัติตามมาตรการ ผลการควบคุม 100% แสดงสีเขียว

(2) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และพนักงานไม่ปฏิบัติตามมาตรการ ผลการควบคุม 40% แสดงสีเหลือง

(3) ปัจจุบันองค์กรไม่มีมาตรการควบคุม การควบคุม 0% แสดงสีแดง

3) ระดับความเสี่ยงปานกลาง (M = Moderate)

(1) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และพนักงานปฏิบัติตามมาตรการ ผลการควบคุม 100% แสดงสีเขียว

(2) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร)และพนักงานไม่ปฏิบัติตามมาตรการ ผลการควบคุม 60% แสดงสีเหลือง

(3) ปัจจุบันองค์กรไม่มีมาตรการควบคุม การควบคุม 0% แสดงสีแดง

4) ระดับความเสี่ยงที่ต่ำ (L = Low)

(1) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และพนักงานปฏิบัติตามมาตรการ ผลการควบคุม 100% แสดงสีเขียว

(2) ปัจจุบันองค์กรมีมาตรการควบคุม (แนบเอกสาร) และพนักงานไม่ปฏิบัติตามมาตรการ ผลการควบคุม 80% แสดงสีเหลือง

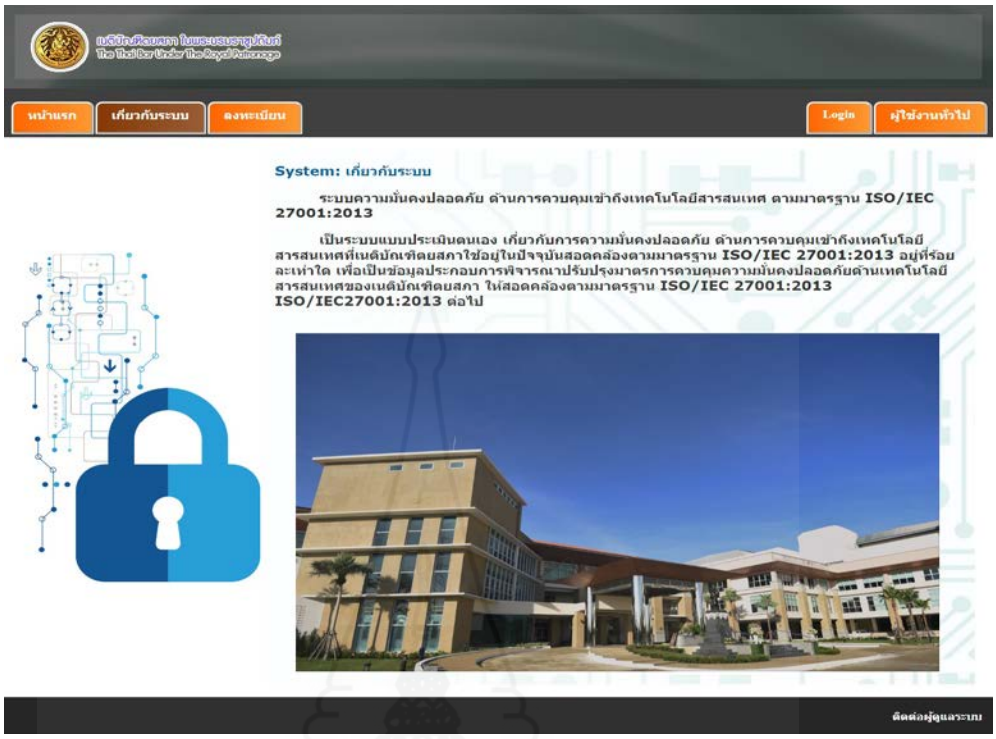
(3) ปัจจุบันองค์กรไม่มีมาตรการควบคุม การควบคุม 0% แสดงสีแดง

6.2.4 หน้า Download

ระบบแสดงรายละเอียด เอกสารตามมาตรการควบคุม ได้แก่ มาตรการควบคุมความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013 นโยบาย แนวปฏิบัติและแบบฟอร์มที่เกี่ยวข้อง โดยสามารถดาวน์โหลดและสามารถพิมพ์ออกทางเครื่องพิมพ์ได้

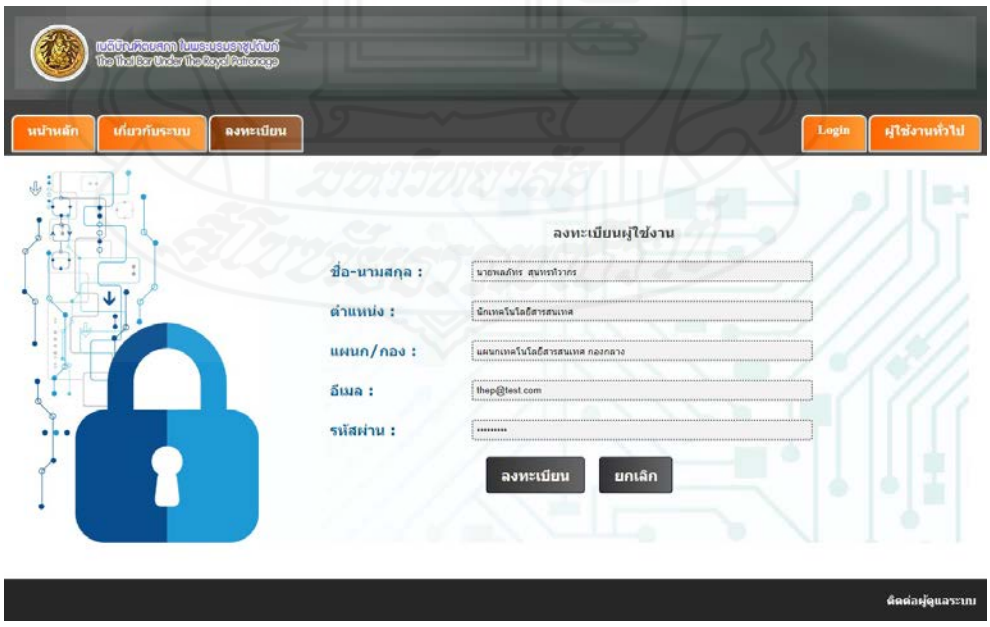
ภาพที่ 4.5 หน้าหลักระบบความมั่นคงปลอดภัย

ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013



ภาพที่ 4.6 หน้าเกี่ยวกับระบบความมั่นคงปลอดภัย

ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013

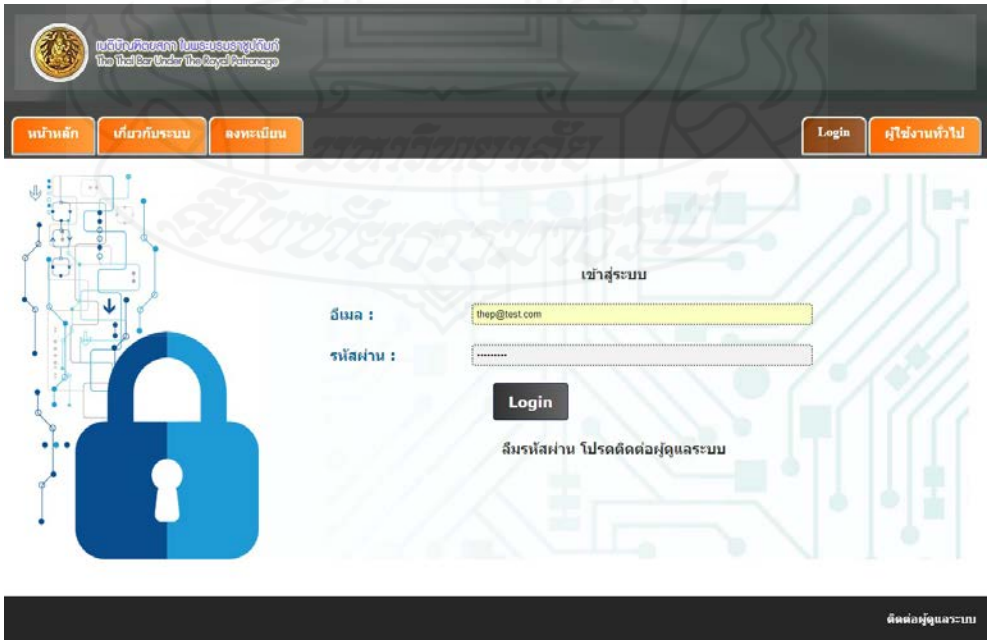


ภาพที่ 4.7 หน้าลงทะเบียนผู้ใช้งาน

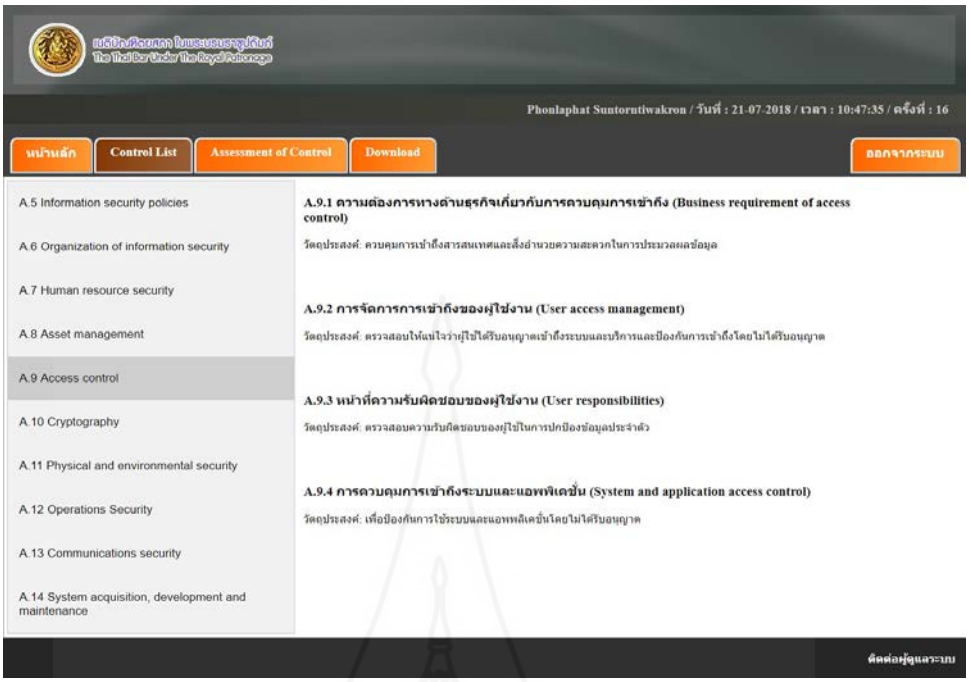
เป็นส่วนของการลงทะเบียนเพื่อให้สามารถเข้าสู่ระบบความมั่นคงปลอดภัย โดยที่ให้ผู้ใช้งานใส่ข้อมูลให้ครบถ้วนเมื่อใส่ข้อมูลเรียบร้อยแล้ว คลิกที่ “**ลงทะเบียน**”

ภาพที่ 4.8 หน้าผู้ใช้งานทั่วไป

แสดงมาตรการควบคุมความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001:2013

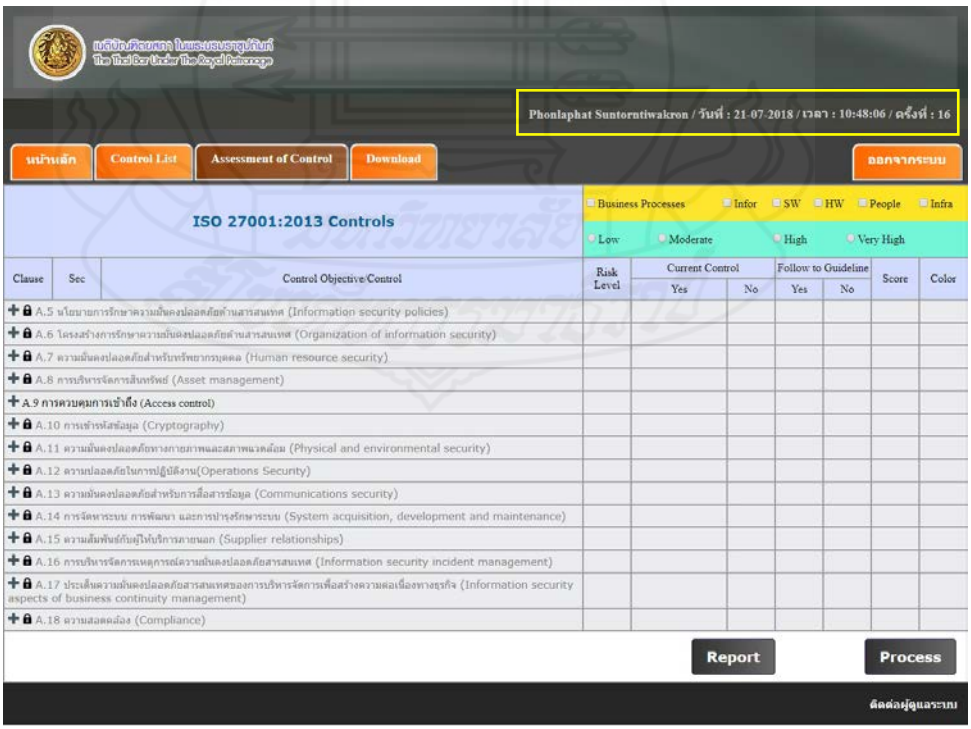


ภาพที่ 4.9 หน้าลงชื่อเข้าสู่ระบบในการเข้าสู่ระบบฯ ต้องใส่ข้อมูลอีเมลและรหัสผ่าน



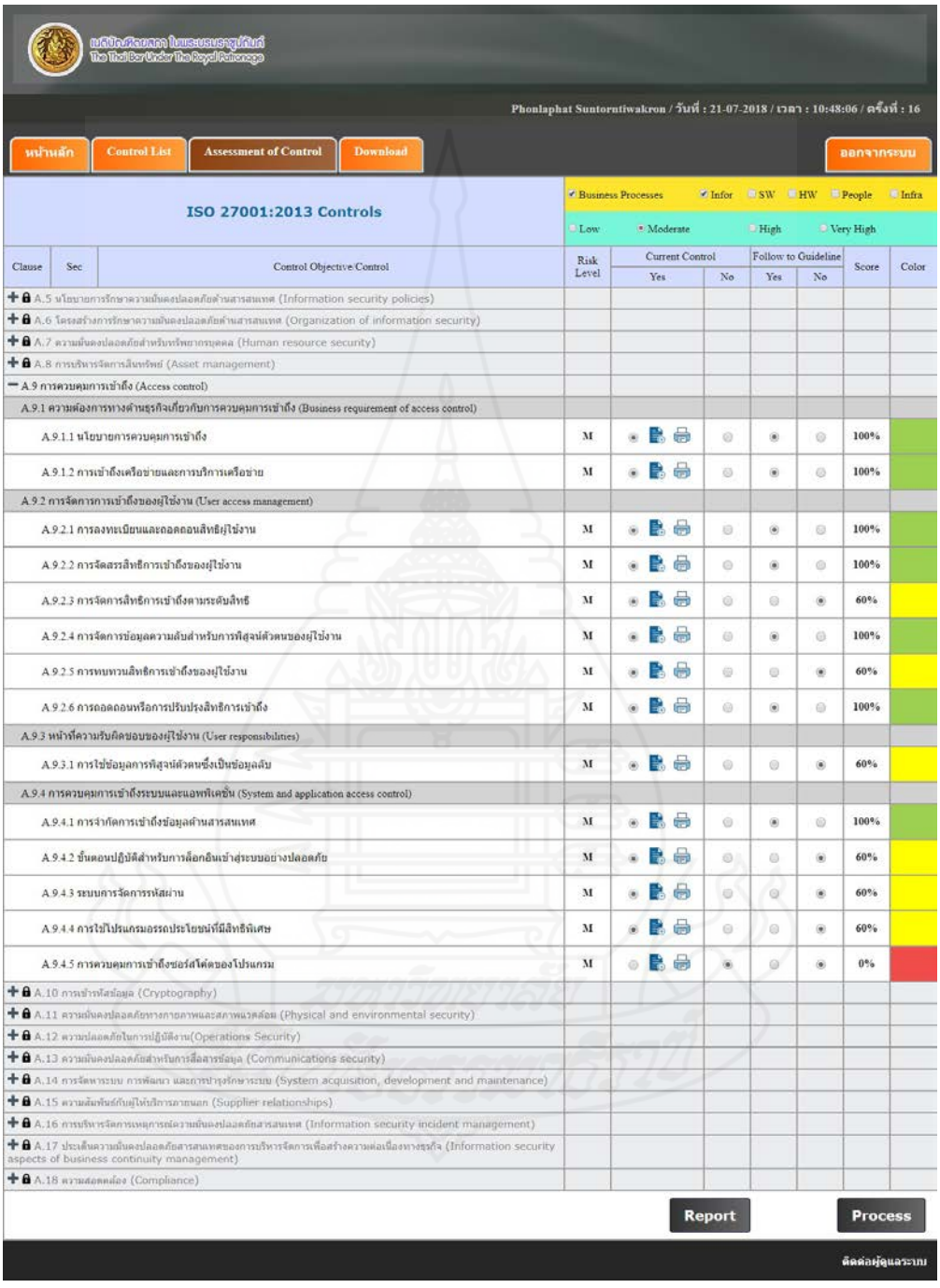
ภาพที่ 4.10 หน้าเมนู Control List

แสดงการควบคุมความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC27001: 2013 (A.5 ถึง A.18)



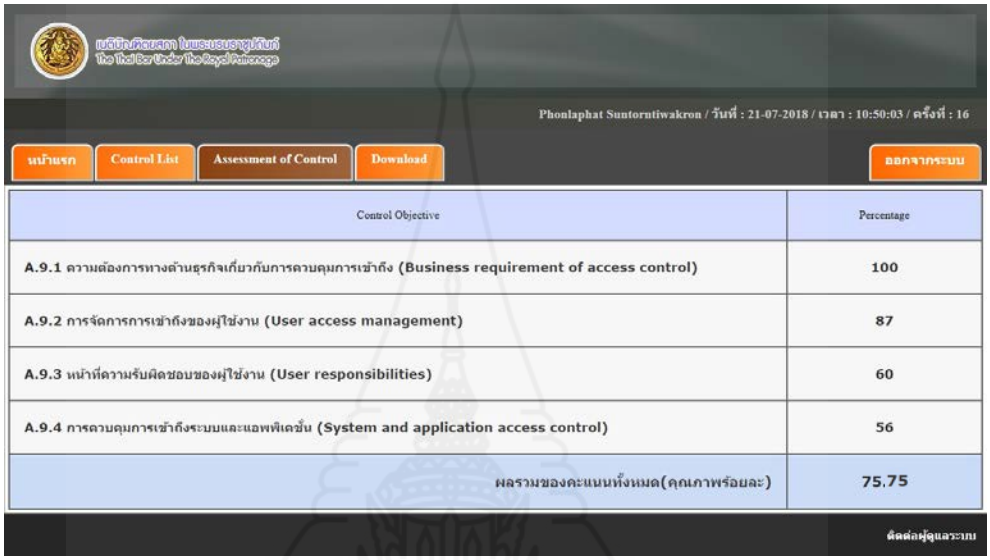
ภาพที่ 4.11 หน้าเมนู Assessment of Control

แสดงเมนูการควบคุมความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC27001: 2013 (A.5 ถึง A.18)



ภาพที่ 4.12 หน้าการทำงานของ เมนู Assessment of Control

แสดงการประเมินมาตรการควบคุมความมั่นคงปลอดภัย เฉพาะด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Access Control) โดยผู้ใช้สามารถเลือกตามข้อมูลข้างต้น เมื่อใส่ข้อมูลเรียบร้อยแล้ว ให้คลิกที่ **“Process”** โดยระบบจะทำการประมวลผลคะแนนคุณภาพร้อยละในแต่ละหัวข้อ



Total Summary Access Control Assessment (ISO/IES 27001:2013) = **75.75%**

ภาพที่ 4.13 หน้ารายงานประเมินผลมาตรการควบคุมความมั่นคงปลอดภัย

ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ (Access Control)

ภาพที่ 4.14 หน้าเมนู Download

ระบบแสดงรายละเอียด เอกสารตามมาตรการควบคุม ได้แก่ มาตรการควบคุมความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001: 2013 นโยบายทางเทคโนโลยีสารสนเทศขององค์กร แนวปฏิบัติทางเทคโนโลยีสารสนเทศขององค์กร และแบบฟอร์มที่เกี่ยวข้อง โดยสามารถดาวน์โหลดและสามารถพิมพ์ออกทางเครื่องพิมพ์ได้

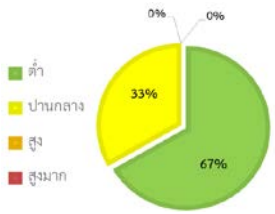
บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

1. สรุปผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศตามหลัก CIA Triad

หลังจากที่มีการพัฒนาระบบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงได้ทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรทำให้ทราบถึงสถานะความเสี่ยงขององค์กรว่าอยู่ในระดับต่ำถึงปานกลาง โดยได้พบความเสี่ยงขององค์กรในแต่ละด้าน ดังตารางด้านล่างนี้

