# การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง

**นางสาวรัตนาภรณ์ บุญสิน**

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
เขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2558

# Development of IT Security Policy Framework and Management based on ISO/IEC 27001:2013 Standard : A Case Study of the Governor's Office of Phatthalung Province

**Miss Rattanaporn Boonsin**

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
2015

| | |
|---|---|
| **หัวข้อการศึกษาค้นคว้าอิสระ** | การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง |
| **ชื่อและนามสกุล** | นางสาวรัตนาภรณ์ บุญสิน |
| **แขนงวิชา** | เทคโนโลยีสารสนเทศและการสื่อสาร |
| **สาขาวิชา** | วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช |
| **อาจารย์ที่ปรึกษา** | ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน |

การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 31 สิงหาคม 2559

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน)

.....กรรมการ
(อาจารย์ ดร. อำนาจ ขาวเน)

.....
(รองศาสตราจารย์ณัฏฐพร พิมพายน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

**ชื่อการศึกษาค้นคว้าอิสระ** การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง

**ผู้ศึกษา** นางสาวรัตนาภรณ์ บุญสิน**รหัสนักศึกษา** 2569600063

**ปริญญา** วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

**อาจารย์ที่ปรึกษา** ผู้ช่วยศาสตราจารย์ ดร. ขจิตพรรณ กฤตพลวิมาน **ปีการศึกษา** 2558

## บทคัดย่อ

การค้นคว้าอิสระนี้ มีวัตถุประสงค์เพื่อ 1) พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ตามมาตรฐาน ISO/IEC 27001:2013 2) เพื่อลดและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อสำนักงานจังหวัดพัทลุง

งานวิจัยนี้ได้ดำเนินการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสำนักงานจังหวัดพัทลุง ตามมาตรฐาน ISO/IEC 27001:2013 และดำเนินงานตามระบบบริหารด้านความมั่นคงปลอดภัยสารสนเทศ โดยการติดตั้งอุปกรณ์และระบบรักษาความมั่นคงปลอดภัย ให้สอดคล้องตามกรอบนโยบายด้านความมั่นคงปลอดภัยที่ได้พัฒนาขึ้น ทั้งนี้เพื่อเพิ่มประสิทธิภาพในการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อสำนักงานจังหวัดพัทลุง

ผลการประเมินพบว่าการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง ทำให้หน่วยงานมีนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ใช้เป็นแนวทางปฏิบัติงานของเจ้าหน้าที่และระบบบริหารด้านความมั่นคงปลอดภัยสารสนเทศสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงลดลง โดยระดับความเสี่ยงสูงลดลงจนเป็นศูนย์

**คำสำคัญ** ระบบบริหารด้านความมั่นคงปลอดภัยสารสนเทศ, นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ, ISO/IEC 27001:2013

**Independent Study title:** Development of IT Security Policy Framework and Management based on ISO/IEC 27001:2013 Standard: A Case Study of the Governor's Office of Phatthalung Province
**Author:** Miss Rattanaporn Boonsin; **ID:** 2569600063;
**Degree:** Master of Science (Information and Communication Technology);
**Independent Study advisor:** Dr. Khajitpan Kritpolviman, Assistant Professor;
**Academic year:** 2015

## Abstract

The Research Independent Study aimed 1) to develop IT security policy framework for the governor's office of Phatthalung Province based on ISO/IEC 27001:2013 and 2) to decrease and protect IT risks that might occur and effect to the governor’s office of Phatthalung Province.

This research has processed by the IT analysis and IT risk evaluation. Then, the IT security policy framework for the Governor's Office of Phatthalung Province was developed based on ISO/IEC 27001:2013 and implemented by following the Information Security Management System (ISMS) process. The devices and security systems were practically installed according to the developed IT security policy framework in order to prevent the IT risks that possibly occur at the governor’s office of Phatthalung Province.

The evaluation results were found that IT security policy framework of the governor's office of Phatthalung Province based on ISO/IEC 27001:2013 was used as the guideline for IT process operated by staffs, and ISMS process. This implementation effectively decreased the IT risks of the governor’s office of Phatthalung Province to level 0, as described in the IT risk assessment and evaluation results after the implementation.

**Keyword**: Information Security Management System, IT Security Policy, ISO/IEC 27001:2013

# กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระฉบับนี้สำเร็จได้นั้น เนื่องด้วยได้รับคำแนะนำจากผู้ช่วยศาสตราจารย์.ดร.ขจิตพรรณ กฤตพลวิมาน ที่ให้คำปรึกษา ชี้แนะแนวทางการศึกษาค้นคว้าอิสระฉบับนี้ด้วยดีตลอดมา และมหาวิทยาลัยสุโขทัยธรรมธิราชที่มอบทุนสนับสนุนการศึกษาค้นคว้าอิสระฉบับนี้ รวมถึงได้รับการสนับสนุนจากผู้บังคับบัญชาและเจ้าหน้าที่ผู้ร่วมงานทุกท่านที่ให้ความร่วมมือในการจัดการบริหารรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน ตลอดจนครอบครัวที่ให้การสนับสนุนและเป็นกำลังใจในการศึกษาตลอดมาด้วย ผู้จัดทำจึงขอขอบพระคุณทุกท่านมา ณ โอกาสนี้

รัตนาภรณ์ บุญสิน

สิงหาคม 2559

# สารบัญ

# สารบัญ (ต่อ)

หน้า

# สารบัญตาราง

หน้า

# สารบัญภาพ

หน้า

# บทที่ 1
# บทนำ

## 1. ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศมีการพัฒนาอย่างต่อเนื่อง ทำให้เกิดความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศอย่างไม่หยุดยั้ง มีการนำระบบเทคโนโลยีสารสนเทศมาเชื่อมโยงเป็นเครือข่ายทั่วโลก จึงทำให้เกิดการนำเทคโนโลยีสารสนเทศและการสื่อสารเหล่านี้มาใช้ประโยชน์อย่างกว้างขวาง ตั้งแต่การใช้งานเพื่ออำนวยความสะดวก เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการให้บริการข้อมูลข่าวสาร งานบริการด้านการทำธุรกิจเพื่อสร้างความได้เปรียบทางการแข่งขัน ซึ่งต้องยอมรับว่ายุคนี้เป็นยุคแห่งข้อมูลข่าวสาร ยุคแห่งการแข่งขันด้านข้อมูลสารสนเทศ กล่าวคือ หน่วยธุรกิจที่สามารถเข้าถึงข้อมูลและวิเคราะห์ข้อมูลได้ก่อนจะเป็นผู้ได้เปรียบทางการแข่งขัน ทำให้ปัจจุบันนี้ระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาททางการแข่งขันทางธุรกิจสูงมาก ระบบเทคโนโลยีสารสนเทศไม่เพียงแต่ช่วยอำนวยความสะดวกในการทำงานเท่านั้น ทุกวันนี้ระบบเทคโนโลยีสารสนเทศถือเป็นกุญแจสำคัญในการประกอบธุรกิจก็ว่าได้ หน่วยงานที่ประสบความสำเร็จทุกวันนี้ล้วนนำระบบเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานด้วยกันทั้งสิ้น เนื่องจากระบบเทคโนโลยีสารสนเทศสามารถช่วยให้หน่วยงานมีความสามารถทางการแข่งขันในโลกไร้พรมแดนได้อย่างมีประสิทธิภาพ เทคโนโลยีสารสนเทศช่วยให้หน่วยธุรกิจสามารถเข้าถึงลูกค้าได้อย่างรวดเร็ว และช่วยให้การให้บริการเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ซึ่งหมายถึงว่า ถ้าหน่วยธุรกิจสามารถประยุกต์ใช้เทคโนโลยีสารสนเทศอย่างชาญฉลาดแล้ว หน่วยธุรกิจนั้นก็สามารถอยู่รอดและเอาชนะคู่แข่งขันในเชิงธุรกิจได้

ด้วยคุณประโยชน์ของระบบเทคโนโลยีสารสนเทศเหล่านี้ ทำให้ผู้ไม่ประสงค์ดีอาศัยช่องโหว่ของระบบเทคโนโลยีสารสนเทศขโมยข้อมูลสารสนเทศของหน่วยงานไปใช้เพื่อประโยชน์ส่วนตน ทำลายระบบเทคโนโลยีสารสนเทศของหน่วยงาน หรือที่ทราบกันดีว่าปัจจุบันนี้เกิดปัญหาภัยคุกคามทางด้านระบบเทคโนโลยีสารสนเทศ ปัญหาอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นอย่างมาก เช่น การโจมตีหน้าเว็บไซต์ การขโมยข้อมูลสำคัญทางธุรกิจ การเจาะทำลายระบบสารสนเทศของหน่วยงาน ปัญหาไวรัส มัลแวร์ เป็นต้น ภัยคุกคามทางระบบเทคโนโลยีสารสนเทศเหล่านี้ ล้วนทำให้หน่วยงานประสบปัญหาในการให้บริการระบบเทคโนโลยีสารสนเทศ สร้างความ

เสียหายทั้งด้านการเงินและชื่อเสียงให้แก่หน่วยงาน ส่งผลให้หน่วยงานจะต้องให้ความสำคัญในการดูแลความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้เพิ่มขึ้น องค์กรต่างๆ ทั้งภาครัฐและภาคเอกชนต้องตระหนักถึงภัยคุกคามด้านระบบเทคโนโลยีสารสนเทศต่างๆ ที่อาจจะเกิดขึ้นต่อหน่วยงาน หน่วยงานต้องมีการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในระดับสากลนั้น ได้กำหนดให้ ISO/IEC 27001 เป็นมาตรฐาน เพื่อใช้เป็นแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ปัจจุบันได้พัฒนามาตรฐานเวอร์ชัน 2013สำหรับประเทศไทยรัฐบาลได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยออกเป็นพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และประกาศคณะธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐรวมถึงพระราชบัญญัติว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ พ.ศ. 2540 ด้วย ดังนั้นเพื่อหาแนวทางป้องกันไม่ให้เกิดความเสียหายแก่หน่วยงาน หน่วยงานต้องมีการเตรียมพร้อมรับมือกับปัญหาด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้มากขึ้น โดยหน่วยงานต้องมีการพัฒนานโยบายหรือมาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยอย่างต่อเนื่องเพื่อป้องกันภัยคุกคามรูปแบบต่าง ๆ ที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน

สำหรับสำนักงานจังหวัดพัทลุง เป็นหน่วยงานภาครัฐ สังกัดสำนักงานปลัดกระทรวงมหาดไทย ทำหน้าที่บูรณาการทุกส่วนราชการภายในจังหวัด สำนักงานจังหวัดพัทลุงได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้เป็นเครื่องมือในการสนับสนุนและอำนวยความสะดวกในการปฏิบัติงาน การติดต่อประสานงาน การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้บริการข้อมูลข่าวสารกับทุกส่วนราชการเพื่อขับเคลื่อนการจัดทำแผนพัฒนาจังหวัด ซึ่งล้วนแต่ต้องอาศัยระบบเทคโนโลยีสารสนเทศในการดำเนินงานทั้งสิ้น โดยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดประกอบด้วย ระบบเครือข่ายของกระทรวงมหาดไทยที่รับสัญญาณผ่านสายไฟเบอร์ออฟติกมายังอาคารศาลากลางจังหวัดพัทลุง ระบบเครือข่ายของหน่วยงานภาครัฐ (Government Infrastructure Network: GIN) พร้อมอุปกรณ์กระจายสัญญาณไปยังทุกชั้นภายในอาคารศาลากลางจังหวัดพัทลุง เครื่องคอมพิวเตอร์แม่ข่ายจังหวัดที่ให้บริการฐานข้อมูลต่างๆ กับทุกส่วนราชการภายในจังหวัด รวมถึงระบบสารสนเทศต่างๆ ที่ให้บริการ ของจังหวัดพัทลุง เช่น เว็บไซต์จังหวัดพัทลุง ระบบจองห้องประชุม ระบบรับส่งหนังสือจังหวัดพัทลุงระบบการประชุมทางไกล (VDO Conference) เป็นต้น

จะเห็นได้ว่า สำนักงานจังหวัดมีระบบเทคโนโลยีสารสนเทศที่ให้บริการส่วนราชการทั้งภายในและภายนอกจังหวัด ดังนั้น เพื่อให้สำนักงานจังหวัดพัทลุงสามารถให้บริการระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง สำนักงานจังหวัดพัทลุงจึงควรตระหนักถึงการดูแลรักษา

ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงาน รวมถึงความเสี่ยงและภัยคุกคามที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงาน ซึ่งปัจจุบันสำนักงานจังหวัดพัทลุงยังไม่ได้มีการกำหนดกรอบนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงาน หรือแนวทางปฏิบัติในการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน เพื่อรองรับและป้องกันภัยคุกคามที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงาน

ในการนี้ผู้วิจัย จึงเห็นว่าสำนักงานจังหวัดพัทลุงควรตระหนักและเล็งเห็นถึงความสำคัญของการกำหนดกรอบนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อรับมือกับภัยคุกคามด้านระบบเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น และเพื่อเพิ่มศักยภาพในการรักษาระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงให้มีความปลอดภัยและพร้อมใช้งาน ด้วยเหตุนี้ผู้จัดทำจึงเห็นว่าสำนักงานจังหวัดพัทลุงควรพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง ขึ้น

## 2. วัตถุประสงค์การวิจัย

2.1 เพื่อพัฒนากรอบนโยบายรักษาความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศให้กับหน่วยงานให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013

2.2 เพื่อลดและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงาน

## 3. กรอบแนวคิดการวิจัย

ตามแนวทางสากลด้านการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ได้กำหนดมาตรฐาน ISO/IEC27001 เพื่อเป็นแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) สร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงาน ให้หน่วยงานสามารถรับมือกับภัยคุกคามระบบสารสนเทศที่อาจจะเกิดขึ้นกับหน่วยงาน และช่วยให้หน่วยงานสามารถดำเนินการต่างๆ ด้านระบบความมั่นคงปลอดภัยเพื่อให้บริการได้อย่างต่อเนื่อง โดยล่าสุดมาตรฐาน ISO/IEC 27001 ออกมาในปี 2013 (ISO/IEC27001 :2013) ในการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศนั้น มีกระบวนการหรือขั้นตอน ที่เกี่ยวข้อง เรียกว่า กระบวนการ PDCA (Plan Do Check Act)

ได้แก่ กระบวนการวางแผน (Plan) เป็นการกำหนดรายการควบคุม การประเมินความเสี่ยงตามรายการควบคุม และกำหนดเป็นนโยบายความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยระบบสารสนเทศ กระบวนการลงมือปฏิบัติ (Do) เป็นการลงมือปฏิบัติตามระบบบริหารจัดการความมั่นคงปลอดภัยที่ได้ประเมินไว้ เพื่อลดช่องโหว่ที่จะเกิดขึ้น กระบวนการการตรวจสอบ (Check) เป็นการประเมินผล ทบทวนสิ่งที่ได้ดำเนินการบริหารจัดการความมั่นคงปลอดภัยไว้ ทบทวนนโยบายด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ ว่าครบถ้วนครอบคลุม ทันสมัยกับภัยคุกคามใหม่ๆ หรือไม่ และการปรับปรุงแก้ไข (Act) ระบบบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน เป็นการนำผลที่ได้จากการตรวจสอบ มาปรับปรุงให้ดีขึ้น

ดังนั้น ในการพัฒนากรอบนโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง ให้มีความน่าเชื่อถือจึงได้นำมาตรฐาน ISO/IEC 27001 : 2013 มาเป็นแนวทางในการพัฒนากรอบนโยบายรักษาความมั่งคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยดำเนินการตามกระบวนการของการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อปรับปรุงระบบรักษาความมั่นคงปลอดภัยของสำนักงานจังหวัดพัทลุงให้มีประสิทธิภาพเพิ่มขึ้น

## 4. ขอบเขตของการวิจัย

4.1 ศึกษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน และเอกสารต่างๆ ที่เกี่ยวข้อง

4.2 ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศปัจจุบันกับมาตรฐานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013 ประกอบด้วย 14 หัวข้อ (Domain) สำคัญดังนี้ คือ

A.5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security)

A.8 การบริหารจัดการทรัพย์สิน (Asset Management)

A.9 การควบคุมการเข้าถึง (Access Control)

A.10 การเข้ารหัสข้อมูล (Cryptography)

A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security)

A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance)

A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

A.18 ความสอดคล้อง (Compliance)

4.3 พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013

4.4 ติดตั้งระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง

4.5 ตรวจสอบและประเมินผลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้กำหนดไว้

## 5. นิยามศัพท์เฉพาะ

**5.1 ทรัพย์สิน** หมายถึง ระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง เช่น อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ รวมถึงระบบเครือข่าย ข้อมูลสำคัญและระบบสารสนเทศที่อยู่ในความรับผิดชอบของสำนักงานจังหวัดพัทลุง

**5.2 ผู้ให้บริการภายนอก** หมายถึง ผู้ให้บริการสัญญาณเครือข่าย หรือผู้รับจ้างพัฒนาระบบสารสนเทศให้กับสำนักงานจังหวัดพัทลุง

**5.3 ภัยคุกคาม** หมายถึง สิ่งที่ทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง

**5.4 ATM Access** หมายถึง อุปกรณ์รับสัญญาณเครือข่ายอินเทอร์เน็ตที่ส่งมาจากกระทรวงมหาดไทย

## 6. ประโยชน์ที่คาดว่าจะได้รับ

6.1 สำนักงานจังหวัดพัทลุงมีกรอบนโยบายรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013

6.2 สำนักงานจังหวัดพัทลุงมีระบบรักษาความมั่นคงปลอดภัยที่สามารถลดและป้องกันความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงานได้

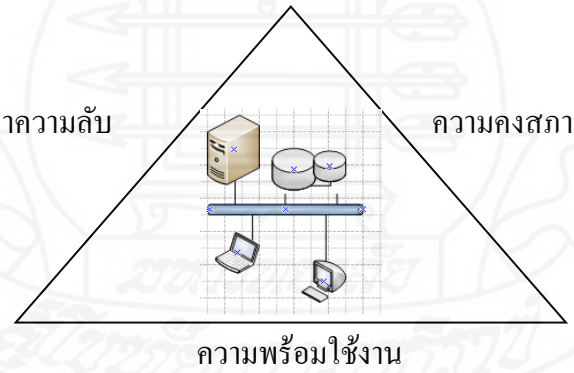
# บทที่ 2
# วรรณกรรมที่เกี่ยวข้อง

## 1. การรักษาความปลอดภัยของข้อมูล

จากปัจจุบันข้อมูลที่สำคัญของหน่วยงานเปรียบเสมือนทรัพย์สินอันมีค่า ซึ่งมักจัดเก็บลงในระบบฐานข้อมูลของหน่วยงาน ระบบคราวด์ (cloud) และเรียกใช้งานผ่านระบบเครือข่าย ทำให้ข้อมูลสารสนเทศที่สำคัญๆ ของหน่วยงานมักถูกขโมยไปใช้ สร้างความเสียหายให้กับหน่วยงาน หน่วยงานจึงต้องมีการรักษาความปลอดภัยให้กับข้อมูลสารสนเทศที่สำคัญเหล่านั้น โดยมีรายละเอียดในการรักษาความปลอดภัยของข้อมูล ดังนี้

### 1.1 หลักการของการรักษาความปลอดภัย

ระบบรักษาความปลอดภัยมีจุดประสงค์ เพื่อรักษาความลับ (Confidentiality) ป้องกันการเปลี่ยนแปลงข้อมูลหรือความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) นิยมเรียกว่า CIA




ภาพที่ 2.1 หลักการของระบบรักษาความปลอดภัย

จากภาพที่ 2.1 แสดงหลักการในของการรักษาความปลอดภัยข้อมูลมีจุดประสงค์ 3 ประการ (จตุชัย แพงจันทร์และอนุโชต วุฒิพรพงษ์, 2555) ดังนี้

***1.1.1 ความพร้อมใช้งาน (Availability)*** เป็นการที่ข้อมูลต้องสามารถเข้าถึงได้ตลอดทุกครั้งที่มีผู้ใช้งานที่มีสิทธิเข้าถึงข้อมูลนั้นร้องขอ ซึ่งอาจมีผู้ไม่ประสงค์ดีพยายามเข้ามาโจมตี

ระบบไม่ให้สามารถใช้งานได้ ซึ่งเป็นหน้าที่ของการรักษาความปลอดภัยที่จะต้องป้องกันไม่ให้เกิดเหตุการณ์ที่ระบบหรือข้อมูลไม่พร้อมใช้งาน

***1.1.2 ความคงสภาพ (Integrity)*** เป็นการทำให้ข้อมูลมีความถูกต้อง ทันสมัยอยู่เสมอ ทำให้ข้อมูลน่าเชื่อถือ โดยต้องรักษาความปลอดภัยให้ข้อมูลสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิให้เข้าแก้ไขหรือเข้าถึงข้อมูลเท่านั้น ประกอบด้วยกระบวนการ ได้แก่ กระบวนการป้องกันเป็นการรักษาความความถูกต้องของข้อมูล ไม่ให้ผู้ไม่ได้รับอนุญาตเข้ามาเปลี่ยนแปลง แก้ไขข้อมูล โดยอาจกำหนดสิทธิและระดับในการเข้าถึงข้อมูลสารสนเทศนั้นๆ และกระบวนการตรวจสอบเป็นการตรวจสอบความถูกต้องของข้อมูลว่ายังคงมีความน่าเชื่อถือ และทันสมัย ตามที่ผู้ใช้งานต้องการ

***1.1.3 การรักษาความลับ (Confidentiality)*** เป็นการป้องกันข้อมูลให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ข้อมูลที่ต้องรักษาความลับ เช่น ข้อมูลส่วนบุคคล ข้อมูลสำคัญทางธุรกิจ วิธีการรักษาความมั่นคงปลอดภัยที่ใช้ในการรักษาความลับ ได้แก่ การควบคุมการเข้าถึง การกำหนดรหัส การเข้ารหัสข้อมูลและการถอดรหัสข้อมูล เพื่อให้แน่ใจว่าเป็นผู้สิทธิในการเข้าถึงข้อมูลชั้นความลับอย่างแท้จริง

ซึ่งการควบคุมการเข้าถึงข้อมูลสารสนเทศนั้น โดยทั่วไปมี 2 ระดับ ได้แก่

การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) เป็นการป้องกันการเข้าถึงของสิ่งของทางกายภาพ เช่น คน สัตว์ ยานพาหนะ เป็นต้น ตัวอย่างการควบคุม เช่น การควบคุมการเข้าออกห้องสื่อสาร การควบคุมอุณหภูมิปรับอากาศ วิธีการควบคุม เช่น การใช้บัตรสมาท์การ์ดเข้าออกห้องสื่อสาร

การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control) เป็นป้องกันการเข้าถึงการใช้งานระบบสารสนเทศ เช่น การแก้ไขข้อมูล การเชื่อมต่อระบบ ตัวอย่างการควบคุม เช่น การกำหนดชั้นความลับ การกำหนดนโยบายในการเข้าถึง วิธีการควบคุม เช่น การกำหนดรหัสผ่าน โดยการควบคุมจะต้องกำหนดระดับสิทธิในการเข้าถึง กำหนดผู้ได้รับอนุญาต อาจกำหนดเป็นรายบุคคลหรือรายกลุ่ม โดยให้สิทธิในการเข้าถึงตามระดับต่างๆ จากนั้นก็เข้าสู่กระบวนการพิสูจน์สิทธิ พร้อมกับการเก็บข้อมูลการเข้าออกระบบ ตลอดจนกิจกรรมต่างๆ ที่เกี่ยวข้อง เพื่อตรวจสอบหาข้อผิดพลาดต่างๆ ได้

**1.2 กระบวนการรักษาความปลอดภัยข้อมูลขององค์กร**

การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการวิเคราะห์และบริหารความเสี่ยง เฝ้าระวังเหตุการณ์ที่เกิดจากภัยคุกคาม และช่องโหว่หรือจุดอ่อนขององค์กรการติดตั้งระบบรักษาความปลอดภัยให้เหมาะสมกับองค์กร รวมถึงกำหนดนโยบายการรักษาความปลอดภัย

การบังคับใช้นโยบาย หรือการหาวิธีปฏิบัติที่เหมาะสมที่สุดสำหรับการรักษาความปลอดภัยข้อมูลขององค์การ ประกอบด้วย 5 ขั้นตอนหลัก (จตุชัย แพงจันทร์, 2550) ดังนี้

***1.2.1 การประเมินความเสี่ยง (Risk Assessment):*** เป็นการตรวจสอบเพื่อประเมินหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศภายในองค์กรโดยการตรวจประเมินหาความเสี่ยงให้ยึดหลักการของการรักษาความปลอดภัยของข้อมูล ได้แก่ ความพร้อมใช้งาน การรักษาความลับและความคงสภาพของข้อมูล โดยการประเมินสถานการณ์ปัจจุบันด้านระบบเทคโนโลยีสารสนเทศของหน่วยงานทั้งในระบบสารสนเทศ ระบบเครือข่าย ให้ครอบคลุมทุกระดับของหน่วยงาน ทั้งทางกายภาพและทางตรรกะ

***1.2.2 การกำหนดนโยบาย (Policy)***

องค์กรต้องกำหนดนโยบายที่เกี่ยวข้องกับการรักษาความปลอดภัยให้ครอบคลุมทั้งนโยบายการรักษาความปลอดภัยทั่วไป การรักษาความปลอดภัยข้อมูล นโยบายในการสำรองข้อมูล นโยบายการสื่อสารข้อมูลระยะไกล เป็นต้น

***1.2.3 การออกแบบและติดตั้งระบบรักษาความปลอดภัย (Implementation)***

เป็นเรื่องของการดำเนินงานทางด้านเทคนิคเพื่อให้เป็นไปตามนโยบายที่กำหนดไว้ องค์กรจะต้องติดตั้งระบบรักษาความปลอดภัย โดยอาจจัดหาอุปกรณ์เครื่องมือทางเทคนิคต่างๆ เพื่อใช้ในการติดตาม เฝ้าระวัง ไม่ให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร ตัวอย่างเช่น การมอนิเตอร์ดูการใช้งานระบบเครือข่าย การติดตั้งไฟร์วอลล์ การติดตั้งระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เพื่อเพิ่มความปลอดภัยในการใช้งานอินเทอร์เน็ต การทำระบบพิสูจน์ทราบตัวตน เป็นต้น

***1.2.4 การฝึกอบรม (Training)***

บุคลากรในองค์กรเป็นส่วนสำคัญที่จะทำให้การรักษาความปลอดภัยในองค์กรประสบความสำคัญ ดังนั้น องค์กรจึงต้องอบรม เผยแพร่ให้ความรู้ความเข้าใจ ให้บุคลากรมีความตระหนักและให้ความร่วมมือในการป้องกันรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน โดยดำเนินการให้ความรู้จัดอบรมด้านการรักษาความปลอดภัยให้กับบุคลากรในองค์กรอย่างต่อเนื่อง

***1.2.5 การตรวจสอบ (Audit)***

องค์กรต้องมีการตรวจสอบและประเมินผล ว่าองค์กรได้ปฏิบัติตามนโยบายการรักษาความปลอดภัยอย่างต่อเนื่อง เช่น มีการตรวจสอบการปฏิบัติตามนโยบายของพนักงาน การตรวจสอบการเจาะระบบ (Penetration Test) เป็นต้น

กล่าวโดยสรุป กระบวนการรักษาความปลอดภัย เป็นกระบวนการเชิงรุกที่ดำเนินการเพื่อให้ข้อมูลมีความคงสภาพ ความพร้อมใช้งาน และสามารถรักษาความลับไว้ได้ โดยกระบวนการรักษาความปลอดภัยจะเกี่ยวข้องกับการบริหารจัดการความเสี่ยง ทั้งในการค้นหาประเมินความเสี่ยงที่มีและอาจจะเกิดขึ้นเพื่อนำมากำหนดนโยบายในการป้องกันรับมือ โดยการติดตั้งระบบหรือเครื่องมือเพื่อดำเนินการให้เป็นไปตามนโยบายรักษาความปลอดภัยที่กำหนดไว้ รวมถึงต้องได้รับความร่วมมือจากผู้เกี่ยวข้องด้วย และมีการตรวจประเมินผล ทั้งนี้ เพื่อลดความเสี่ยงให้อยู่ในสภาพที่ยอมรับได้ ภายใต้งบประมาณที่มีอยู่ ที่สำคัญต้องดำเนินการอย่างต่อเนื่องทุกๆ ขั้นตอน

## 2. มาตรฐาน ISO/IEC 27001

ISO/IEC27001 เป็นมาตรฐานสากลที่ได้กำหนดแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงาน ให้หน่วยงานสามารถรับมือกับภัยคุกคามระบบสารสนเทศที่จะเกิดขึ้น ไม่ว่าจะเป็น การหลอกลวงทางคอมพิวเตอร์ การโจมตีหน้าเว็บไซต์ การโจรกรรมข้อมูล ไวรัสมัลแวร์ รวมถึงป้องกันภัยด้านอื่นๆ เช่น เหตุการณ์จลาจล แผ่นดินไหว อัคคีภัย อุทกภัย (หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ, 2550)

### 2.1 ISO/IEC 27001:2013

ปัจจุบัน ISO/IEC 27001:2013 มีข้อกำหนดหลักที่ต้องปฏิบัติ 14 โดเมน 114 รายการ โดยข้อกำหนดตามมาตรฐาน ISO/IEC 27001:2013 มี 14 โดเมน (บริษัท ที-เน็ต จำกัด, 2556) ดังนี้

A.5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy): ให้หน่วยงานกำหนดทิศทางในการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับภารกิจของหน่วยงาน

A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security): ให้หน่วยงานจัดทำกรอบในการควบคุมให้เกิดการดำเนินงานด้านความมั่นคงปลอดภัย

A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security): ให้ผู้เกี่ยวข้องในหน่วยงานรู้หน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยของหน่วยงาน

A.8 การบริหารจัดการทรัพย์สิน (Asset Management): ให้หน่วยงานสามารถทรัพย์สินและกำหนดการดูแลรักษาทรัพย์สินของหน่วยงานได้

A.9 การควบคุมการเข้าถึง (Access Control): ให้หน่วยงานจำกัดการเข้าถึงเทคโนโลยีสารสนเทศของหน่วยงาน

A.10 การเข้ารหัสข้อมูล (Cryptography): ให้หน่วยงานมีการเข้ารหัสอย่างเหมาะสมเพื่อให้ข้อมูลมีความถูกต้องพร้อมใช้งาน

A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security): ให้หน่วยงานมีการป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงเทคโนโลยีสารสนเทศของหน่วยงานได้

A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security): ให้หน่วยงานปฏิบัติงานด้านความมั่นคงปลอดภัยอย่างถูกต้อง

A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security): ให้หน่วยงานมีการควบคุมการใช้งานระบบเครือข่ายอย่างเหมาะสมและปลอดภัย

A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance): ให้หน่วยงานมีการจัดหา พัฒนาระบบมีความมั่นคงปลอดภัย

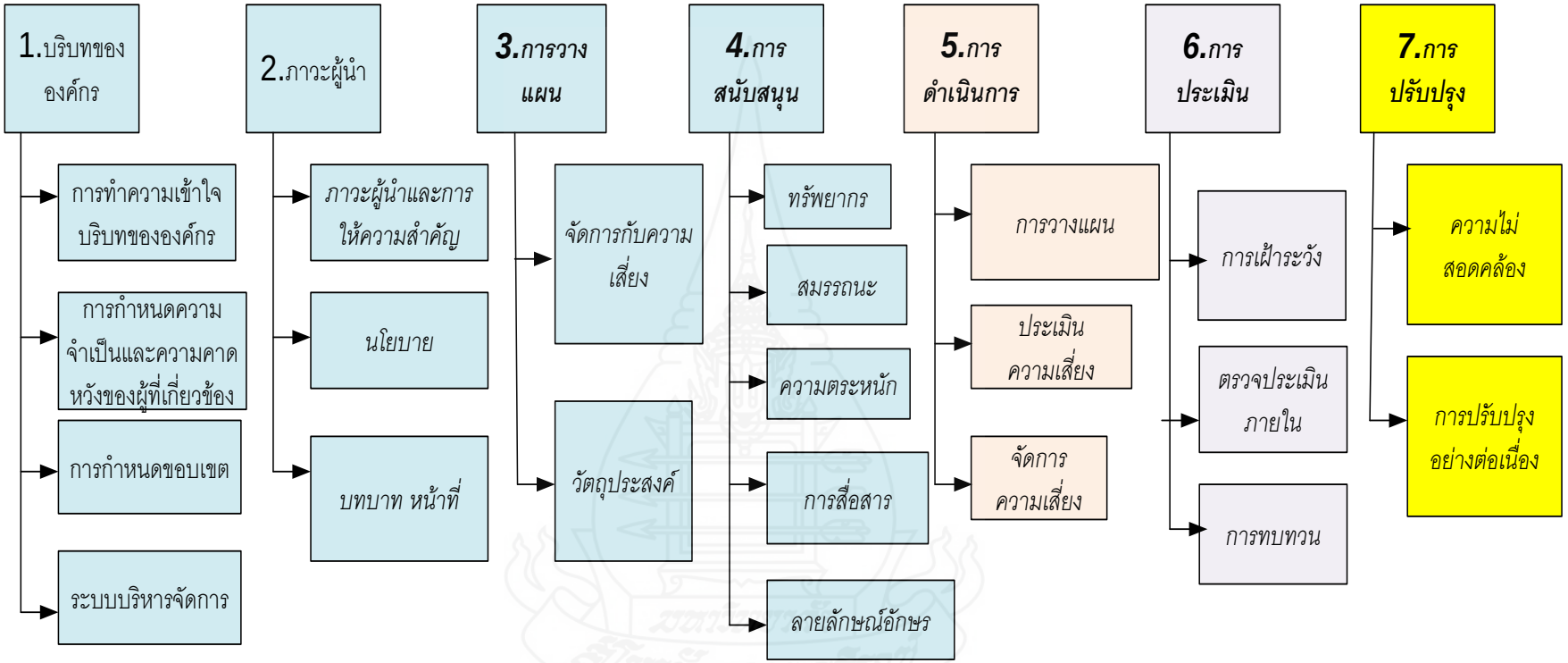
A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships): ให้หน่วยงานมีการป้องกันการเข้าถึงทรัพย์สินจากบุคคลภายนอก

A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management): ให้หน่วยงานมีการบริหารจัดการด้านความมั่นคงปลอดภัยที่เหมาะสม

A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management): ให้หน่วยงานสามารถให้บริการประกอบการได้อย่างต่อเนื่อง

A.18 ความสอดคล้อง (Compliance): ให้หน่วยงานมีการจัดการรักษาความมั่นคงปลอดภัยที่เหมาะสม ไม่ขัดต่อระเบียบ ข้อกฎหมายที่เกี่ยวข้อง

## 2.2 ข้อกำหนดที่ต้องปฏิบัติตามมาตราฐาน ISO/IEC 27001:2013




ภาพที่ 2.2 ข้อกำหนดที่ต้องปฏิบัติตามมาตรฐาน ISO/IEC 27001: 2013

จากภาพที่ 2.2 สามารถอธิบายข้อกำหนดหลักที่ต้องปฏิบัติตามในการขอการรับรองตามมาตรฐาน ISO/IEC 27001:2013 (บริษัท ที-เน็ต จำกัด, 2556) ไว้ดังนี้

***2.2.1 บริบทขององค์กร (Context of the organization)***

1) การทำความเข้าใจบริบทขององค์กร (Understanding the organization and its context): ข้อกำหนดนี้กล่าวถึงว่า องค์กรต้องกำหนดประเด็นที่เกี่ยวข้องทั้งภายในและภายนอกกับให้ครอบคลุมกับวัตถุประสงค์ขององค์กรตามที่ต้องการให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุเป้าหมายตามที่ต้องการ

2) การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties): กำหนดให้องค์กรต้องกำหนดผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและระบุความต้องการที่เกี่ยวข้องระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3) การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system): องค์กรต้องกำหนดกรอบและขอบเขตการประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและจัดทำเป็นลายลักษณ์อักษร

4) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System): องค์กรต้องลงมือปฏิบัติบำรุงรักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

***2.2.2 ภาวะผู้นำ (Leadership)***

1) ภาวะผู้นำและการให้ความสำคัญ (Leadership and Commitment): ในข้อกำหนดนี้ผู้บริหารระดับสูงขององค์กรต้องแสดงภาวะผู้นำและให้ความสำคัญกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ต้องจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับทิศทางกลยุทธ์ขององค์กร ต้องทำให้กระบวนการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเข้ากับกระบวนการขององค์กร ต้องทำให้มีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการดำเนินการ เป็นต้น

2) นโยบาย (Policy): ผู้บริหารระดับสูงขององค์กรต้องจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศซึ่งเหมาะสมกับองค์กรเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้คนในองค์กรทราบและปรับใช้งานตามหน้าที่ที่เกี่ยวข้องได้อย่างเหมาะสม

3) บทบาท หน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ (Organization role, responsibilities and authorities): ผู้บริหารระดับสูงขององค์กรต้องทำให้ผู้ที่เกี่ยวข้องกับความ

มั่นคงปลอดภัยสารสนเทศรับทราบหน้าที่ ความรับผิดชอบ และบทบาทตามที่ได้รับมอบหมาย รวมถึงให้มีการรายงานผลของการดำเนินงานตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

***2.2.3 การวางแผน (Planning)***

1) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Action to address risk and opportunities): องค์กรต้องพิจารณาปัจจัยทั้งภายในและภายนอกที่เกี่ยวข้องที่อาจเป็นความเสี่ยงและโอกาสที่จะทำให้เกิดความเสียหาย เพื่อป้องกันหรือลดหรือจัดการความเสี่ยงและโอกาส และต้องปรับปรุงอย่างต่อเนื่องเพื่อให้บรรลุผลในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามหลักรักษาความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน หลังจากนั้นดำเนินการกำหนดทางเลือกที่เหมาะสมเพื่อจัดการความเสี่ยง พร้อมจัดทำเอกสารมาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษร

2) วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security objective and plans to achieve): องค์กรต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ สามารถวัดได้ในทางปฏิบัติ และสื่อสารให้คนที่เกี่ยวข้องรับทราบ พร้อมปรับปรุงตามความเหมาะสม

***2.2.4 การสนับสนุน (Support)***

1) ทรัพยากร (Resource): องค์กรต้องกำหนดและจัดหาทรัพยากรที่จำเป็นการดำเนินการตามระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ

2) สมรรถนะ (Competence): มีการกำหนดบุคลากรที่เหมาะสมกับงาน มีการอบรมให้ความรู้ในการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ

3) การสร้างความตระหนัก (Awareness): บุคลากรที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศต้องตระหนักถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

4) การสื่อสารให้ทราบ (Communication): องค์กรต้องสื่อสารให้บุคลากรทั้งภายในและภายนอกองค์กรทราบถึงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

5) สารสนเทศที่เป็นลายลักษณ์อักษรการสื่อสารให้ทราบ (Documented information): องค์กรต้องจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นลายลักษณ์อักษร มีการทบทวนปรับปรุงตามความเหมาะสมของบริบทที่เปลี่ยนแปลงไป รวมถึงการจัดเก็บแจกจ่ายและทำลายอย่างเหมาะสมด้วย

***2.2.5 การดำเนินการ (Operation)***

1) การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational planning and control): องค์กรต้องวางแผน ลงมือปฏิบัติ และควบคุมกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามที่ได้กำหนดไว้ พร้อมควบคุมการเปลี่ยนแปลงโดยมีการวางแผนไว้ล่วงหน้า

2) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk assessment): องค์กรต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามรอบเวลาที่กำหนดและจัดเก็บเป็นลายลักษณ์อักษร

3) การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information security risk treatment): องค์กรต้องลงมือปฏิบัติตามแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและจัดเก็บเป็นลายลักษณ์อักษร

***2.2.6 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)***

1) การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน (Monitoring, measurement, analysis and evaluation): องค์กรต้องประเมินประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยการระบุสิ่งที่องค์กรต้องเฝ้าระวัง กำหนดวิธีการเฝ้าระวัง การวัดผล การวิเคราะห์ การประเมินอย่างเหมาะสม พร้อมระบุผู้รับผิดชอบ

2) การตรวจประเมินภายใน (Internal audit): องค์กรต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนดเพื่อให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศยังคงเป็นไปตามความต้องการขององค์กร โดยมีการกำหนดเกณฑ์การตรวจประเมิน การรายงานผล และการจัดเก็บเป็นลายลักษณ์อักษร

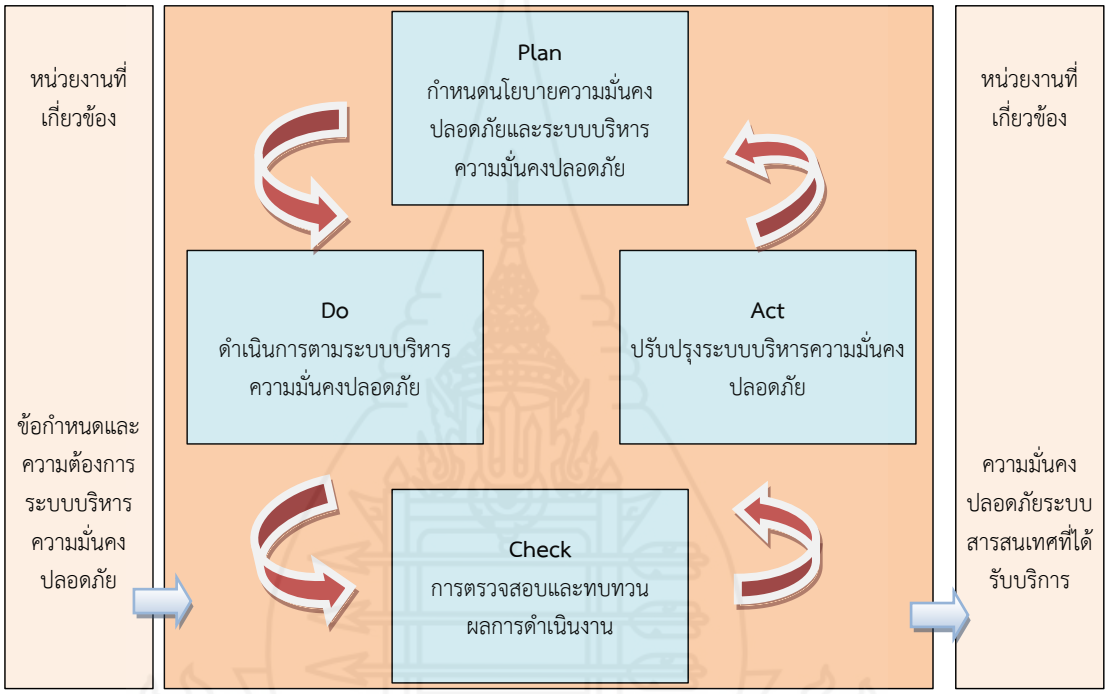
3) การทบทวนของผู้บริหาร (Management review): ผู้บริหารระดับสูงต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามรอบระยะเวลาที่กำหนด เพื่อให้มีความเหมาะสม และเกิดประสิทธิภาพและประสิทธิผลสูงสุดต่อองค์กร และการจัดเก็บเป็นลายลักษณ์อักษร

***2.2.7 การปรับปรุง (Improvment)***

1) ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and corrective action): เมื่อเกิดความไม่สอดคล้ององค์กรต้องตอบสนองต่อความไม่สอดคล้องนั้น โดยทบทวนถึงสาเหตุ และหาแนวทางแก้ไข ทำการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พร้อมจัดเก็บเป็นลายลักษณ์อักษร

2) การปรับปรุงอย่างต่อเนื่อง (Continual improvement): องค์กรต้องปรับปรุงความเหมาะสม เพียงพอ และประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

## 3. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)




ภาพที่ 2.3 กระบวนการ ISMS

จากภาพที่ 2.3 แสดงกระบวนการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) บรรจง หะรังสี (2554) อธิบายกระบวนการ PDCA (Plan, Do, Check, Act) ประกอบด้วย กระบวนการวางแผน (Plan) เป็นการกำหนดรายการควบคุม การประเมินความเสี่ยงตามรายการควบคุม และกำหนดเป็นนโยบายความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยระบบสารสนเทศ กระบวนการลงมือปฏิบัติ (Do) เป็นการลงมือปฏิบัติตามระบบบริหารจัดการความมั่นคงปลอดภัยที่ได้ประเมินไว้ เพื่อลดช่องโหว่ที่จะเกิดขึ้น กระบวนการการตรวจสอบ (Check) การประเมินผลทบทวนสิ่งที่ได้ดำเนินการบริหารจัดการความมั่นคงปลอดภัยไว้ ทบทวนนโยบายด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ ว่าครบถ้วนครอบคลุม ทันสมัยกับภัยคุกคามใหม่ๆ หรือไม่ และ

การปรับปรุงแก้ไข (Act) ระบบบริหารความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน เป็นการนำผลที่ได้จากการตรวจสอบ มาปรับปรุงให้ดีขึ้น โดยมีรายละเอียด ดังนี้

**3.1 การวางแผน (Plan)**

เป็นการประเมินและลดความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศ โดยการระบุความเสี่ยงและวางแผนจัดการความเสี่ยงซึ่งเป็นการลดความเสี่ยง โดยแผนการจัดการความเสี่ยงก็จะประกอบด้วยการจัดทำนโยบายหรือข้อกำหนดความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยมีขั้นตอน ดังนี้