ตารางที่ 5.1 ระดับความเสี่ยงในแต่ละด้านขององค์กร

ระดับความเสี่ยง / สินทรัพย์สารสนเทศ	ต่ำ (L)			ปานกลาง (M)			สูง (H)			สูงมาก (VH)			ระดับความเสี่ยง
	C	I	A	C	I	A	C	I	A	C	I	A	
1. กระบวนการทางธุรกิจ	3	**7**	5	3	8	**11**	**4**	0	1	0	0	0	**M**
(Business Processes)		7			11 (max)			4			0		
2. ข้อมูล	**10**	2	3	5	10	**14**	**2**	0	0	0	0	0	**M**
(Information)		10			14 (max)			2			0		
3. ซอฟต์แวร์	1	1	**9**	0	0	**5**	0	0	0	0	0	0	**L**
(Software)		9 (max)			5			0			0		
4. ฮาร์ดแวร์	1	12	**20**	3	2	**6**	0	0	0	0	0	0	**L**
(Hardware)		20 (max)			6			0			0		
5. บุคลากร	4	4	**11**	1	1	**5**	0	0	3	0	0	0	**L**
(People)		11 (max)			5			3			0		
6. บริการโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานขององค์กร(Infrastructure)	0	0	**12**	0	3	**6**	0	0	0	0	0	0	**L**
		12 (max)			6			0			0		



ภาพที่ 5.1 ภาพรวมระดับความเสี่ยงขององค์กร

2. สรุปผลการประเมินความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ขององค์กร

การพัฒนาระบบความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ที่จัดทำขึ้นเพื่อเป็นต้นแบบในการประเมินความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001: 2013 รายละเอียดในบทที่ 4 ได้ทำการทดลองใช้งานโดยเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศขององค์กร ระบบสามารถใช้งานได้และสามารถประมวลผลได้ตามความต้องการ แต่มีข้อจำกัด ซึ่งระบบสามารถประเมินเบื้องต้นได้ว่า เมื่อทราบระดับความเสี่ยงที่เกิดขึ้นแล้ว ปัจจุบันองค์กรมีเอกสารระบุมาตรการควบคุมความมั่นคงปลอดภัยพร้อมแนวปฏิบัติ และพนักงานปฏิบัติตามมาตรการควบคุมร้อยละเท่าใด

ผู้บริหารต้องมีการตรวจคุณภาพของเอกสารระบุมาตรการควบคุมความมั่นคงปลอดภัย และการปฏิบัติตามของพนักงานในปัจจุบันอีกครั้ง เมื่อทำการทดสอบประเมินความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ขององค์กร พบว่าความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐาน ISO/IEC 27001: 2013 อยู่ที่ร้อยละ 75.75 (ระดับดี) สรุปได้ดังตารางด้านล่างนี้

ตารางที่ 5.2 ผลการประเมินมาตรการความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศขององค์กร

ความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013	ระดับการยอมรับความเสี่ยง	ผลการประเมินการควบคุม (คุณภาพร้อยละ)	แปลความ		
			สอดคล้อง	ไม่สอดคล้อง	ปรับปรุง
1. ความต้องการทางด้านธุรกิจเกี่ยวกับการควบคุมการเข้าถึง (Business requirement of access control)	M	100	✓		
2. การจัดการการเข้าถึงของผู้ใช้งาน (User access management)	M	87		✓	✓
3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	M	60		✓	✓
4. การควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (System and application access control)	M	56		✓	✓
	คุณภาพร้อยละ	**75.75**		✓	✓

รายละเอียดความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศที่ต้องปรับปรุงเพื่อให้สอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 ดังตารางด้านล่างนี้

ตารางที่ 5.3 รายละเอียดความมั่นคงปลอดภัยด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศที่ต้องปรับปรุง

ลำดับ	มาตรการควบคุม	คุณภาพร้อยละ	ส่วนที่ต้องปรับปรุง
1.	**ความต้องการทางด้านธุรกิจเกี่ยวกับการควบคุมการเข้าถึง (Business requirement of access control)**	**100**	
1.1	นโยบายการควบคุมการเข้าถึง (Access control policy)	100	

ตารางที่ 5.3 (ต่อ)

ลำดับ	มาตรการควบคุม	คุณภาพ ร้อยละ	ส่วนที่ต้องปรับปรุง
1.2	การเข้าถึงเครือข่ายและการบริการเครือข่าย (Access to networks and network services)	100	
2.	**การจัดการการเข้าถึงของผู้ใช้งาน (User access management)**	87	
2.1	การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)	100	
2.2	การจัดสรรสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)	100	
2.3	การจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
2.4	การจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	100	
2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
2.6	การถอดถอนหรือการปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)	100	
3.	**หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)**	**60**	
3.1	การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
4.	**การควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (System and application access control)**	**56**	
4.1	การจำกัดการเข้าถึงข้อมูลด้านสารสนเทศ (Information access restriction)	100	

ตารางที่ 5.3 (ต่อ)

ลำดับ	มาตรการควบคุม	คุณภาพร้อยละ	ส่วนที่ต้องปรับปรุง
4.2	ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าสู่ระบบอย่างปลอดภัย(Secure log-on procedures)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
4.3	ระบบการจัดการรหัสผ่าน (Password management system)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
4.4	การใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษ (Use of privileged utility programs)	60	- มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ - พนักงานไม่ปฏิบัติตามมาตรการ
4.5	การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)	**0**	- ไม่มีเอกสารระบุมาตรการควบคุมและแนวปฏิบัติ

การประเมินตนเองตามระบบดังกล่าว เมื่อระบบทำการสรุปผลออกมาเป็นรายงาน ทำให้องค์กรมีแนวทางการปรับปรุงการควบคุมความมั่นคงปลอดภัย ด้านการควบคุมเข้าถึงเทคโนโลยีสารสนเทศได้อย่างเหมาะสมและสอดคล้องตามมาตรฐาน ISO/IEC 27001: 2013

3. ข้อเสนอแนะ

3.1 เพื่อให้เกิดการพัฒนาอย่างต่อเนื่องต้องมีการกำหนดแผนการประเมินความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อทราบสถานะความเสี่ยงให้เป็นปัจจุบัน

3.2 การพัฒนาระบบความมั่นคงปลอดภัยให้ครอบคลุมทุกมาตรการควบคุมความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001: 2013

3.3 เทคโนโลยีมีการพัฒนาอย่างต่อเนื่องและรวดเร็ว ดังนั้นนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต้องมีการพัฒนาและปรับปรุงให้เหมาะสมอยู่เสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ

บรรณานุกรม

บรรณานุกรม

จิรพร สุเมธีประสิทธิ์, มัทธนา พิพิธเนาวรัตน์, กิตติพันธ์ คงสวัสดิ์เกียรติ. (2556). *การบริหารความเสี่ยงอย่างมืออาชีพ*. (พิมพ์ครั้งที่ 2). กรุงเทพฯ: แมคกรอ-ฮิล.

ชุลีกร นวลสมศรี, ดร.สุทธิศักดิ์ จันทรวงษ์โส. (2560). "การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใต้มาตรฐาน ISO27001:2013 กรณีศึกษาขององค์กรด้านการบินแห่งหนึ่ง". *วารสารวิจัย มหาวิทยาลัยขอนแก่น,* 17 (4). สืบค้นจาก https://tci-thaijo.org/index.php/gskku/article/view/102213

ณัทรัฏฐ์ มณีรัสยากร,รุ่งโรจน์ โชคงามวงศ์, บรรจง หะรังษี. (2559). *การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001 ของ บมจ.เซ็กโก้ เอ็นจิเนียริ่ง แอน คอนสตรัคชั่น*. (สารนิพนธ์ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพมหานคร.

ธนวรรธน์ ว่องพิบูลย์, รุ่งโรจน์ โชคงามวงศ์, บรรจง หะรังษี. (2559). *การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและบริหารความเสี่ยง ภายใต้มาตรฐาน ISO27001:2013 กรณีศึกษา บริษัทแปซิฟิค เฮลธ์แคร์ (ไทยแลนด์) จำกัด* (รายงานสารนิพนธ์ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพมหานคร.

รุ่งอรุณ นิรันต์เรือง, วิภา เจริญภัณฑารักษ์. (2557). *การพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ ด้านการควบคุมการเข้าถึงระบบสารสนเทศ* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี.

สุรชาติ จันทสุวรรณ, วิภา เจริญภัณฑารักษ์, สันติพัฒน์ อรุณธารี. (2559). *ระบบประเมินตนเองด้านเทคโนโลยีสารสนเทศ ของบริษัทจดทะเบียนในกลุ่มทรัพยากรตามกรอบโคบิตเพื่อเตรียมความพร้อมในการเข้าตลาดหลักทรัพย์ เอ็ม เอ ไอ แห่งประเทศไทย* (รายงาน (วิทยานิพนธ์ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยสุโขทัยธรรมาธิราช, นนทบุรี.

อัจฉรา เวียงสิมา, สุรณพีร์ ภูมิวุฒิสาร, ศุภกร กังพิสดาร. (2559). *การทบทวนและพัฒนานโยบายการบริหารจัดการความมั่นคงของระบบสารสนเทศภายใต้มาตรฐาน*

ISO/IEC27001:2013. (รายงานสารนิพนธ์ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพมหานคร.

บริษัท BSI Group (Thailand) จำกัด. (2559). *มาตรฐาน ISO/IEC 27001 สารสนเทศเพื่อการจัดการด้านความปลอดภัย*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO-IEC-27001-client-manual-UK-EN.pdf

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานกระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคม. (2555). *ความเป็นมาคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์*. ค้นเมื่อ 5 มกราคม 2561. จาก http://www.etcommission.go.th/etc-backgroud.html

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2555). *การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.etda.or.th/files/1/files/129-191.PDF

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2550). *พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549*. สืบค้นเมื่อ 5 มกราคม 2561. จากhttps://www.etda.or.th/content_files/2/files/decree-defines-rules-procedures-electronic-government-transactions-2549.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2553). *พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.etda.or.th/files/1/files/18.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2553). *ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรของรัฐ พ.ศ. 2553*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.etda.or.th/files/1/files/16.pdf

บริษัท BSI Group (Thailand) จำกัด. (2557). *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide- UK-EN-pdf.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2555). *มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.etda.or.th/files/1/files/129-191.PDF

บริษัท BSI Group (Thailand) จำกัด. (2557). *ภาพรวม ข้อกำหนดระบบการจัดการ ISO/IEC 27001:2013*. สืบค้นเมื่อ 5 มกราคม 2561. จาก https://www.bsigroup.com/en-TH/ISOIEC-27001-Information-Security/article-27001/overview-27001/

Bundesamt für Sicherheit in der Informationstechnik. (2554). *Supplement to BSI-Standard 100-3, Version 2.5 Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses*. สืบค้นเมื่อ 11 มกราคม 2561. จากhttps://www.bsi.bund.de/SharedDocs/Downloads/ EN/BSI/Grundschutz/download/supplement_to_100-3.pdf?__blob=publicationFile&v=1

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. (2560). *คู่มือบริหารความเสี่ยง สวทช. ตามกรอบมาตรฐานบริหารความเสี่ยง ISO 31000:2009 เวอร์ชั่น 5.2 (2561)*. สืบค้นเมื่อ 21 พฤษภาคม 2561. จากhttp://waa.inter.nstda.or.th/stks/pub/2018/20180507-enterprise-risk- management-2561.pdf

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2559). *แผนบริหารความเสี่ยง สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. 2559*. สืบค้นเมื่อ 21 พฤษภาคม 2561. จากhttp://www.mdes.go.th/assets/portals/1/files/590816_%E0%B9%81%E0%B8%9C%E0%B8%99%E0%B8%9A%E0%B8%A3%E0%B8%B4%E0%B8%AB%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%AA%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%87.pdf

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่. (2556). *Introduction to Web Application Development*. สืบค้นเมื่อ 22 มิถุนายน 2561. จาก http://www.cs.science.cmu.ac.th/course/204202/lib/exe/fetch.php?media=lec04_intro_to_webapp.pdf

ภาณุพงศ์ ปัญญาดี. (2561). *AppServ: Apache+PHP+MySQL*. สืบค้นเมื่อ 22 มิถุนายน 2561. จาก https://www.appserv.org/th/

ภาคผนวก

ภาคผนวก ก

รายการภัยคุกคามและมติด้าน CIA Triad

รายการภัยคุกคามและมติด้าน CIA

ที่มา Overview of the elementary threats ของ supplement to BSI Standard 100-3, Version 2.5

	ชื่อภัยคุกคาม	Confidentiality	Integrity	Availability
T0.01	เพลิงไหม้	N	Y	Y
T0.02	สภาพอากาศที่ไม่เป็นใจ	N	Y	Y
3	ความเสียหายจากน้ำ	N	Y	Y
4	ฝุ่น สนิม มลพิษ	N	Y	Y
5	ภัยธรรมชาติ	N	N	Y
6	สภาพแวดล้อมที่เป็นพิษ	N	N	Y
7	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง	N	Y	Y
8	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา	N	Y	Y
9	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง	N	N	Y
10	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา	Y	Y	Y
11	ปัญหาจากสัญญาณรบกวน	N	Y	Y
12	การดักฟังข้อมูลผ่านสัญญาณหรือคลื่นแม่เหล็กไฟฟ้า	Y	N	N
13	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที	Y	N	N
14	การดักฟังข้อมูลในระบบไอทีหรือระบบคอมพิวเตอร์	Y	N	N
15	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y
16	อุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร สูญหาย	Y	N	Y
17	การวางแผนและออกแบบที่ไม่เหมาะสม หรือผลกระทบจากระบบอื่น	Y	Y	Y
18	ความลับถูกเปิดเผย	Y	N	N

19	ใช้ข้อมูลจากแหล่งข้อมูลที่ไม่น่าเชื่อถือ	Y	Y	Y
20	การเข้าถึงระบบไอทีโดยไม่ได้รับอนุญาต	Y	Y	N
21	การนำ Hardware และ Software ไปใช้ในทางที่ไม่ถูกต้อง	Y	Y	Y
22	การนำข้อมูลไปใช้ในทางที่ไม่ถูกต้อง (Information Manipulation)	N	Y	N
23	อุปกรณ์และอุปกรณ์ที่เก็บข้อมูล ถูกทำลาย	N	N	Y
24	การเข้าถึงระบบไอทีโดยไม่ได้รับอนุญาต	Y	Y	N

ภาคผนวก ข

การเปลี่ยนแปลงหมวด (Clause) จาก ISO/IEC 27001:2005 เป็น ISO/IEC 27001:2013

การเปลี่ยนแปลงหมวด (Clause)

จาก ISO/IEC 27001: 2005 เป็น ISO/IEC 27001: 2013

Clause in ISO/IEC 27001:2005 (เดิม)		Clause in ISO/IEC 27001:2013 (ปัจจุบัน)
8.3 Preventive action ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้เหมาะสมและมีประสิทธิภาพ	⇨	4.1 Understanding the organization and its Context เข้าใจองค์กรและภูมิหลังขององค์กร
5.2 1(c) Identify and address legal and regulatory requirements and contractual security obligations ระบุข้อกำหนดที่เกี่ยวข้องกับกฎหมายและระเบียบปฏิบัติ	⇨	4.2 Understanding the needs and expectations of interested parties ทำความเข้าใจกับความต้องการและความคาดหวังของผู้ที่เกี่ยวข้องกับ ISMS และการรักษาข้อมูล
4.2.1 a) Define scope and boundaries กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย 4.2.3 f) Ensure the scope remains adequate ตรวจสอบขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย	⇨	4.3 Determining the scope of the Information security management system กำหนดขอบเขตและการประยุกต์ ISMS เพื่อกำหนดขอบเขตการดำเนินการ
4.1 General requirements ข้อกำหนดทั่วไป องค์กรต้องกำหนด ลงมือปฏิบัติดำเนินการเฝ้าระวัง ทบทวน บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่กำหนดไว้	⇨	4.4 Information security management System จัดทำ ลงมือปฏิบัติ และปรับปรุง ISMS อย่างต่อเนื่องตามข้อกำหนดของมาตรฐานนี้

5.1 Management commitment ผู้บริหารแสดงถึงการให้ความสำคัญต่อการกำหนดลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง ทบทวนบำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่งคงปลอดภัย	⇨	5.1 Leadership and commitment ผู้บริหารควรแสดงให้เห็นถึงความเป็นผู้นำและความมุ่งมั่นต่อ ISMS
4.2.1 b) Define an ISMS policy กำหนดนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ	⇨	5.2 Policy ผู้บริหารระดับสูงควรกำหนดนโยบายความปลอดภัยด้านสารสนเทศ
5.1 c) Establishing roles and responsibilities for information security กำหนดหน้าที่ความรับผิดชอบ	⇨	5.3 Organizational roles, responsibilities and authorities ผู้บริหารระดับสูงควรให้ความสำคัญกับบทบาทของความมั่นคงปลอดภัยด้านสารสนเทศ มีการมอบหมายและสื่อสารความรับผิดชอบให้รับทราบโดยทั่วกัน
8.3 Preventive action ปรับปรุงระบบบริหารจัดการความมั่งคงปลอดภัยสารสนเทศให้เหมาะสมและมีประสิทธิภาพ	⇨	6.1.1 Actions to address risks and opportunities – general เมื่อวางแผน ISMS องค์กรควรพิจารณาถึงบริบทขององค์กรและตรวจสอบความเสี่ยงและโอกาสการเกิด
4.2.1 c) Define the risks assessment approach กำหนดวิธีประเมินความเสี่ยง 4.2.1 d) Identify the risks ระบุความเสี่ยง 4.2.1 e) Analyze and evaluate the risks วิเคราะห์และประเมินความเสี่ยง	⇨	6.1.2 Information security risk assessment กำหนดกระบวนการประเมินความเสี่ยงด้านสารสนเทศ
4.2.1 f) Identify and evaluate options for the treatment of risks ระบุและประเมินทางเลือกในการจัดการความเสี่ยง	⇨	6.1.3 Information security risk treatment กำหนดและใช้กระบวนการรักษาความปลอดภัยด้านสารสนเทศ

4.2.1 g) Select control objectives and controls for the treatment of risks เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัย 4.2.1 h) Obtain management approval of the proposed residual risks ขออนุมัติความเห็นชอบสำหรับความเสี่ยงที่ยังเหลืออยู่ 4.2.1 j) Prepare a Statement of Applicability จัดทำเอกสารตรวจมาตรการควบคุม 4.2.2 a) Formulate a risk treatment plan จัดทำแผนการลดความเสี่ยง		
5.1 b) Ensuring that ISMS objectives and plans are established กำหนดวัตถุประสงค์และแผนสำหรับระบบ ISMS	⇨	6.2 Information security objectives and planning to achieve them กำหนดวัตถุประสงค์ความมั่นคงด้านสารสนเทศไว้ในฟังก์ชันงานและระดับที่เกี่ยวข้อง
4.2.2 g) Manage resources for the ISMS บริหารทรัพยากรสำหรับระบบ ISMS 5.2.1 Provision of resources การจัดการทรัพยากร	⇨	7.1 Resources กำหนดและจัดเตรียมการดำเนินงานการบำรุงรักษาทรัพยากรที่จำเป็นต่อการปรับปรุง ISMS อย่างต่อเนื่อง
5.2.2 Training, awareness and competence การอบรม การสร้างความตระหนัก และการเพิ่มขีดความสามารถ	⇨	7.2 Competence สมรรถนะของบุคลากร
4.2.2 e) Implement training and awareness programmer จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก 5.2.2 Training, awareness and competence	⇨	7.3 Awareness การสร้างความตระหนักของบุคลากร

การอบรม การสร้างความตระหนัก และการเพิ่ม ขีดความสามารถ		
4.2.4 c) Communicate the actions and Improvements แจ้งการดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง 5.1 d) Communicating to the organization การสื่อสารภายในองค์กร	⇨	7.4 Communication กำหนดความจำเป็นสำหรับการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับ ISMS
4.3 Documentation requirements ข้อกำหนดทางด้านการจัดทำเอกสาร	⇨	7.5 Documented information เอกสารสารสนเทศที่เป็นลายลักษณ์อักษร
4.2.2 f) Manage operations of the ISMS การดำเนินงานสำหรับระบบ ISMS	⇨	8.1 Operational planning and control การวางแผนและควบคุมการดำเนินงาน
4.2.3 d) Review risk assessments at planned intervals ทบทวนผลการประเมินความเสี่ยง	⇨	8.2 Information security risk assessment การประเมินความเสี่ยงความมั่นคงด้านสารสนเทศ
4.2.2 b) Implement the risk treatment plan ปฏิบัติตามแผนลดความเสี่ยง 4.2.2 c) Implement controls ปฏิบัติตามแผนลดความเสี่ยงที่เลือกไว้	⇨	8.3 Information security risk treatment evaluation ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงด้านสารสนเทศ และเก็บรักษาเอกสารลายลักษณ์อักษรเกี่ยวกับผลของกระบวนการความเสี่ยงความปลอดภัยสารสนเทศ
4.2.2 d) Define how to measure effectiveness กำหนดวิธีการในการวัดความสัมฤทธิผล 4.2.3 b) Undertake regular reviews of the effectiveness of the ISMS ทบทวนความสัมฤทธิผล 4.2.3 c) Measure the effectiveness of Controls วัดความสัมฤทธิผล	⇨	9.1 Monitoring, measurement, analysis and evaluation ประเมินประสิทธิภาพของการรักษาความปลอดภัยด้านสารสนเทศและประสิทธิภาพของ ISMS

4.2.3 e) Conduct internal ISMS audits ดำเนินการตรวจสอบระบบ ISMS ภายในองค์กร 6 Internal ISMS audits การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย	⇨	9.2 Internal Audit การตรวจสอบภายในตามช่วงระยะเวลาที่วางแผนไว้
4.2.3 f) Undertake a management review of the ISMS ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหารอยู่เสมอ	⇨	9.3 Management review ผู้บริหารระดับสูงควรตรวจสอบ ISMS ขององค์กรในช่วงระยะเวลาที่กำหนดไว้เพื่อให้เกิดความมั่นใจ เพียงพอ และมีประสิทธิผลอย่างต่อเนื่อง
4.2.4 Maintain and improve the ISMS บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย 8.2 Corrective action การดำเนินการเชิงแก้ไข	⇨	10.1 Nonconformity and corrective action เมื่อเกิดความไม่สอดคล้อง ต้องดำเนินการแก้ไขและจัดการกับผลที่ตามมา
4.2.4 Maintain and improve the ISMS บำรุงรักษาและปรับปรุงบริหารจัดการความมั่งคงปลอดภัย 8.1 Continual improvement การปรับปรุงอย่างต่อเนื่อง	⇨	10.2 Continual improvement องค์กรควรปรับปรุงความเหมาะสม และความเพียงพอของ ISMS อย่างต่อเนื่องและมีประสิทธิผล