***3.1.1 การกำหนดขอบเขตระบบบริหารความมั่นคงปลอดภัย*** โดยพิจารณาถึงลักษณะหน่วยงานเป้าหมาย ภารกิจ ตลอดจนทรัพย์สินต่างๆ ของหน่วยงานที่ต้องการบริการความมั่นคงปลอดภัย

***3.1.2 การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ*** โดยที่นโยบายจะต้องกำหนดประกอบวัตถุประสงค์ (Objectives) ในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ การกำหนดบทบาทผู้รับผิดชอบให้สอดคล้องกับการบริหารความเสี่ยงเชิงกลยุทธ์ของหน่วยงาน ในการกำหนดนโยบายต้องคำนึงถึงข้อกำหนดทางธุรกิจและกฎหมาย รวมถึงข้อบังคับตามสัญญาที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

***3.1.3 การกำหนดแนวทางในการประเมินความเสี่ยงสำหรับองค์กร*** ที่เหมาะสมกับระบบบริหารความมั่นคงปลอดภัยขององค์กร รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

***3.1.4 การระบุความเสี่ยง*** ได้แก่ การระบุทรัพย์สินภายในขอบเขตของระบบบริหารความมั่นคงปลอดภัยของ การระบุภัยคุกคามที่มีต่อทรัพย์สิน การระบุจุดอ่อนที่ทำให้ภัยคุกคามมีผลกับทรัพย์สินรวมถึงการระบุถึงผลกระทบที่มีต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้ของทรัพย์สิน

***3.1.5 การวิเคราะห์และประเมินความเสี่ยง*** โดยการประเมินถึงผลกระทบซึ่งเกิดจากความล้มเหลวในความมั่นคงปลอดภัยต่อหน่วยงาน ตามหลักการในการรักษาความลับ ความสมบูรณ์หรือความพร้อมใช้งานของทรัพย์สิน การประเมินถึงโอกาสที่จะเกิดความล้มเหลวขึ้นที่มีต่อความมั่นคงปลอดภัย ระดับของความเสี่ยง พิจารณาถึงความเสี่ยงที่สามารถยอมรับได้หรือความจำเป็นในการจัดการกับความเสี่ยง

***3.1.6 การกำหนดและประเมินแนวทางในการจัดการความเสี่ยง*** โดยแนวทางที่ใช้ในการจัดการความเสี่ยง จะประกอบด้วยการกำหนดมาตรการควบคุมที่เหมาะสม การยอมรับความเสี่ยงที่เกิดขึ้นการหลีกเลี่ยงความเสี่ยง การถ่ายโอนย้ายความเสี่ยง

***3.1.7 การคัดเลือกรายการควบคุม*** มาตรการทางด้านความมั่นคงปลอดภัย เพื่อจัดการกับความเสี่ยง รวมถึงการนำไปปฏิบัติเพื่อให้สอดคล้องกับแนวทางที่กำหนดตามกระบวนการจัดการความเสี่ยง

***3.1.8 ขอการอนุมัติและความเห็นชอบ*** สำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

***3.1.9 ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ***

***3.1.10 จัดทำเอกสาร SoA (Statement of Applicability)*** เพื่อแสดงการใช้งานให้เป็นไปตามมาตรการที่กำหนดไว้ในของมาตรฐานการรักษาความมั่นคงปลอดภัย

**3.2 ดำเนินการตามระบบบริหารความมั่นคงปลอดภัยที่กำหนดไว้ (Do)** ในขั้นตอนของการลงมือทำจะประกอบด้วย

***3.2.1 การจัดทำแผนการจัดการความเสี่ยง*** โดยระบุรายละเอียดของการดำเนินงาน ทรัพยากรที่ต้องการ ความรับผิดชอบและลำดับความสำคัญในการดำเนินงาน สำหรับการจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ

***3.2.2 การดำเนินการตามแผนการจัดการความเสี่ยง*** เพื่อให้บรรลุตามวัตถุประสงค์การควบคุมที่ได้กำหนดไว้ รวมถึงการพิจารณาจัดสรรเงินทุนและกำหนดหน้าที่ความรับผิดชอบในการดำเนินการด้วย

***3.2.3 การดำเนินการตามการควบคุมที่ได้กำหนดไว้*** เพื่อให้ได้ตามวัตถุประสงค์การควบคุม

*3.2.4 การกำหนดแนวทางในการวัดความมีประสิทธิผล*ของการควบคุม หรือกลุ่มการควบคุมที่ได้กำหนด

***3.2.5 การจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กร***

***3.2.6 การบริหารงาน ISMS***

***3.2.7 การจัดการทรัพยากรสำหรับ ISMS***

***3.2.8 การดำเนินงานตามวิธีการปฏิบัติงาน*** และการควบคุมอื่นๆ เพื่อให้สามารถตรวจสอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์นั้นๆ

**3.3 การตรวจสอบและทบทวนผลการดำเนินงาน (Check)** ประกอบด้วยขั้นตอนต่างๆ ดังนี้

***3.3.1 การดำเนินการเฝ้าติดตาม*** และทบทวนวิธีการปฏิบัติงาน และการควบคุมต่างๆ เพื่อตรวจจับความผิดพลาดของผลลัพธ์ที่ได้ดำเนินการ ระบุถึงการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ต่างๆ ที่เกิดขึ้น ช่วยในการตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคง

ปลอดภัยโดยการใช้ดัชนีวัดที่เหมาะสมบ่งชี้ในการตรวจจับเหตุการณ์ต่างๆ ที่ไม่คาดคิด และพิจารณาถึงประสิทธิภาพการดำเนินการเพื่อแก้ไขการละเมิดทางด้านความมั่นคงปลอดภัยมีความสัมฤทธิผลหรือไม่

***3.3.2 การดำเนินการทบทวนความมีประสิทธิผล***ของระบบบริหารความมั่นคงปลอดภัย อย่างสม่ำเสมอ โดยคำนึงถึงผลของการตรวจประเมินความมั่นคงปลอดภัย เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ จากหน่วยงานต่างๆ ที่เกี่ยวข้อง

***3.3.3 การวัดความมีประสิทธิผล***ของมาตรการทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย

***3.3.4 ทบทวนการประเมินความเสี่ยงตามแผนที่ได้กำหนดไว้*** รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงบริบทต่างๆ ในหน่วยงานที่เปลี่ยนแปลงไป เช่น เทคโนโลยี วัตถุประสงค์ เป้าหมาย ภัยคุกคาม ความเสี่ยงจากสังคม สิ่งแวดล้อม ข้อกำหนดกฎหมายที่เปลี่ยนไป

***3.3.5 การดำเนินการตรวจประเมินระบบบริหารความมั่นคงปลอดภัยภายใน***

***3.3.6 การดำเนินการทบทวนโดยฝ่ายบริหาร*** เพื่อดูแลความเพียงพอของขอบเขตและการดำเนินการปรับปรุงกระบวนการระบบบริหารความมั่นคงปลอดภัย

***3.3.7 การปรับปรุงแผนความมั่นคงปลอดภัย*** โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตามและการทบทวน

***3.3.8 การบันทึกผลการดำเนินการ*** และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผลหรือผลการดำเนินงานของระบบบริหารความมั่นคงปลอดภัย

**3.4 ลงมือดำเนินการตามระบบบริหารความมั่นคงปลอดภัย (Act)** ในขั้นตอนการของการปรับปรุงและแก้ไขระบบ จะประกอบด้วย

***3.4.1 การดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยที่ได้กำหนดไว้***

***3.4.2 การปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม*** รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคงปลอดภัยขององค์กรอื่นๆ และขององค์กรเองมาปรับใช้อย่างเหมาะสม

***3.4.3 การสื่อสารการดำเนินการ*** และการปรับปรุงไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งหมด

***3.4.4 การดูแลให้มั่นใจ***ว่าการปรับปรุงเป็นไปตามวัตถุประสงค์ที่ได้กำหนดไว้

## 4. งานวิจัยที่เกี่ยวข้อง

กรกฎ สราญสุทธิ์ (2556) ได้พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001 ของกรมทรัพยากรน้ำบาดาล พร้อมประเมินความเสี่ยงและจัดทำรายงานผลกระทบ รายงานวิธีการจัดการกับความเสี่ยง โดยดำเนินการศึกษาข้อมูลด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล วิเคราะห์และประเมินความเสี่ยงระบบความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศของศูนย์ข้อมูล ในการวิเคราะห์ความเสี่ยงนั้นได้ระบุรายการความเสี่ยง ระดับความเสี่ยงแยกเป็นรายอุปกรณ์พร้อมกับการกำหนดรายการควบคุมตามมาตรฐาน ISO27001 ผลการวิเคราะห์ความเสี่ยงก่อนการดำเนินการพบว่าส่วนใหญ่อยู่ในระดับกลางและต่ำ จากนั้นดำเนินการจัดการความเสี่ยง โดยจัดทำนโยบายด้านความมั่นคงปลอดภัยมาตรฐาน ISO27001 ให้กรมประกอบด้วย นโยบายการควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน นโยบายการเข้าถึงระบบปฏิบัติการ แนวปฏิบัติการจัดทาระบบสารองและแผนเตรียมความพร้อมกรณีฉุกเฉิน แนวปฏิบัติการประเมินความเสี่ยง แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ จากนั้นปรับปรุงระบบระบบเทคโนโลยีสารสนเทศเพื่อลดช่องโหว่ทั้งฮาร์ดแวร์และซอฟต์แวร์ และอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยให้ผู้ใช้งาน สุดท้ายดำเนินการประเมินทบทวนวิเคราะห์ความเสี่ยงหลังจากดำเนินการ พบว่าหน่วยงานมีความเสี่ยงระดับกลางลดลง และความเสี่ยงที่เหลืออยู่ส่วนใหญ่เป็นความเสี่ยงในระดับต่ำ ซึ่งผู้จัดทำได้มีข้อเสนอแนะให้ตรวจสอบทบทวน และปรับปรุงระบบอยู่เสมอ เพื่อลดความเสี่ยง ช่องโหว่ และโอกาสที่จะถูกโจมตีต่อภัยคุกคามต่างๆ

จุติชัย ทองกระจาย (2557) ได้พัฒนาระบบตรวจจับการบุกรุกเครือข่ายกรณีศึกษาบริษัทเวนด้า ซอฟแวร์ ดีเวลอปเมนท์ จำกัด เพื่อตรวจจับภัยคุกคามที่เกิดขึ้นต่อระบบเครือข่ายของบริษัท และปรับปรุงระบบเครือข่ายของบริษัทให้มีความมั่นคงปลอดภัย โดยทำการเก็บข้อมูลจากระบบเครือข่ายที่ได้พัฒนาขึ้น ตรวจจับภัยคุกคาม ปรับปรุงซิกเนเจอร์ของระบบ และแสดงผลรายงานผ่านเว็บแอพพลิเคชัน ผลจากการดำเนินงานพบว่า ระบบที่พัฒนาขึ้นสามารถตรวจจับการบุกรุกและการโจมตีบนเครือข่ายได้จริง ผู้ดูแลระบบสามารถนำไปใช้เฝ้าดูสถานการณ์ที่เกิดขึ้นบนระบบเครือข่ายได้อย่างทันท่วงที และสามารถนำผลจากการตรวจจับไปใช้ในการปรับปรุงไฟร์วอลล์และระบบเครือข่ายของบริษัท เพื่อเพิ่มความมั่นคงปลอดภัยด้านเครือข่ายของบริษัทให้มากยิ่งขึ้น

เฉลิม สุวรรณ (2554) ได้จัดทำกรอบนโยบายด้านความมั่นคงปลอดภัยอ้างอิงตามมาตรฐานสากล ISO/IEC 27001 ของศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี

และดำเนินการจัดการความเสี่ยงให้กับระบบสารสนเทศของหน่วยงาน มีแนวทางดำเนินงานคือ ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน กับมาตรฐานและข้อกำหนดด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 จากนั้นจัดทำนโยบายความมั่นคงปลอดภัยให้กับหน่วยงาน แบ่งกลุ่มผู้เกี่ยวข้องออกเป็น 2 กลุ่ม คือ กลุ่มผู้ใช้งานระบบสารสนเทศและเครือข่าย กลุ่มผู้ดูแลระบบสารสนเทศและเครือข่าย มีกำหนดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต นโยบายการบริหารจัดการการเข้าถึงระบบสารสนเทศ การฝ่าฝืนและการลงโทษ จากนั้นแก้ไข ควบคุมความเสี่ยง โดยการปรับปรุงระบบเครือข่าย เปลี่ยนอุปกรณ์สวิตซ์ อุปกรณ์กระจายสัญญาณ ระบบไฟฟ้าสำรอง และติดตั้งโปรแกรมแอนตี้ไวรัส พร้อมทดสอบระบบ และสุดท้ายประเมินความเสี่ยงหลังจากดำเนินโครงการพบว่า ร่างนโยบายความมั่นคงปลอดภัยที่จัดทำขึ้นและการแก้ไขช่องโหว่ต่างๆ ทำให้ความเสี่ยงลดลงอยู่ในระดับกลางและต่ำ และมีข้อเสนอแนะให้หน่วยงานขอใบรับรองมาตรฐาน ISO 27001 เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัย น่าเชื่อถือ และให้บริการผู้ป่วยได้อย่างรวดเร็วและมีประสิทธิภาพ

ประกิจ อินทรักษ์ (2556) พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001:2005 กรณีศึกษาสาหรับ สถาบันวิจัยแห่งหนึ่ง เพื่อใช้เป็นแนวทางในการปฏิบัติงาน รวมถึงการวิเคราะห์ และการประเมินความเสี่ยงให้กับองค์กร เพื่อให้องค์กรได้ทราบถึงระดับของความเสี่ยงที่องค์กรมีอยู่ และจัดทำแผนการบริหารจัดการความเสี่ยงลดระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ มีแนวทางดำเนินงานคือ การกำหนดขอบเขตในการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยแบ่งทรัพย์สินขององค์กรเป็น 5 ประเภท คือ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล คน และงานบริการ จากนั้นกำหนดวิธีวิเคราะห์ประเมินความเสี่ยงตามรายการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Control Checklist) ของ ISO/IEC27001:2005 และกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ได้แก่ นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต นโยบายความมั่นคงปลอดภัยของอีเมล์ นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ นโยบายการบริหารจัดการทรัพย์สิน นโยบายด้านการปฏิบัติตามกฎหายและข้อบังคับนโยบายด้านความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย พร้อมจัดทำเอกสาร SOA (Statement Of Applicability) และตรวจสอบผลการดำเนินงาน พบว่ามีสามารถขจัดระดับความเสี่ยงสูงได้หมด ระดับความเสี่ยงปานกลางลดลง เหลือระดับความเสี่ยงต่ำซึ่งอยู่สภาพที่องค์กรรับได้

ไพศาล จันทร์เลื่อน (2557) ได้จัดทำร่างนโยบายความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO 27001 กรณีศึกษา ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับหน่วยงาน โดยการกำหนดขอบเขตระบบเทคโนโลยีสารสนเทศที่จะดำเนินการ และวิเคราะห์ความเสี่ยงก่อนดำเนินการ จากนั้นกำหนดมาตการควบคุมความเสี่ยง และจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยการจัดทำเอกสาร Statement of Applicability (SOA) ประกอบด้วย นโยบาย 8 ด้าน ได้แก่ นโยบายความมั่นคงปลอดภัยสารสนเทศ ที่กำหนดให้ต้องมีการทบทวนทุกๆ ปี นโยบายโครงสร้างความมั่นคงปลอดภัยสารสนเทศ ที่กำหนดถึงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง นโยบายการบริหารจัดการทรัพย์สิน กำหนดผู้ดูแลทรัพย์สิน นโยบายการควบคุมการเข้าถึง นโยบายความมั่นคงปลอดภัยทางสภาพแวดล้อม นโยบายการใช้งานเครื่องคอมพิวเตอร์ และนโยบายการใช้งานระบบเครือข่ายไร้สาย จากนั้น ได้ดำเนินการะการอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ จากนั้น ประเมินความเสี่ยงหลังดำเนินงานและนำผลที่ได้เสนอผู้บริหาร เพื่อพิจารณาตรวจสอบ ซึ่งจากการประเมินความเสี่ยงพบว่า ความเสี่ยงสูงได้รับการจัดการ เหลือเพียงความเสี่ยงสูงเรื่องของซอฟต์แวร์ผิดกฎหมายเท่านั้น ในส่วนของมาตรการควบคุมก็ยังไม่สามารถดำเนินการใช้ทั้งหมดตามที่เลือกในเอกสาร SOA เนื่องด้วยเวลาอันกำจัดของการดำเนินงาน

จากการศึกษางานวิจัยที่เกี่ยวข้องนั้น พบว่าผู้จัดทำมีแนวคิดพัฒนานโยบายด้านความมั่นคงปลอดภัยดังกล่าว เป็นไปตามมาตรฐาน ISO/IEC 27001:2005 และมีแนวทางควบคุมความเสี่ยงโดยเน้นการปรับปรุงระบบและอุปกรณ์ที่เกี่ยวข้องให้มีประสิทธิภาพเพิ่มขึ้น สำหรับงานค้นคว้าอิสระนี้ ผู้วิจัยทำได้พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ตามมาตรฐาน ISO/IEC 27001: 2013 ซึ่งได้ปรับปรุงล่าสุด และใช้วิธีการติดตั้งอุปกรณ์และระบบรักษาความปลอดภัยเพื่อควบคุมความเสี่ยงของหน่วยงาน

# บทที่ 3
# วิธีดำเนินการวิจัย

สำหรับแนวทางและวิธีการดำเนินการเสริมสร้างความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานนั้นได้วางกรอบและวิธีดำเนินงานดังต่อไปนี้

1. ศึกษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน และเอกสารต่างๆ ที่เกี่ยวข้อง
2. ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ
3. พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
4. ดำเนินการติดตั้งระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
5. ดำเนินการตรวจสอบและประเมินผล

## 1. ศึกษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน และเอกสารต่างๆ ที่เกี่ยวข้อง

### 1.1 ศึกษาระบบโครงสร้างเครือข่ายที่มีอยู่

เก็บรวบรวมข้อมูลของระบบเครือข่ายเดิม การเชื่อมโยงของอุปกรณ์ภายในระบบเครือข่ายต่างๆ จากนั้น ค้นหาและวิเคราะห์จุดอ่อนของระบบ การป้องกันและรักษาความปลอดภัยของระบบเครือข่ายเดิม ทั้งการรักษาความปลอดภัยทางด้านเทคนิคและการรักษาความปลอดภัยทางด้านกายภาพ

### 1.2 ศึกษาข้อมูลที่เกี่ยวข้อง

เนื่องจากสำนักงานจังหวัดพัทลุง เป็นหน่วยงานในสังกัดสำนักงานปลัดกระทรวงมหาดไทย อยู่ภายใต้การกำกับดูแลของกระทรวงมหาดไทย ซึ่งกระทรวงมหาดไทยได้กำหนดแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงมหาดไทย ดังนั้นเพื่อให้เกิดความสอดคล้องกัน จึงได้นำแผนบริหารจัดการความเสี่ยง มาใช้ต้นแบบในการวิเคราะห์และประเมินความเสี่ยง

สำหรับการพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงดำเนินการศึกษามาตรฐาน ISO/IEC 27001:2013 เพื่อเป็นกรอบในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง เพื่อยกระดับการบริหารด้านการรักษาความมั่นคงปลอดภัยให้ได้มาตรฐาน รวมถึงได้ศึกษา

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 พระราชบัญญัติว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ พ.ศ. 2540 ทั้งนี้เพื่อให้สอดคล้องตามข้อกฎหมาย ระเบียบ กฎเกณฑ์ต่างๆ ของหน่วยงานภาครัฐ ตามข้อกำหนดที่ ISO/IEC 27001:2013 ได้กำหนดไว้ด้วย

## 2. ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

### 2.1 วิเคราะห์และประเมินความเสี่ยง

วิเคราะห์และประเมินความเสี่ยงโดยพิจารณาองค์ประกอบของระบบคอมพิวเตอร์ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ข้อมูลและสารสนเทศ มาประเมินค่าความเสี่ยง ซึ่งเป็นการพิจารณาจุดบกพร่อง หรือภัยคุกคาม ทั้งที่เคยเกิดขึ้นกับหน่วยงานมาแล้ว และที่คาดว่าจะเกิดขึ้นกับหน่วยงาน จากนั้นนำมาประเมินโอกาส ประเมินความรุนแรงหรือความเสียหายที่จะเกิดขึ้นจากความเสี่ยงนั้นๆ ว่ามีมากน้อยระดับใด ส่งผลกระทบต่อหน่วยงานมากน้อยแค่ไหน ตามขั้นตอนการบริหารจัดการความเสี่ยง ดังรายละเอียดต่อไปนี้

ประเมินหาโอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง (Likelihood) แบ่งเป็น 5 ระดับ ดังนี้

ตารางที่ 3.1 ระดับโอกาสของการเกิดความเสียง

| โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง (Likelihood) | | | | | |
|---|---|---|---|---|---|
| ประเด็นในการพิจารณา | ระดับคะแนน | | | | |
| | น้อยมาก=1 | น้อย=2 | ปานกลาง=3 | สูง=4 | สูงมาก=5 |
| ระเบียบและคู่มือปฏิบัติงานด้านระบบสารสนเทศ | ได้มีการกำหนดอย่างชัดเจนและปฏิบัติตามอย่างต่อเนื่อง | ได้มีการกำหนดไว้และมีการปฏิบัติตามเป็นครั้งคราว | ไม่มีแต่ปฏิบัติตามที่ดำเนินการต่อกันมา | มีการกำหนดไว้แต่ไม่ได้มีการดำเนินการตาม | ไม่ได้กำหนดไว้และขาดการปฏิบัติตาม |

ตารางที่ 3.1 (ต่อ)

| โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง (Likelihood) | | | | | |
|---|---|---|---|---|---|
| ประเด็นในการพิจารณา | ระดับคะแนน | | | | |
| | น้อยมาก=1 | น้อย=2 | ปานกลาง=3 | สูง=4 | สูงมาก=5 |
| การควบคุมและติดตามตรวจสอบระบบสารสนเทศ | 1-2 สัปดาห์ | 1 เดือน | 3 เดือน | 6 เดือน | มากกว่า 1 ปี |
| การอบรม/ทบทวนการปฏิบัติงานด้านระบบสารสนเทศ | ทุกเดือน | ทุก 3 เดือน | ทุก 6 เดือน | ทุกปี | มากกว่า 1 ปี |
| ความถี่ในการเกิดภัยคุกคามด้านระบบสารสนเทศ | ปีละ 1 ครั้งหรือไม่เกิดเลย | 6 เดือน/ครั้ง | 3 เดือน/ครั้ง | 1 เดือน/ครั้ง | มากกว่า 2 ครั้ง/เดือน |

พิจารณาความรุนแรงของผลกระทบของความเสี่ยงต่อองค์การ (Impact) แบ่งออกเป็น 5 ระดับ ดังนี้

ตารางที่ 3.2 ระดับความรุนแรงของผลกระทบต่อองค์กร

| ความรุนแรงของผลกระทบต่อองค์การ (Impact) | | | | | |
|---|---|---|---|---|---|
| ประเด็นในการพิจารณา | ระดับคะแนน | | | | |
| | น้อยมาก=1 | น้อย=2 | ปานกลาง=3 | สูง=4 | สูงมาก=5 |
| ผู้รับบริการได้รับความเสียหายหรือผลกระทบต่อการใช้งานระบบสารสนเทศ | บางราย | เฉพาะกลุ่มงาน | หลายกลุ่มงาน | ผู้บริหารระดับสูง | ทั้งหน่วยงาน |
| ระดับความปลอดภัยของข้อมูล | ข้อมูลทั่วไปเปิดเผยได้ไม่ส่งผลกระทบต่อหน่วยงาน | ข้อมูลเปิดเผยส่งผลกระทบต่อหน่วยงานเล็กน้อย | ข้อมูลเปิดเผยส่งผลกระทบต่อหน่วยงานปานกลาง | ข้อมูลเปิดเผยส่งผลกระทบร้ายแรงต่อหน่วยงาน | ข้อมูลชั้นความลับสูงสุดของทางราชการ |
| ผลกระทบต่อภาพลักษณ์ด้านการให้บริการระบบสารสนเทศ | น้อยมาก | น้อย | ปานกลาง | สูง | สูงมาก |
| ระดับความเสียหายต่อระบบสารสนเทศ | ไม่ส่งผลกระทบต่อระบบ | ระบบบางส่วนได้รับผลกระทบทำให้ไม่สามารถใช้งานได้ | ระบบบางส่วนเสียหายใช้งานไม่ได้เป็นเวลานาน | ได้รับผลกระทบทั้งระบบและใช้งานไม่ได้ชั่วคราว | ได้รับผลกระทบทั้งระบบและใช้งานไม่ได้เป็นเวลานาน |

สามารถดู ตารางที่ 3.3 เพื่อคำนวณค่าระดับความเสี่ยง ตามสูตรหาระดับความเสี่ยงได้ดังนี้

ระดับความเสี่ยง (Risk Level) = ระดับความรุนแรงของโอกาส (Likelihood) × ระดับความรุนแรงของผลกระทบ (Impact)

ตารางที่ 3.3 ระดับความรุนแรงของผลกระทบความเสี่ยง

| | | | | | | |
|---|---|---|---|---|---|---|
| ระดับความรุนแรง/ผลกระทบ | สูงมาก | 5 | 10 | 15 | 20 | 25 |
| | สูง | 4 | 8 | 12 | 16 | 20 |
| | ปานกลาง | 3 | 6 | 9 | 12 | 15 |
| | น้อย | 2 | 4 | 6 | 8 | 10 |
| | น้อยมาก | 1 | 2 | 3 | 4 | 5 |
| ระดับความเสี่ยง | | น้อยมาก (1) | น้อย (2) | ปานกลาง (3) | สูง (4) | สูงมาก (5) |
| | | โอกาสที่จะเกิด | | | | |

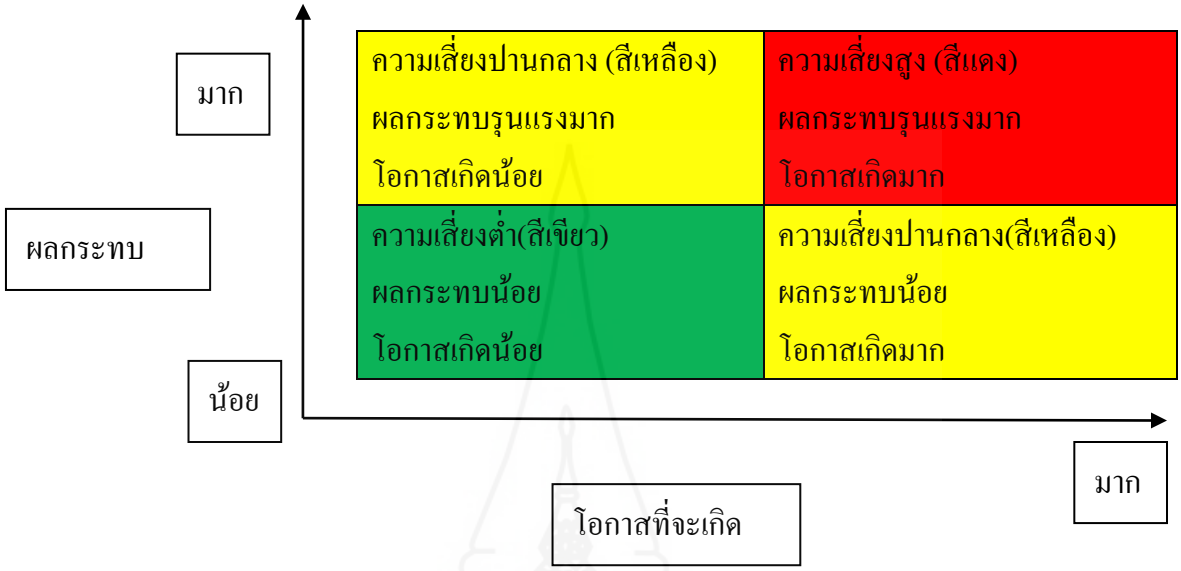
โดย กำหนดเกณฑ์การวัดระดับความเสี่ยง โดยจัดแบ่งระดับความเสี่ยงเป็น 3 ระดับ คือ ต่ำ กลาง สูง ดังนี้

ระดับความเสี่ยง 16-25 (High): เป็นระดับความเสียงที่หน่วยงานไม่สามารถยอมรับความเสี่ยงได้ ต้องลดความเสี่ยงโดยกำหนดมาตรการลดความเสี่ยงอย่างเร่งด่วน

ระดับความเสี่ยง 9-15 (Medium): เป็นระดับความเสียงที่หน่วยงานสามารถยอมรับได้ แต่ต้องลดความเสี่ยงโดยมีมาตรการที่จะลดความเสี่ยง

ระดับความเสี่ยง 1- 8 (Low): เป็นระดับความเสียงที่หน่วยงานสามารถยอมรับได้ โดยไม่ต้องมีการควบคุมเพิ่มเติม แต่ต้องติดตามตรวจสอบเพื่อให้แน่ใจว่าการควบคุมยังคงมีอยู่

สามารถวัดระดับความเสี่ยงโดยจัดลำดับจากผลกระทบและความเป็นไปได้ที่จะเกิด ตามภาพที่ 3.1 ได้ดังนี้




ภาพที่ 3.1 ระดับความเสี่ยง

### 3. พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013

จากการที่ได้ศึกษาทฤษฎี มาตรฐานความปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013 กฎหมาย ระเบียบ นโยบายที่เกี่ยวข้อง และระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลสารสนเทศของหน่วยงาน มาวิเคราะห์ รวมถึงประเมินความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์ตามรายการควบคุมที่กำหนดไว้ในมาตรฐาน ISO/IEC 27001:2013 มาพัฒนากรอบนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

### 4. ดำเนินการติดตั้งระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

เพิ่มประสิทธิภาพการใช้งานเครือข่ายและป้องกันความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยการจัดหาอุปกรณ์รักษาความมั่นคงปลอดภัย ได้แก่ อุปกรณ์ไฟร์วอลล์ อุปกรณ์ป้องกันและตรวจจับการบุกรุก เพื่อเพิ่มความปลอดภัยในการใช้

งานอินเทอร์เน็ต พร้อมกำหนดค่าทางเทคนิคให้กับอุปกรณ์ป้องกันรักษาความปลอดภัยบนระบบเครือข่ายกรอบนโยบายรักษาความปลอดภัยของสำนักงานจังหวัดพัทลุง

## 5. ดำเนินตรวจสอบและการประเมินผล

ทำการตรวจสอบและประเมินผลการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ดังนี้

5.1 ดำเนินการทดสอบทางด้านเทคนิค เป็นการทดสอบการทำงานของระบบรักษาความมั่นคงปลอดภัยตามที่ได้กำหนดค่าไว้ให้กับอุปกรณ์รักษาความปลอดภัย พร้อมกับตรวจสอบการใช้งานให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามที่ได้กำหนดไว้

5.2 ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง หลังจากดำเนินการปฏิบัติตามกรอบนโยบายความมั่นคงปลอดภัยที่ได้กำหนดไว้

5.3 ประเมินผลความพึงพอใจของบุคลากรผู้ใช้งานระบบระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงโดยการสำรวจความคิดเห็นด้านการให้บริการระบบเครือข่าย และประเมินผลการรับรู้นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยจะสอบถามผู้บริหารสำนักงานจังหวัดพัทลุง (หัวหน้าสำนักงานจังหวัด,ผู้อำนวยการกลุ่มงาน) ผู้ดูแลระบบ บุคลากรของสำนักงานจังหวัดพัทลุง ซึ่งเป็นผู้ใช้งานระบบเครือข่ายของสำนักงานจังหวัดพัทลุง และสอบถามจากเจ้าหน้าที่จากส่วนราชการอื่นๆ ภายในจังหวัดพัทลุงที่ขอใช้บริการระบบเครือข่ายอินเทอร์เน็ตของสำนักงานจังหวัดพัทลุง จำนวน 53 ราย เพื่อนำผลการประเมินที่ได้มาวางแผนและหาแนวทางปรับปรุงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ต่อไป

# บทที่ 4
# ผลการดำเนินการวิจัย

สำหรับบทนี้ จะได้อธิบายถึงผลการดำเนินงานเพื่อสร้างความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน ดังต่อไปนี้

1. ผลการศึกษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน และเอกสารต่างๆ ที่เกี่ยวข้อง
2. ผลการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ
3. กรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
4. ผลการติดตั้งระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
5. ผลการดำเนินการตรวจสอบและประเมินผล

## 1. ผลศึกษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน และเอกสารต่างๆ ที่เกี่ยวข้อง

### 1.1 ระบบเครือข่ายที่มีอยู่

***1.1.1 รายการอุปกรณ์ระบบเครือข่ายของสำนักงานจังหวัดพัทลุง*** ประกอบด้วยอุปกรณ์ดังนี้

1) Nortel Network/Passport 7480 (ATM Access) ทำหน้าที่เป็นอุปกรณ์หลักในการรับสัญญาณเครือข่ายอินเทอร์เน็ตจากสำนักงานปลัดกระทรวงมหาดไทย ด้วยความเร็ว 10/100Mpbs

ภาพที่ 4.1 อุปกรณ์ Nortel Network/Passport 7480 (ATM Access)

2) Nortel Network/ Baystack 425-24T (Layer 2 Switch) เป็นอุปกรณ์หลักในการกระจายสัญญาณในอาคารศาลากลางจังหวัดพัทลุง ทั้งอาคารศาลากลางหลักเก่าและหลังใหม่ และ Nortel Network/ Baystack 425-24T_C1 (Layer 2 Switch) เป็นอุปกรณ์หลักในการกระจายสัญญาณไปยังระบบการประชุมทางไกลกระทรวงมหาดไทยและจังหวัด (VDO Conference)

ภาพที่ 4.2 อุปกรณ์ Baystack 425-24T และ Baystack 425-24T_C1

3) Fortigate60 Firewall อุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย

4) TP-Link 8 port อุปกรณ์กระจายสัญญาณไปยังสำนักงานจังหวัด

5) D- Link 8 port อุปกรณ์กระจายสัญญาณไปแต่ละกลุ่มงานยังสำนักงานจังหวัด

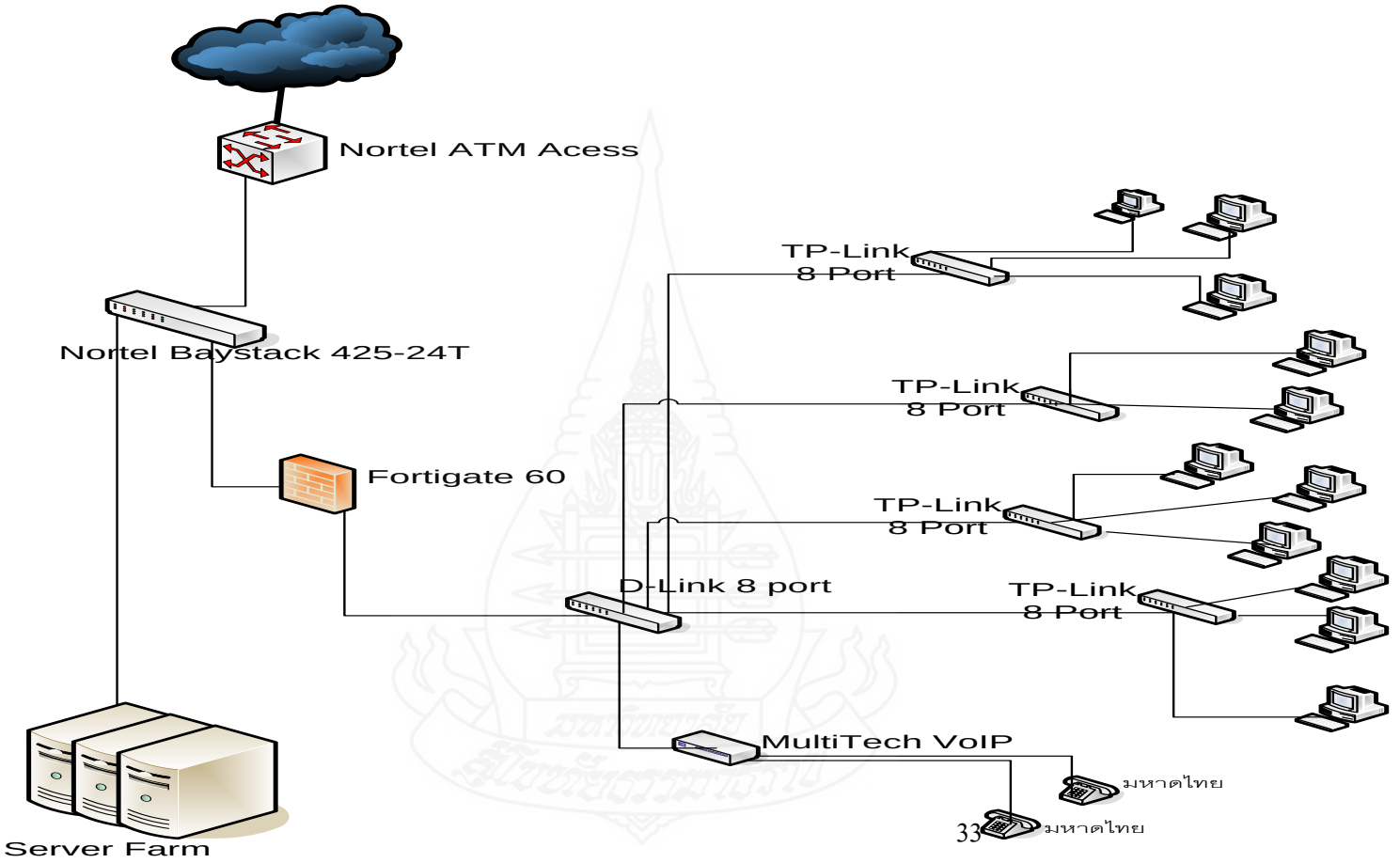
6) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการข้อมูลจังหวัดและกระทรวงมหาดไทย (MOC) เครื่องคอมพิวเตอร์แม่ข่ายข้อมูลบุคลากรภาครัฐของสำนักงานจังหวัดพัทลุง

7) ระบบสำรองไฟฟ้าทำหน้าที่จ่ายไฟให้กับ ATM Access และ Nortel Network/ Baystack 425-24T ประกอบด้วย

- DC Power Supply (Delta MCS1800) 1 ชุด
- MGE UPS Systems Pulsar Extreme 2000 VA 1 ชุด
- MGE UPS Systems Pulsar Evolution 500 VA 3 ชุด

8) ระบบปรับอากาศในห้องสื่อสาร ประกอบด้วยแอร์ ขนาด 800 BTU จำนวน 2 ตัว

*1.1.2 ผังระบบเครือข่าย*




ภาพที่ 4.3 ระบบเครือข่ายของสำนักงานจังหวัดพัทลุงที่มีอยู่

จากภาพที่ 4.3 จะเห็นได้ว่า ระบบเครือข่ายที่ติดตั้ง ณ สำนักงานจังหวัด ใช้ระบบ ATM Access รับสัญญาณไฟเบอร์ออฟติกจากกระทรวงมหาดไทย เข้ามายังศาลากลางจังหวัด จากนั้นใช้ อุปกรณ์ Layer 2 Switch กระจายสัญญาณไปยังชั้นต่างๆ ภายในอาคารศาลากลางจังหวัด รวมถึงสำนักงานจังหวัดพัทลุงจากนั้นต่อเข้าไฟร์วอลล์ และกระจายสัญญาณไปยังกลุ่มงานต่างๆ ภายในสำนักงานจังหวัดพัทลุง จากระบบเครือข่ายเดิม สามารถสรุปปัญหาระบบเครือข่ายภายในหน่วยงานได้ดังนี้

- อุปกรณ์ที่ติดตั้งตั้งเป็นอุปกรณ์รุ่นเก่า ตัวอย่างเช่น อุปกรณ์ไฟร์วอลล์ ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีรูปแบบใหม่ๆ ได้ เป็นสาเหตุหนึ่งที่ทำให้ระบบเครือข่ายช้า ขาดเสถียรภาพในการใช้งาน

- เครื่องคอมพิวเตอร์แม่ข่ายสามารถเข้าถึงได้โดยตรง โดยที่ไม่มีไฟร์วอลล์กั้นอยู่เลย

- การเชื่อมต่อสวิตซ์หลายตัวแบบเชื่อมต่อกันไปเรื่อยๆ จะทำให้เป็นการลดทอนสัญญาณ ส่งผลให้ประสิทธิภาพในการใช้งานช้าลง

- ไม่สามารถบริหารจัดการเครือข่ายได้ ขาดอุปกรณ์ในการควบคุมและบริหารจัดการระบบเครือข่าย

- ปัญหาความเร็วที่จำกัด แบนด์วิดท์ในการใช้งานอินเทอร์เน็ต และหากมีการประชุมทางไกลก็จะทำให้ระบบเครือข่ายช้า

**1.2 ศึกษาข้อมูลที่เกี่ยวข้อง**

สำหรับการพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงดำเนินการศึกษามาตรฐาน ISO/IEC 27001:2013 เพื่อเป็นกรอบในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง เพื่อยกระดับการบริหารด้านการรักษาความมั่นคงปลอดภัยให้ได้มาตรฐาน รวมถึงได้ศึกษาแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 พระราชบัญญัติว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ พ.ศ. 2540 และนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงมหาดไทย ทั้งนี้เพื่อให้สอดคล้องตามข้อกฎหมาย ระเบียบ กฎเกณฑ์ต่างๆ ของหน่วยงานภาครัฐ ตามข้อกำหนดที่ ISO/IEC 27001:2013 ได้กำหนดไว้ด้วย จากการศึกษาข้อกฎหมาย ระเบียบ กฎเกณฑ์ดังกล่าว พบว่า

ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 โดยสรุปต้องมีการจัดกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

โดยต้องประกอบด้วยเนื้อหา คือ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ จัดให้มีระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ

พระราชบัญญัติว่าด้วยการกระทำความผิดด้านคอมพิวเตอร์ พ.ศ. 2540 โดยสรุป กำหนดให้หน่วยงานมีการพิสูจน์ทราบตัวจริงก่อนการใช้งานระบบเครือข่าย และหน่วยงานต้องมีการเก็บข้อมูลการใช้งานหรือข้อมูลการจราจรทางคอมพิวเตอร์ไว้เป็นเวลาไม่น้อยกว่า 90 วัน

นโยบายด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงมหาดไทย โดยสรุป ได้กำหนดให้มีนโยบายรักษาความปลอดภัยด้านต่างๆ ไว้ 8 นโยบาย ดังนี้ นโยบายการใช้งานอย่างถูกต้อง นโยบายด้านการเชื่อมโยงเครือข่ายแบบไร้สาย นโยบายด้านการรักษาความปลอดภัยเครือข่าย นโยบายด้านการใช้จดหมายอิเล็กทรอนิกส์ นโยบายด้านการใช้งานอินเทอร์เน็ต นโยบายด้านการเข้าถึงข้อมูลการใช้งานเครื่องแม่ข่าย และการใช้เครือข่าย นโยบายด้านการป้องการการบุกรุกเครือข่าย นโยบายด้านการป้องกันสิ่งแปลกปลอมในองค์กร

## 2. ผลการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

จากปัญหาของระบบเครือข่ายของสำนักงานจังหวัดพัทลุงที่ได้วิเคราะห์ไว้ ได้แก่ อุปกรณ์ที่ติดตั้งตั้งเป็นอุปกรณ์รุ่นเก่า ตัวอย่างเช่น อุปกรณ์ไฟร์วอลล์ ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีรูปแบบใหม่ๆ ได้ เป็นสาเหตุหนึ่งที่ทำให้ระบบเครือข่ายช้า ขาดเสถียรภาพในการใช้งาน เครื่องคอมพิวเตอร์แม่ข่ายสามารถเข้าถึงได้โดยตรง โดยที่ไม่มีไฟร์วอลล์กั้นอยู่เลย การเชื่อมต่อสวิทซ์หลายตัวแบบเชื่อมต่อกันไปเรื่อยๆ จะทำให้เป็นการลดทอนสัญญาณ ส่งผลให้ประสิทธิภาพในการใช้งานช้าลง ไม่สามารถบริหารจัดการเครือข่ายได้ ขาดอุปกรณ์ในการควบคุมและบริหารจัดการระบบเครือข่าย ปัญหาความเร็วที่จำกัด แบนด์วิดท์ในการใช้งานอินเทอร์เน็ต และหากมีการประชุมทางไกลก็จะทำให้ระบบเครือข่ายช้า

ด้วยเหตุดังกล่าวข้างต้นทำให้ เกิดปัญหายุ่งยากในการบริหารจัดการเครือข่ายภายในสำนักงานจังหวัดพัทลุง ซึ่งสามารถประเมินความเสี่ยงของระบบ จากโอกาสที่จะเกิด (Likelihood) และระดับของผลกระทบ (Impact) ตามที่ได้ระบุไว้ เทียบกับมาตรฐาน ISO/IEC 27001: 2013 ประกอบด้วย 14 โดเมน 114 รายการ ดังต่อไปนี้

2.1 ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงก่อนดำเนินการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง

ตารางที่ 4.1 ประเมินความเสี่ยงก่อนดำเนินการ

| A5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) | | | | | | |
|---|---|---|---|---|---|---|
| A.5.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.5.1.1 | นโยบายสำหรับความมั่นคงปลอดภัย | สำนักงานจังหวัดพัทลุงยังไม่ได้มีการจัดทำนโยบายความปลอดภัยสารสนเทศขอสำนักงานอย่างเป็นลายลักษณ์อักษร | 4 | 5 | 20 | สำนักงานจังหวัดพัทลุงต้องกำหนดนโยบายความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร |
| A.5.1.2 | การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | - ยังไม่ได้จัดทำนโยบายความมั่นคงปลอดภัย จึงไม่มีการทบทวนนโยบาย | 4 | 5 | 20 | ต้องการทบทวนนโยบายความมั่นคงปลอดภัย |



36

ตารางที่ 4.1 (ต่อ)

| A.6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security) | | | | | | |
|---|---|---|---|---|---|---|
| A.6.1 โครงสร้างภายในองค์กร | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.6.1.1 | มีการบทบาทและหน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัย | ปฏิบัติตามหน้าที่ในภาพรวมเท่านั้น ขาดการมอบหมายอย่างจริงจัง | 4 | 5 | 20 | หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยต้องมีการกำหนดและมอบหมายความรับผิดชอบ |
| A.6.1.2 | มีการแบ่งหน้าที่และส่วนงานที่รับผิดชอบกับงาน | ขาดการแบ่งแยกหน้าที่และความรับผิดชอบ | 3 | 4 | 12 | ควรมีการแบ่งหน้าที่และส่วนงานที่รับผิดชอบอย่างชัดเจน |
| A.6.1.3 | การติดต่อกับหน่วยงานผู้มีอำนาจ | มีการติดต่อกับส่วนราชการทั้งระดับบนและล่างโดยใช้หนังสือราชการ | 5 | 1 | 5 | ควรกำหนดวิธีการให้ส่วนราชการที่ติดต่อด้วยให้สามารถติดต่อได้อย่างต่อเนื่อง |

ตารางที่ 4.1 (ต่อ)

| A.6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security) | | | | | | |
|---|---|---|---|---|---|---|
| A.6.1 โครงสร้างภายในองค์กร | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.6.1.4 | การมีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน | มีรายชื่อ และข้อมูลนักวิชาการคอมพิวเตอร์ไว้สอบถาม | 2 | 1 | 2 | ควรรวบรวมรายชื่อผู้เชี่ยวชาญด้านคอมพิวเตอร์จากส่วนราชการอื่นๆ ด้วย |
| A.6.1.5 | ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ | ในการบริหารจัดการโครงการสารสนเทศมีการคำนึงถึงความปลอดภัย แต่อาจไม่ครอบคลุมทุกเรื่องที่เกี่ยวข้อง | 4 | 1 | 4 | ควรให้ความสำคัญ ประเด็นด้านความมั่นคงปลอดภัยให้เพิ่มขึ้น |

ตารางที่ 4.1 (ต่อ)

| A.6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security) | | | | | | |
|---|---|---|---|---|---|---|
| A.6.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.6.2.1 | การกำหนดนโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา | ขาดความตระหนักถึงความสำคัญในการจัดการความเสี่ยงที่จะเกิดจากการนำอุปกรณ์คอมพิวเตอร์แบบพกพามาใช้ ทำให้ไม่มีการกำหนดนโยบายฯ | 2 | 4 | 8 | ควรมีการกำหนดมาตรการการนำเครื่องคอมพิวเตอร์แบบพกพามาใช้ในสำนักงานจังหวัดพัทลุง |
| A.6.2.2 | การกำหนดนโยบายการปฏิบัติงานระยะไกล | สำนักงานจังหวัดพัทลุงไม่ได้กำหนดการเชื่อมต่อและควบคุมการใช้งานระบบเครือข่ายระยะไกล | 2 | 2 | 4 | ควรกำหนดนโยบายการเชื่อมต่อระบบเครือข่ายระยะไกล |

ตารางที่ 4.1 (ต่อ)

| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.7.1 ก่อนการจ้างงาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.7.1.1 | การคัดเลือก | มีการการตรวจสอบคุณสมบัติของผู้สมัครตามระเบียบทางราชการ แต่ยังไม่ครอบคลุมถึงการกำหนดชั้นความลับในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง | 3 | 4 | 12 | ควรพิจารณาคุณสมบัติของเจ้าหน้าที่/ลูกจ้างในการเข้าถึงชั้นความลับของข้อมูลของสำนักงานจังหวัดพัทลุง ให้เหมาะสมสอดคล้องกับกฎหมายระเบียบ ต่างๆ ที่เกี่ยวข้อง |
| A.7.1.2 | ข้อตกลงและเงื่อนไขการจ้างงาน | มีการกำหนดเงื่อนไขการจ้างทั่วไปไม่ได้ระบุถึงความมั่นคงปลอดภัยสารสนเทศใดๆ ในเงื่อนไขสัญญาจ้าง | 3 | 4 | 12 | ควรระบุข้อตกลงในการเข้าใช้งานสารสนเทศในสัญญาจ้างของสำนักงานจังหวัดพัทลุง |

ตารางที่ 4.1 (ต่อ)

| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.7.2 ระหว่างการจ้างงาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.7.2.1 | หน้าที่ความรับผิดชอบของผู้บริหาร | สำนักงานจังหวัดพัทลุงยังไม่กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้เจ้าหน้าที่ และลูกจ้าง ปฏิบัติตามอย่างเป็นทางการ | 3 | 3 | 9 | หัวหน้าสำนักงานจังหวัดต้องกำหนดหน้าที่ในการรักษาความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่ และลูกจ้างของสำนักงานมีการปฏิบัติตามอย่างเป็นทางการ |

ตารางที่ 4.1 (ต่อ)

| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.7.2 ระหว่างการจ้างงาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.7.2.2 | การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดให้แก่พนักงาน | ขาดการสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดให้แก่พนักงาน | 3 | 5 | 15 | ต้องสร้างความตระหนัก การให้ความรู้ ด้านความมั่นคงปลอดให้แก่เจ้าหน้าที่และลูกจ้างของสำนักงานจังหวัดพัทลุง |
| A.7.2.3 | กระบวนการทางวินัย | มีกระบวนการลงโทษตามกฎหมาย แต่ไม่มีกระบวนการทางวินัยเพื่อลงโทษของสำนักงานจังหวัดพัทลุง | 5 | 1 | 5 | ต้องมีบทลงโทษของสำนักงานจังหวัดพัทลุงอย่างเป็นทางการ |

ตารางที่ 4.1 (ต่อ)

| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.7.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.7.3.1 | การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน | เมื่อมีการเปลี่ยนหน้าที่มีเพียงการส่งมอบแฟ้มงานเท่านั้น ไม่มีการกำหนดขั้นตอนการปฏิบัติหรือหน้าที่ความรับผิดชอบอย่างชัดเจน | 5 | 1 | 5 | ควรมีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจนและสื่อสารให้เจ้าหน้าที่และลูกจ้างสำนักงานจังหวัดทราบ |

ตารางที่ 4.1 (ต่อ)

| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.8.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.8.1.1 | บัญชีทรัพย์สิน | มีการจัดทำบัญชีอุปกรณ์ระบบเทคโนโลยีฯไว้กับฝ่ายอำนวยการ สำนักงานจังหวัดพัทลุง | 2 | 2 | 4 | ต้องจัดทำบัญชีอุปกรณ์ระบบเทคโนโลยีฯให้ชัดเจนถึงระดับบุคคล |
| A.8.1.2 | ผู้ถือครองทรัพย์สิน | ไม่ได้มีการระบุผู้รับผิดชอบอย่างชัดเจน | 1 | 3 | 3 | ควรระบุชื่อผู้รับผิดชอบอุปกรณ์ต่างๆ อย่างชัดเจน |
| A.8.1.3 | การใช้ทรัพย์สินอย่างเหมาะสม | การปฏิบัติในการใช้งานอุปกรณ์ไม่ได้คำนึงถึงความเสียหายแต่อย่างใด | 5 | 3 | 15 | สำนักงานจังหวัดพัทลุงต้องจัดทำกฎ ระเบียบการใช้อุปกรณ์ที่เกี่ยวข้องอย่างเหมาะสม |
| A.8.1.4 | การคืนทรัพย์สิน | การยืม-คืนอุปกรณ์ไม่ได้ปฏิบัติอย่างเคร่งครัดตามขั้นตอน | 1 | 3 | 3 | ต้องกำหนดขั้นตอนการยืม-คืนอุปกรณ์อย่างชัดเจน |

ตารางที่ 4.1 (ต่อ)

| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.8.2 การจัดชั้นความลับของสารสนเทศ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.8.2 .1 | ชั้นความลับของสารสนเทศ | สำนักงานจังหวัดพัทลุงไม่ได้กำหนดจัดชั้นความลับของสารสนเทศอย่างเป็นทางการ | 4 | 3 | 12 | สำนักงานจังหวัดพัทลุงต้องจัดชั้นความลับให้สอดคล้องกับ กฎหมาย ระเบียบที่เกี่ยวข้อง |
| A.8.2 .2 | การบ่งชี้สารสนเทศ | มีการจัดทำทำป้ายของอุปกรณ์บางรายการ ยังไม่ครบถ้วนและเป็นปัจจุบัน | 2 | 2 | 4 | สำนักงานจังหวัดต้องกำหนดขั้นตอนปฏิบัติในการจัดการอุปกรณ์ระบบสารสนเทศให้รัดกุม |
| A.8.2.3 | การจัดการทรัพย์สิน | ยังไม่ได้ดำเนินการ จัดหมวดหมู่อุปกรณ์และระบบสารสนเทศอย่างเป็นทางการ | 2 | 5 | 10 | ควรมีการจัดการอุปกรณ์ระบบเทคโนโลยีฯ ให้เป็นหมวดหมู่สอดคล้องกับชั้นความลับ |

ตารางที่ 4.1 (ต่อ)

| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.8.3 การจัดการสื่อบันทึกข้อมูล | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.8.3.1 | การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ | สำนักงานจังหวัดพัทลุงไม่ได้ ควบคุมอุปกรณ์บันทึกข้อมูลต่าง ๆแต่อย่างใด | 3 | 3 | 9 | ควรกำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก |
| A.8.3.2 | การทำลายสื่อบันทึกข้อมูล | สำนักงานจังหวัดพัทลุงไม่ได้มีการกำหนดขั้นตอนการทำลายสื่อบันทึกข้อมูลใดๆ | 4 | 2 | 8 | สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย |
| A.8.3.3 | การขนย้ายสื่อบันทึกข้อมูล | ไม่มีการกำหนดการเข้าถึงและขนย้ายสื่อบันทึกข้อมูลใดๆ | 3 | 2 | 6 | ต้องมีการป้องกันสื่อบันทึกข้อมูล จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น |

ตารางที่ 4.1 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
|---|---|---|---|---|---|---|
| A.9.1 ความต้องการทางธุรกิจสำหรับควบคุมการเข้าถึง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.9.1.1 | นโยบายควบคุมการเข้าถึง | ไม่มีการกำหนดสิทธิ ระยะเวลา การให้อำนาจในการเข้าออก พื้นที่ เพื่อควบคุมการเข้าถึง | 3 | 5 | 15 | นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร |
| A.9.1.2 | การเข้าถึงเครือข่ายและบริการเครือข่าย | มีการพิสูจน์ตัวจริงบนเครือข่าย แต่ยังไม่ครอบคลุมทุกอุปกรณ์ | 3 | 4 | 12 | เจ้าหน้าที่ และลูกจ้างของสำนักงานจังหวัดพัทลุงต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติในการเข้าถึงเท่านั้น |

ตารางที่ 4.1 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
|---|---|---|---|---|---|---|
| A.9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.9.2.1 | การลงทะเบียนและการถอนสิทธิผู้ใช้งาน | ขาดการควบคุมให้-ถอนสิทธิการใช้งานอย่างเป็นทางการ | 3 | 4 | 12 | ต้องกำหนดขั้นตอนการลงทะเบียนและถอดถอนสิทธิอย่างเป็นทางการ |
| A.9.2.2 | การจัดการสิทธิการเข้าถึงของผู้ใช้งาน | ทำตามดุลยพินิจของผู้ดูแลระบบโดยหัวหน้าสำนักงานจังหวัดไม่จำเป็นต้องอนุมัติ | 3 | 4 | 12 | ควรกำหนดขั้นตอนการบริหารจัดการสิทธิอย่างเป็นทางการให้หัวหน้าสำนักงานจังหวัดรับทราบ |
| A.9.2.3 | การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ | มีการจัดลำดับความสำคัญในการเข้าถึงข้อมูลของผู้ใช้แต่ละระดับโดยผู้ดูแลระบบ | 2 | 5 | 10 | ต้องมีการควบคุมอย่างเหมาะสมจากหัวหน้าสำนักงานจังหวัดพัทลุง |
| A.9.2.4 | การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวจริงของผู้ใช้งาน | ไม่มีกระบวนการการควบคุมการมอบข้อมูลการพิสูจน์ตัวจริงของผู้ใช้งาน | 5 | 3 | 15 | ต้องมีการมอบข้อมูลการพิสูจน์ตัวจริงของผู้ใช้งานซึ่งเป็นข้อมูลความลับที่เป็นทางการ |

ตารางที่ 4.1 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
|---|---|---|---|---|---|---|
| A.9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.9.2.5 | การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน | มีการทบทวนสิทธิ์ แต่ไม่ได้กำหนดเวลาไว้อย่างชัดเจน | 3 | 4 | 12 | สำนักงานจังหวัดพัทลุงต้องมีการกำหนดระยะเวลา ขั้นตอนการทบทวนสิทธิอย่างชัดเจน |
| A.9.2.6 | การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง | ไม่มีการระบุขั้นตอนปรับปรุงสิทธิการเข้าถึงอย่างเป็นทางการ | 3 | 4 | 12 | สำนักงานจังหวัดพัทลุงต้องระบุขั้นตอนการถอนสิทธิเมื่อเจ้าหน้าที่ลาออก ย้าย หรือสิ้นสุดข้อตกลงการจ้าง |
| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
| A.9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน | | | | | | |
| A.9.3.1 | การใช้ข้อมูลการพิสูจน์ตัวจริงซึ่งเป็นความลับ | ไม่ได้กำหนดวิธีปฏิบัติการใช้ข้อมูลการพิสูจน์ตัวจริงซึ่งเป็นความลับ | 4 | 5 | 20 | ต้องกำหนดวิธีปฏิบัติในการให้ข้อมูลซึ่งเป็นข้อมูลลับ |

ตารางที่ 4.1 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
|---|---|---|---|---|---|---|
| A.9.4 การควบคุมการเข้าถึงระบบ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.9.4.1 | การจำกัดการเข้าถึงสารสนเทศ | มีการกำหนดการรหัสผ่านการเข้าใช้งานระบบสารสนเทศ | 3 | 3 | 9 | ต้องกำหนดขั้นตอนการเข้าถึงสารสนเทศให้สอดคล้องกับนโยบายควบคุมการเข้าถึง |
| A.9.4.2 | ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย | เป็นที่รับทราบเฉพาะผู้ดูแลระบบสำหรับขั้นตอนการล็อกอินเข้าระบบ | 3 | 2 | 6 | ต้องมีการควบคุมขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบอย่างเป็นทางการ |
| A.9.4.3 | ระบบบริหารจัดการรหัสผ่าน | มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน แต่ไม่เป็นทางการ | 3 | 2 | 6 | ต้องมีจัดการกับรหัสผ่าน และบังคับการตั้งรหัสผ่านที่มีคุณภาพ |

ตารางที่ 4.1 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | | |
|---|---|---|---|---|---|---|
| A.9.4 การควบคุมการเข้าถึงระบบ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.9.4.4 | การใช้โปรแกรมอรรถประโยชน์ | ไม่มีการควบคุมการใช้งาน การติดตั้งโปรแกรมประเภทยูทิลิตี้ | 3 | 5 | 15 | ต้องมีการจำกัดและควบคุมการใช้งานอย่างใกล้ชิด |
| A.9.4.5 | การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม | มีการการควบคุมการเข้าถึงซอร์สโค้ด สำหรับระบบ กำหนดการเข้ารหัสและรหัสผ่าน | 2 | 3 | 6 | การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม |

ตารางที่ 4.1 (ต่อ)

| A.10 การเข้ารหัสข้อมูล (Cryptography) | | | | | | |
|---|---|---|---|---|---|---|
| A.10.1 มาตรการเข้ารหัสข้อมูล | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.10.1.1 | นโยบายการใช้มาตรการเข้ารหัสข้อมูล | สำนักงานจังหวัดพัทลุงไม่มีงานให้บริการทางธุรกรรมอิเล็กทรอนิกส์ใดๆ จึงไม่มีการกำหนดมาตรฐานการเข้ารหัส | 2 | 2 | 4 | ควรมีแนวทางการกำหนดนโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อรองรับงานในอนาคต |
| A.10.1.2 | การบริหารจัดการกุญแจ | ยังไม่ได้ดำเนินการใดๆ ที่เกี่ยวข้อง | 2 | 1 | 2 | ควรคำนึงถึงนโยบายการบริหารจัดการกุญแจไว้รองรับการให้บริการในอนาคตถ้าหากมี |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.1.1 | พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย | มีการจัดสรรพื้นที่กั้น จัดทำประตูเข้าออก เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของหน่วยงาน | 5 | 1 | 5 | มีการกำหนดพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย |
| A.11.1.2 | การควบคุมการเข้าออกทางกายภาพ | - มีการลงบันทึกควบคุมการเข้าออกพื้นที่จัดเก็บสารสนเทศ<br>- มีกล้องวงจรปิด<br>- มีการล็อคห้องสื่อสารเพื่อป้องกันการเข้าถึงโดยบุคคลภายนอกกรณีไม่มีเจ้าหน้าที่ประจำที่ทำการ | 5 | 1 | 5 | พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย ต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสม โดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงพื้นที่สำคัญได้ |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.1.3 | การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ต่างๆ | มีการรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ต่างๆ | 4 | 2 | 8 | ต้องมีการออกแบบและดำเนินการความมั่นคงปลอดภัยทางกายภาพของสำนักงานจังหวัด ห้องทำงานและอุปกรณ์ต่างๆ |
| A.11.1.4 | การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม | มีถังดับเพลิง แต่ไม่ได้มีไซต์สำรอง | 3 | 2 | 6 | ต้องมีการออกแบบและดำเนินการป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุกหรืออุบัติเหตุ |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.1.5 | การปฏิบัติงานในพื้นที่ต้องรักษาความมั่นคงปลอดภัย | ไม่มีการกำหนดขั้นตอนใดๆ สำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย | 3 | 3 | 9 | ต้องมีการจัดทำและปฏิบัติตามขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย |
| A.11.1.6 | พื้นที่สำหรับรับส่งสิ่งของ | ไม่มีการจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก | 3 | 2 | 6 | ต้องมีการควบคุม เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.2 อุปกรณ์ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.2.1 | การจัดตั้งและป้องกันอุปกรณ์ | มีถังดับเพลิง แต่ไม่ได้มีไซต์สำรอง | 4 | 2 | 8 | ต้องมีป้องกันเพื่อลดความเสี่ยงจากภัยคุกคาม |
| A.11.2.2 | ระบบและอุปกรณ์สนับสนุนการทำงาน | มีระบบต่างๆ เช่น ระบบไฟฟ้า ระบบระบายอากาศ เป็นต้น แต่เก่าขาดการบำรุงรักษา และขาดระบบสายสื่อสารสำรอง | 4 | 2 | 8 | ต้องได้รับการป้องกันการหยุดชะงักโดยมีการติดตั้งระบบและอุปกรณ์สนับสนุนการทำงาน |
| A.11.2.3 | ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร | มีการร้อยสายบางส่วนเฉพาะลิงค์ที่สำคัญเท่านั้น | 3 | 3 | 9 | ต้องมีการป้องกัน การขัดขวางการทำงาน หรือการทำให้เสียหาย |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.2 อุปกรณ์ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.2.4 | การบำรุงรักษาอุปกรณ์ | ขาดงบประมาณในการบำรุงรักษาอุปกรณ์ | 4 | 3 | 12 | อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง |
| A.11.2.5 | การนำทรัพย์สินขององค์กรออกนอกสำนักงาน | ไม่ได้กำหนดขั้นตอน กฎเกณฑ์การนำอุปกรณ์ออกนอกสำนักงานจังหวัดพัทลุง | 3 | 1 | 3 | อุปกรณ์ สารสนเทศหรือซอฟต์แวร์ต้องไม่มีการนำออกนอกสำนักงานโดยปราศจากการขออนุญาตก่อน |
| A.11.2.6 | ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน | ไม่มีกำหนดขั้นตอน การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงานเข้าถึงระบบภายในสำนักงาน | 3 | 2 | 6 | ต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน |

ตารางที่ 4.1 (ต่อ)

| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.11.2 อุปกรณ์ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.11.2.7 | ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น | ไม่มีขั้นตอนการปฏิบัติสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น | 3 | 3 | 9 | ต้องมีการตรวจสอบ ก่อนการกำจัดอุปกรณ์หรือก่อนนำอุปกรณ์ไปใช้งานอย่างอื่น |
| A.11.2.8 | อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล | ไม่มีการป้องกัน ควบคุม การดูแลอุปกรณ์ใดมีแต่ทะเบียนคุมเลขครุภัณฑ์คอมพิวเตอร์ | 2 | 3 | 6 | ต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม |
| A.11.2.9 | นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ | ไม่มีการกำหนดนโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ | 1 | 5 | 5 | ต้องกำหนดนโยบายโต๊ะทำงานปลอดเอกสารสำคัญ เพื่อป้องกันสารสนเทศในอุปกรณ์ประมวลสารสนเทศ และต้องมีการนำมาใช้ |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.1.1 | ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร | สำนักงานจังหวัดพัทลุงไม่มีวิธีการปฏิบัติงานด้านความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร | 3 | 1 | 3 | สำนักงานจังหวัดพัทลุงต้องจัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร |
| A.12.1.2 | การบริหารจัดการการเปลี่ยนแปลง | สำนักงานจังหวัดพัทลุงยังไม่ได้กำหนดกระบวนการบริหารการเปลี่ยนแปลงใดๆ | 5 | 1 | 5 | ต้องควบคุมการเปลี่ยนแปลงที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศของสำนักงานจังหวัดพัทลุง |
| A.12.1.3 | การบริหารขีดความสามารถของระบบ | ไม่มีการติดตาม ประเมินผลขีดความสามารถของระบบ | 5 | 4 | 20 | ต้องมีการติดตาม ปรับปรุง การใช้ทรัพยากรของระบบ เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ |
| A.12.1.4 | มีการแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน | เมื่อมีการพัฒนาระบบจะแยกทดสอบต่างหาก เพื่อให้ระบบต่างๆ สามารถใช้งานได้ปกติ | 4 | 1 | 4 | ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.2 การป้องกันโปรแกรมไม่ประสงค์ดี | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.2.1 | การป้องกันโปรแกรมที่ไม่ประสงค์ดี | ไม่มีอุปกรณ์การตรวจจับ การป้องกัน มีแต่แอนตี้ไวรัส | 5 | 3 | 15 | ต้องมีมาตรการสำหรับการตรวจหา การป้องกัน และการกู้กลับคืนจากโปรแกรมไม่ประสงค์ดี |
| A.12.3 การสำรองข้อมูล | | | | | | |
| A.12.3.1 | การสำรองข้อมูล | มีการสำรองข้อมูลเป็นประจำ | 5 | 1 | 5 | ต้องจัดให้มีการสำรองและทดสอบข้อมูลสำรองเก็บไว้อย่างสม่ำเสมอ |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.4 การบันทึกข้อมูลล็อคและการเฝ้าระวัง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.4.1 | การบันทึกข้อมูลล็อคแสดงเหตุการณ์ | สำนักงานปลัดกระทรวงมหาดไทยทำการบันทึกกิจการรมการใช้งาน สำนักงานจังหวัดพัทลุงยังไม่มีการดำเนินการใดๆ | 3 | 5 | 15 | สำนักงานจังหวัดพัทลุงควรดำเนินการบันทึกกิจกรรมการใช้งานระบบต่างๆ |
| A.12.4.2 | การป้องกันข้อมูลล็อค | ไม่มีการกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรม หรือเหตุการณ์ใดๆ ที่เกี่ยวกับการใช้งานสารสนเทศ | 3 | 5 | 15 | สำนักงานจังหวัดพัทลุงต้องมีข้อมูลล็อกและต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.4 การบันทึกข้อมูลล็อคและการเฝ้าระวัง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.4.3 | ข้อมูลล็อคกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ | ไม่มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของเจ้าที่ที่เกี่ยวข้องกับระบบ | 3 | 5 | 15 | กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบต้องมีการบันทึกข้อมูลล็อค และต้องมีการป้องกันทบทวนอย่างสม่ำเสมอ |
| A.12.4.4 | การตั้งนาฬิกาให้ถูกต้อง | ไม่มีการกำหนดเวลาของเครื่องคอมพิวเตอร์ในสำนักงานให้ตรงกัน | 2 | 5 | 10 | ต้องมีการกำหนดเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงเวลาที่ถูกต้องเพื่อช่วยตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ถูกบุกรุก |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.5.1 | การติดตั้งซอฟต์แวร์บนระบบให้บริการ | สำนักงานจังหวัดพัทลุงไม่ได้แนวทางปฏิบัติติดตั้งซอฟต์แวร์บนระบบให้บริการ | 3 | 5 | 15 | ต้องมีการกำหนดขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ |
| A.12.6 การบริหารจัดการช่องโหว่ทางเทคนิค | | | | | | |
| A.12.6.1 | การบริหารจัดการช่องโหว่ทางเทคนิค | มีการดำเนินการบ้างแต่ไม่ต่อเนื่องและไม่สามารถทำได้ครอบคลุม | 2 | 4 | 8 | ต้องกำหนดติดตามข่าวสารสที่เกี่ยวกับช่องโหว่ และประเมินความเสี่ยง พร้อมกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว |
| A.12.6.2 | การจำกัดการติดตั้งซอฟต์แวร์ | ไม่มีการควบคุมการติดตั้งซอฟต์แวร์ใดๆ | 2 | 3 | 6 | ต้องกำหนดกฎเกณฑ์การควบคุมการจำกัดการติดตั้งซอฟต์แวร์และผู้ใช้งานปฏิบัติตาม |

ตารางที่ 4.1 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.12.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.12.7.1 | มาตรการการตรวจประเมินระบบ | ไม่มีมาตรการการตรวจประเมินระบบสารสนเทศ | 3 | 4 | 12 | ต้องกำหนด การวางแผนและตกลงร่วมกันที่เกี่ยวข้องกับ การตรวจประเมินระบบ |

ตารางที่ 4.1 (ต่อ)

| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.13.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.13.1.1 | มาตรการเครือข่าย | ใช้งานได้ตามอิสระไม่มีการกำหนดมาตรการใด ๆ | 5 | 5 | 25 | ต้องมีการบริหารจัดการและควบคุมระบบเครือข่าย |
| A.13.1.2 | ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย | ขาดการบริหารความมั่นคงปลอดภัย ไม่มีการติดตั้งระบบป้องกันใดๆ | 3 | 5 | 15 | ต้องมีกำหนดข้อตกลงการให้บริการเครือข่าย การรักษาความมั่นคงปลอดภัยในการให้บริการ |
| A.13.1.3 | การแบ่งแยกเครือข่าย | ไม่มีการกำหนด แผนผังการใช้งานระบบเครือข่าย และขาดการแบ่งพื้นที่การใช้งานตามความเหมาะสม | 3 | 5 | 15 | ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด และป้องกันการเข้าถึงจากบุคคลภายนอก |

ตารางที่ 4.1 (ต่อ)

| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.13.2 การถ่ายโอนสารสนเทศ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.13.2.1 | นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ | สามารถถ่ายโอนข้อมูลต่างๆ ได้โดยไม่ได้กำหนดขั้นตอนปฏิบัติใด ๆ | 3 | 5 | 15 | ต้องมีนโยบาย ขั้นตอนปฏิบัติและมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการ |
| A.13.2.2 | ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ | สามารถถ่ายโอนข้อมูลต่างๆ ได้โดยไม่ได้กำหนดข้อตกลงใด ๆ | 3 | 5 | 15 | ต้องจัดทำข้อตกลงในการถ่ายโอนสารสนเทศ ระหว่างหน่วยงานอย่างเป็นลายลักษณ์อักษร |
| A.13.2.3 | การส่งข้อความอิเล็กทรอนิกส์ | การส่งผ่านทางข้อความอิเล็กทรอนิกส์สามารถดำเนินการได้โดยไม่มีข้อกำหนดใดๆ | 3 | 5 | 15 | ต้องกำหนดการส่งข้อความทางอิเล็กทรอนิกส์อย่างเหมาะสม |
| A.13.2.4 | ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ | ไม่มีการกำหนดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ | 5 | 4 | 20 | ต้องกำหนดการรักษาความลับ ทบทวนอย่างสม่ำเสมอและบันทึกไว้อย่างเป็นลายลักษณ์อักษร |

ตารางที่ 4.1 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | | |
|---|---|---|---|---|---|---|
| A.14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.14.1.1 | การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ | ยังไม่เคยดำเนินการวิเคราะห์ความมั่นคงปลอดภัยสารสนเทศใดๆ | 5 | 4 | 20 | ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว |
| A.14.1.2 | ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ | การดำเนินการความมั่นคงปลอดภัยบนระบบเครือข่ายมักไม่ได้รับงบประมาณสนับสนุน | 4 | 3 | 12 | หัวหน้าสำนักงานจังหวัดต้องให้ความสำคัญในการจัดระบบสารสนเทศในการให้บริการด้วยความมั่นคงปลอดภัยผ่านระบบเครือข่าย |
| A.14.1.3 | การป้องกันธุรกรรมของบริการสารสนเทศ | ระบบสารสนเทศที่มีของสำนักงานจังหวัดพัทลุงมักโดนลบข้อมูลในฐานข้อมูลอยู่เสมอ | 5 | 1 | 5 | สารสนเทศต้องได้รับการป้องกันตามหลักความปลอดภัยของข้อมูล |

ตารางที่ 4.1 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | | |
|---|---|---|---|---|---|---|
| A.14.2 ความความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.14.2.1 | นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย | การกำหนดขอบเขตงานไม่ได้คำนึงถึงนโยบายความมั่นคงปลอดภัย | 5 | 5 | 25 | การพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดให้มีความมั่นคงปลอดภัยด้วย |
| A.14.2.2 | ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ | การกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบไม่ได้ถูกกำหนดในเงื่อนไขการพัฒนาระบบ | 5 | 1 | 5 | ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ |
| A.14.2.3 | การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ | การทบทวนทางเทคนิคมักไม่ได้ดำเนินการ | 2 | 5 | 10 | ต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อด้านความมั่นคงปลอดภัย |

ตารางที่ 4.1 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | | |
|---|---|---|---|---|---|---|
| A.14.2 ความความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.14.2.4 | การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป | โดยปกติไม่มีการแก้ไขซอฟต์แวร์ใดๆ แต่ไม่ได้กำหนดอย่างเป็นทางการ | 5 | 2 | 10 | ต้องกำหนดให้ไม่เปลี่ยนแปลงใดๆ ยกเว้นกรณีจำเป็น |
| A.14.2.5 | หลักการวิศวะกรรมของระบบด้านความมั่นคงปลอดภัย | การพัฒนาระบบไม่ได้คำนึงถึงหลักการวิศวะกรรมของระบบด้านความมั่นคงปลอดภัย | 5 | 3 | 15 | การพัฒนาระบบของสำนักงานจังหวัดพัทลุงต้องกำหนดด้านความมั่นคงปลอดภัยเป็นลายลักษณ์อักษรตามหลักวิศวะกรรมระบบ |
| A.14.2.6 | สภาพแวดล้อมการพัฒนาระบบที่มีความมั่นคงปลอดภัย | มีการพัฒนาระบบสารสนเทศแต่มักไม่ได้คำนึงเรื่องความมั่นคงปลอดภัย | 3 | 3 | 9 | ต้องจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย ชีวิตของการพัฒนาระ |

ตารางที่ 4.1 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | | |
|---|---|---|---|---|---|---|
| A.14.2 ความความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.14.2.7 | การจ้างหน่วยงานจากภายนอกพัฒนาระบบ | ไม่ได้ดำเนินการตรวจสอบทุกกระบวนการในการพัฒนาระบบ | 5 | 2 | 10 | ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์ |
| A.14.2.8 | การทดสอบด้านความมั่นคงปลอดภัยของระบบ | มีการดำเนินการบ้างแต่ไม่ต่อเนื่องและไม่สามารถทำได้ครอบคลุม | 5 | 5 | 25 | การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการทุกช่วงของการพัฒนา |
| A.14.2.9 | การทดสอบเพื่อรับรองระบบ | ดำเนินการการตามสถานการณ์ที่เกิดขึ้น | 5 | 3 | 15 | ต้องมีการจัดทำแผนการทดสอบสำหรับระบบใหม่ |
| A.14.3 ข้อมูลสำหรับการทดสอบ | | | | | | |
| A.14.3.1 | การป้องกันข้อมูลสำหรับการทดสอบ | ทดสอบข้อมูลตามความต้องการของเจ้าหน้าที่ | 3 | 3 | 9 | ต้องมีการกำหนดแผน ข้อมูลและกฎเกณฑ์ในการทดสอบ |

ตารางที่ 4.1 (ต่อ)

| A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) | | | | | | |
|---|---|---|---|---|---|---|
| A.15.1 ความความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.15.1.1 | นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก | กำหนดขอบเขตงานแต่คำนึงถึงความมั่นคงปลอดภัยในการเข้าถึงข้อมูลสำคัญต่างๆ ของสำนักงาน | 3 | 5 | 15 | ต้องมีการกำหนดและตกลงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ กับผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร |
| A.15.1.2 | การระบุความมั่นคงปลอดภัยในการให้ตกลงการให้บริการของผู้ให้บริการภายนอก | ไม่มีการกำหนดข้อตกลงในการเข้าถึงระบบเทคโนโลยีสารสนเทศต่างๆ ของสำนักงานจังหวัด | 2 | 4 | 8 | ต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับการเข้าถึง การประมวลผล การจัดเก็บการสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบ |
| A.15.1.3 | ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก | ไม่เคยมีการประเมินความเสี่ยงการเข้าถึงสารสนเทศ | 3 | 5 | 15 | ต้องกำหนดข้อตกลงกับผู้ให้บริการภายนอกโดยคำนึงถึงความเสี่ยงที่อาจจะเกิดขึ้น |

ตารางที่ 4.1 (ต่อ)

| A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) | | | | | | |
|---|---|---|---|---|---|---|
| A.15.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.15.2.1 | การติดตามและทบทวนบริการของผู้ให้บริการภายนอก | มีเอกสารแจ้งผลการดำเนินงานจากผู้ให้บริการภายนอกเป็นระยะๆ | 5 | 1 | 5 | ต้องมีการติดตาม ทบทวนและประเมินผลการให้บริการของผู้ให้บริการภายนอก |
| A.15.2.2 | การบริหารจัดการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก | ไม่มีการกำหนดนโยบายด้านการเปลี่ยนแปลงผู้ให้บริการใดๆ | 5 | 2 | 10 | ต้องกำหนดขั้นตอนปฏิบัติ โดยต้องกำหนดระดับความสำคัญของระบบสารสนเทศ และประเมินความเสี่ยงที่อาจจะเกิดขึ้น |

ตารางที่ 4.1 (ต่อ)

| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.16.1.1 | หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ | เจ้าหน้าที่คอมพิวเตอร์เท่านั้นที่ดูแลแต่ไม่ได้กำหนดขั้นตอนปฏิบัติอย่างเป็นทางการ | 2 | 2 | 4 | ต้องกำหนด บทบาท หน้าที่รับผิดชอบที่ชัดเจน สำหรับการบริหารจัดกาตามลำดับต่อเหตุความมั่นคงปลอดภัยสารสนเทศ |
| A.16.1.2 | มีการรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ | เจ้าหน้าที่คอมพิวเตอร์ไม่ได้รายงานผลการปฏิบัติงานอย่างเป็นทางการ | 1 | 2 | 2 | ต้องรายงานสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรวดเร็วที่สุด |
| A.16.1.3 | การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ | เจ้าหน้าที่คอมพิวเตอร์รายงานด้วยวาจาหรืออาจไม่ได้รายงานเลย | 5 | 2 | 10 | ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างเป็นทางการ |

ตารางที่ 4.1 (ต่อ)

| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.16.1.4 | การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ | เจ้าหน้าที่คอมพิวเตอร์เป็นคนประเมินและตัดสินใจ เพื่อแก้ไขปัญหาที่เกิดขึ้น | 5 | 1 | 5 | ต้องมีการประเมินและมีการตัดสินว่าสถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่ |
| A.16.1.5 | การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | แก้ไขปัญหาเฉพาะหน้าโดยไม่มีขั้นตอนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างเป็นทางการ | 5 | 4 | 20 | ต้องกำหนดขั้นตอนปฏิบัติไว้เป็นลายลักษณ์อักษร |

ตารางที่ 4.1 (ต่อ)

| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | | | | | | |
|---|---|---|---|---|---|---|
| A.16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.16.1.6 | การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | ไม่มีการจดบันทึกเหตุการณ์และการแก้ไขปัญหาที่เกิดขึ้น | 5 | 3 | 15 | ต้องจดบันทึกและนำผลมาวิเคราะห์เพื่อลดความเสี่ยงของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่จะเกิดในอนาคต |
| A.16.1.7 | การเก็บรวบรวมหลักฐาน | มีการจดบันทึกไอพีสำหรับผู้ใช้งานแต่ละเครื่อง | 3 | 2 | 6 | องค์กรต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหาและการจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน |

ตารางที่ 4.1 (ต่อ)

| A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) | | | | | | |
|---|---|---|---|---|---|---|
| A.17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.17.1.1 | การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | เป็นเพียงการแก้ไขปัญหาเฉพาะหน้าไม่มีการวางแผนบริการจัดการความต่อเนื่อง | 3 | 2 | 6 | ต้องกำหนดบริหารความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องเพื่อลดความเสียหาย |
| A.17.1.2 | การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | แก้ไขปัญหาตามประสบการณ์ ไม่มีการวางแผนเตรียมการล่วงหน้า | 5 | 3 | 15 | ต้องกำหนดขั้นตอนปฏิบัติ เพื่อความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศเป็นจัดทำเป็นลายลักษณ์อักษรและปฏิบัติตาม |
| A.17.1.3 | การตรวจสอบ การทบทวน และการเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | สำนักงานจังหวัดพัทลุงไม่มีแผนสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | 2 | 4 | 8 | ต้องมีการตรวจสอบ การทบทวน และการเมินความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนดไว้ |

ตารางที่ 4.1 (ต่อ)

| A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) | | | | | | |
|---|---|---|---|---|---|---|
| A.17.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.17.2.1 | สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ | ไม่มีงบประมาณเพียงพอในการจัดหาเพื่อทดแทนของเดิม | 3 | 2 | 6 | ต้องจัดหาอุปกรณ์ประมวลผลสารสนเทศสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้ |

ตารางที่ 4.1 (ต่อ)

| A.18 ความสอดคล้อง (Compliance) | | | | | | |
|---|---|---|---|---|---|---|
| A.18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.18.1.1 | การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง | ใช้กฎหมาย ระเบียบทางราชการเป็นสำคัญ | 1 | 2 | 2 | ต้องคำนึงถึงกฎหมาย ระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัย และระบุในสัญญาจ้างให้ครอบคลุม |
| A.18.1.2 | สิทธิและทรัพย์สินทางปัญญา | มีการคำนึงถึงกฎหมายป้องกันสิทธิและทรัพย์สินทางปัญญา แต่ไม่เป็นลายลักษณ์อักษร | 1 | 3 | 3 | ต้องกำหนดขั้นตอนปฏิบัติที่เหมาะสม อย่างเป็นทางการเพื่อควบคุมให้เป็นไปตามกฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้อง |
| A.18.1.3 | การป้องกันข้อมูล | มีการกำหนดโทษทางวินัย แต่ไม่ได้กำหนดเงื่อนไขการทำความผิดด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นทางการ | 1 | 2 | 2 | ต้องกำหนดมาตรการป้องกันให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง |

ตารางที่ 4.1 (ต่อ)

| A.18 ความสอดคล้อง (Compliance) | | | | | | |
|---|---|---|---|---|---|---|
| A.18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.18.1.4 | ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล | เจ้าหน้าที่ป้องกันข้อมูลส่วนตัวตามความต้องการของตัวเอง ไม่ได้กำหนดอย่างเป็นทางการ | 1 | 4 | 4 | ต้องมีกำหนดให้สอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้องอย่างเป็นทางการ |
| A.18.1.5 | ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล | มาตรการเข้ารหัสข้อมูลไม่ได้ถูกใช้งานอย่างเป็นทางการ มีเพียงการ encode ข้อมูลบ้างบางส่วน | 2 | 2 | 4 | มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง กฎหมายและระเบียบที่เกี่ยวข้อง |

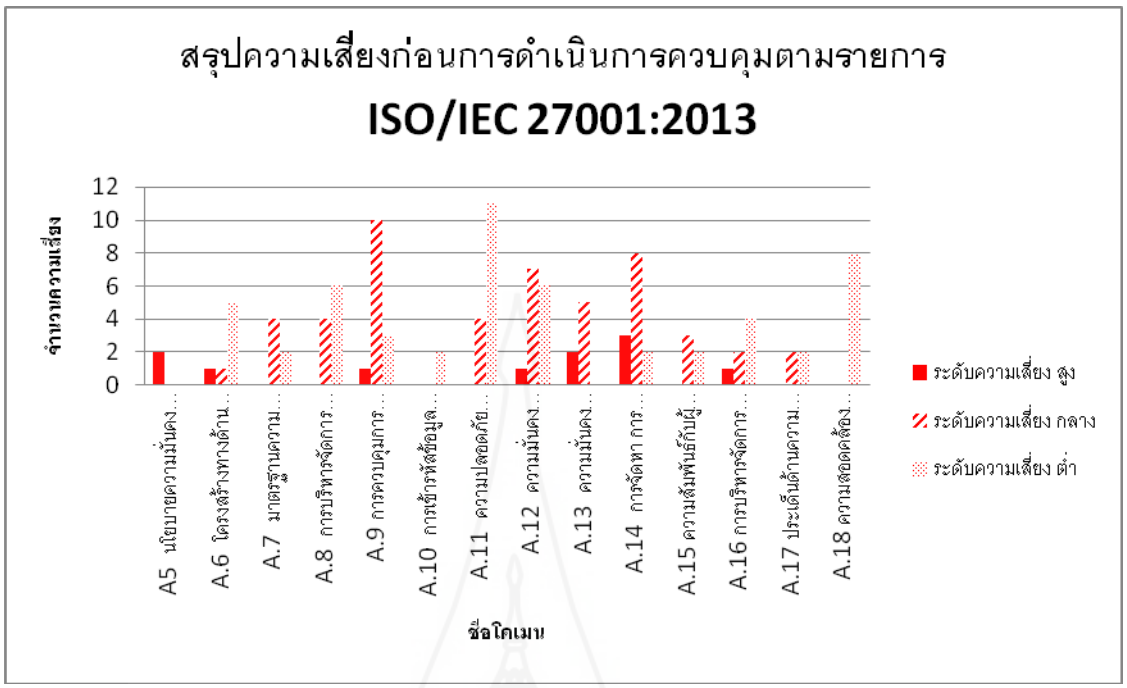
ตารางที่ 4.1 (ต่อ)

| A.18 ความสอดคล้อง (Compliance) | | | | | | |
|---|---|---|---|---|---|---|
| A.18.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.18.2.1 | การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ | ไม่ได้กำหนดแผนการทบทวนความมั่นคงปลอดภัย | 3 | 2 | 6 | ต้องกำหนดแผนการทบทวนความมั่นคงปลอดภัยตามระยะเวลาที่เหมาะสม |
| A.18.2.2 | ความสอดคล้องกับนโยบายมาตรฐานด้านมั่นคงปลอดภัยสารสนเทศ | ขาดการทบทวนความสอดคล้องในมาตรการด้านความมั่นคงปลอดภัยต่างๆ | 3 | 2 | 6 | ต้องทบทวนความสอดคล้องอย่างสม่ำเสมอ |
| A.18.2.3 | การทบทวนความสอดคล้องด้านเทคนิค | ไม่มีการดำเนินการอย่างชัดเจน มีแต่การปฏิบัติตามหน้าที่ | 5 | 1 | 5 | ต้องทบทวนพิจารณาความสอดคล้องด้านเทคนิคกับนโยบายความมั่นคงปลอดภัยอย่างสม่ำเสมอ |

จากการประเมินค่าความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนการดำเนินงาน ตามรายการควบคุม 14 โดเมน 114 ตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง สรุปได้ดังนี้

ตารางที่ 4.2 สรุประดับความเสี่ยงของสำนักงานจังหวัดพัทลุงตามมาตฐาน ISO/IEC 27001 :2013 ก่อนดำเนินการ

| ISO/IEC27001:2013 | ระดับความเสี่ยง | | |
|---|---|---|---|
| 14 Domain | สูง | กลาง | ต่ำ |
| A5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) | 2 | - | - |
| A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) | 1 | 1 | 5 |
| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | - | 4 | 2 |
| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | - | 4 | 6 |
| A.9 การควบคุมการเข้าถึง (Access Control) | 1 | 10 | 3 |
| A.10 การเข้ารหัสข้อมูล (Cryptography) | - | - | 2 |
| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | - | 4 | 11 |
| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | 1 | 7 | 6 |
| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | 2 | 5 | - |
| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | 3 | 8 | 2 |
| A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) | - | 3 | 2 |
| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | 1 | 2 | 4 |
| A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) | - | 2 | 2 |
| A.18 ความสอดคล้อง (Compliance) | - | - | 8 |
| รวม | 11 | 50 | 53 |