ภาคผนวก ค

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001: 2013

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013

วัตถุประสงค์ในการควบคุมและการควบคุมที่ระบุไว้ A.5 ถึง A.18	**A.5.1 ทิศทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information)**		
	วัตถุประสงค์: ให้คำแนะนำด้านการจัดการและการสนับสนุนด้านความปลอดภัยสารสนเทศตามข้อกำหนดทางธุรกิจและกฎหมายที่เกี่ยวข้อง		
A.5 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information security policies)	1.	5.1.1 นโยบายความมั่นคงด้านสารสนเทศ (Policies for information security)	มาตรการควบคุมแนวทางการรักษาความปลอดภัยสารสนเทศควรกำหนดแนวทางการรักษาความปลอดภัยด้านสารสนเทศโดยผู้บริหารระดับสูงและสื่อสารบุคคลภายในและภายนอกองค์กร
	2.	5.1.2 การทบทวนนโยบายความปลอดภัยของสารสนเทศ (Review of the information security policy)	มาตรการด้านความปลอดภัยควรมีการทบทวนนโยบายด้านความปลอดภัยด้านสารสนเทศควรดำเนินการตามระยะเวลาที่วางแผนไว้หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเพื่อให้มั่นใจว่ามีความเหมาะสมและมีประสิทธิผลอย่างต่อเนื่อง
A.6 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of information security)	**A.6.1 โครงสร้างภายในองค์กร (Internal organization)**		
	วัตถุประสงค์: สร้างกรอบการจัดการเพื่อเริ่มต้นและควบคุมการใช้งานและการดำเนินงานด้านความมั่นคงสารสนเทศภายในองค์กร		
	3.	A.6.1.1 บทบาทความปลอดภัยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และความรับผิดชอบ (Information security roles and responsibilities)	หน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศทั้งหมดควรได้รับการกำหนดและมอบหมายความรับผิดชอบ

	4.	A.6.1.2 การแบ่งหน้าที่และความรับผิดชอบ (Segregation of duties)	มาตรการการแบ่งหน้าที่และความรับผิดชอบการแก้ไขปัญหาความขัดแย้งสำหรับการเปลี่ยนแปลงและการใช้สินทรัพย์ขององค์กรในทางที่ผิด
	5.	A.6.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)	มาตรการในเรื่องการติดต่อประสานงานกับหน่วยงานหรือผู้ที่เกี่ยวข้องที่มีอำนาจอย่างเหมาะสม
	6.	A.6.1.4 การติดต่อและความร่วมมือกับกลุ่มคนที่มีความสนใจในเรื่องเดียวกัน (Contact with special interest groups)	มาตรการในการติดต่อและประสานงานความร่วมมือกันระหว่างกลุ่มคนที่มีความสนใจในเรื่องเดียวกันอย่างระดับมืออาชีพ
	7.	A.6.1.5 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศเกี่ยวกับบริหารจัดการโครงการ (Information security in project management)	มาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการให้ได้รับการรักษาความปลอดภัยอย่างสูงสุด
	6.2 อุปกรณ์เคลื่อนที่และการสื่อสารโทรคมนาคม (Mobile devices and teleworking)		
	วัตถุประสงค์ : ตรวจสอบความปลอดภัยของการสื่อสารโทรคมนาคมและการใช้โทรศัพท์มือถือ		
	8.	A.6.2.1 นโยบายสำหรับอุปกรณ์แบบเคลื่อนที่ หรือโทรศัพท์มือถือ (Mobile device policy)	มาตรการสนับสนุนและนโยบายการรักษาความปลอดภัยในการใช้อุปกรณ์แบบเคลื่อนที่หรือโทรศัพท์มือถือ
	9.	A.6.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)	มาตรการสนับสนุนและนโยบายการรักษาความปลอดภัยเพื่อปกป้องการปฏิบัติงานจากระยะไกล

A.7 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human resource security)	**A.7.1 ก่อนการจ้างงาน (Prior to employment)**		
	วัตถุประสงค์: เพื่อให้มั่นใจว่าพนักงานและผู้รับเหมาเข้าใจถึงความรับผิดชอบและพิจารณาบทบาทที่ตนรับผิดชอบ		
	10.	A.7.1.1 การคัดเลือก (Screening)	มาตรการควบคุมการตรวจสอบอย่างถูกต้องสำหรับผู้ที่เข้ารับการคัดเลือกให้ปฏิบัติงาน โดยจะต้องปฏิบัติตามกฎระเบียบและข้อกำหนดที่เกี่ยวข้องกับประเภทของการเข้าถึงสารสนเทศและความเสี่ยงอื่นๆ
	11.	A.7.1.2 ข้อตกลงและเงื่อนไขในการจ้างงาน (Terms and conditions of employment)	การทำข้อตกลงและเงื่อนไขของสัญญาสำหรับผู้รับเหมาที่ได้รับการจ้างให้ทำงาน โดยรายละเอียดแสดงถึงความรับผิดชอบด้านความปลอดภัยของสารสนเทศต่างๆ
	A.7.2 ระหว่างการจ้างงาน (During employment)		
	วัตถุประสงค์ : ตรวจสอบให้แน่ใจว่าพนักงานและผู้รับเหมามีความตระหนักและปฏิบัติตามความรับผิดชอบด้านความปลอดภัยข้อมูลของตน		
	12.	A.7.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)	ผู้ที่ทำหน้าที่บริหารจัดการควรกำหนดให้มีมาตรฐานในการรักษาความปลอดภัยตามหลักเกณฑ์ที่องค์กรกำหนดไว้เพื่อให้พนักงาน ผู้รับเหมา ปฏิบัติอย่างดีที่สุด
	13.	A.7.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมความมั่นคงปลอดภัยด้านสารสนเทศ (Information security awareness)	นโยบายส่งเสริมความรู้ความเข้าใจถึงความสำคัญของการรักษาความปลอดภัยสารสนเทศในหน้าที่การงาน โดยจัดฝึกอบรมแก่พนักงานขององค์กรรวมทั้งผู้รับเหมาเป็นระยะๆ
	14.	A.7.2.3 กระบวนการทางวินัย (Disciplinary process)	มาตรการทางวินัยเพื่อให้เกิดความปลอดภัยและป้องกันการฝ่าฝืนแก่พนักงานขณะปฏิบัติหน้าที่ และมีกระบวนการทำวินัยอย่างเป็นทางการ

	A.7.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)		
	วัตถุประสงค์ : เพื่อให้มั่นใจว่าผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการการเปลี่ยนแปลงการจ้างงานหรือเลิกจ้าง		
	15.	A.7.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)	มาตรการควบคุมพนักงานหรือผู้รับเหมาที่ยังต้องรับผิดชอบรักษาความปลอดภัยของสารสนเทศและภาระหน้าที่บางอย่างหลังสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งจะต้องมีการกำหนดการสื่อสาร และการดำเนินการอย่างชัดเจน
A.8 การบริหารจัดการสินทรัพย์ (Asset management)	**8.1 หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for assets)**		
	วัตถุประสงค์: เพื่อให้บรรลุการรักษาความปลอดภัยที่เหมาะสมกับสินทรัพย์ขององค์กร		
	16.	A.8.1.1 รายการสินทรัพย์ (Inventory of asset)	การระบุสินทรัพย์ที่เกี่ยวกับข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลและเก็บรวบรวมสินค้าและบำรุงรักษา
	17.	A.8.1.2 ผู้ถือครองสินทรัพย์ (Ownership of assets) ผู้เป็นเจ้าของสินทรัพย์	มาตรการควบคุมผู้ที่รับผิดชอบสินทรัพย์ โดยรายการสินทรัพย์ควรได้รับการกำหนด
	18.	A.8.1.3 การใช้สินทรัพย์อย่างเหมาะสม (Acceptable use of assets)	มาตรการการใช้สินทรัพย์ให้เหมาะสม ควรมีการระบุเอกสารลายลักษณ์อักษรและวิธีดำเนินการเกี่ยวกับการใช้ตลอดจนสารสนเทศที่เกี่ยวข้อง
	19.	A.8.1.4 การคืนสินทรัพย์ (Return of assets)	มาตรการในการส่งคืนสินทรัพย์สำหรับพนักงานและผู้ใช้ภายนอก ซึ่งจะส่งคืนสินทรัพย์ขององค์กรหลังจากสิ้นสุดสัญญาหรือบอกเลิกสัญญา

	A.8.2 การจัดลำดับชั้นความลับของข้อมูลสารสนเทศ (Information classification)		
	วัตถุประสงค์ : ตรวจสอบให้แน่ใจว่าสารสนเทศ ได้รับการคุ้มครองตามลำดับชั้นความลับ		
	20.	A.8.2.1 ชั้นความลับของสารสนเทศ (Classification of information)	มาตรการควบคุมสารสนเทศจัดให้ได้รับความคุ้มครองสารสนเทศโดยคำนึงถึงความสำคัญและลำดับชั้นความลับของสารสนเทศ ซึ่งเป็นไปตามกฎหมาย
	21.	A.8.2.2 การบ่งชี้ข้อมูลด้านสารสนเทศ (Labeling of information)	มาตรการควบคุมการทำเครื่องหมายบ่งชี้ข้อมูลด้านสารสนเทศและการทำเครื่องหมายขั้นตอนการดำเนินการที่เหมาะสมเพื่อใช้ในการประมวลผลข้อมูลที่องค์กรรับรอง
	22.	A.8.2.3 การจัดการสินทรัพย์ (Handling of assets)	มาตรการการกำหนดจัดหมวดหมู่ข้อมูลสินทรัพย์และดำเนินการขั้นตอนการประมวลผลอย่างเหมาะสมที่องค์กรกำหนด
	A.8.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)		
	วัตถุประสงค์: เพื่อป้องกันการเปิดเผยสารสนเทศแก้ไขลบหรือทำลายข้อมูลที่เก็บไว้ในสื่อโดยไม่ได้รับอนุญาต		
	23.	A.8.3.1 การจัดการสื่อบันทึกข้อมูลที่สามารถถอดได้ (Management of removable media)	มาตรการกระบวนการจัดการสื่อบันทึกข้อมูลแบบถอดได้โดยจำแนกประเภทข้อมูลตามที่องค์กรใช้
	24.	A.8.3.2 การกำจัดหรือการทำลายสื่อบันทึกข้อมูล (Disposal of media)	มาตรการควบคุมสื่อที่ไม่จำเป็นโดยการกำจัดหรือทำลายอย่างเป็นทางการและมีขั้นตอนอย่างปลอดภัย
	25.	A.8.3.3 การถ่ายโอนสื่อบันทึกข้อมูล (Physical media transfer)	มาตรฐานการป้องกันการถ่ายโอนสื่อบันทึกข้อมูลให้มีความปลอดภัย

A.9 การควบคุมการเข้าถึง (Access control)	**A.9.1 ความต้องการทางด้านธุรกิจเกี่ยวกับการควบคุมการเข้าถึง (Business requirement of access control)**		
	วัตถุประสงค์ : ควบคุมการเข้าถึงสารสนเทศและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล		
	26.	A.9.1.1 นโยบายการควบคุมการเข้าถึง (Access control policy)	มาตรการนโยบายการควบคุมการเข้าถึงสารสนเทศตามความต้องการทางด้านธุรกิจโดยมีการกำหนดเอกสารเป็นลายลักษณ์อักษรและการรักษาความปลอดภัยของสารสนเทศทางธุรกิจ
	27.	A.9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย (Access to networks and network services)	มาตรการการควบคุมผู้ใช้สำหรับการเข้าถึงเครือข่ายและการได้รับอนุญาตให้ใช้บริการเครือข่ายเฉพาะ
	A.9.2 การจัดการการเข้าถึงของผู้ใช้งาน (User access management)		
	วัตถุประสงค์ : ตรวจสอบให้แน่ใจว่าผู้ใช้ได้รับอนุญาตเข้าถึงระบบและบริการและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต		
	28.	A.9.2.1 การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration)	มาตรการการควบคุมโดยจัดให้มีขั้นตอนการลงทะเบียนสำหรับผู้ใช้และสามารถที่จะถอดถอนการลงทะเบียนของผู้ใช้อย่างถูกต้อง เพื่อจัดสรรสิทธิในการเข้าถึงระบบและบริการได้
	29.	A.9.2.2 การจัดสรรสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)	มาตรการควบคุมขั้นตอนการควบคุมสิทธิของผู้ใช้อย่างถูกต้องเพื่ออนุญาตหรือถอดถอนการเข้าถึงระบบข้อมูลสารสนเทศและบริการต่างๆ
	30.	A.9.2.3 การจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)	มาตรการควบคุมการจัดการสิทธิการเข้าถึงตลอดจนการได้รับการยกเว้นสิทธิในการเข้าถึงระบบข้อมูลสารสนเทศ
	31.	A.9.2.4 การจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน(Management of secret authentication information of users)	มาตรการควบคุมการจัดการบริการข้อมูลที่เป็นความลับอย่างเป็นทางการเพื่อให้สามารถพิสูจน์ตัวตนผู้ใช้งานได้

	32.	A.9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน(Review of user access rights)	มาตรการควบคุมการตรวจสอบสิทธิและยืนยันสิทธิในการเข้าถึงของผู้ใช้งาน
	33.	A.9.2.6 การถอดถอนหรือการปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)	มาตรการควบคุมสิทธิของผู้ใช้ทั้งภายในและภายนอกควรจัดให้มีการถอดสิทธิหรือปรับเปลี่ยนสิทธิในการเข้าถึงระบบ
	A.9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)		
	วัตถุประสงค์: ตรวจสอบความรับผิดชอบของผู้ใช้ในการปกป้องข้อมูลประจำตัว		
	34.	A.9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)	มาตรการควบคุมข้อมูลที่เป็นความลับของผู้ใช้ระบบควรกำหนดให้มีการพิสูจน์สารสนเทศที่เป็นความลับของผู้ใช้ระบบเพื่อใช้ในการตรวจสอบพิสูจน์ตัวตน
	A.9.4 การควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (System and application access control)		
	วัตถุประสงค์: เพื่อป้องกันการใช้ระบบและโปรแกรมประยุกต์โดยไม่ได้รับอนุญาต		
	35.	A.9.4.1 การจำกัดการเข้าถึงข้อมูลด้านสารสนเทศ (Information access restriction)	การควบคุมการจำกัดการเข้าถึงข้อมูลสารสนเทศและการเข้าถึงโปรแกรมประยุกต์ตามมาตรการการควบคุมการเข้าถึงระบบ
	36.	A.9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedures)	มาตรการควบคุมขั้นตอนการเข้าสู่ระบบข้อมูลสารสนเทศและโปรแกรมประยุกต์อย่างปลอดภัยตามนโยบายการควบคุมการเข้าถึง
	37.	A.9.4.3 ระบบการจัดการรหัสผ่าน (Password management system)	มาตรการควบคุมระบบควรจัดให้มีการใส่รหัสผ่านสำหรับการเข้าถึงระบบข้อมูลสารสนเทศและสามารถตรวจสอบได้
	38.	A.9.4.4 การใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษ (Use of privileged utility programs)	มาตรการควบคุมการใช้โปรแกรมอรรถประโยชน์ที่มีสิทธิพิเศษหรือเกินกว่าระบบและมาตรการควบคุมโปรแกรมประยุกต์ ควรจำกัดและควบคุมอย่างเข้มงวด

	39.	A.9.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)	มาตรการการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรมโดยมีข้อจำกัด
A.10 การเข้ารหัสข้อมูล (Cryptography)	**A.10.1 มาตรการเข้ารหัสข้อมูล (Cryptographic controls)**		
	วัตถุประสงค์ : ใช้รหัสผ่านเพื่อปกป้องข้อมูลที่เป็นความลับความถูกต้องและ / หรือความสมบูรณ์ของข้อมูลอย่างเหมาะสมและมีประสิทธิภาพ		
	40.	A.10.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)	มาตรการควบคุมให้มีการพัฒนาและการป้องกันของรหัสผ่านที่เข้าสู่ระบบข้อมูลอย่างมีประสิทธิภาพ
	41.	A.10.1.2 การบริหารจัดการกุญแจ (Key management)	มาตรการการควบคุมควรมีการพัฒนาสำหรับการใช้และการป้องกันในการจัดการกุญแจให้มีประสิทธิภาพ
A.11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	**A.11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)**		
	วัตถุประสงค์ : ป้องกันการเข้าถึงข้อมูลองค์กรและข้อมูลที่ไม่ได้รับอนุญาตในองค์กรและความเสียหายและการแทรกแซง		
	42.	A.11.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)	มาตรการควบคุมขอบเขตความปลอดภัยหรือเพิ่มความสามารถในการรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงของข้อมูลที่สำคัญและการแทรกแซงข้อมูล
	43.	A.11.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)	มาตรการควบคุมบริเวณพื้นที่ที่ต้องการรักษาความปลอดภัยอย่างเหมาะสมเพื่อให้แน่ใจว่ามีเพียงผู้ที่มีอำนาจเท่านั้นที่ได้รับอนุญาตให้เข้าออกข้อมูลได้
	44.	A.11.1.3 การรักษาความปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก(Securing office, room and facilities)	มาตรการการควบคุมด้านความปลอดภัยทางกายภาพและสิ่งอำนวยความสะดวกสำหรับสำนักงาน ห้องทำงาน

	45.	A.11.1.4 การป้องกันต่อภัย	มาตรการด้านความปลอดภัยควรจัดให้มี

		คุกคามจากภายนอก และสภาพแวดล้อม (Protection against external and environmental threats)	การป้องกันภัยภายในและป้องกันภัยคุกคามจากภายนอกเพื่อป้องกันการโจมตีที่เป็นอันตรายหรือเหตุที่คาดไม่ถึง (อุบัติเหตุ)
	46.	A.11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)	มาตรการควบคุมจัดให้มีการปฏิบัติงานในบริเวณพื้นที่ที่มีการรักษาความปลอดภัย
	47.	A.11.1.6 พื้นที่จัดส่งและการบรรทุกสิ่งของ (Delivery and loading areas)	การควบคุมพื้นที่ในการรับส่งและจัดส่งสิ่งของควรแยกออกจากบริเวณพื้นที่ที่มีการประมวลผลข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
	A.11.2 อุปกรณ์ (Equipment)		
	วัตถุประสงค์: เพื่อป้องกันการสูญหายของทรัพย์สินความเสียหายการโจรกรรมหรือความเสี่ยงต่อความปลอดภัยของทรัพย์สินและกิจกรรมภายในองค์กร		
	48.	A.11.2.1 การติดตั้งและการป้องกันอุปกรณ์ (Equipment sitting and protection)	มาตรการในการจัดตั้งอุปกรณ์ควรมีการวางแผนสำหรับการป้องกันความปลอดภัยเพื่อลดอันตรายจากภัยภายในและภายนอกตลอดจนการเข้าถึงโดยไม่ได้รับอนุญาต
	49.	A.11.2.2 ระบบและอุปกรณ์ในการสนับสนุนการปฏิบัติงาน(Supporting utilities)	มาตรการควรจัดให้มีระบบและอุปกรณ์ในการสนับสนุนในการปฏิบัติงานเพื่อป้องกันความล้มเหลวที่จะเกิดขึ้นระบบหรืออุปกรณ์
	50.	A.11.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)	มาตรการการรักษาความปลอดภัยในการปกป้องสายไฟและการสื่อสารที่นำข้อมูลไม่ให้เกิดความเสียหาย
	51.	A.11.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	มาตรการในการควบคุมอุปกรณ์ให้มีการป้องกันและการบำรุงรักษาอุปกรณ์เพื่อให้เกิดความปลอดภัยและสามารถใช้งานได้อย่างสมบูรณ์

	52.	A.11.2.5 การนำทรัพย์สินขององค์กรออกจากสำนักงาน (Removal of assets)	มาตรการควบคุมสินทรัพย์ควรมีการให้ได้รับอนุญาตก่อนที่จะกำจัดสินทรัพย์หรือนำสินทรัพย์ออกจากองค์กรหรือสำนักงาน
	53.	A.11.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises)	มาตรการการควบคุมด้านความปลอดภัยสำหรับสินทรัพย์ที่อยู่ภายนอกสถานที่ขององค์กร โดยคำนึงหรือพิจารณาถึงความเสี่ยงในการทำงานนอกสถานที่ขององค์กร
	54.	A.11.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)	การควบคุมอุปกรณ์ทั้งหมดที่มีสื่อเก็บข้อมูลควรตรวจสอบเพื่อให้มั่นใจว่าข้อมูลที่สำคัญนั้นถูกลบและซอฟต์แวร์ลงทะเบียนถูกลบหรือเขียนอย่างปลอดภัยก่อนการถูกกำจัดหรือทำลายทิ้ง
	55.	A.11.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)	มาตรการควบคุมผู้ใช้ควรตรวจสอบให้แน่ใจว่ามีการป้องกันอุปกรณ์ป้องกันผู้ใช้ที่ไม่ได้รับการควบคุมอย่างเหมาะสม
	56.	A.11.2.9 นโยบายโต๊ะทำงานโดยปราศจากเอกสารและนโยบายป้องกันจอภาพคอมพิวเตอร์อย่างปลอดภัย (Clear desk and clear screen policy)	มาตรการควบคุมการป้องกันข้อมูลสารสนเทศควรใช้นโยบายเพื่อล้างไฟล์บนเดสก์ท็อป สื่อเก็บข้อมูลแบบถอดได้ และป้องกันหน้าจอข้อมูล เพื่อป้องกันการประมวลผลข้อมูลที่ชัดเจน
A.12 ความปลอดภัยในการปฏิบัติงาน (Operations Security)	**A.12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)**		
	วัตถุประสงค์: เพื่อให้แน่ใจว่าการดำเนินงานของห้องประมวลผลข้อมูลมีความถูกต้องและปลอดภัย		
	57.	A.12.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	มาตรการการควบคุมขั้นตอนการปฏิบัติงานควรได้รับการจัดทำเป็นเอกสารเพื่อให้ผู้ใช้งานสามารถเข้าถึงได้ทั้งหมด

	58.	A.12.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)	การควบคุมควรควบคุมการเปลี่ยนแปลงที่มีผลต่อการจัดองค์กรข้อมูล กระบวนการทางธุรกิจสิ่งอำนวยความสะดวกและระบบการประมวลผลข้อมูล
	59.	A.12.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)	มาตรการการควบคุมการใช้ทรัพยากรควรได้รับการตรวจสอบปรับปรุงและคาดการณ์เกี่ยวกับข้อกำหนดด้านกำลังการผลิตในอนาคตเพื่อให้มั่นใจได้ว่าประสิทธิภาพของระบบที่ต้องการอยู่ในสถานที่
	60.	A.12.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation or development, testing and operational environments)	มาตรการควบคุมสิ่งแวดล้อมด้านการพัฒนาและการทดสอบควรแยกออกจากสภาพแวดล้อมการทำงานและลดความเสี่ยงในการเข้าถึงโดยไม่ได้รับอนุญาตและการเปลี่ยนแปลงระบบปฏิบัติการ
	A.12.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Control against malware)		
	วัตถุประสงค์ : เพื่อให้แน่ใจว่าไม่ได้รับข้อมูลจากมัลแวร์		
	6.1	A.12.2.1 มาตรการการป้องกันและการควบคุมโปรแกรมที่ไม่ประสงค์ดี (Control against malware)	มาตรการควบคุมด้านการตรวจสอบ การป้องกัน และการกู้คืนรหัสจากระบบที่เป็นอันตราย ควรมีการใช้มาตรการควบคุมร่วมกับการปรับปรุงเกี่ยวกับความปลอดภัยให้กับผู้ใช้งานที่เหมาะสม
	A.12.3 การสำรองข้อมูลเพื่อความปลอดภัย (Backup)		
	วัตถุประสงค์ : ป้องกันข้อมูลสูญหาย		
	62.	A.12.3.1 การสำรองข้อมูล (Information backup)	มาตรการการควบคุมข้อมูลการสำรองข้อมูลและการทดสอบซอฟต์แวร์และภาพระบบควรได้รับการสนับสนุนเป็นประจำตามนโยบายการสำรองข้อมูลที่ได้กำหนดไว้

	A.12.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)		
	วัตถุประสงค์ : เพื่อบันทึกเหตุการณ์และเฝ้าระวัง		
	63.	A.12.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)	การควบคุมควรสร้างบันทึกที่บันทึกกิจกรรมของผู้ใช้ความผิดปกติข้อบกพร่องและความปลอดภัยของข้อมูลและได้รับการประเมินเป็นประจำ
	64.	A.12.4.2 การป้องกันข้อมูลล็อก (Protection of log information)	มาตรการควบคุมข้อมูลการบันทึกและข้อมูลบันทึกควรได้รับการปกป้องจากการปลอมแปลงและการเข้าถึงโดยไม่ได้รับอนุญาต
	65.	A.12.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)	มาตรการควบคุมผู้ดูแลระบบและกิจกรรมของผู้ปฏิบัติการระบบควรได้รับการบันทึกไว้เพื่อป้องกันและตรวจสอบอย่างสม่ำเสมอ
	66.	A.12.4.4 การตั้งเวลาให้ถูกต้อง (Clock synchronization)	ควบคุมนาฬิกาของสิ่งอำนวยความสะดวกการประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือโดเมนความปลอดภัยควรทำข้อมูลให้ตรงกันโดยใช้แหล่งอ้างอิงเดียวที่ได้รับการตั้งค่า
	A.12.5 การใช้งานและการควบคุมการติดตั้งซอฟต์แวร์ (Control of operational software)		
	วัตถุประสงค์: เพื่อความสมบูรณ์ของระบบปฏิบัติการ		
	67.	A.125.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)	มาตรการควบคุมต้องดำเนินการเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ
	A.12.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability		

	management)		
	วัตถุประสงค์: เพื่อป้องกันการใช้ช่องโหว่ทางเทคโนโลยี		
	68.	A.12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	มาตรการการควบคุมควรมีการประเมินข้อมูลเกี่ยวกับช่องโหว่ด้านเทคนิคของระบบสารสนเทศในปัจจุบันต้องมีการกำหนดขั้นตอนการปฏิบัติที่เหมาะสมเพื่อรับมือกับความเสี่ยงที่เกี่ยวข้อง
	69.	A.12.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)	มาตรการควบคุมกฎระเบียบที่ใช้ในการติดตั้งซอฟต์แวร์โดยผู้ใช้ควรจะต้องมีการติดตามอย่างเป็นปัจจุบัน และมีการประเมินตรวจสอบมาตรการการควบคุมอย่างเหมาะสมเพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง
	A.12.7 ข้อควรพิจารณาในการตรวจประเมินระบบ (Information systems audit considerations)		
	วัตถุประสงค์: เพื่อลดผลกระทบของกระบวนการตรวจสอบระบบธุรกิจ		
	70.	A.12.7.1 มาตรการตรวจประเมินระบบ (Information system audit controls)	มาตรการการควบคุมต้องมีการวางแผนและอนุมัติอย่างรอบคอบเพื่อลดความเสี่ยงต่อการหยุดชะงักของกระบวนการทางธุรกิจ
A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	**A.13.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management)**		
	วัตถุประสงค์: เพื่อความปลอดภัยของข้อมูลในเครือข่ายและเพื่อปกป้องสิ่งอำนวยความสะดวกการประมวลผลข้อมูลสนับสนุน		
	71.	A.13.1.1 มาตรการเครือข่าย (Network controls)	การควบคุมควรจัดการและควบคุมเครือข่ายเพื่อปกป้องข้อมูลในระบบและแอพพลิเคชันต่างๆ
	72.	A.13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services	มาตรการการควบคุมกลไกการรักษาความปลอดภัยระดับการให้บริการและความต้องการด้านการจัดการสำหรับบริการเครือข่ายทั้งหมดควรได้รับการกำหนดและรวมอยู่ในข้อตกลงในการให้บริการเครือข่ายไม่ว่าบริการเหล่านี้จะมีให้จากภายในหรือภายนอกโดย บริษัท

	73.	A.13.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)	มาตรการของกลุ่มบริการสารสนเทศ ผู้ใช้และระบบ ต้องมีการควบคุมการจัดแบ่งเครือข่าย
	A.13.2 การถ่ายโอนสารสนเทศ (Information transfer) การถ่ายโอนข้อมูลสารสนเทศ		
	วัตถุประสงค์: เพื่อรักษาความปลอดภัยในการรับส่งข้อมูลระหว่างองค์กรและหน่วยงานภายนอกใด ๆ		
	74.	A.13.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)	มาตรการการควบคุมควรมีการกำหนดกลยุทธ์ขั้นตอนและการควบคุมอย่างเป็นทางการเพื่อให้แน่ใจว่ามีการส่งผ่านข้อมูลอย่างปลอดภัยระหว่างสิ่งอำนวยความสะดวกด้านการติดต่อสื่อสารทุกประเภท
	75.	A.13.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)	มาตรการการควบคุมต้องมีการกำหนดข้อตกลงเพื่อให้การส่งผ่านข้อมูลระหว่างองค์กรและบุคคลภายนอกเป็นไปอย่างปลอดภัย
	76.	A.13.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)	มาตรการควบคุมการส่งข้อความทางอิเล็กทรอนิกส์ควรมีมาตรการด้านความปลอดภัยและป้องกันความเสียหายขณะส่งข้อความ
	77.	A.13.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)	มาตรการการควบคุมควรระบุความลับของข้อกำหนดในการป้องกันข้อมูลขององค์กรหรือไม่เปิดเผยข้อกำหนดของข้อตกลงนี้รวมทั้งทบทวนและจัดทำเอกสารเป็นระยะ ๆ

A.14	**A.14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security**

การจัดหาระบบ การพัฒนาและการบำรุงรักษาระบบ (System acquisition, development and maintenance)	**requirements of information systems)**		
	วัตถุประสงค์ : ตรวจสอบให้แน่ใจว่าการรักษาความปลอดภัยเป็นส่วนสำคัญของวงจรชีวิตของระบบข้อมูล รวมถึงข้อกำหนดของระบบข้อมูลสำหรับการให้บริการผ่านเครือข่ายสาธารณะ		
	78.	A.14.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information requirements analysis and specification)	มาตรการควบคุมในระบบข้อมูลใหม่หรือเพื่อเพิ่มความต้องการในการปฏิบัติงานของระบบสารสนเทศที่มีอยู่ควรกำหนดข้อกำหนดสำหรับมาตรการควบคุมความปลอดภัย
	79.	A.14.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)	มาตรการการควบคุมข้อมูลที่ส่งผ่านบริการแอพพลิเคชันเครือข่ายสาธารณะควรได้รับการปกป้องจากกลโกงในการเปิดเผยข้อมูลและการปรับเปลี่ยนโดยไม่ได้รับอนุญาต
	80.	A.14.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)	การควบคุมข้อมูลที่ครอบคลุมในธุรกรรมการให้บริการแอพพลิเคชั่นควรได้รับความคุ้มครองจากการส่งโดยไม่ตั้งใจผิดพลาดเกี่ยวกับเส้นทางการเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาตการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตและการคัดลอกหรือการเล่นซ้ำข้อความที่ไม่ได้รับอนุญาต
	A.14.2 การพัฒนาและสนับสนุนความปลอดภัยในกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)		

	วัตถุประสงค์ : ตรวจสอบให้แน่ใจว่าการรักษาความปลอดภัยข้อมูลได้รับการออกแบบและใช้งานตลอดวงจรชีวิตของการพัฒนาระบบสารสนเทศ		
	81.	A.14.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)	มาตรการการควบคุมควรมีการพัฒนาและประยุกต์ใช้กฎการพัฒนาซอฟต์แวร์และระบบ
	82.	A.14.2.2 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)	มาตรการควบคุมขั้นตอนการควบคุมการเปลี่ยนแปลงอย่างเป็นทางการควรใช้เพื่อควบคุมการเปลี่ยนแปลงของระบบในช่วงวัฏจักรชีวิตการพัฒนา
	83.	A.14.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)	มาตรการการควบคุมเมื่อแพลตฟอร์มปฏิบัติการเปลี่ยนแปลงแอพพลิเคชันที่สำคัญของธุรกิจควรได้รับการตรวจสอบและทดสอบเพื่อให้แน่ใจว่าไม่มีผลเสียต่อการดำเนินงานและความปลอดภัยขององค์กร
	84.	A.14.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)	มาตรการควบคุมป้องกันการเปลี่ยนแปลงแพ็คเกจซอฟต์แวร์ จำกัด การเปลี่ยนแปลงเท่านั้นและควบคุมการเปลี่ยนแปลงทั้งหมด
	85.	A.14.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)	ควรมีมาตรการควบคุมเพื่อรักษาหลักการออกแบบของวิศวกรรมระบบความปลอดภัยที่มีการบันทึกไว้และนำไปใช้กับงานพัฒนาระบบข้อมูลใดๆ
	86.	A.14.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure envelopment environment)	มาตรการการควบคุมองค์กรต้องสร้างและปกป้องความปลอดภัยของสภาพแวดล้อมการพัฒนาอย่างถูกต้องและครอบคลุมวงจรการพัฒนาระบบทั้งหมด
	87.	A.14.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ	มาตรการควบคุมองค์กรควรดูแลและตรวจสอบกิจกรรมการพัฒนาระบบ

		(Outsourced development)	ภายนอก
	88.	A.14.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)	มาตรการควบคุมในระหว่างกระบวนการพัฒนาต้องมีการทดสอบความปลอดภัย
	89.	A.14.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)	มาตรการการควบคุมการทดสอบในการจัดตั้งระบบการอัพเกรดและการปรับปรุงระบบใหม่ต้องมีการกำหนดขั้นตอนการทดสอบอย่างชัดเจนเพื่อให้เกิดการยอมรับระบบ
	A.14.3 ข้อมูลสำหรับการทดสอบ (Test data)		
	วัตถุประสงค์ : เพื่อให้มั่นใจถึงความปลอดภัยของข้อมูลการทดสอบ		
	90.	A.14.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)	มาตรการการควบคุมข้อมูลการทดสอบควรได้รับการคัดเลือกป้องกันและควบคุมอย่างรอบคอบ
A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)	**A.15.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)**		
	วัตถุประสงค์ : ตรวจสอบความปลอดภัยของเนื้อหาองค์กรที่บริการภายนอกเข้าถึงได้		
	91.	A.15.1.1 นโยบายความปลอดภัยของข้อมูลด้านความสัมพันธ์กับคนหรือองค์การที่ให้บริการภายนอก (Information security policy for supplier relationships)	มาตรการการควบคุมข้อกำหนดด้านความปลอดภัยข้อมูลเพื่อลดความเสี่ยงของผู้จัดหาสินค้าที่เข้าถึงสินทรัพย์ขององค์กรควรได้รับการอนุมัติและจัดทำเป็นเอกสารจาก ซัพพลายเออร์
	92.	A.15.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)	มาตรการควบคุมความต้องการที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลควรได้รับการยอมรับและยอมรับจากผู้จัดหาสินค้า รวมถึงผู้ขายที่สามารถประมวลผลจัดเก็บและแลกเปลี่ยนข้อมูลองค์กรหรือจัดหาส่วนประกอบโครงสร้างพื้นฐานด้านไอที

	93.	A.15.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)	การควบคุมมาตรการข้อตกลงกับซัพพลายเออร์ควรรวมถึงข้อกำหนดสำหรับการระบุข้อมูลบริการด้านเทคโนโลยีการสื่อสารและความเสี่ยงด้านความปลอดภัยของข้อมูลที่เกี่ยวข้องกับห่วงโซ่อุปทานของผลิตภัณฑ์
	A.15.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)		
	วัตถุประสงค์ : เพื่อรักษาความปลอดภัยข้อมูลและระดับการให้บริการที่กำหนดไว้		
	94.	A.15.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)	มาตรการการควบคุมองค์กรควรตรวจสอบทบทวนและตรวจสอบบริการที่ซัพพลายเออร์เป็นประจำ
	95.	A.15.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)	มาตรการการควบคุมการจัดการการเปลี่ยนแปลงการให้บริการของผู้จัดหาโดยรวมถึงการบำรุงรักษาและการปรับปรุงกลยุทธ์และขั้นตอนการรักษาความปลอดภัยข้อมูลที่มีอยู่ควรคำนึงถึงความสำคัญของข้อมูลธุรกิจระบบกระบวนการที่เกี่ยวข้องและการประเมินความเสี่ยงอีกครั้ง
A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)	**A.16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)**		
	วัตถุประสงค์ : เพื่อให้แน่ใจว่ามีวิธีการที่สอดคล้องและมีประสิทธิภาพในการจัดการเหตุการณ์ความปลอดภัยของข้อมูลรวมถึงการรายงานเหตุการณ์ความปลอดภัยและความเสี่ยง		
	96.	A.16.1.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ (Responsibilities and procedures)	มาตรการด้านการควบคุมควรมีการกำหนดหน้าที่และขั้นตอนของการปฏิบัติต่อเหตุการณ์ความปลอดภัยของข้อมูลอย่างรวดเร็ว

	97.	A.16.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)	มาตรการด้านความปลอดภัยควรจัดให้มีการรายงานข้อมูลด้านความปลอดภัยโดยเร็วที่สุดผ่านทางช่องทางการจัดการที่เหมาะสม
	98.	A.16.1.3 การรายงานจุดอ่อนทางความมั่นคงสารสนเทศ (Reporting information security weaknesses)	มาตรการการควบคุมควรกำหนดให้พนักงานทุกคนของระบบข้อมูลและบริการพนักงานผู้รับเหมาบันทึกและรายงานจุดอ่อนด้านความปลอดภัยในระบบหรือบริการใด ๆ ที่พวกเขาสังเกตหรือสงสัย
	99.	A.16.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)	มาตรการการควบคุมสถานการณ์ด้านความปลอดภัยของข้อมูลควรได้รับการประเมินเพื่อพิจารณาว่าควรจัดประเภทเป็นเหตุการณ์ด้านความมั่นคงสารสนเทศหรือไม่
	100.	A.16.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)	มาตรการด้านความปลอดภัยข้อมูลเกี่ยวกับการรักษาความปลอดภัยข้อมูลควรได้รับการตอบสนองต่อขั้นตอนการจัดทำเอกสาร
	101.	A.16.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning form information security incidents)	มาตรการควบคุมช่วยเพิ่มความรู้จากการวิเคราะห์และแก้ไขปัญหาความมั่นคงสารสนเทศและลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต
	102.	A.16.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)	มาตรการการควบคุมองค์กรควรพัฒนาและใช้ขั้นตอนเพื่อระบุเก็บรวบรวมและจัดเก็บข้อมูลที่สามารถใช้เป็นหลักฐานได้

A.17 ประเด็นความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	**A.17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)**		
	วัตถุประสงค์ : การรักษาความปลอดภัยข้อมูลการจัดการความต่อเนื่องทางธุรกิจควรนำไปรวมในความต่อเนื่องขององค์กร		
	103.	A.17.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัย สารสนเทศ (Planning information security continuity)	มาตรการควบคุมองค์กรควรกำหนดความต่อเนื่องในการรักษาความปลอดภัยของข้อมูลและการจัดการความปลอดภัยของข้อมูลในสถานการณ์ที่ไม่พึงประสงค์เช่นวิกฤติหรือภัยพิบัติ
	104.	A.17.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)	มาตรการการควบคุมองค์กรต้องจัดทำใช้และดูแลกระบวนการและมาตรการการควบคุมเพื่อให้มั่นใจถึงระดับความปลอดภัยของข้อมูลที่จำเป็นต่อเนื่องในสถานการณ์ที่ไม่พึงประสงค์
	105.	A.17.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)	มาตรการควบคุมองค์กรควรตรวจสอบอย่างต่อเนื่องตลอดเวลาการควบคุมความต่อเนื่องด้านความปลอดภัยของข้อมูลมีการจัดตั้งและดำเนินการเพื่อให้มั่นใจว่ามีประสิทธิภาพในสถานการณ์ที่ไม่พึงประสงค์
	A.17.2 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)		
	วัตถุประสงค์: เพื่อให้แน่ใจว่ามีความพร้อมและเทคนิคในการตรวจสอบการประมวลข้อมูล		
	106.	A.17.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)	มาตรการการควบคุมความพร้อมใช้งานเพื่อความสะดวกในการประมวลผลของข้อมูลสารสนเทศเพื่อตอบสนองความต้องการของผู้ใช้งาน

A.18 **ความสอดคล้อง** **(Compliance)**	**A.18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง** **(Compliance with legal and contractual requirements)**		
	วัตถุประสงค์: เพื่อหลีกเลี่ยงข้อกำหนดด้านความปลอดภัยที่ละเมิดกฎหมายกฎเกณฑ์ข้อบังคับหรือข้อกำหนดด้านข้อมูลที่เกี่ยวกับความปลอดภัยของข้อมูล		
	107.	A.18.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)	มาตรการควบคุมสำหรับแต่ละระบบสารสนเทศและองค์กรต้องมีการระบุเอกสารและเก็บข้อมูลไว้อย่างชัดเจน รวมทั้งต้องมีการระบุเอกสารและกฎระเบียบข้อบังคับข้อกำหนดและข้อบังคับที่เกี่ยวข้องตลอดจนวิธีการที่ใช้เพื่อตอบสนองความต้องการเหล่านี้
	108.	A.18.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)	มาตรการการควบคุมขั้นตอนที่เหมาะสมควรดำเนินการเพื่อให้มั่นใจว่ามีการปฏิบัติตามกฎหมายข้อบังคับและข้อกำหนดตามสัญญาเมื่อใช้ผลิตภัณฑ์ซอฟต์แวร์ที่เป็นกรรมสิทธิ์
	109.	A.18.1.3 การป้องกันข้อมูล (Protection of records)	มาตรการควบคุมข้อมูลที่เป็นเอกสารได้รับการคุ้มครองตามกฎหมายข้อบังคับสัญญาและข้อกำหนดทางธุรกิจเพื่อป้องกันความสูญเสียความเสียหายการเปลี่ยนแปลงการเข้าถึงโดยไม่ได้รับอนุญาตและการแจกจ่ายโดยไม่ได้รับอนุญาต
	110.	A.18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)	มาตรการควบคุมควรเป็นไปตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องเพื่อให้มั่นใจถึงความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล
	111.	A.18.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Refutation of cryptographic controls)	มาตรการควบคุมใช้มาตรการควบคุมรหัสผ่านควรเป็นไปตามข้อตกลงกฎหมายและข้อบังคับที่เกี่ยวข้อง

	A.18.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)		
	วัตถุประสงค์ : เพื่อให้มั่นใจว่าระบบรักษาความปลอดภัยข้อมูลมีการดำเนินการและดำเนินการตามนโยบายและขั้นตอนขององค์กร		
	112.	A.18.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)	มาตรการการควบคุมการจัดการข้อมูลองค์กรการรักษาความปลอดภัยข้อมูลและวิธีปฏิบัติของพวกเขา (เช่นวัตถุประสงค์ด้านการควบคุมความมั่นคงสารสนเทศมาตรการควบคุมกลยุทธ์กระบวนการและขั้นตอน) ควรได้รับการทบทวนอย่างเป็นอิสระในช่วงเวลาที่วางแผนไว้และควรเป็นอิสระเมื่อมีการเปลี่ยนแปลงที่สำคัญในการใช้ความปลอดภัย ทบทวน
	113.	A.18.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)	ผู้บริหารควรตรวจสอบขั้นตอนและขั้นตอนการประมวลผลข้อมูลภายในความรับผิดชอบของตนเป็นระยะ ๆ เพื่อให้มั่นใจว่าสอดคล้องกับนโยบายด้านความปลอดภัยมาตรฐานและข้อกำหนดด้านความปลอดภัยอื่นๆ
	114.	A.18.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)	มาตรการควบคุมควรได้รับการตรวจสอบเป็นระยะเพื่อดูว่าระบบข้อมูลสอดคล้องกับนโยบายและมาตรฐานด้านความปลอดภัยข้อมูลขององค์กรหรือไม่

ภาคผนวก ง

การควบคุมความมั่นคงปลอดภัย

ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์

การควบคุมความมั่นคงปลอดภัย
ด้านการเข้าถึงระบบเทคโนโลยีสารสนเทศ เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์
ฯลฯ

๗.๖) การควบคุมการเข้าถึงระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบสารสนเทศ

พ.ร.ฎ.วิธีการแบบปลอดภัยฯ มาตรา ๗ (๗) ประกาศ คธอ. ข้อ ๒ (๑)

จัดให้มีควบคุมการเข้าถึงระบบสารสนเทศ

๗.๖.๑) ผู้ดูแลสินทรัพย์ต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงสินทรัพย์ของหน่วยงานให้เหมาะสมกับระดับความสำคัญของสินทรัพย์ หน้าที่และความรับผิดชอบของผู้ใช้งานตามความจำเป็น และ เสนอต่อคณะอนุกรรมการพัฒนาระบบอิเล็กทรอนิกส์ เนติบัณฑิตยสภาพิจารณาเห็นชอบ โดยต้องตรวจสอบและทบทวนการกำหนดสิทธิอย่างน้อยปีละ ๑ ครั้ง

ISO/IEC 27001:2005 Control A.11.1

การควบคุมการเข้าถึงระบบสารสนเทศ

๗.๖.๒) การบริหารการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของผู้ใช้งาน

ISO/IEC 27001:2005 Control A.11.2

(๑) ผู้ใช้งานสินทรัพย์ต้องยื่นคำขอการใช้งานสินทรัพย์ที่ได้รับการอนุมัติจากผู้บังคับบัญชาแก่ผู้ดูแลสินทรัพย์ เพื่อจัดทำทะเบียนรายชื่อบัญชีผู้ใช้ (Account) และปรับปรุงทะเบียนเมื่อมีการเปลี่ยนแปลง หรือเมื่อผู้ใช้งานสิ้นสุดสถานะการเป็นผู้ปฏิบัติงานของหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเกี่ยวกับการเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

(๒) ผู้ดูแลสินทรัพย์ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่าน (Password) ที่มีความมั่นคงปลอดภัย โดยการจัดส่งรหัสผ่าน (Password) ให้ผู้ใช้งานนั้นผู้ดูแลสินทรัพย์ต้องกระทำด้วยวิธีแบบมั่นคงปลอดภัย

หน้าที่ของผู้ใช้งาน

๗.๖.๓) หน้าที่ความรับผิดชอบของผู้ใช้งาน

ISO/IEC 27001:2005 Control A.11.3

(๑) ผู้ใช้งานต้องตั้งรหัสผ่าน (Password) ที่ไม่สามารถเดาได้ง่าย เช่น ไม่กำหนดรหัสผ่าน (Password) จากวันเดือนปีเกิด หมายเลขโทรศัพท์ของผู้ใช้งาน

(๒) ผู้ใช้งานต้องตั้งรหัสผ่าน (Password) ที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร

(๓) ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) หรือใช้รหัสผ่าน (Password) ร่วมกับผู้อื่น และจัดเก็บรหัสผ่าน (Password) ไว้ในที่ปลอดภัย

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทันทีเมื่อรหัสผ่าน (Password) ถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ในแต่ละระบบตามระยะเวลาที่กำหนด

(๖) ผู้ใช้งานต้องทำการออกจากระบบ (Log Off) สารสนเทศทันทีเมื่อสิ้นสุดการใช้งาน

(๗) ผู้ใช้งานต้องกำหนดให้มีการป้องกันการเข้าถึงอุปกรณ์หน่วยงานเมื่อไม่ได้ใช้งานอุปกรณ์ หรืออุปกรณ์นั้นถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

(๘) ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของตนเอง เพื่อป้องกันผู้อื่นใช้งานโดยไม่ได้รับอนุญาต

(๙) ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้งานสินทรัพย์ของหน่วยงาน เช่น เอกสาร สื่อบันทึกข้อมูล ที่อยู่ภายใต้ความรับผิดชอบของตนโดยไม่ได้รับอนุญาต

(๑๐) ผู้ใช้งานต้องป้องกันสินทรัพย์ของหน่วยงานเมื่อสินทรัพย์นั้นอยู่ในสถานที่สาธารณะ หรือสถานที่ที่บุคคลภายนอกเข้าถึงได้โดยง่าย

การควบคุมการเข้าถึงเครือข่าย

๗.๖.๔) การควบคุมการเข้าถึงเครือข่าย

ISO/IEC 27001:2005 Control A.11.4

(๑) ผู้ใช้งานต้องทำการยืนยันตัวตน (Authentication) ในการเข้าใช้งานระบบเครือข่ายของหน่วยงานตามสิทธิการใช้งานระบบ

(๒) ผู้ดูแลสินทรัพย์ต้องกำหนดให้อุปกรณ์ที่หน่วยงานอนุญาตเท่านั้นสามารถเชื่อมต่อระบบเครือข่ายของหน่วยงานได้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเกี่ยวกับการเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

(๓) ผู้ดูแลสินทรัพย์ต้องมีการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยให้สิทธิเฉพาะผู้ที่มีหน้าที่รับผิดชอบเท่านั้นเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๔) ผู้ดูแลสินทรัพย์ต้องแบ่งแยกระบบเครือข่ายภายในหน่วยงานและภายนอกหน่วยงานออกจากกัน

(๕) ผู้ดูแลสินทรัพย์ต้องควบคุมการเชื่อมต่อระบบเครือข่ายกับหน่วยงานภายนอก โดยเปิดให้บริการเข้าถึงระบบเครือข่ายเฉพาะบริการที่อนุญาตเท่านั้น

(๖) ผู้ดูแลสินทรัพย์ต้องควบคุมเส้นทางบนระบบเครือข่ายภายในหน่วยงาน ให้การใช้งานระบบเครือข่ายและสารสนเทศเป็นไปตามนโยบายการใช้งานระบบเครือข่ายของหน่วยงานอย่างมั่นคงปลอดภัย

การควบคุมการเข้าถึงระบบปฏิบัติการ

๗.๖.๕) การควบคุมการเข้าถึงระบบปฏิบัติการ

ISO/IEC 27001:2005 Control A.11.5

(๑) ผู้ดูแลสินทรัพย์ต้องกำหนดให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้ (Account) โดยบัญชีผู้ใช้ (Account) จะต้องไม่ซ้ำซ้อนกันเพื่อสามารถระบุตัวตนได้ และจัดให้มีกระบวนการยืนยันตัวตนด้วยวิธีการที่มั่นคงปลอดภัยก่อนเข้าใช้งานระบบปฏิบัติการ

(๒) ผู้ดูแลสินทรัพย์ต้องทำการยกเลิกบัญชีผู้ใช้ (Account) เริ่มต้นของระบบปฏิบัติการหรือทำการเปลี่ยนรหัสผ่าน (Password) ของบัญชีผู้ใช้ (Account) เริ่มต้นของระบบปฏิบัติการทันทีเมื่อดำเนินการติดตั้งระบบปฏิบัติการเสร็จสิ้น

(๓) ผู้ดูแลสินทรัพย์ต้องควบคุมและกำหนดสิทธิการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการด้านการรักษาความมั่นคงปลอดภัย

(๔) ผู้ดูแลสินทรัพย์ต้องกำหนดระยะเวลาให้ระบบปฏิบัติการตัดการใช้งานของผู้ใช้งาน เมื่อผู้ใช้งานไม่ใช้งานระบบปฏิบัติการในระยะเวลาเกิน ๑๕ นาที

(๕) ผู้ดูแลสินทรัพย์ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบปฏิบัติการและระบบสารสนเทศที่มีความสำคัญยิ่งยวดเพื่อควบคุมให้การใช้งานเป็นไปอย่างมั่นคงปลอดภัย

การควบคุมการเข้าถึงโปรแกรมประยุกต์

๗.๖.๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ *ISO/IEC 27001:2005 Control A.11.6*

(๑) ผู้ใช้งานต้องยืนยันตัวด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งานโปรแกรมประยุกต์และสารสนเทศตามสิทธิ ซึ่งกำหนดจากหน้าที่ความรับผิดชอบ และความจำเป็น

(๒) ผู้ดูแลสินทรัพย์ต้องแยกโปรแกรมประยุกต์และสารสนเทศที่มีความสำคัญยิ่งยวดออกจากระบบปกติเพื่อควบคุมการเข้าถึงและป้องกันการใช้งานโดยไม่ได้รับอนุญาต

การควบคุมอุปกรณ์พกพา และการปฏิบัติงานจากภายนอกหน่วยงาน

๗.๖.๗) การควบคุมอุปกรณ์ประมวลผลประเภทพกพาและการปฏิบัติงานจากภายนอกหน่วยงาน *ISO/IEC 27001:2005 Control A.11.7*

(๑) ผู้ใช้งานอุปกรณ์ประมวลผลประเภทพกพาควรใช้เครื่องมือในการรักษาความมั่นคงปลอดภัยของข้อมูลในอุปกรณ์ดังกล่าว เช่น โปรแกรมเข้ารหัสลับข้อมูลในอุปกรณ์ และโปรโตคอลเข้ารหัสข้อมูลที่รับส่งทางเครือข่ายคอมพิวเตอร์ เป็นต้น

(๒) ผู้ปฏิบัติงานของหน่วยงานสามารถปฏิบัติงานนอกสถานที่ได้ตามความเห็นชอบของผู้บังคับบัญชา โดยผู้ปฏิบัติงานมีหน้าที่รักษาความมั่นคงปลอดภัยของสินทรัพย์ของหน่วยงานที่นำไปใช้นอกสถานที่

๗.๗) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่าย ระบบคอมพิวเตอร์ และระบบสารสนเทศ *พ.ร.ฎ.วิธีการแบบปลอดภัยฯ มาตรา ๗ (๘)*

การระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการพัฒนาระบบ

๗.๗.๑) ผู้รับผิดชอบสินทรัพย์ต้องวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศที่พัฒนาใหม่ หรือระบบสารสนเทศที่ปรับปรุงจากระบบเดิม *ISO/IEC 27001:2005 Control A.12.1*

การควบคุมการประมวลผลของโปรแกรมประยุกต์

๗.๗.๒) การประมวลผลอย่างถูกต้องในโปรแกรมประยุกต์ *ISO/IEC 27001:2005 Control A.12.2*

(๑) โปรแกรมประยุกต์ที่ใช้ในหน่วยงาน ควรมีความสามารถในการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation) มีการประเมินผลที่ถูกต้อง มีการรักษาความมั่นคงปลอดภัยของข้อความที่สร้าง รับ ส่ง และแสดงผลรวมทั้งกำหนดมาตรการป้องกันการเปลี่ยนแปลงแก้ไขข้อความโดยไม่ได้รับอนุญาต

(๒) โปรแกรมประยุกต์ควรมีความสามารถในการตรวจสอบความถูกต้องของข้อมูลนำออก (Output Validation)

การควบคุมการเข้ารหัสข้อมูล

๗.๗.๓) การควบคุมการเข้ารหัสข้อมูล *ISO/IEC 27001:2005 Control A.12.3*

(๑) ผู้ดูแลสินทรัพย์ควรใช้การเข้ารหัสข้อมูลเพื่อรักษาความมั่นคงปลอดภัยตามระดับความสำคัญของข้อมูล และในการรับ-ส่งข้อมูลดังกล่าวควรใช้กลไกในการยืนยันตัวผู้รับ-ส่งด้วย

(๒) ผู้ดูแลสินทรัพย์ต้องนำกุญแจที่ใช้ในการเข้ารหัสข้อมูลไปเก็บไว้ในอุปกรณ์กลางของหน่วยงานเพื่อประโยชน์ในการถอดรหัสข้อมูลกรณีฉุกเฉิน

การสร้างความมั่นคงปลอดภัยให้กับไฟล์ในระบบให้บริการ

๗.๗.๔) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ในระบบให้บริการ *ISO/IEC 27001:2005 Control A.12.4*

(๑) การติดตั้งซอฟต์แวร์ลงในระบบที่ให้บริการของหน่วยงานต้องได้รับการเห็นชอบจากผู้รับผิดชอบระบบ และคณะอนุกรรมการพัฒนาระบบอิเล็กทรอนิกส์เนติบัณฑิตยสภาเพื่อลดความเสี่ยงที่จะทำให้ระบบบริการเกิดความเสียหายหรือทำงานผิดปกติ

(๒) ผู้ดูแลสินทรัพย์ต้องหลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบให้บริการที่พัฒนาใหม่ หากจำเป็นต้องใช้ผู้ดูแลสินทรัพย์ต้องกำหนดให้มีมาตรการป้องกันและควบคุมข้อมูลในส่วนที่เป็นความลับและข้อมูลสำคัญ

(๓) ผู้ดูแลสินทรัพย์ต้องจำกัดการเข้าถึงซอร์สโค้ดของโปรแกรมโดยการกำหนดให้สิทธิเฉพาะผู้มีหน้าที่รับผิดชอบ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการเปลี่ยนแปลงแก้ไขซอร์สโค้ดโดยไม่ได้รับอนุญาต

การควบคุมการพัฒนาระบบ

๗.๗.๕) การสร้างความมั่นคงปลอดภัยในการพัฒนาระบบและกระบวนการสนับสนุน *ISO/IEC 27001:2005 Control A.12.5*

(๑) การเปลี่ยนแปลง และการแก้ไขระบบสารสนเทศของหน่วยงานต้องได้รับความเห็นชอบจากผู้รับผิดชอบระบบ และคณะอนุกรรมการพัฒนาระบบอิเล็กทรอนิกส์เนติบัณฑิตยสภา โดยผู้รับผิดชอบระบบมีหน้าที่ตรวจสอบการทำงานของโปรแกรมประยุกต์ว่ามีปัญหาทางด้านความมั่นคงปลอดภัยหรือไม่ สามารถทำงานได้ตามปกติหรือไม่ เพื่อไม่ให้ส่งผลกระทบต่อการปฏิบัติงานของหน่วยงาน

(๒) ผู้ดูแลสินทรัพย์ต้องจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไขควรขอคำปรึกษาจากผู้ผลิตและแก้ไขตามความจำเป็นโดยต้องมีการควบคุมการแก้ไขอย่างเข้มงวด

(๓) ผู้ดูแลสินทรัพย์ต้องตรวจระบบเป็นประจำเพื่อป้องกันการรั่วไหลของข้อมูล

(๔) ในกรณีที่มีการจ้างพัฒนาซอฟต์แวร์ ผู้รับผิดชอบสินทรัพย์มีหน้าที่ควบคุมการพัฒนาซอฟต์แวร์ โดยต้องมีการตรวจสอบด้านความมั่นคงปลอดภัยอย่างเข้มงวด

ฯลฯ

ประกาศ ณ วันที่ ๑๙ กันยายน ๒๕๕๖

ภาคผนวก จ

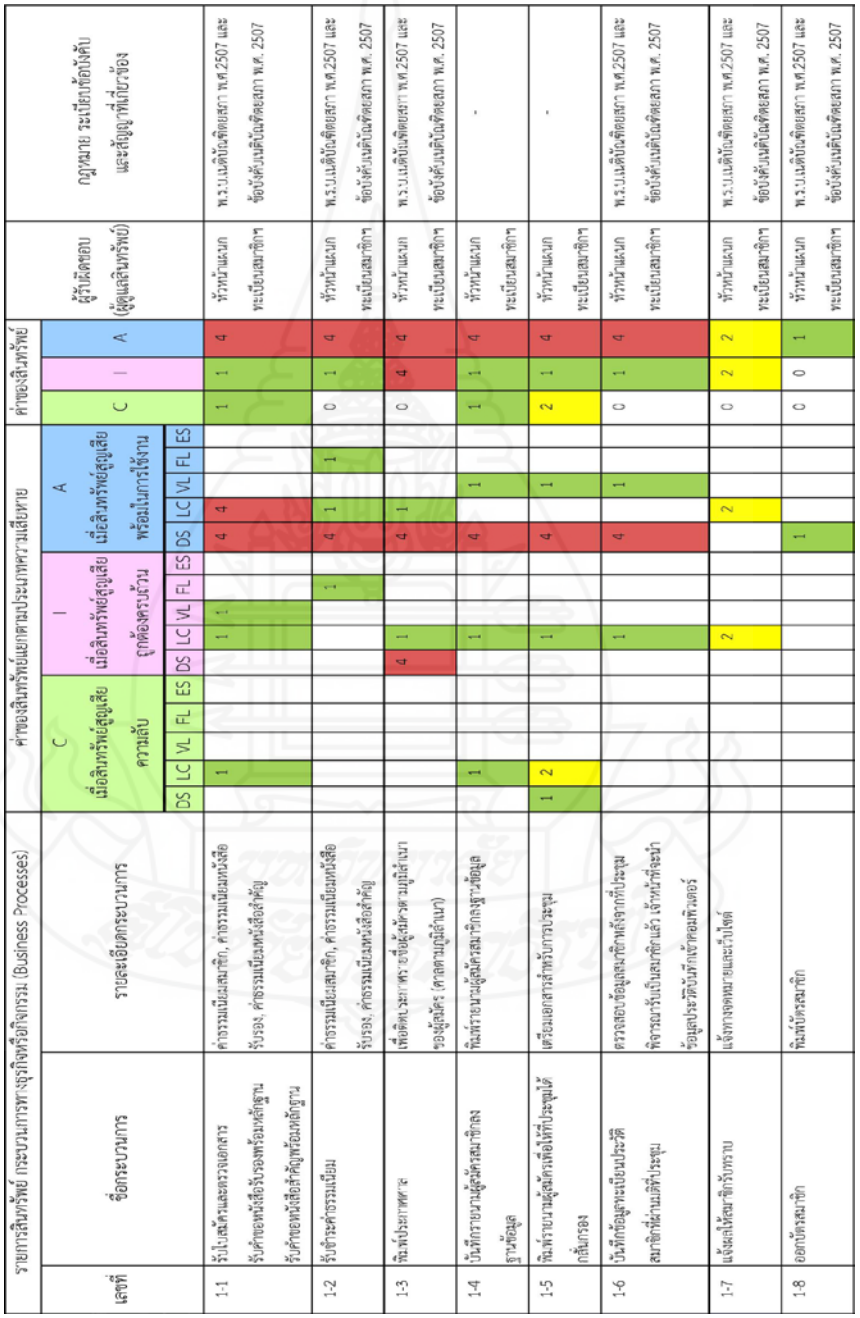
ทะเบียนสินทรัพย์และมูลค่าของสินทรัพย์ (Asset Identification and Valuation)

ทะเบียนสินทรัพย์และมูลค่าของสินทรัพย์

(Asset Identification and Valuation)

1. สินทรัพย์เกี่ยวกับ งานทะเบียนสมาชิกและทนายความ (กองกลาง)

1.1 รายการสินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)



รายการสินทรัพย์ กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)			ค่าของสินทรัพย์ตามประเภทความสูญเสียหาย																		ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และข้อบัญญัติที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียพร้อมในการใช้งาน						C	I	A		
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES						
1-1	รับไปสืบหาและตรวจเอกสาร รับคำขอหนังสือรับรองพร้อมหลักฐาน รับคำขอหนังสือสำคัญพร้อมหลักฐาน	คำร้องแบบสมาชิก, คำร้องแบบโอนหนังสือ รับรอง, คำร้องแบบโอนหนังสือสำคัญ		1					1	1			4	4					1	1	4	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507
1-2	รับคำร้องต่างๆแบบ	คำร้องแบบสมาชิก, คำร้องแบบโอนหนังสือ รับรอง, คำร้องแบบโอนหนังสือสำคัญ									1		4	1		1			0	1	4	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507
1-3	พิมพ์ประกาศ	เพื่อพิมพ์ประกาศรายชื่อผู้ที่ขาดจากการเป็นสมาชิกของสภาทนายความ (ตามกฎหมายกำหนด)						4	1				4	1					0	4	4	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507
1-4	บันทึกรายการผู้สมัครสมาชิกลงฐานข้อมูล	พิมพ์รายการผู้สมัครสมาชิกลงฐานข้อมูล		1					1				4		1				1	1	4	หัวหน้างานทะเบียนสมาชิกฯ	-
1-5	พิมพ์รายการผู้สมัครเพื่อให้ประชุมใหญ่กลั่นกรอง	เตรียมเอกสารสำหรับการประชุม		1	2				1				4		1				2	1	4	หัวหน้างานทะเบียนสมาชิกฯ	-
1-6	บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ผ่านมติที่ประชุม	ตรวจสอบข้อมูลสมาชิกพร้อมรูปถ่ายที่ประชุมพิจารณารับเป็นสมาชิกแล้ว, เข้าหน้าที่จะนำข้อมูลประวัติไปบันทึกเข้าคอมพิวเตอร์							1				4		1				0	1	4	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507
1-7	แจ้งผลให้สมาชิกทราบ	แจ้งการลงทะเบียนเป็นสมาชิก							2					2					0	2	2	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507
1-8	ออกบัตรสมาชิก	พิมพ์บัตรสมาชิก											1						0	0	1	หัวหน้างานทะเบียนสมาชิกฯ	พ.ร.บ.ทนายความ พ.ศ.2507 และข้อบังคับสภาทนายความ พ.ศ. 2507

1.1 รายการสินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes) (ต่อ)

รายการสินทรัพย์ กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย														ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียพร้อมในการใช้งาน					C	I	A		
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
1-9	สแกนใบสมัครและเอกสารประกอบการสมัครสมาชิกลง Server	เพื่อสำรองข้อมูลเป็นเก่า ลง Server											1					0	0	1	หัวหน้าแผนกทะเบียนสมาชิก	-
1-10	การออกหนังสือรับรองการเป็นสมาชิก	พิมพ์หนังสือรับรองด้วยมือ ประเภทหนังสือหนังสือสำคัญไว้เป็นหลัก												1				0	0	1	หัวหน้าแผนกทะเบียนสมาชิก	
1-11	กระบวนการแก้ไขข้อมูลสมาชิก	กรอกคำร้องที่ขอแก้ไขข้อมูลโดยมีเจ้าหน้าที่พิจารณาและลงนามประกอบ							1					3				0	1	3	หัวหน้าแผนกทะเบียนสมาชิก	-
1-12	เตรียมบัญชีรายชื่อผู้มีสิทธิได้รับเลือกเป็น คกก. เนติบัณฑิตยสภา	4 ปีครั้ง เป็นสามัญสมาชิกไม่น้อยกว่า 10 ปี ประเภท 1 ข้าราชการตุลาการ (ผู้พิพากษา) 2.ข้าราชการอัยการ 3.ทนายความ 4.อื่นๆ							4					1				0	4	1	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507
1-13	เตรียมบัญชีรายชื่อผู้มีสิทธิเลือก คกก. เนติบัณฑิตยสภา	4 ปีครั้ง เป็นสามัญสมาชิก ส่งบัตรเลือกตั้ง							4					1				0	4	1	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507
1-14	ตรวจสอบบัญชีรายชื่อผู้มีสิทธิได้รับเลือกเป็น คกก. เนติบัณฑิตยสภา	4 ปีครั้ง เป็นสามัญสมาชิกไม่น้อยกว่า 10 ปี ประเภท 1 ข้าราชการตุลาการ (ผู้พิพากษา) 2.ข้าราชการอัยการ 3.ทนายความ 4.อื่นๆ												1				0	0	1	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507
1-15	ตรวจสอบบัญชีรายชื่อผู้มีสิทธิเลือก คกก. เนติบัณฑิตยสภา	4 ปีครั้ง เป็นสามัญสมาชิก												1				0	0	1	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507
1-16	นับคะแนน รวบรวมและจัดเก็บบัตรเลือกตั้งและประมวล	4 ปีครั้ง เจ้าหน้าที่รวบรวมบัตรเลือกตั้ง												3				0	0	3	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507
1-17	ประกาศผลการเลือกตั้ง	ประกาศในเนติบัณฑิตยสภา,เว็บไซต์,จดหมายปิดประกาศที่ชั้น 1 อาคารเนติฯ												3				0	0	3	หัวหน้าแผนกทะเบียนสมาชิก	พ.ร.บ.เนติบัณฑิตยสภา พ.ศ.2507 และข้อบังคับเนติบัณฑิตยสภา พ.ศ. 2507

1.2 รายการสินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

รายการสินทรัพย์ ข้อมูลสารสนเทศ (Information Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และข้อกฎหมายที่เกี่ยวข้อง
			C					I						A									
เลขที่	ชื่อข้อมูล	รายละเอียดข้อมูล	เมื่อสินทรัพย์สูญเสียความลับ					เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน						เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน						C	I	A		
			DS	LC	VL	FL	ES	DS	LC	VL	FL	ES		DS	LC	VL	FL	ES					
1-18	เอกสารการสมัครสมาชิกวิสามัญ ข้อ5 (1)	5 สถาบัน ได้แก่ ม.บูรพา ม.ธรรมศาสตร์ ม.รามฯ ม.เชียงใหม่ และ ม.สุโขทัยธรรมาธิราช						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	พ.ร.บ.แพทย์แผนไทย พ.ศ. 2507 และข้อบังคับ
1-19	เอกสารการสมัครสมาชิกวิสามัญ ข้อ5 (2)	มหาวิทยาลัยฯ นอกเหนือจาก ข้อ5 (1) ที่แพทย์แผนไทยรับรอง						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	พ.ร.บ.แพทย์แผนไทย พ.ศ. 2507 และข้อบังคับ
1-20	ฐานข้อมูลรายนามสมาชิกวิสามัญ	ไฟล์ Ms. Access 2010 ไฟล์ Typo (My SQL)						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	-
1-21	ฐานข้อมูลรายนามสามัญสมาชิก	ไฟล์ Ms. Access 2010 ไฟล์ Typo (My SQL)						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	-
1-22	ฐานข้อมูลรายนามสมาชิกสมทบ	ไฟล์ Ms. Access 2010						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	-
1-23	รายงานการประชุม	มติที่ประชุมในการพิจารณารับ-ไม่รับสมาชิก						1	3					4						0	3	4	หัวหน้าแผนกทะเบียนสมาชิกฯ	พ.ร.บ.แพทย์แผนไทย พ.ศ. 2507 และข้อบังคับ

1.3 รายการสินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

รายการสินทรัพย์ ซอฟต์แวร์ (Software Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย														ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-24	OS : Microsoft Windows 8.1	ระบบปฏิบัติการเพื่อใช้ในการปฏิบัติงานในสำนักงาน											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-25	Microsoft Office2013	โปรแกรมพื้นฐานในการจัดการเอกสารในสำนักงาน											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-26	Microsoft access 2010	โปรแกรมฐานข้อมูลที่ใช้เก็บข้อมูลสมาชิก (พัฒนาขึ้นเอง)											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-27	Typo (MySQL)	โปรแกรมฐานข้อมูลที่ใช้เก็บข้อมูลสมาชิก (จ้างบริษัทพัฒนา)											3					0	0	3	แผนกทะเบียนสมาชิกฯ

1.4 รายการสินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

รายการสินทรัพย์ ฮาร์ดแวร์ (Hardware Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
1-28	เครื่อง Server Intel QuadCore Q9400	no. 01-44-0154											4					0	0	4	แผนกทะเบียนสมาชิกฯ
1-29	printer HP LASER JET 1200	no. 01-45-0045											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-30	scanner HP SCANJET 7650	no. 01-52-0010											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-31	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ Intal P4/3.0 GHz.	no. 01-44-0107											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-32	printer HP LASER JET 5652	no. 01-45-0054											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-33	printer EURAKA พิมพ์บัตรชนิดแข็ง	no. 01-45-0107											4					0	0	4	แผนกทะเบียนสมาชิกฯ
1-34	scanner HP Scanjet 5590	no. 01-52-0012											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-35	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ intel Core2D E4400 2.0/800/2M/775	no. 01-44-0116											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-36	scanner HP Scanjet 5590	no. 01-52-0011											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-37	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ intel Core2D E4400 2.0/800/2M/775	no. 01-44-0117											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-38	printer HP LASER JET 1022	no. 01-45-0082											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-39	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ intael Core2DUo E6440 2.33 GHz.	no. 01-44-0123											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-40	printer HP Laserjet 1150	no. 01-45-0061											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-41	scanner MCROTECH X12USL	no. 01-52-0006											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-42	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ intel Core 5-650 32 GHz	no. 01-44-0158											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-43	printer HP Laserjet 1200	no. 01-45-0034											3					0	0	3	แผนกทะเบียนสมาชิกฯ
1-44	scanner HP 7456C SCSI CARD	no. 01-52-0003											3					0	0	3	แผนกทะเบียนสมาชิกฯ

1.5 รายการสินทรัพย์ ด้านบุคลากร (People Assets)

เลขที่	รายการสินทรัพย์ บุคลากร (People Assets)		ค่าของสินทรัพย์และการประเมินความเสี่ยงหาย														ค่าของสินทรัพย์			ผู้บังคับบัญชา (ผู้ดูแลสินทรัพย์)	สถานที่ทำงาน
	ตำแหน่ง	รายละเอียด	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A		
			DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
1-45	หัวหน้าแผนกทะเบียนสมาชิกฯ	กำกับ ควบคุม ดูแลความเรียบร้อยในแผนก											3					0	0	3	ผู้อำนวยการกองกลาง	แผนกทะเบียนสมาชิกฯ ชั้น 2
1-46	เจ้าหน้าที่งานทะเบียน	admin รับชำระค่าธรรมเนียม											3					0	0	3	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2
1-47	เจ้าหน้าที่งานทะเบียน	admin พิมพ์ประกาศนียบัตร											1					0	0	1	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2
1-48	เจ้าหน้าที่งานทะเบียน	admin บันทึกระเบียนผู้สมัครสมาชิกลงฐานข้อมูล											3					0	0	3	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2
	เจ้าหน้าที่งานทะเบียน	admin บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ต่อเนื่อง																				
	เจ้าหน้าที่งานทะเบียน	admin แก้ไขที่ประชุม																				
	เจ้าหน้าที่งานทะเบียน	admin แจ้งผลให้สมาชิกรับทราบ																				
1-49	เจ้าหน้าที่งานทะเบียน	admin พิมพ์รายงานเพื่อให้ที่ประชุมใช้กลั่นกรอง											2					0	0	2	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2
	เจ้าหน้าที่งานทะเบียน	admin ออกบัตรสมาชิก																				
1-50	เจ้าหน้าที่งานทะเบียน	admin การออกหนังสือรับรอง											1					0	0	1	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2
1-51	เจ้าหน้าที่งานทะเบียน	admin กระบวนการเปลี่ยนข้อมูลสมาชิก											1					0	0	1	หัวหน้าแผนกทะเบียนสมาชิกฯ	แผนกทะเบียนสมาชิกฯ ชั้น 2

ทั้งนี้ผู้ดูแลระบบทุกคนสามารถปฏิบัติงานแทนกันได้ ในกระบวนงานต่อไปนี้

- รับใบสมัครสมาชิกและตรวจเอกสาร รับคำขอหนังสือรับรองพร้อมหลักฐาน
- สแกนใบสมัครและเอกสารประกอบการสมัครสมาชิกลง Server
- เตรียมบัญชีรายชื่อผู้มีสิทธิเลือกคณะกรรมการเนติบัณฑิตยสภา
- ตรวจสอบบัญชีรายชื่อผู้มีสิทธิเข้าเลือกเป็นคณะกรรมการเนติบัณฑิตยสภา
- ตรวจสอบบัญชีรายชื่อผู้มีสิทธิเข้าเลือกตั้งกรรมการเนติบัณฑิตยสภา
- รวมรวมและจัดเก็บบัตรเลือกตั้งแต่ละประเภท
- นับคะแนนบัตรเลือกตั้ง

1.6 รายการสินทรัพย์ ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

รายการสินทรัพย์ โครงสร้างพื้นฐาน (Infrastructure Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C					I					A						C	I	A	
			เมื่อสินทรัพย์สูญเสียความลับ					เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					เมื่อสินทรัพย์สูญเสียความพร้อมใช้งาน									
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
1-52	ห้องแผนกทะเบียนเรียนและทะเบียนความ	ชั้น 2 กองกลาง	2	2									3	2					2	0	3	แผนกทะเบียนเรียนฯ
1-53	ระบบไฟฟ้า	ระบบไฟฟ้าสำนักงาน											1						0	0	1	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
1-54	ระบบโทรศัพท์	ระบบโทรศัพท์ภายในสำนักงาน											2						0	0	2	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
1-55	ระบบอินเทอร์เน็ต	ระบบอินเทอร์เน็ตที่ให้ในหน่วยงาน/แผนกต่างๆ											2						0	0	2	แผนกเทคโนโลยีสารสนเทศ
1-56	ระบบเครื่องปรับอากาศ	เครื่องปรับอากาศ											1						0	0	1	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
1-57	อุปกรณ์ดับเพลิง	เป็นถังดับเพลิงชนิดผงและสายน้ำดับเพลิง						4	4	4	4	4	4	4	4	4	4		0	4	4	แผนกอาคาร สถานที่ และสิ่งแวดล้อม

2. สินทรัพย์เกี่ยวกับงานเงิน (กองคลัง)

2.1 รายการสินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)

รายการสินทรัพย์ กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ถูกสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมใช้งาน					C	I	A		
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
2-1	กระบวนการส่ง ภงด.1 แผ่นดีดี แดชบอร์ดจัด ให้กรมสรรพากร	แดชบอร์ดจัด ทุกเดือน แผ่นดิสก์ ทุกเดือน											3					0	2	3	หัวหน้าแผนกการเงิน	ตามมาตรา 40 (1) และ (2) แห่งประมวลรัษฎากร ภาษีเงินได้บุคคลธรรมดา
2-2	กระบวนการตั้งบิลภูมิภาคเดือน	เพื่อเบิกเงินมาจ่ายเงินเดือน พนักงานทุกเดือน		2						2			4					2	2	4	หัวหน้าแผนกการเงิน	ระเบียบกระทรวงการคลัง ว่าด้วยการเบิกจ่ายเงินเดือน เงินปี บำเหน็จ
2-3	กระบวนการส่งเงินให้สหกรณ์ สำนักงานศาลยุติธรรม	ทุกเดือน เป็นเช็ค											4					0	0	4	หัวหน้าแผนกการเงิน	ระเบียบสหกรณ์ออมทรัพย์กระทรวงยุติธรรม จำกัด ว่าด้วยการให้เงินกู้แก่สมาชิกและตอกเบี้ยเงินกู้ (ฉบับที่ 3) พ.ศ.2552 /ระเบียบสหกรณ์ออมทรัพย์กระทรวงยุติธรรม จำกัด ว่าด้วยหุ้น พ.ศ. 2548
2-4	กระบวนการส่งเงินธนาคารอาคาร สงเคราะห์ (ธอส.)	ทุกเดือน											4					0	0	4	หัวหน้าแผนกการเงิน	ตามวิธีการกำหนดอัตราดอกเบี้ยเงินกู้ธนาคาร อาคารสงเคราะห์
2-5	กระบวนการจ่ายเงินลดให้ สวัสดิการพนักงานเงินสัมพันธ์	ทุกเดือน		2									4					2	0	4	หัวหน้าแผนกการเงิน	พ.ร.บ.ระเบียบข้าราชการพลเรือน พ.ศ. 2551
2-6	กระบวนการโอนเงินเดือนเข้าบัญชี พนักงาน	ทุกเดือน		2						2	1							2	2	0	หัวหน้าแผนกการเงิน	พ.ร.บ.ระเบียบข้าราชการพลเรือน พ.ศ. 2551
2-7	กระบวนการจัดทำบัญชีเงินฝาก สถิเงินเดือน	ทุกเดือน		2														2	0	0	หัวหน้าแผนกการเงิน	พ.ร.บ.ระเบียบข้าราชการพลเรือน พ.ศ. 2551

2.2 รายการสินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

รายการสินทรัพย์ ข้อมูลสารสนเทศ (Information Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และสัญญาที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A		
เลขที่	ชื่อข้อมูล	รายละเอียดข้อมูล	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
2-8	เอกสารข้อมูลเงินภาษีเงิน ณ ที่จ่าย ของพนักงาน (และไฟล์)	สำหรับส่งสรรพากร			2					1					2			2	1	2	แผนกการเงิน	ตามมาตรา 40 (1) และ (2) แห่งประมวลรัษฎากร ภาษีเงินได้บุคคลธรรมดา
2-9	แคช.ชีย์รับชีคเงินตาม กงต.1	สำหรับส่งสรรพากร			1					1					1			1	1	1	แผนกการเงิน	ตามมาตรา 40 (1) และ (2) แห่งประมวลรัษฎากร ภาษีเงินได้บุคคลธรรมดา
2-10	แผ่นซีดี ข้อมูลการหักเงินภาษี ณ ที่จ่าย ของ พนง.	สำหรับส่งสรรพากร			1					1					1			1	1	1	แผนกการเงิน	ตามมาตรา 40 (1) และ (2) แห่งประมวลรัษฎากร ภาษีเงินได้บุคคลธรรมดา
2-11	เอกสารฎีกาเงินเดือน (และไฟล์)	สำหรับเบิกเงินเพื่อจ่ายเงินเดือน พนง.			1					1								1	1	0	แผนกการเงิน	ระเบียบกระทรวงการคลัง ว่าด้วยการเบิกจ่ายเงินเดือน เงินปี
2-12	แคช.เชียร์เช็ค สั่งจ่ายเงินให้สหกรณ์ สำนักงานศาลยุติธรรม	สำหรับส่งสหกรณ์ สำนักงานศาลยุติธรรม			1					1								1	1	0	แผนกการเงิน	ระเบียบสหกรณ์ออมทรัพย์ กระทรวงยุติธรรม จำกัด
2-13	เอกสารสั่งโอน เงิน พนง.ให้ ธอส. (กรณี พนง.กู้) (และไฟล์)	สำหรับส่งธนาคาร อาคารสงเคราะห์			2					1								2	1	0	แผนกการเงิน	ตามวิธีการกำหนดอัตราดอกเบี้ยเงินกู้ ธนาคารอาคารสงเคราะห์
2-14	ใบแจ้งการโอนเงินของ พนง. แต่ละคน ให้ ธอส. (และไฟล์)	สำหรับส่งให้ พนง. เป็นต้น			1													1	0	0	แผนกการเงิน	ตามวิธีการกำหนดอัตราดอกเบี้ยเงินกู้ ธนาคารอาคารสงเคราะห์
2-15	สลิปเงินเดือน พนง. (และไฟล์)	สำหรับส่งให้ พนง. เป็นต้น			2					2								2	2	0	แผนกการเงิน	พระราชบัญญัติระเบียบข้าราชการพลเรือน
2-16	username/password สำหรับเข้าใช้งานโปรแกรมคำนวณภาษีฯ	สำหรับคำนวณภาษีฯ			2					2					1			2	2	1	แผนกการเงิน	ตามมาตรา 40 (1) และ (2) แห่งประมวลรัษฎากร ภาษีเงินได้บุคคลธรรมดา
2-17	เอกสารแจ้งยอดการถอนเงินจากธนาคาร เพื่อไปจ่ายเงินเดือน พนง.	สำหรับส่งให้ธนาคารออมสิน			2					2								2	2	0	แผนกการเงิน	พ.ร.บ.ระเบียบข้าราชการพลเรือน พ.ศ. 2551

2.3 รายการสินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

รายการสินทรัพย์ ซอฟต์แวร์ (Software Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน						C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
2-18	โปรแกรมคำนวณภาษีเงินได้หัก ณ ที่จ่าย	พัฒนาโดยกรมสรรพากร			2	2				1	1				2	2			2	1	2	แผนกการเงิน
2-19	Microsoft Windows 8.1	ระบบปฏิบัติการเพื่อใช้ในการปฏิบัติงานในสำนักงาน											3						0	0	3	แผนกการเงิน
2-20	Microsoft Office2013	โปรแกรมพื้นฐานในการจัดการเอกสารในสำนักงาน											1						0	0	1	แผนกการเงิน
2-21	Microsoft excel	ใช้ในการคำนวณเงินเดือน		2		1			2					3					2	2	3	แผนกการเงิน
2-22	Microsoft Word	บันทึกข้อความ		2		1			2					3					2	2	3	แผนกการเงิน

2.4 รายการสินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

รายการสินทรัพย์ ฮาร์ดแวร์ (Hardware Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
2-23	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ Intel Core-5-650 32GHz.	no.1-45-113	2					2					2					2	2	2	แผนกการเงิน
2-24	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ Intel Core-5-650 32GHz.	no.1-45-159	2					2					2					2	2	2	แผนกการเงิน
2-25	Printter HP Laser 1200 - ไฟล์ excel ที่เก็บข้อมูลสลิปเงินเดือน	no.1-45-103			1	1				1	1				1	1		1	1	1	แผนกการเงิน
2-26	Printter HP Laser 1200 - ไฟล์ฎีกาเงินเดือน - ไฟล์สั่งโอนเงิน พนง. ให้ ธอส. (กรณีพนักงานกู้) - ไฟล์สั่งถอนเงินสด เพื่อส่งสวัสดิการพนักงานเบิกา (กรณี พนง กู้) - ไฟล์สั่งโอนเงินเดือน เข้าบัญชีเงินเดือน พนง. ผ่าน S.ออมสิน	no1-45-195			1	1				1	1				1	1		1	1	1	แผนกการเงิน

2.5 รายการสินทรัพย์ ด้านบุคลากร (People Assets)

เลขที่	รายการสินทรัพย์ บุคลากร (People Assets)		ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้บังคับบัญชา (ผู้ดูแลสินทรัพย์)	สถานที่ทำงาน
	ตำแหน่ง	รายละเอียด	C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A		
			DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
2-27	หัวหน้าแผนกการเงิน	กำกับ ควบคุม ดูแลความเรียบร้อยในแผนก		2	2				2	3	3							2	3	0	ผู้อำนวยการกองคลัง	แผนกการเงิน ชั้น 2
2-28	เจ้าพนักงานการเงินและบัญชี	เขียนใบเสร็จรับเงินค่าสมัครสมาชิก		2	2				1	2	2							2	2	0	หัวหน้าแผนกการเงิน	แผนกการเงิน ชั้น 2
2-29	เจ้าพนักงานการเงินและบัญชี	งานเงินเดือน		2	2				1	2	2							2	2	0	หัวหน้าแผนกการเงิน	แผนกการเงิน ชั้น 2
2-30	เจ้าพนักงานการเงินและบัญชี	งานภาษี		2	2				1	2	2							2	2	0	หัวหน้าแผนกการเงิน	แผนกการเงิน ชั้น 2
2-31	เจ้าพนักงานการเงินและบัญชี	รับเงินค่าหนังสือ		2	2				1	2	2							2	2	0	หัวหน้าแผนกการเงิน	แผนกการเงิน ชั้น 2

2.6 รายการสินทรัพย์ ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

รายการสินทรัพย์ โครงสร้างพื้นฐาน (Infrastructure Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้ดูแลสินทรัพย์
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
2-32	ห้องแผนกการเงิน	ชั้น 2 กองคลัง	2	2									3	2				2	0	3	หัวหน้าแผนกการเงิน
2-33	ระบบไฟฟ้า	ระบบไฟฟ้าสำนักงาน											1					0	0	1	แผนกอาคาร สถานที่ และยานพาหนะ
2-34	ระบบโทรศัพท์	ระบบโทรศัพท์ภายในสำนักงาน											2					0	0	2	แผนกอาคาร สถานที่ และยานพาหนะ
2-35	ระบบอินเทอร์เน็ต	ระบบอินเทอร์ที่มีไว้ให้ใช้ในหน่วยงาน/แผนกต่างๆ											2					0	0	2	แผนกเทคโนโลยีสารสนเทศ
2-36	ระบบเครื่องปรับอากาศ	เครื่องปรับอากาศ											1					0	0	1	แผนกอาคาร สถานที่ และยานพาหนะ
2-37	อุปกรณ์ดับเพลิง	เป็นถังดับเพลิงชนิดหัวและสายน้ำดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	แผนกอาคาร สถานที่ และยานพาหนะ

3. สินทรัพย์เกี่ยวกับการบริหารจัดการศึกษา (กองบริการ)

3.1 รายการสินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)

รายการสินทรัพย์ กระบวนการทางธุรกิจหรือกิจกรรม (Business Processes)			ค่าของสินทรัพย์แยกตามประมาทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)	กฎหมาย ระเบียบข้อบังคับ และข้อบัญญัติที่เกี่ยวข้อง
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A		
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
3-1	บริการรับสมัครนักศึกษาใหม่ - เก่า เรียนภาคปกติ	เป็นการรับสมัครนักศึกษาใหม่ และสมัครนักศึกษาเก่า (เรียนซ้ำกลุ่มใหม่เดิม) นักศึกษาใหม่ คนละ 2,100 บาท นักศึกษาเก่า คนละ 1,800 บาท						3	3				3	3				0	3	3	แผนกทะเบียนและประเมินผล	ระเบียบสำนักอบรมศึกษากฎหมายแห่งมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยการเป็นนักศึกษา การสอบ การสอบไล่ วินัยและการยุติ พ.ศ. 2507
3-2	บริการรับสมัครนักศึกษาเรียนภาคค่ำ เรียนภาคทฤษฎี	เปิดรับนักศึกษาเพื่อเข้าเรียนทฤษฎีภาคค่ำ คนละ 1,000 บาท (จ-ศ 17.00 - 20.30 น.) ภาคทฤษฎีรวมคนละ 2,000 บาท (ส-อา 09.00 - 16.00 น.)						3	3				3	3				0	3	3	แผนกทะเบียนและประเมินผล	ระเบียบสำนักอบรมศึกษากฎหมายแห่งมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยการเป็นนักศึกษา การสอบ การสอบไล่ วินัยและการยุติ พ.ศ. 2507
3-3	บริการรับสมัครสอบไล่	รับสมัครสอบประจำภาคการศึกษา ตามกลุ่มวิชา - กลุ่มแพทและพาณิชย์ / กลุ่มอายุมาก - กลุ่มวิแพ่งและพาณิชย์ / กลุ่มวิอายุมาก กลุ่มวิชาละ 600 บาท						3	3		1		3	3				0	3	3	แผนกทะเบียนและประเมินผล	ระเบียบสำนักอบรมศึกษากฎหมายแห่งมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยการเป็นนักศึกษา การสอบ การสอบไล่ วินัยและการยุติ พ.ศ. 2507
3-4	บริการ Video Streamming	บริการงานด้านการบรรยายแต่ละคลุ่มวิชาไปยังศูนย์รับถ่ายทอด มหาวิทยาลัย หรือ ศาลในแต่ละจังหวัด (ถ่ายถอดเฉพาะการสอบภาคค่ำ)			4	2							1					4	0	1	แผนกทะเบียนและประเมินผล	ระเบียบสำนักอบรมศึกษากฎหมายแห่งมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยการเป็นนักศึกษา การสอบ การสอบไล่ วินัยและการยุติ พ.ศ. 2507
3-5	บริการ Video ย้อนหลัง (เฉพาะภาคค่ำ)	บริการงานด้านการสอน ตามความต้องการโดยจัดส่ง DVD ไปยังศูนย์รับถ่ายทอด			4	2							1					4	0	1	แผนกทะเบียนและประเมินผล	อนุกรรมการกำกับการเรียนการสอน

3.2 รายการสินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

รายการสินทรัพย์ ข้อมูลสารสนเทศ (Information Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อกระบวนการ	รายละเอียดกระบวนการ	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
3-6	ฐานข้อมูลทะเบียนนักศึกษา	เป็นข้อมูลของผู้มาสมัครเรียนและผู้สมัครสอบ						3	3				3	3				0	3	3	แผนกธุรการ
3-7	ไฟล์ข้อมูลการชำระเงินที่ธนาคาร	ข้อมูลการชำระค่าลงทะเบียนเรียนและสมัครสอบ						2					2					0	2	2	แผนกธุรการ
3-8	ไฟล์ข้อมูลทะเบียนการรับรถนำเข้า	ข้อมูลการชำระค่าลงทะเบียนเรียนและสมัครสอบ						2					2					0	2	2	แผนกธุรการ
3-9	สมุดทะเบียนนักศึกษา	รายชื่อนักศึกษา																0	0	0	แผนกทะเบียนและประเมินผล
3-10	ใบสมัครนักศึกษา	รายละเอียดของผู้สมัครเรียน						3	3				3	3				0	3	3	แผนกทะเบียนและประเมินผล
3-11	ใบบันทึกคะแนนสอบ	ใบบันทึกคะแนนสอบ		3				4	3				4	3				3	4	4	แผนกทะเบียนและประเมินผล
3-12	แผ่นซีดี บันทึกข้อมูลคะแนนสอบ	เป็นการทำสำเนาเพื่อจัดเก็บข้อมูลคะแนนสอบ		3				4	3				4	3				3	4	4	แผนกทะเบียนและประเมินผล
3-13	วิดีโอ บันทึกการบรรยาย	เทปวิดีโอ (สำเนาบันทึกการถ่ายทอด)			4	2												4	0	0	แผนกธุรการ
3-14	ไฟล์วิดีโอการบรรยาย	ไฟล์ที่ตัดเก็บในเครื่องบันทึก			4	2												4	0	0	แผนกธุรการ
3-15	CD Video บรรยาย	Video ที่จัดส่งให้ตามคำขอของศูนย์รับถ่ายทอด			4	2												4	0	0	แผนกธุรการ

3.3 รายการสินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

รายการสินทรัพย์ ซอฟต์แวร์ (Software Assets)			ค่าของสินทรัพย์แยกตามประเมินความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
3-16	OS: Microsoft Windows Server 2008	ระบบปฏิบัติการของเครื่อง Server ทะเบียนนักศึกษา											2					0	0	2	แผนกธุรการ
3-17	Microsoft SQL Server 2008	ฐานข้อมูลที่เก็บข้อมูลนักศึกษา											2					0	0	2	แผนกธุรการ
3-18	โปรแกรมบริหารจัดการฐานข้อมูลทะเบียนนักศึกษา	โปรแกรมที่ใช้ในการรับสมัครเรียนและสมัครสอบ											2					0	0	2	แผนกธุรการ
3-19	OS: Microsoft Windows 8.1	ระบบปฏิบัติการเพื่อใช้ในการปฏิบัติงานในสำนักงาน											3					0	0	3	แผนกธุรการ
3-20	Microsoft Office 2013	โปรแกรมพื้นฐานในการจัดการเอกสารในสำนักงาน											1					0	0	1	แผนกธุรการ

3.4 รายการสินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

รายการสินทรัพย์ ฮาร์ดแวร์ (Hardware Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน						C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
3-21	Web Server	Server ที่ให้บริการ Website						1	1				1						0	1	1	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-22	Database Server	database เกี่ยวกับข้อมูลนักศึกษาเท่านั้น						2					2						0	2	2	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-23	TOKEN	Tiken key ที่จะใช้เข้าระบบเพื่ออัพโหลดข้อมูลคะแนนสอบเข้าระบบ											2						0	0	2	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-24	เครื่องพิมพ์บัตรประจำตัวนักศึกษา	เครื่องพิมพ์บัตรชนิดแข็ง											1						0	0	1	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-25	เครื่องสแกน	เครื่องสแกนเอกสารชนิดสิ่งกระดาษอัตโนมัติ Feed											1						0	0	1	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-26	Laser Printer	เครื่องพิมพ์เอกสารใช้พิมพ์งานทั่วไป											1						0	0	1	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย
3-27	Barcode Reader	เครื่องอ่าน Barcode จากเอกสารในสมัคร											1						0	0	1	ผู้อำนวยการกองบริการ สำนักศึกษาทบทวนกฎหมาย

3.4 รายการสินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets) (ต่อ)

รายการสินทรัพย์ ฮาร์ดแวร์ (Hardware Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
3-28	เครื่องคอมพิวเตอร์ตั้งโต๊ะ	เครื่องคอมพิวเตอร์ทั่วไปในสำนักงาน											1					0	0	1	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-29	UPS Victron	เครื่องสำรองไฟขนาดใหญ่สำหรับห้องบรรยาย											1					0	0	1	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-30	Server ระบบลงทะเบียน	Server ที่ใช้รันโปรแกรมลงทะเบียน		3				3					3					3	3	3	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-31	Server Streamming	Server ที่ใช้ในการถ่ายทอด Video บรรยาย				2			2									2	2	0	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-32	เครื่องบันทึกเทปวีดีโอ	อุปกรณ์บันทึกเทปการบรรยาย											2					0	0	2	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-33	Comodo Firewall กำแพงป้องการโดนยิง	Five Wall ที่ใช้ในการจัดการระบบอินเตอร์เน็ต เป็นกำแพงป้องกันเจลาโดนยิง											1					0	0	1	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ
3-34	เครื่องคอมพิวเตอร์พิมพ์งานรับสมัครสอบ 1	เครื่องคอมพิวเตอร์ที่ใช้เฉพาะงาน						1	1				1					0	1	1	ผู้อำนวยการกองบริการสำนักศึกษาอบรมกฎหมายฯ

3.5 รายการสินทรัพย์ ด้านบุคลากร (People Assets)

รายการสินทรัพย์ บุคลากร (People Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย																ค่าของสินทรัพย์			ผู้บังคับบัญชา (ผู้ดูแลสินทรัพย์)	สถานที่ทำงาน
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A		
เลขที่	ตำแหน่ง	รายละเอียด	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES					
3-35	เลขาธิการสำนักอธบรม฿	เป็นผู้ถือรหัส เข้าระบบเพื่อโหลดข้อมูล											2					0	0	2	นายกนมัติบัณฑิตยสภา	เนติบัณฑิตยสภา
3-36	รอง.เลขาธิการสำนักอธบรม฿	เป็นผู้ถือรหัส เข้าระบบเพื่อโหลดข้อมูล											2					0	0	2	เลขาธิการสำนักอธบรม฿	เนติบัณฑิตยสภา
3-37	ผู้อำนวยการกองบริการ฿	เป็นผู้ถือรหัส เข้าระบบเพื่อโหลดข้อมูล											2					0	0	2	เลขาธิการสำนักอธบรม฿	เนติบัณฑิตยสภา
3-38	หัวหน้าแผนกทะเบียนและประเมินผล	เป็นผู้ถือ Token และเป็นผู้ถือรหัส เข้าระบบเพื่อโหลดข้อมูล											2					0	0	2	ผู้อำนวยการกองบริการ฿	แผนกทะเบียนและประเมินผล
3-39	เจ้าหน้าที่แผนกธุรการ (นายช่างไฟฟ้า)	เป็นผู้ให้บริการจัดการธุรกรรมและประสานงานการเงินกับธนาคาร											1					0	0	1	หัวหน้าแผนกธุรการ	แผนกทะเบียนและประเมินผล
3-40	เจ้าหน้าที่แผนกทะเบียนและประเมินผล	เป็นผู้ให้บริการจัดการธุรกรรมและสอบ											1					0	0	1	หัวหน้าแผนกทะเบียนและประเมินผล	แผนกทะเบียนและประเมินผล
3-41	เจ้าหน้าที่แผนกธุรการ (นายช่างไฟฟ้า)	เป็นเจ้าหน้าที่ Admin ในทุกระบบของสำนักอบรม											4					0	0	4	หัวหน้าแผนกธุรการ	ห้องโสตทัศนูปกรณ์ ชั้น 4 (แผนกธุรการดูแล)
3-42	หัวหน้าแผนกทะเบียนและประเมินผล	เป็นผู้ดูแลและแก้ไขข้อมูลการสมัครของนักศึกษา											1					0	0	1	ผู้อำนวยการกองบริการ฿	แผนกทะเบียนและประเมินผล
3-43	เจ้าหน้าที่งานทะเบียนแผนกทะเบียนและประเมินผล	เป็นผู้ให้บริการจัดการธุรกรรมและสอบ											1					0	0	1	หัวหน้าแผนกทะเบียนนักศึกษา	แผนกทะเบียนและประเมินผล

3.6 รายการสินทรัพย์ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

รายการสินทรัพย์ โครงสร้างพื้นฐาน (Infrastructure Assets)			ค่าของสินทรัพย์แยกตามประเภทความเสียหาย															ค่าของสินทรัพย์			ผู้รับผิดชอบ (ผู้ดูแลสินทรัพย์)
			C เมื่อสินทรัพย์สูญเสียความลับ					I เมื่อสินทรัพย์สูญเสียความถูกต้องครบถ้วน					A เมื่อสินทรัพย์สูญเสียความพร้อมในการใช้งาน					C	I	A	
เลขที่	ชื่อสินทรัพย์	รายละเอียดสินทรัพย์	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES	DS	LC	VL	FL	ES				
3-44	ห้อง OSS: One Stop Server	ศูนย์บริการจุดเดียวเบ็ดเสร็จ	2	2									3	2				2	0	3	หัวหน้าแผนกทะเบียนและประเมินผล
3-45	ระบบไฟฟ้า	ระบบไฟฟ้าสำนักงาน											1					0	0	1	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
3-46	ระบบโทรศัพท์	ระบบโทรศัพท์ภายในสำนักงาน											2					0	0	2	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
3-47	ระบบอินเทอร์เน็ต	ระบบอินเทอร์เน็ตไร้สายในหน่วยงาน/แผนกต่างๆ											2					0	0	2	แผนกเทคโนโลยีสารสนเทศ
3-48	ระบบเครื่องปรับอากาศ	เครื่องปรับอากาศ											1					0	0	1	แผนกอาคาร สถานที่ และสิ่งแวดล้อม
3-49	อุปกรณ์ดับเพลิง	เป็นถังดับเพลิงชนิดหิ้วและสายน้ำดับเพลิง						4	4	4	4	4	4	4	4	4	4	0	4	4	แผนกอาคาร สถานที่ และสิ่งแวดล้อม

ภาคผนวก ฉ

ผลการประเมินความเสี่ยงของสินทรัพย์ (Asset Risk Assessment)

ผลการประเมินความเสี่ยงของสินทรัพย์ (Asset Risk Assessment)

1.1 งานทะเบียนสมาชิกและทนายความ (กองกลาง)

1.1 สินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-1	รับใบสมัครและตรวจเอกสาร รับคำขอหนังสือรับรองพร้อมหลักฐาน รับคำขอหนังสือสำคัญพร้อมหลักฐาน	1	1	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		1		1		L		พลภัทร
1-3	พิมพ์ประกาศนาม	0	4	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		4		1		M		พลภัทร
1-4	บันทึกรายงานผู้สมัครสมาชิกของฐานข้อมูล	1	1	4	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		1		3		M		พลภัทร
1-4	บันทึกรายงานผู้สมัครสมาชิกของฐานข้อมูล	1	1	4	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	1	1	4	2	M	M	H	พลภัทร
1-5	พิมพ์รายงานผู้สมัครเพื่อให้ที่ประชุมได้กลั่นกรอง	2	1	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	1		3	M	M		พลภัทร
1-5	พิมพ์รายงานผู้สมัครเพื่อให้ที่ประชุมได้กลั่นกรอง	2	1	4	เพลิงไหม้	N	Y	Y	2	1	4	1		L	M	พลภัทร
1-6	บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ผ่านมติที่ประชุม	0	1	4	Software มีจุดอ่อนหรือมีข้อผิดพลาด	Y	Y	Y	0	1	4	1	N/A	L	M	พลภัทร
1-6	บันทึกข้อมูลทะเบียนประวัติสมาชิกที่ผ่านมติที่ประชุม	0	1	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	1		1	N/A	L		พลภัทร
1-7	แจ้งผลให้สมาชิกรับทราบ	0	2	2	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา (Service)	Y	Y	Y	0	2	2	1	N/A	L	L	พลภัทร

1.1 สินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes) (ต่อ)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-7	แจ้งผลให้สมาชิกรับทราบ	0	2	2	เพลิงไหม้	N	Y	Y		2	2	1		L	L	พลภัทร
1-8	ออกบัตรสมาชิก	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถ	N	N	Y			1	1			L	พลภัทร
1-9	สแกนใบสมัครและเอกสารประกอบการสมัครสมาชิกลง Server	0	0	1	เพลิงไหม้	N	Y	Y		0	1	1		N/A	L	พลภัทร
1-9	สแกนใบสมัครและเอกสารประกอบการสมัครสมาชิกลง Server	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร
1-10	การออกหนังสือรับรองการเป็นสมาชิก	0	0	1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity of sentisive information)	N	Y	N		0		2		N/A		พลภัทร
1-11	กระบวนการเปลี่ยนข้อมูลสมาชิก	0	1	3	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			3	1			M	
1-11	กระบวนการเปลี่ยนข้อมูลสมาชิก	0	1	3	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of Information/ Espionage)	Y	N	N	0			1	N/A			พลภัทร
1-11	กระบวนการเปลี่ยนข้อมูลสมาชิก	0	1	3	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	1		1	N/A	L		พลภัทร
1-12	เตรียมบัญชีรายชื่อผู้มีสิทธิเข้ารับเลือกเป็น คกก. เนติบัณฑิตยสภา	0	4	1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity fo sentisive information)	N	Y	N		4		1		M		พลภัทร
1-14	ตรวจสอบบัญชีรายชื่อผู้มีสิทธิได้รับเลือกเป็น คกก. เนติบัณฑิตยสภา	0	0	1	ข้อมูลสำคัญมีความไม่สมบูรณ์ถูกต้อง (Loss integrity fo sentisive information)	N	Y	N		0		1		N/A		พลภัทร

1.2 สินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อข้อมูล	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-18	เอกสารการสมัครสมาชิกวิสามัญ ข้อ 5(1)	0	3	4	ข้อมูลสูญหาย	N	N	Y			4	1			M	พลภัทร
1-19	เอกสารการสมัครสมาชิกวิสามัญ ข้อ 5(2)	0	3	4	ข้อมูลสูญหาย	N	N	Y			4	1			M	พลภัทร
1-20	ฐานข้อมูลรายนามสมาชิกวิสามัญ	0	3	4	ข้อมูลสูญหาย	N	N	Y			4	1			M	พลภัทร
1-20	ฐานข้อมูลรายนามสมาชิกวิสามัญ	0	3	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	3		2	N/A	M		พลภัทร
1-21	ฐานข้อมูลรายนามสามัญสมาชิก	0	3	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	3		2	N/A	M		พลภัทร
1-21	ฐานข้อมูลรายนามสามัญสมาชิก	0	3	4	ข้อมูลสูญหาย	N	N	Y			4	1			M	พลภัทร
1-22	ฐานข้อมูลรายนามสมาชิกสมทบ	0	3	4	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	0	3		2	N/A	M		พลภัทร
1-22	ฐานข้อมูลรายนามสมาชิกสมทบ	0	3	4	ข้อมูลสูญหาย	N	N	Y			4	1			M	พลภัทร
1-23	รายงานการประชุม	0	3	4	เพลิงไหม้	N	Y	Y		3	4	1		M	L	พลภัทร

1.3 สินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อซอฟต์แวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-24	OS: Microsoft Windows 8.1	0	0	3	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			3	2			M	พลภัทร
1-24	OS: Microsoft Windows 8.1	0	0	3	ความลับถูกเปิดเผย	Y	N	N	0			2	N/A			พลภัทร
1-25	Microsoft Office2013	0	0	3	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			3	2			M	พลภัทร
1-26	Microsoft access 2010	0	0	3	ความลับถูกเปิดเผย	Y	N	N	0			2	N/A			พลภัทร
1-27	Typo (MySQL)	0	0	3	ข้อมูลสูญหาย	N	N	Y			3	2			M	พลภัทร

1.4 สินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อฮาร์ดแวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-28	เครื่อง Server Intel QuadCore Q9400	0	0	4	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง (Power supply)	N	Y	Y		0	4	1		N/A	M	พลภัทร
1-28	เครื่อง Server Intel QuadCore Q9400	0	0	4	เพลิงไหม้	N	Y	Y		0	4	1		N/A	M	พลภัทร
1-28	เครื่อง Server Intel QuadCore Q9400	0	0	4	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบโอที (Interception)	Y	N	N	0			3	N/A			พลภัทร
1-28	เครื่อง Server Intel QuadCore Q9400	0	0	4	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	4	1	N/A	N/A	M	พลภัทร

1.5 สินทรัพย์ ด้านบุคลากร (People Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ตำแหน่ง	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
1-45	หัวหน้าแผนกทะเบียนสมาชิกา	0	0	3	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	3	1	N/A	N/A	M	พลภัทร
1-45	เจ้าพนักงานทะเบียน	0	0	3	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			3	3			H	พลภัทร
1-46	เจ้าพนักงานทะเบียน	0	0	3	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	3	1	N/A	N/A	M	พลภัทร
1-47	เจ้าพนักงานทะเบียน	0	0	1	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	1	1	N/A	N/A	L	พลภัทร
1-48	เจ้าพนักงานทะเบียน	0	0	3	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	3	1	N/A	N/A	M	พลภัทร
1-48	เจ้าพนักงานทะเบียน	0	0	3	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			3	3			H	พลภัทร
1-48	เจ้าพนักงานทะเบียน	0	0	3	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	3	1	N/A	N/A	M	พลภัทร
1-50	เจ้าพนักงานทะเบียน	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	3			M	พลภัทร
1-50	เจ้าพนักงานทะเบียน	0	0	1	แอบอ้างสิทธิการใช้งาน (Abuse of Authorisations)	Y	Y	Y	0	0	1	1	N/A	N/A	L	พลภัทร
1-51	เจ้าพนักงานทะเบียน	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	1			L	พลภัทร

1.6 สินทรัพย์ ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์		ค่าของสินทรัพย์			ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อโครงสร้างพื้นฐาน		C	I	A	ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
							C	I	A	C	I	A		C	I	A	
1-52	ห้องแผนกทะเบียนสมาชิกและทนายความ		2	0	3	เพลิงไหม้	N	Y	Y		0	3	1		N/A	M	พลภัทร
1-53	ระบบไฟฟ้า		0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
1-54	ระบบโทรศัพท์		0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
1-55	ระบบอินเตอร์เน็ต		0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
1-56	ระบบเครื่องปรับอากาศ		0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
1-57	อุปกรณ์ดับเพลิง		0	4	4	อุปกรณ์และระบบทำงานผิดพลาด	Y	Y	Y	4		4	1	N/A	M	M	พลภัทร

2. งานการเงิน (กองคลัง)

2.1 สินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-1	กระบวนการส่ง ภงด.1 แผ่นซีดี แคชเชียร์เช็ค ให้กรมสรรพากร	0	2	3	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y	0		3	1	N/A		M	พลภัทร
2-1	กระบวนการส่ง ภงด.1 แผ่นดิสก์ แคชเชียร์เช็ค ให้กรมสรรพากร	0	2	3	ความลับถูกเปิดเผย	Y	N	N	0			3	N/A			พลภัทร
2-2	กระบวนการตั้งเบิกฎีกาเงินเดือน	2	1		ความลับถูกเปิดเผย	Y	N	N	2			1	L			พลภัทร
2-3	กระบวนการส่งเงินให้สหกรณ์ สำนักงานศาลยุติธรรม	0	0	4	ความลับถูกเปิดเผย	Y	N	N	0			3	N/A			พลภัทร
2-4	กระบวนการส่งเงินที่ พนง. กู้ให้ ธนาคารอาคารสงเคราะห์ (ธอส.)	0	0	4	ความลับถูกเปิดเผย	Y	N	N	0			3	N/A			พลภัทร
2-5	กระบวนการส่งเงินสดให้สวัสดิการพนักงานนนทบุรีพิทยสภา	2	0	4	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y	2		4	1	L		M	พลภัทร
2-6	กระบวนการโอนเงินเดือนเข้าบัญชีพนักงาน	2	2	0	ความลับถูกเปิดเผย	Y	N	N	2			2	M			พลภัทร
2-7	กระบวนการจัดทำ/จัดพิมพ์/จัดส่งสลิปเงินเดือน	2	0	0	ความลับถูกเปิดเผย	Y	N	N	2			1	L			พลภัทร

2.2 สินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อข้อมูล	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-8	เอกสารข้อมูลเงินภาษีหัก ณ ที่จ่าย ของ พนง. (และไฟล์)	2	1	2	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร
2-9	แคชเชียร์เช็คเงินตาม ภงด.1	1	1	1	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	1			2	L			พลภัทร
2-10	แผ่นซีดี ข้อมูลการหักเงินภาษี ณ ที่จ่าย ของ พนง.	1	1	1	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	1			2	L			พลภัทร
2-11	เอกสารฎีกาเงินเดือน (และไฟล์)	1	1	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	1			2	L			พลภัทร
2-12	แคชเชียร์เช็ค สั่งจ่ายเงินให้สหกรณ์สำนักงานศาลยุติธรรม	1	1	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	1			2	L			พลภัทร

2.2 สินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets) (ต่อ)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อข้อมูล	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-13	เอกสารสั่งโอนเงิน พนง. ให้ ธอส. (กรณี พนง.กู้) (และไฟล์)	2	1	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร
2-14	ใบเสร็จการโอนเงินของ พนง. แต่ละคนให้ ธอส. (และไฟล์)	1	0	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	1			2	L			พลภัทร
2-15	สลิปเงินเดือน พนง. (และไฟล์)	2	2	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร
2-16	username/password สำหรับเข้าใช้งาน	2	2	1	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร
2-17	เอกสารแจ้งยอดการถอนเงินจากธนาคารเพื่อไปจ่ายเงินเดือน พนง.	2	2	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร

2.3 สินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง				
	ชื่อซอฟต์แวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-18	โปรแกรมคำนวณภาษีเงินได้ หัก ณ ที่จ่าย	2	1	2	หยุดทำงานเนื่องจากระบบไฟฟ้า	N	Y	Y		1	2	1		L	L	พลภัทร
2-18	โปรแกรมคำนวณภาษีเงินได้ หัก ณ ที่จ่าย	2	1	2	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			1	L			พลภัทร
2-19	OS: Microsoft Windows 8.1	0	0	3	ความลับถูกเปิดเผย	Y	N	N	0			2	N/A			พลภัทร
2-20	Microsoft Office2013	0	0	1	อุปกรณ์และระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร
2-21	Microsoft excel	2	2	3	อุปกรณ์และระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			3	2			M	พลภัทร
2-22	Microsoft Word	2	2	3	อุปกรณ์และระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			3	2			M	พลภัทร

2.4 สินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อฮาร์ดแวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-23	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ Intel คำนวณภาษีสรรพากร, และเก็บไฟล์ข้อมูลเงินภาษีหัก ณ ที่จ่าย ของพนง.	2	2	2	ข้อมูลสูญหาย	N	N	Y			2	2			M	พลภัทร
2-24	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ Intel เอกสารธุรการ งานบันทึก เงินเดือน	2	2	2	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of information/ Espionage)	Y	N	N	2			2	M			พลภัทร
2-25	Printer HP Laser 1200 - ไฟล์ Ms.Excel ที่เก็บข้อมูลสลิปเงินเดือน	1	1	1	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง (Power supply)	N	Y	Y	1	1		1		L	L	พลภัทร
2-26	Printer HP Laser 1200 - ไฟล์ภูกาเงินเดือน - ไฟล์สั่งโอนเงิน พนง. ให้ ธอส. (กรณี พนง.กู้) - ไฟล์สั่งถอนเงินสด เพื่อส่งสวัสดิการพนักงานเนติฯ (กรณี พนง.กู้) - ไฟล์สั่งโอนเงินเดือน เข้าบัญชีเงินเดือน พนง. ผ่าน ธนาคารออมสิน	1	1	1	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง (Power supply)	N	Y	Y	1	1		1		L	L	พลภัทร

2.5 สินทรัพย์ ด้านบุคลากร (People Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ตำแหน่ง	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-27	หัวหน้าแผนกการเงิน	2	3	0	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	3		2	M	M		พลภัทร
3-28	เจ้าพนักงานการเงินและบัญชี	2	2	0	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	2		1	L	L		พลภัทร
3-29	เจ้าพนักงานการเงินและบัญชี	2	2	0	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	2		1	L	L		พลภัทร
3-30	เจ้าพนักงานการเงินและบัญชี	2	2	0	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	2		1	L	L		พลภัทร
3-31	เจ้าพนักงานการเงินและบัญชี	2	2	0	การปฏิเสธความรับผิดชอบ (Repudiation of actions)	Y	Y	N	2	2		1	L	L		พลภัทร

2.6 สินทรัพย์ ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อโครงสร้างพื้นฐาน	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
2-32	ห้องแผนกการเงิน	2	0	3	เพลิงไหม้	N	Y	Y		0	3	1		N/A	M	พลภัทร
2-33	ระบบไฟฟ้า	0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
2-34	ระบบโทรศัพท์	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
2-35	ระบบอินเตอร์เน็ต	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
2-36	ระบบเครื่องปรับอากาศ	0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
2-37	อุปกรณ์ดับเพลิง	0	4	4	อุปกรณ์และระบบทำงานผิดพลาด	Y	Y	Y		4	4	1	N/A	M	M	พลภัทร

3. งานบริหารจัดการนักศึกษา (กองบริการ)

3.1 สินทรัพย์ ด้านกระบวนการทางธุรกิจหรือกิจกรรม (Business processes)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อกระบวนการ	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-1	บริการรับสมัครนักศึกษาใหม่ - เก่า เรียนภาคปกติ	0	3	3	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา	Y	Y	Y	0	3	3	1	N/A	M	M	พลภัทร
3-1	บริการรับสมัครนักศึกษาใหม่ - เก่า เรียนภาคปกติ	0	3	3	ภัยธรรมชาติ เช่น น้ำท่วม	N	N	Y			3	1			M	พลภัทร
3-2	บริการรับสมัครนักศึกษาเรียนภาคค่ำ เรียนภาคทบทวน	0	3	3	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา	Y	Y	Y	0	3	3	1	N/A	M	M	พลภัทร
3-2	บริการรับสมัครนักศึกษาเรียนภาคค่ำ เรียนภาคทบทวน	0	3	3	ภัยธรรมชาติ เช่น น้ำท่วม	N	N	Y			3	1			M	พลภัทร
3-3	บริการรับสมัครสอบไล่	0	3	3	หยุดทำงานเนื่องจากผู้ให้บริการมีปัญหา	Y	Y	Y	0	3	3	1	N/A	M	M	พลภัทร
3-3	บริการรับสมัครสอบไล่	0	3	3	ภัยธรรมชาติ เช่น น้ำท่วม	N	N	Y			3	1			M	พลภัทร
3-4	บริการ Video Streamming	4	0	1	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of Information/ Espionage)	Y	N	N	4			3	H			พลภัทร
3-4	บริการ Video Streamming	4	0	1	การดักฟังข้อมูลในระบบไอทีหรือระบบคอมพิวเตอร์ (Eavesdropping)	Y	N	N	4			3	H			พลภัทร
3-5	บริการ Video ย้อนหลัง	4	0	1	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of Information/ Espionage)	Y	N	N	4			3	H			พลภัทร
3-5	บริการ Video ย้อนหลัง	4	0	1	การดักฟังข้อมูลในระบบไอทีหรือระบบคอมพิวเตอร์ (Eavesdropping)	Y	N	N	4			3	H			พลภัทร

3.2 สินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อข้อมูล	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-6	ฐานข้อมูลทะเบียนนักศึกษา	0	3	3	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา (Communication Network)	N	Y	Y		3	3	1		M	M	พลภัทร
3-6	ฐานข้อมูลทะเบียนนักศึกษา	0	3	3	เพลิงไหม้	N	Y	Y		3	3	1		M	M	พลภัทร
3-6	ฐานข้อมูลทะเบียนนักศึกษา	0	3	3	ข้อมูลสูญหาย	N	N	Y			3	1			M	พลภัทร
3-7	ไฟล์ข้อมูลการชำระเงินที่ธนาคาร	0	2	2	ความเสียหายจากน้ำ	N	Y	Y		2	2	1		L	L	พลภัทร
3-8	ไฟล์ข้อมูลทะเบียนการรับธนาณัติ	0	2	2	ความเสียหายจากน้ำ	N	Y	Y		2	2	1		L	L	พลภัทร
3-10	ใบสมัครนักศึกษา	0	3	3	ข้อมูลสูญหาย	N	N	Y			3	1			M	พลภัทร
3-10	ใบสมัครนักศึกษา	0	3	3	เพลิงไหม้	N	Y	Y		3	3	1		M	M	พลภัทร
3-11	ใบบันทึกคะแนน (แผ่นใหญ่)	3	4	4	เพลิงไหม้	N	Y	Y		3	3	1		M	M	พลภัทร
3-11	ใบบันทึกคะแนน (แผ่นใหญ่)	3	4	4	การเข้าถึงสถานที่หรือบริเวณต้องห้าม	Y	Y	Y	3	4	4	1	M	M	M	พลภัทร
3-11	ใบบันทึกคะแนน (แผ่นใหญ่)	3	4	4	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูลและเอกสาร	Y	N	Y	3		4	1	M		M	พลภัทร

3.2 สินทรัพย์ ด้านข้อมูลสารสนเทศ (Information Assets) (ต่อ)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ชื่อข้อมูล	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-12	แผ่นซีดี บันทึกข้อมูลคะแนนสอบ	3	4	4	เพลิงไหม้	N	Y	Y		3	3	1		M	M	พลภัทร
3-13	วีดีโอ บันทึกการบรรยาย	4	0	0	Abuse of personal data	Y	N	N	4			2	H			พลภัทร
3-13	วีดีโอ บันทึกการบรรยาย	4	0	0	การขโมยอุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสาร	Y	N	Y	4		0	1	M		N/A	พลภัทร
3-14	ไฟล์วีดีโอการบรรยาย	4	0	0	การล้วงความลับหรือข้อมูลจากระบบคอมพิวเตอร์หรือระบบไอที (Interception of Information)	Y	N	N	4			1	M			พลภัทร
3-14	ไฟล์วีดีโอการบรรยาย	4	0	0	อุปกรณ์ อุปกรณ์ที่เก็บข้อมูล และเอกสารสูญหาย	Y	N	Y	4		0	1	M		N/A	พลภัทร
3-15	CD Video บรรยาย	4	0	0	Abuse of personal data	Y	N	N	4			2	H			พลภัทร

3.3 สินทรัพย์ ด้านซอฟต์แวร์ (Software Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อซอฟต์แวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-16	OS: Microsoft Windows Server 2008	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
3-16	OS: Microsoft Windows Server 2008	0	0	2	อุปกรณ์ละระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			2	1			L	พลภัทร
3-17	Micosoft SQL Server 2008	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
3-17	Micosoft SQL Server 2008	0	0	2	อุปกรณ์ละระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			2	1			L	พลภัทร
3-18	โปรแกรมบริหารจัดการฐานข้อมูลทะเบียนนักศึกษา	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
3-18	โปรแกรมบริหารจัดการฐานข้อมูลทะเบียนนักศึกษา	0	0	2	อุปกรณ์ละระบบ ขัดข้องไม่สามารถใช้งานได้	N	N	Y			2	1			L	พลภัทร
3-19	OS: Microsoft Windows 8.1	0	0	3	ความลับถูกเปิดเผย	Y	N	N				2	N/A			พลภัทร
3-20	Microsoft Office 2013	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร

3.4 สินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง				
	ชื่อฮาร์ดแวร์	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-21	Web Server	0	1	1	เพลิงไหม้	N	Y	Y		1	1	1		L	L	พลภัทร
3-21	Web Server	0	1	1	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง (Power supply)	N	Y	Y		1	1	1		L	L	พลภัทร
3-21	Web Server	0	1	1	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา (Communication Network)	N	Y	Y		1	1	1		L	L	พลภัทร
3-22	Database Server	0	2	2	เพลิงไหม้	N	Y	Y		2	2	1		L	L	พลภัทร
3-22	Database Server	0	2	2	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา (Communication Network)	N	Y	Y		2	2	1		L	L	พลภัทร
3-22	Database Server	0	2	2	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา (Communication Network)	N	Y	Y		2	2	1		L	L	พลภัทร
3-23	TOKEN	0	0	2	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	Y	Y			2	1			L	พลภัทร
3-24	เครื่องพิมพ์บัตรประจำตัวนักศึกษา	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร
3-25	เครื่องสแกน	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร
3-26	Laser Printer	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร
3-27	Barcode Reader	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้	N	N	Y			1	1			L	พลภัทร

3.4 สินทรัพย์ ด้านฮาร์ดแวร์ (Hardware Assets) (ต่อ)

เลขที่	สินทรัพย์					ประเมินความเป็นไปได้ (จากภัยคุกคาม)									ความเสี่ยง			
	ชื่อฮาร์ดแวร์	ค่าของสินทรัพย์				ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A			C	I	A	C	I	A		C	I	A	
3-28	เครื่องคอมพิวเตอร์ชนิดตั้งโต๊ะ	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้		N	N	Y			1	1			L	พลภัทร
3-29	UPS Victron	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้		N	N	Y			1	1			L	พลภัทร
3-30	Server ระบบลงทะเบียน	3	3	3	การโจมตี (Attack)		Y	Y	Y	3	3	3	1	M	M	M	พลภัทร
3-30	Server ระบบลงทะเบียน	3	3	3	Software ประสงค์ร้าย		Y	Y	Y	3	3	3	1	M	M	M	พลภัทร
3-31	Server Streamming	2	2	0	การเข้าถึงระบบไอทีโดยไม่ได้รับอนุญาต		Y	Y	N	2	2		1	L	L		พลภัทร
3-32	เครื่องบันทึกเทปวีดีโอ	0	0	2	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้		N	N	Y			2	1			L	พลภัทร
3-33	Comodo Firewall	0	0	1	อุปกรณ์และระบบขัดข้องไม่สามารถใช้งานได้		N	N	Y			1	1			L	พลภัทร
3-34	เครื่องคอมพิวเตอร์พิมพ์งานรับสมัครสอบ 1	0	1	1	เพลิงไหม้		N	Y	Y		1	1	1		L	L	พลภัทร
3-34	เครื่องคอมพิวเตอร์พิมพ์งานรับสมัครสอบ 1	0	1	1	หยุดทำงานเนื่องจากระบบไฟฟ้าขัดข้อง (Power supply)		N	Y	Y		1	1	1		L	L	พลภัทร
3-34	เครื่องคอมพิวเตอร์พิมพ์งานรับสมัครสอบ 1	0	1	1	หยุดทำงานเนื่องจากเครือข่ายสื่อสารมีปัญหา (Communication Network)		N	Y	Y		1	1	1		L	L	พลภัทร

3.5 สินทรัพย์ ด้านบุคลากร (People Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)								ความเสี่ยง			
	ตำแหน่ง	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-35	เลขาธิการสำนักอบรมฯ	0	0	2	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			2	1			L	พลภัทร
3-36	รองเลขาธิการสำนักอบรมฯ	0	0	2	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			2	1			L	พลภัทร
3-37	ผู้อำนวยการกองบริการฯ	0	0	2	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			2	1			L	พลภัทร
3-38	หัวหน้าแผนกทะเบียนและประเมินผล	0	0	2	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			2	1			L	พลภัทร
3-39	เจ้าหน้าที่แผนกธุรการ (นายช่างไฟฟ้า)	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	1			L	พลภัทร
3-40	เจ้าพนักงานทะเบียนแผนกทะเบียนและประเมินวัดผล	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	1			L	พลภัทร
3-41	เจ้าหน้าที่แผนกธุรการ (นายช่างไฟฟ้า)	0	0	4	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			4	2			H	พลภัทร
3-42	หัวหน้าแผนกทะเบียนและประเมินผล	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	1			L	พลภัทร
3-43	เจ้าพนักงานทะเบียนแผนกทะเบียนและประเมินผล	0	0	1	การขาดงานของพนักงานที่รับผิดชอบ (Absence of Personnel)	N	N	Y			1	1			L	พลภัทร

3.6 สินทรัพย์ ด้านโครงสร้างพื้นฐาน (Infrastructure Assets)

เลขที่	สินทรัพย์				ประเมินความเป็นไปได้ (จากภัยคุกคาม)							ความเสี่ยง			
	ชื่อโครงสร้างพื้นฐาน	ค่าของสินทรัพย์			ภัยคุกคาม	มีผลต่อ			ผลกระทบ			โอกาสที่จะเกิด	ระดับความเสี่ยง			ผู้ประเมิน
		C	I	A		C	I	A	C	I	A		C	I	A	
3-44	ห้อง OSS: One Stop Server	2	0	3	เพลิงไหม้	N	Y	Y		0	3	1		N/A	M	พลภัทร
3-45	ระบบไฟฟ้า	0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
3-46	ระบบโทรศัพท์	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
3-47	ระบบอินเตอร์เน็ต	0	0	2	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			2	1			L	พลภัทร
3-48	ระบบเครื่องปรับอากาศ	0	0	1	หยุดทำงานเนื่องจากบริการพื้นฐานทั้งหมดขัดข้อง (Mains supply)	N	N	Y			1	1			L	พลภัทร
3-49	อุปกรณ์ดับเพลิง	0	4	4	อุปกรณ์และระบบทำงานผิดพลาด	Y	Y	Y		4	4	1	N/A	M	M	พลภัทร

ประวัติผู้ศึกษา

ชื่อ	นายพลภัทร สุนทรทิวากร
วัน เดือน ปีเกิด	1 กุมภาพันธ์ 2527
สถานที่เกิด	ภาชี จังหวัดพระนครศรีอยุธยา
ประวัติการศึกษา	เทคโนโลยีบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช 2549
	ศึกษาศาสตรบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช 2552
สถานที่ทำงาน	เนติบัณฑิตยสภา ในพระบรมราชูปถัมภ์ กรุงเทพมหานคร
ตำแหน่ง	นักวิชาการเทคโนโลยีสารสนเทศ