ภาพที่ 4.4 ระดับความเสี่ยงก่อนการดำเนินการ

จากภาพที่ 4.4 แสดงกราฟสรุประดับความเสี่ยงแต่ละรายการควบคุมตามมาตรฐาน ISO/IEC 27001:2013 จะเห็นได้ว่า สำนักงานจังหวัดพัทลุงยังมีระดับความเสี่ยงตามรายการควบคุมของมาตรฐาน ISO/IEC27001:2013 อยู่หลายรายการ ทั้งนี้จากการวิเคราะห์ระบบเครือข่ายเดิมและประเมินความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานอ้างอิงตามมาตรฐาน ISO/IEC27001:2013 สามารถสรุปผลได้ ดังนี้

1) สำนักงานจังหวัดพัทลุงไม่ได้กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2) สำนักงานจังหวัดพัทลุงขาดการกำหนดบทบาทและหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3) สำนักงานจังหวัดพัทลุงไม่ได้กำหนดการควบคุมการใช้งานระบบเครือข่ายและสารสนเทศ

4) สำนักงานจังหวัดพัทลุงขาดการจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

5) อุปกรณ์ที่ติดตั้งตั้งของสำนักงานจังหวัดพัทลุงเป็นอุปกรณ์รุ่นเก่า ตัวอย่างเช่น อุปกรณ์ไฟร์วอลล์ ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีรูปแบบใหม่ๆ ได้ เป็นสาเหตุหนึ่งที่ทำให้ระบบเครือข่ายช้า ขาดเสถียรภาพในการใช้งาน

6) สำนักงานจังหวัดพัทลุงขาดอุปกรณ์ในการควบคุมและบริหารจัดการระบบเครือข่าย ไม่สามารถบริหารจัดการเครือข่ายได้

7) สำนักงานจังหวัดพัทลุงมีปัญหาความเร็วที่จำกัด แบนด์วิดท์ในการใช้งานอินเทอร์เน็ต การเชื่อมต่อสวิตซ์หลายตัวแบบเชื่อมต่อกันไปเรื่อยๆ จะทำให้เป็นการลดทอนสัญญาณ ส่งผลให้ประสิทธิภาพในการใช้งานช้าลง

## 3. พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

จากการประเมินความเสี่ยงตามมาตรฐาน ISO/IEC27001:2013 ของสำนักงานจังหวัดพัทลุง พบว่า สำนักงานจังหวัดพัทลุงยังขาดนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งจะเป็นเครื่องมือสำคัญในการสร้างแนวทางปฏิบัติร่วมกันของเจ้าหน้าที่ภายในสำนักงานจังหวัดพัทลุงในการควบคุมและป้องกันความเสียหายจากการบุกรุก ผู้วิจัยจึงได้พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุงขึ้น เพื่อเป็นแนวทางยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง ให้มีความสามารถรับมือกับภัยคุกคามที่จะเกิดขึ้น และใช้เป็นแนวทางปฏิบัติให้กับเจ้าหน้าที่ผู้ดูแลระบบ และผู้ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง เพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน

โดยผู้วิจัยได้นำผลลัพธ์ที่ได้จาก ขั้นตอนที่ 1 และ 2 มากำหนดกรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ประกอบด้วย

3.1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security) โดยสรุปกล่าวถึง การกำหนดพื้นที่เข้าออก พื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย การกำหนดส่วนของระบบเครือข่าย การกำหนดสิทธิและวิธีปฏิบัติในการเข้าออกพื้นที่

3.2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control) โดยสรุปกล่าวถึง การกำหนดสิทธิและหน้าที่ในการปฏิบัติงานเพื่อควบคุมการใช้งานระบบ การบริหารจัดการการเข้าถึง เช่น การให้-ยกเลิกสิทธิการใช้งาน การกำหนดระยะเวลาการใช้งาน การจำกัดสิทธิการใช้งาน การบันทึกการใช้งาน รวมถึงการควบคุมการเข้าใช้งานจากภายนอก

3.3 การใช้ควบคุมการใช้งานอินเทอร์เน็ต (Use of the Internet) โดยสรุปกล่าวถึง การกำหนดเส้นทางการเชื่อมต่อ การกำหนดจริยธรรมผู้ใช้งาน เช่น ห้ามเปิดเผยข้อมูลเชิงความลับผ่านอินเทอร์เน็ต จำกัดการเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม เป็นต้น

3.4 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยสรุปกล่าวถึง การกำหนดสิทธิการเข้าใช้งานระบบเครือข่าย การเปลี่ยนค่าอุปกรณ์กระจายสัญญาณที่กำหนดมาจากโรงงาน และตั้งค่าการทำงานใหม่ให้เหมาะสม เพื่อป้องกันการโจมตีหรือบุกรุก รายละเอียดกรอบนโยบาย 6 ด้าน ที่พัฒนาขึ้นแสดงในภาคผนวก ก

## 4. ดำเนินการติดตั้งและทดสอบระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

จากการวิเคราะห์ระบบเครือข่ายเดิมที่มีปัญหาขาดเสถียรภาพในการใช้งาน อุปกรณ์ล้าสมัย ไม่สามารถรองรับภัยคุกคามคอมพิวเตอร์หรือการโจมตีแบบใหม่ๆ ได้ ไม่สามารถบริหารจัดการเครือข่ายได้ และผลจากการประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดตามมาตรฐาน ISO/IEC 27001:2013 ตามที่ได้วิเคราะห์ไว้ข้างต้น ผู้วิจัยจึงได้ติดตั้งระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันรักษาความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ให้เกิดความสอดคล้องตามกรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงที่ได้กำหนดไว้ รายละเอียด ดังนี้

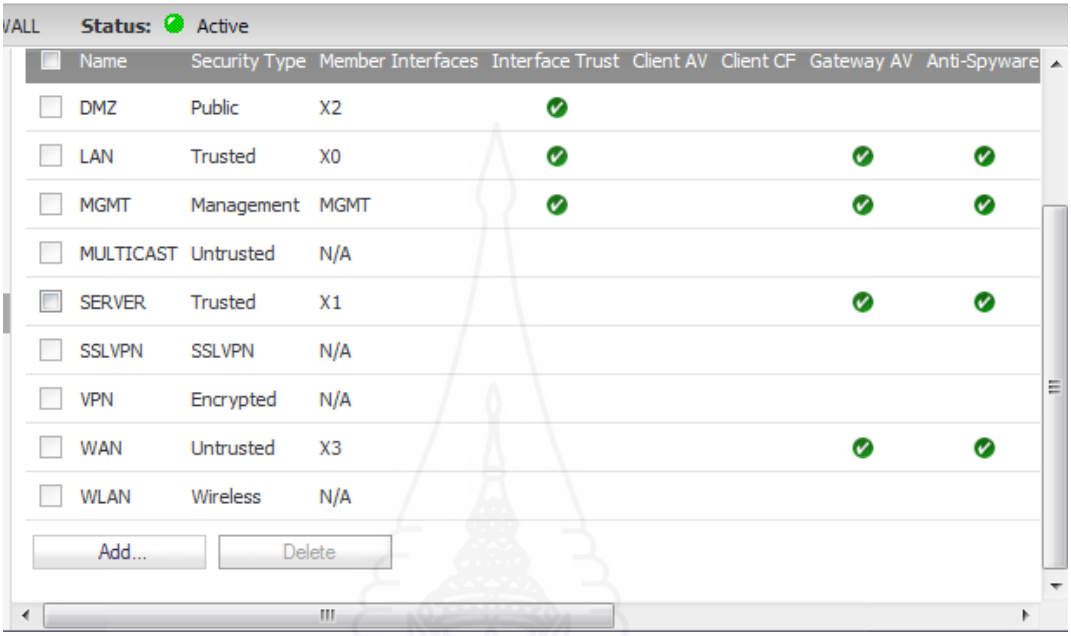
4.1 ติดตั้งอุปกรณ์และระบบรักษาความปลอดภัย ได้แก่ DELL SonicWALL NSA3600 Firewall, DELL SonicWALL NSA3600 IPS, Blue Coat Proxy SG200-10 Proxy, Logger L120 (Dell R220), Authentication SQL Local (Dell R320) , Dell E1914H Monitor for SQL Local Search Log, ZyXEL GS2210-24 Switch, Syndome HE3000 UPS,computer and scanner

ภาพที่ 4.5 รายการอุปกรณ์ระบบเครือข่ายที่ติดตั้ง

จากภาพที่ 4.5 แสดงรายการอุปกรณ์ที่ได้ดำเนินการติดตั้งเพื่อป้องกันและรักษาความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยได้ติดตั้งอุปกรณ์เชื่อมโยงกับระบบเครือข่ายสื่อสารข้อมูลภาครัฐ (Government Infrastructure Network: GIN) ของกระทรวงเทคโนโลยีสารสนเทศ ให้บริการด้วยความเร็ว 50 Mbps ติดตั้งอยู่ในบริเวณศาลากลางเข้ากับเครือข่ายของสำนักงานสำนักงานจังหวัด เพื่อเป็นอีกช่องในการให้บริการสัญญาณอินเทอร์เน็ต และเพื่อให้อุปกรณ์สามารถทำหน้าที่ในการรักษาความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงได้อย่างสอดคล้องกับกรอบนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงด้วยนั้น ผู้วิจัยจึงได้ดำเนินการตั้งค่าการทำงาน (Configuration) ให้อุปกรณ์ไฟร์วอลล์และอุปกรณ์รักษาความปลอดภัยอื่นๆ เพื่อควบคุมการเข้าถึงและจำกัดการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยมีรายละเอียดดังต่อไปนี้

***4.1.1 กำหนดพื้นที่บนระบบเครือข่าย (Network Zone)*** เพื่อควบคุมการการเข้าถึงระบบจากภายนอกสำนักงานจังหวัดพัทลุงให้สามารถเข้าถึงได้เฉพาะพื้นที่ที่กำหนดให้บริการ

เท่านั้น และควบคุมการใช้งานภายในสำนักงานจังหวัดพัทลุงให้สามารถใช้งานได้เฉพาะพื้นที่ที่กำหนดไว้เช่นกัน




ภาพที่ 4.6 การกำหนดค่าโซนให้กับอุปกรณ์ไฟร์วอลล์

จากภาพที่ 4.6 สามารถอธิบายได้ว่า สำนักงานจังหวัดพัทลุงมีการกำหนดพื้นที่บนระบบเครือข่าย ได้แก่

- พื้นที่สำหรับให้บริการเครือข่ายภายในสำนักงาน (LAN Zone) ติดตั้งอุปกรณ์ เช่น เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์กระจายสัญญาณ เป็นต้น

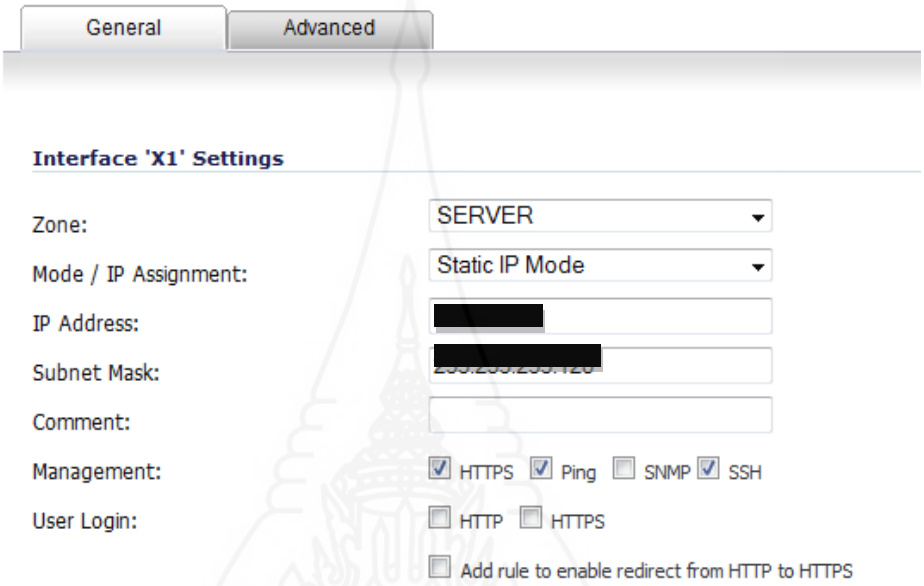
- พื้นที่สำหรับอุปกรณ์แม่ข่ายที่มีความสำคัญสูง (Server Zone) ติดตั้งอุปกรณ์ เช่น เครื่องคอมพิวเตอร์แม่ข่ายสำหรับงานพิสูจน์ตัวจริง เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบเก็บบันทึกข้อมูลจราจร

- พื้นที่สำหรับเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดที่อยู่ภายในระบบซึ่งสามารถให้บริการบุคคลภายนอกสำนักงานเข้ามาใช้บริการได้ (DMZ Zone) ติดตั้งอุปกรณ์ คือ เครื่องคอมพิวเตอร์แม่ข่ายศูนย์ข้อมูลกลางกระทรวงมหาดไทยและจังหวัด

- พื้นที่ใช้สำหรับในการเชื่อมต่อเครือข่ายภายนอกสำนักงาน (WAN Zone) เพื่อออกอินเทอร์เน็ต ติดตั้งอุปกรณ์ คือ IPS Untrust Sensor

### *4.1.2 กำหนดช่องทางการเชื่อมต่อ (Port Networking)*

กำหนดช่องทางการเชื่อมต่อเพื่อควบคุมการเข้าถึงการใช้งานระบบ โดยการกำหนดช่องทางการเชื่อมต่อ ให้ผู้ใช้บริการเข้าถึงพื้นที่และอุปกรณ์บนระบบเครือข่ายได้ตามที่อนุญาตเท่านั้น

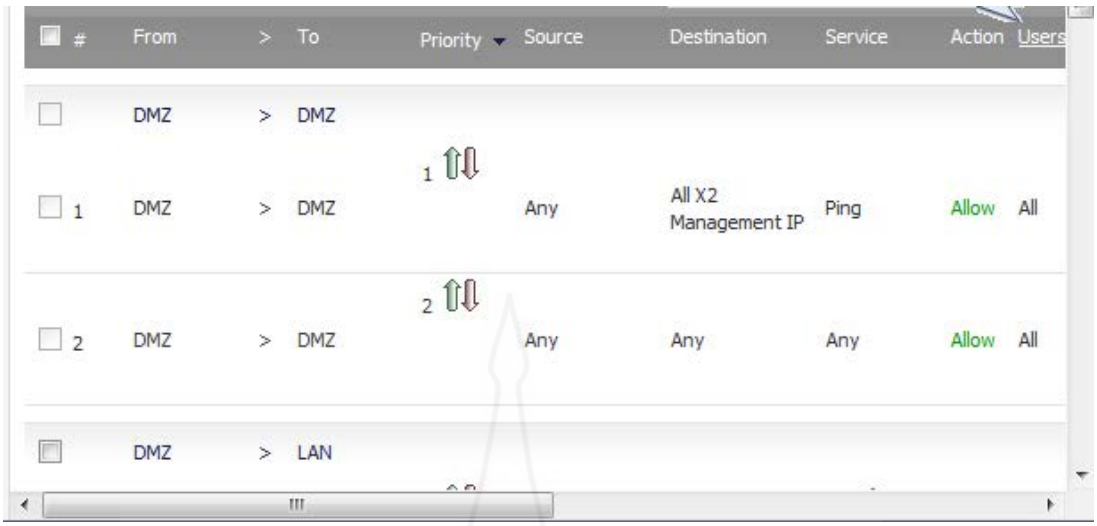



ภาพที่ 4.7 การกำหนดค่า Zone ต่าง ๆ

จากภาพที่ 4.7 แสดงให้เห็นการกำหนดช่องทางการเชื่อมต่อ โดยกำหนดให้พื้นที่ที่ติดตั้งอุปกรณ์แม่ข่ายที่มีความสำคัญสูง (Server Zone) สามารถเข้าถึงได้โดยช่องทาง ได้แก่ HTTPS ,Ping และ SSH เท่านั้น

### *4.1.3 กำหนดกฎการเข้าใช้งาน (Access Rule)*

เป็นการควบคุมการเข้าถึงระบบโดยการกำหนดให้อนุญาตเข้าใช้งานหรือไม่ให้เข้าใช้งาน พื้นที่ต่างๆ บนระบบเครือข่าย

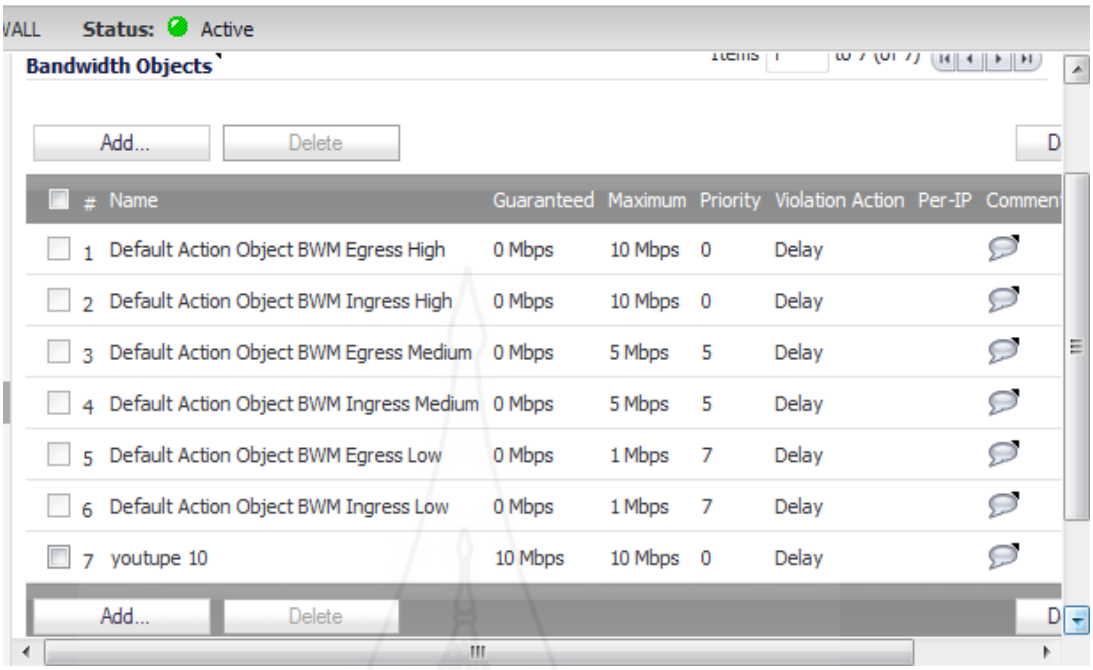



ภาพที่ 4.8 ตัวอย่างกฎการเข้าใช้งานระบบเครือข่าย

จากภาพที่ 4.8 อธิบายได้ว่ามีการกำหนดให้พื้นที่สำหรับใช้งานบริการเครื่องแม่ข่าย (DMZ Zone) สามารถถูกเข้าถึงได้จากทุกๆ พื้นที่หรือจากระบบเครือข่ายใดๆ ตามที่ร้องขอ และอนุญาตให้สามารถเชื่อมต่อได้โดยการปิง (ping) ในวงแลน (LAN) เดียวกัน

### *4.1.4 บริหารจัดการแบนด์วิดท์*

ควบคุมการใช้งานโดยการจำกัดแบนด์วิดท์ในการเชื่อมต่อระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายให้มีสัญญาณเพียงพอสำหรับการให้บริการงานประชุมทางไกล หรืองานบริการสารสนเทศด้านอื่นๆ

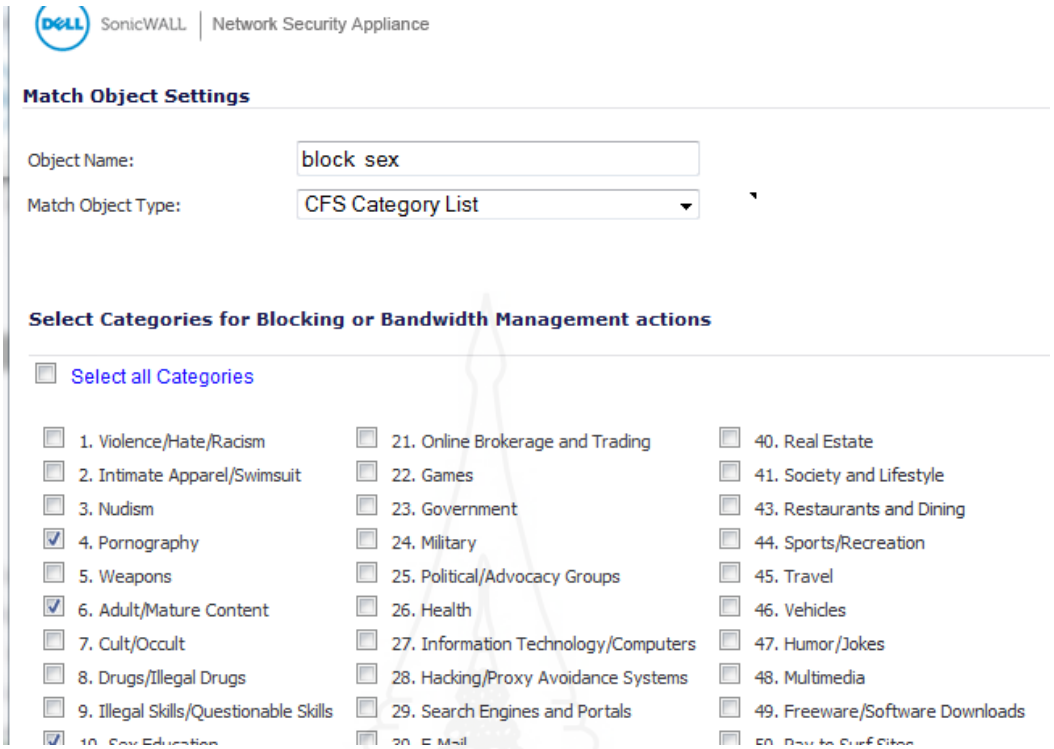



ภาพที่ 4.9 การกำหนดแบนด์วิดท์ให้กับการใช้งาน youtube

จากภาพที่ 4.9 จะเห็นได้ว่า มีการจำกัดการใช้งานเว็บยูทูป (Youtube) ให้จำกัดความเร็วการใช้งานอยู่ที่ 10 Mbps เพื่อให้การบริหารจัดการสัญญาณระบบเครือข่ายสามารถรองรับงานบริการสารสนเทศอื่นๆ ที่มีความจำเป็นต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ

### *4.1.5 กำหนดกฎการใช้แอพพลิเคชันต่างๆ (App Rule)*

กำหนดกฎการใช้แอพพลิเคชันต่างๆ (App Rule) เพื่อจำกัดหรือควบคุมการใช้งานแอพพลิเคชันหรือเว็บไซต์ให้เป็นไปตามกรอบนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุงที่ได้จัดทำขึ้น ตัวอย่างเช่น ควบคุมการใช้งานแอพพลิเคชัน ประเภทเครือข่ายสังคมออนไลน์ (SOCIAL-NETWORKING) เช่น facebook ,Hi5 ,Twitter, MySpace และควบคุมการเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม

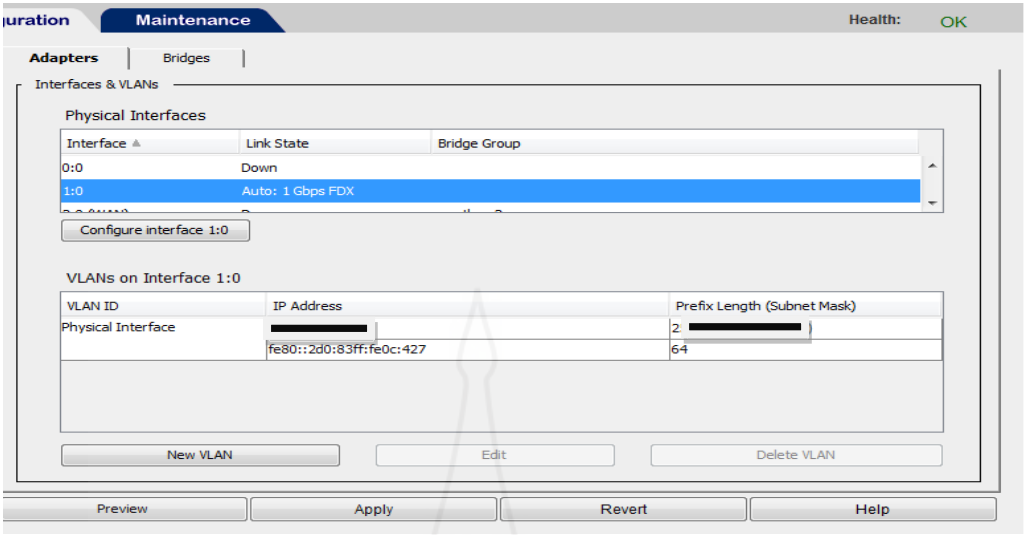



ภาพที่ 4.10 การจำกัดการเข้าใช้งานเว็บประเภทล่อแหลม

จากภาพที่ 4.10 แสดงการจำกัดการใช้งานระบบเครือข่าย โดยจำกัดไม่ให้ผู้ใช้งานระบบเครือข่ายสามารถเข้าเว็บที่ล่อแหลมได้

### *4.1.6 ควบคุมการใช้งานระบบอินเทอร์เน็ต*

จัดทำระบบพิสูจน์สิทธิ์ เพื่อควบคุมการใช้งานระบบอินเทอร์เน็ตให้มีความมั่นคงปลอดภัยสอดคล้องตามกรอบนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์



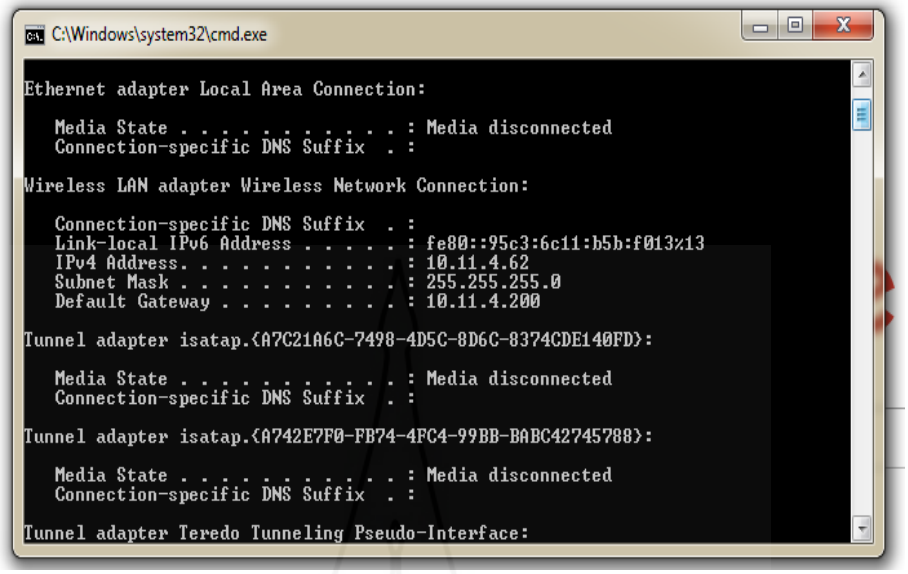

ภาพที่ 4.11 การกำหนดในการจำกัดสิทธิการใช้งานระบบเครือข่าย

จากภาพที่ 4.11 แสดงการกำหนดค่าการให้กับอุปกรณ์รักษาความปลอดภัย โดยได้กำหนดหมายเลขไอพี 10.11.xxx.xxx เพื่อให้อุปกรณ์รักษาความปลอดภัยข้างต้นสามารถเชื่อมต่อเข้ากับระบบพิสูจน์สิทธิ (Authentication) ในการเข้าใช้งานระบบอินเทอร์เน็ตและตรวจสอบรายชื่อผู้มีสิทธิเข้าใช้งานระบบอินเทอร์เน็ตกับฐานข้อมูลระบบพิสูจน์สิทธิ ได้

**4.2 ทดสอบการดำเนินงาน**

เป็นการทดสอบผลการกำหนดค่าการทำงานให้กับอุปกรณ์รักษาความปลอดภัยต่างๆ ข้างต้นเพื่อให้มั่นใจว่าการติดตั้งระบบรักษาปลอดภัยเป็นไปตามที่กำหนดไว้ โดยดำเนินการทดสอบตามรายการดังนี้

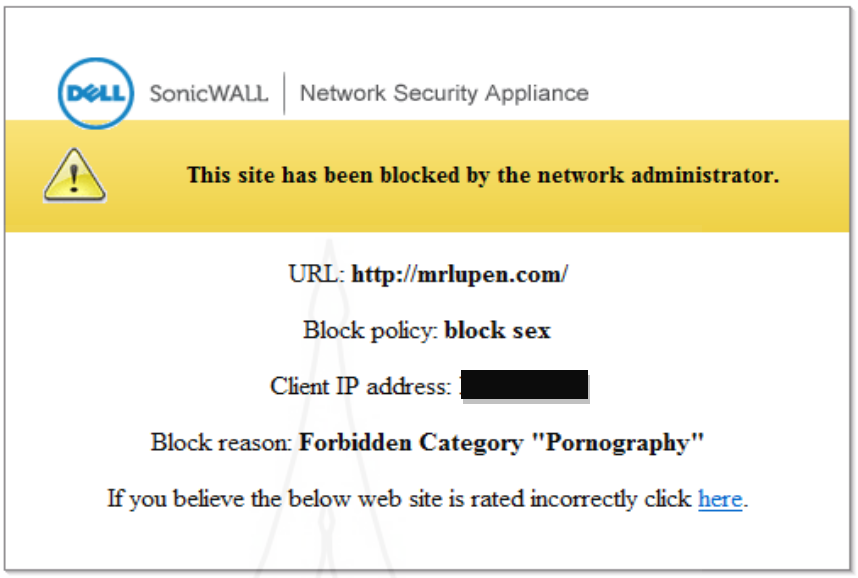
***4.2.1 ทดสอบการทำงานอุปกรณ์ไฟล์วอล์*** ซึ่งหากอุปกรณ์ไฟล์วอล์ทำงานปกติเป็นไปตามที่ได้กำหนดหรือออกแบบการทำงานระบบเครือข่ายไว้ อุปกรณ์จะสามารถแจกหมายเลขไอพีให้กับคอมพิวเตอร์ลูกข่ายในสำนักงานให้สามารถใช้งานระบบอินเทอร์เน็ตได้




ภาพที่ 4.12 แสดงการจ่ายไอพี

ภาพที่ 4.12 แสดงผลการทำงานของอุปกรณ์ไฟร์วอลล์ โดยเครื่องคอมพิวเตอร์ลูกข่ายจะได้รับหมายเลขไอพีสำหรับการเข้าใช้งานระบบอินเทอร์เน็ต กรณีที่อุปกรณ์ทำงานได้ปกติและสมบูรณ์

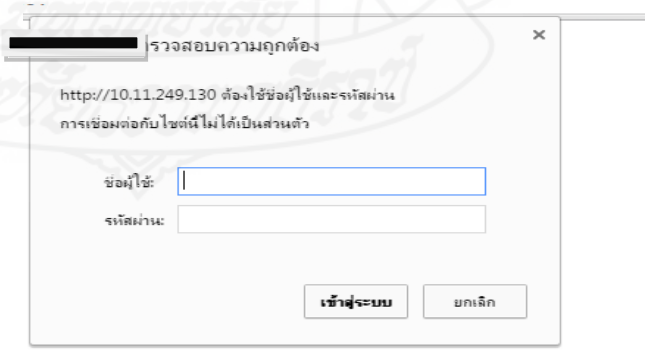
***4.2.2 ทดสอบการทำงานอุปกรณ์ไฟร์วอลล์*** ซึ่งหากไฟร์วอลล์ทำงานตามกฎ (App Rule) ที่กำหนดไว้ ตัวอย่าง กรณีมีผู้เข้าใช้งานเว็บไซต์ไม่เหมาะสมหรือล่อแหลมจะอุปกรณ์ไฟร์วอลล์จะทำงานโดยกำจัดสิทธิ์การใช้งาน




ภาพที่ 4.13 การควบคุมจำกัดการใช้งานเว็บไซต์ที่ไม่เหมาะสม

ภาพที่ 4.13 แสดงการทำงานของอุปกรณ์การรักษาความปลอดภัย โดยแสดงการแจ้งเตือนและไม่ให้เข้าใช้งานเว็บไซต์เมื่อมีผู้เรียกใช้งานเว็บไซต์ที่ไม่เหมาะสมหรือล่อแหลม เนื่องจากได้กำหนดให้อุปกรณ์ตรวจสอบและห้ามไม่ให้มีการเรียกใช้งานเว็บไซต์ดังกล่าว

***4.2.3 ทดสอบการทำงานระบบพิสูจน์ตัวจริง (Authentication)*** ซึ่งหากอุปกรณ์รักษาความปลอดภัยทำงานปกติ เมื่อมีผู้ใช้งานพิมพ์ชื่อเว็บไซต์เพื่อเข้าใช้งานเว็บไซต์ใดๆ ระบบพิสูจน์ตัวจริงจะถูกเรียกขึ้นมาทำงานตามที่ได้ตั้งค่าการทำงานไว้ ดังภาพที่ 4.18




ภาพที่ 4.14 ผลการทำงานระบบพิสูจน์ตัวจริง (Authentication)

ภาพ 4.14 แสดงผลการทำงานระบบพิสูจน์ตัวจริง (Authentication) ที่ได้ทำการเชื่อมโยงไว้กับอุปกรณ์รักษาความมั่นคงปลอดภัย โดยเมื่อผู้ใช้งานต้องการเข้าใช้งานเว็บไซต์ใดๆ ผู้ใช้งานจะต้องระบุชื่อผู้ใช้งานพร้อมกับรหัสผ่านตามที่ได้รับสิทธิไว้ เพื่อแสดงตัวตนเข้าใช้งานระบบเครือข่ายสำนักงานจังหวัดพัทลุง

## 5. ดำเนินการตรวจสอบและประเมินผล

จากการพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง และบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดให้เป็นไปตามมาตรฐาน ISO/IEC 27001:2013 โดยการติดตั้งอุปกรณ์และระบบรักษาความมั่นคงปลอดภัย แล้วนั้น ผู้วิจัยได้ประเมินและตรวจสอบผลการดำเนินงาน ดังนี้

5.1 วิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงหลังดำเนินการบริหารด้านความมั่นคงปลอดภัยภายใต้กรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง ดังตารางที่ 4.3 โดยผู้วิจัยได้แสดงรายการความเสี่ยงหลังการประเมินเฉพาะรายการความเสี่ยงที่มีระดับความเสี่ยงลดลงหลังจากดำเนินการตามโครงการแล้วเท่านั้น

5.1 ประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงหลังดำเนินการบริหารด้านความมั่นคงปลอดภัยภายใต้กรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัดพัทลุง

ตารางที่ 4.3 ประเมินความเสี่ยงหลังดำเนินการ

| A5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) | | | | | |
|---|---|---|---|---|---|
| A.5.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.5.1.1 | นโยบายสำหรับความมั่นคงปลอดภัย | มีการพัฒนากรอบนโยบายความปลอดภัยสารสนเทศของสำนักงานอย่างเป็นลายลักษณ์อักษร | 4 | 3 | 15 |
| A.5.1.2 | การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | มีการตระหนักถึงการทบทวนนโยบายความมั่นคงปลอดภัย | 4 | 3 | 12 |

ตารางที่ 4.3 (ต่อ)

| A.6 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security) | | | | | |
|---|---|---|---|---|---|
| A.6.1 โครงสร้างภายในองค์กร | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.6.1.1 | มีการบทบาทและหน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัย | มีการกำหนดความรับผิดชอบชัดเจนมากขึ้น | 4 | 3 | 12 |
| A.6.1.2 | มีการแบ่งหน้าที่และส่วนงานที่รับผิดชอบกับงาน | ขาดการแบ่งแยกหน้าที่และความรับผิดชอบ | 3 | 2 | 6 |
| A.6.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล | | | | | |
| A.6.2.1 | การกำหนดนโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา | ต้องได้รับสิทธิในการเชื่อมต่อเข้าใช้งานในระบบเครือข่ายถึงจะใช้งานได้ | 2 | 4 | 8 |
| A.6.2.2 | การกำหนดนโยบายการปฏิบัติงานระยะไกล | สำนักงานจังหวัดพัทลุงไม่ได้กำหนดการเชื่อมต่อและควบคุมการใช้งานระบบเครือข่ายระยะไกล | 2 | 2 | 4 |

ตารางที่ 4.3 (ต่อ)

| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | | | | | |
|---|---|---|---|---|---|---|
| A.7.1 ก่อนการจ้างงาน | | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง | ข้อเสนอแนะ |
| A.7.1.1 | การคัดเลือก | คำนึงถึงการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียดมากขึ้น | 3 | 3 | 9 | เริ่มมีการตระหนักถึงการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียด แต่ไม่คำนึงถึงชั้นความลับของทรัพย์สินสารสนเทศ |
| A.7.1.2 | ข้อตกลงและเงื่อนไขการจ้างงาน | มีการแจ้งให้เจ้าหนาที่คำนึงถึงการกำหนดข้อตกลงในการดูแลรักษาความมั่นคงปลอดภัย สารสนเทศในสัญญาจ้าง | 3 | 2 | 6 | ควรระบุข้อตกลงในการเข้าใช้งานสารสนเทศในสัญญาจ้างของสำนักงานจังหวัดพัทลุง |

ตารางที่ 4.3 (ต่อ)

| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | | | | | |
|---|---|---|---|---|---|
| A.8.2 การจัดชั้นความลับของสารสนเทศ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.8.2 .1 | ชั้นความลับของสารสนเทศ | มีการควบคุมการเข้าข้อมูลมากขึ้น | 3 | 3 | 9 |

ตารางที่ 4.3 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | |
|---|---|---|---|---|---|
| A.9.1 ความต้องการทางธุรกิจสำหรับควบคุมการเข้าถึง | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.9.1.1 | นโยบายควบคุมการเข้าถึง | มีนโยบายควบคุมชัดเจน โดยการกำหนดค่าการเข้าถึงระบบเครือข่ายบนอุปกรณ์ไฟร์วอลล์ | 3 | 2 | 6 |
| A.9.1.2 | การเข้าถึงเครือข่ายและบริการเครือข่าย | มีการควบคุมการเข้าถึงอุปกรณ์โดยทำระบบพิสูจน์ตัวจริงใช้กับทุกอุปกรณ์ | 3 | 3 | 9 |

ตารางที่ 4.3 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | |
|---|---|---|---|---|---|
| A.9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.9.2.1 | การลงทะเบียนและการถอนสิทธิผู้ใช้งาน | มีการลงทะเบียนร้องขอการเข้าใช้งานตามแบบฟอร์มที่กำหนด | 3 | 2 | 6 |
| A.9.2.2 | การจัดการสิทธิการเข้าถึงของผู้ใช้งาน | ผู้ดูแลระบบมีการบริหารจัดการสิทธิผู้ใช้งานมากขึ้น | 3 | 2 | 6 |
| A.9.2.3 | การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ | มีการขั้นตอนการบริหารจัดการสิทธิชัดเจน ต้องยื่นคำร้องขอลงทะเบียน มีการทบทวนสิทธิ การใช้งาน และยกเลิกสิทธิเมื่อผู้ใช้งานลาออกหรือย้าย | 2 | 3 | 6 |
| A.9.2.4 | การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวจริงของผู้ใช้งาน | มีกระบวนการการควบคุม การส่งมอบรหัสผ่านโดยให้ผู้ใช้งานมารับด้วยตนเองหรือแจ้งผ่านอีเมล์เท่านั้น | 4 | 2 | 8 |

ตารางที่ 4.3 (ต่อ)

| A.9 การควบคุมการเข้าถึง (Access Control) | | | | | |
|---|---|---|---|---|---|
| A.9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.9.3.1 | การใช้ข้อมูลการพิสูจน์ตัวจริงซึ่งเป็นความลับ | มีระบบพิสูจน์ตัวจริงที่น่าเชื่อถือ | 4 | 3 | 12 |

ตารางที่ 4.3 (ต่อ)

| | | | | | |
|---|---|---|---|---|---|
| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | |
| A.12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.12.1.3 | การบริหารขีดความสามารถของระบบ | ติดตั้งอุปกรณ์รักษาความปลอดภัยและมีระบบรายงานแจ้งสถานระบบ | 5 | 3 | 15 |
| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | |
| A.12.2 การป้องกันโปรแกรมไม่ประสงค์ดี | | | | | |
| A.12.2.1 | การป้องกันโปรแกรมที่ไม่ประสงค์ดี | ใช้อุปกรณ์ไฟล์วอล์และอุปกรณ์ป้องกันการตรวจจับการบุกรุกช่วยในการจำกัดและป้องกันโปรแกรมไม่ประสงค์ดี | 4 | 2 | 8 |

ตารางที่ 4.3 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | |
|---|---|---|---|---|---|
| A.12.4 การบันทึกข้อมูลล็อคและการเฝ้าระวัง | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.12.4.1 | การบันทึกข้อมูลล็อคแสดงเหตุการณ์ | ติดตั้งระบบพิสูจน์ตัวจริงและมีฐานข้อมูลในการเก็บข้อมูลการจราจรต่างๆ | 3 | 2 | 6 |
| A.12.4.2 | การป้องกันข้อมูลล็อค | มีการกำหนดให้สามารถเข้าถึงฐานข้อมูลเก็บล็อคได้เฉพาะเจ้าหน้าที่ดูแลระบบเท่านั้น | 3 | 3 | 9 |
| A.12.4.3 | ข้อมูลล็อคกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ | มีการกำหนดให้มีการบันทึกข้อมูลการดำเนินงานของเจ้าที่ผู้ดูแลระบบ | 3 | 3 | 9 |
| A.12.4.4 | การตั้งนาฬิกาให้ถูกต้อง | มีการกำหนดเวลาของเครื่องคอมพิวเตอร์เก็บล็อคตามการอ้างอิงเวลาทั่วโลกตามมาตรฐานสากล | 2 | 3 | 6 |

ตารางที่ 4.3 (ต่อ)

| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | | | | |
|---|---|---|---|---|---|
| A.12.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.12.5.1 | การติดตั้งซอฟต์แวร์บนระบบให้บริการ | มีแนวทางการปฏิบัติในการติดตั้งซอฟต์แวร์สำหรับผู้ดูแลระบบชัดเจนขึ้น | 3 | 2 | 6 |

ตารางที่ 4.3 (ต่อ)

| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | | | | | |
|---|---|---|---|---|---|
| A.13.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.13.1.1 | มาตรการเครือข่าย | กำหนดมาตรการอย่างเป็นลายลักษณ์อักษรและปฏิบัติตามโดยการติดตั้งอุปกรณ์ควบคุมและรักษาความปลอดภัย | 5 | 2 | 10 |
| A.13.1.3 | การแบ่งแยกเครือข่าย | กำหนดพื้นที่ระบบเครือข่ายออกเป็นโซนต่างๆ เพื่อรักษาระดับความปลอดภัยของระบบเครือข่าย | 3 | 2 | 6 |

ตารางที่ 4.3 (ต่อ)

| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | | | | | |
|---|---|---|---|---|---|
| A.13.2 การถ่ายโอนสารสนเทศ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.13.2.3 | การส่งข้อความอิเล็กทรอนิกส์ | มีการกำหนดมาตรการในการส่งข้อมูลผ่านทางอีเมล์ | 3 | 2 | 6 |
| A.13.2.4 | ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ | มีการกำหนดนโยบายการรักษาความลับของข้อมูลสำคัญของสำนักงานจังหวัดพัทลุง | 4 | 3 | 12 |

ตารางที่ 4.3 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | |
|---|---|---|---|---|---|
| A.14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.14.1.1 | การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ | สำนักงานจังหวัดพัทลุงเริ่มมีการเข้าใจถึงภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศของสำนักงานเพิ่มขึ้น | 4 | 3 | 12 |
| A.14.2 ความความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน | | | | | |
| A.14.2.1 | นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย | ผู้พัฒนาระบบของสำนักงานจังหวัดพัทลุงมีการตระหนักถึงการพัฒนาระบบให้มีความมั่นคงปลอดภัย มากขึ้น | 4 | 3 | 12 |
| A.14.2.3 | การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ | ผู้ดูแลระบบของสำนักงานจังหวัดพัทลุงให้ความสำคัญกับการทบทวนการออกแบบระบบเครือข่ายมากขึ้น | 5 | 1 | 5 |

ตารางที่ 4.3 (ต่อ)

| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | | | | |
|---|---|---|---|---|---|
| A.14.2 ความความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.14.2.4 | การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป | ผู้พัฒนาระบบของสำนักงานจังหวัดพัทลุงมีการตระหนักการกำหนดให้ซอฟต์แวร์ไม่ให้มีการเปลี่ยนแปลงใดๆยกเว้นกรณีจำเป็น | 5 | 2 | 10 |
| A.14.2.6 | สภาพแวดล้อมการพัฒนาระบบที่มีความมั่นคงปลอดภัย | ผู้ดูแลระบบของสำนักงานมีการคำนึงถึงขั้นตอนการพัฒนาระบบและสภาพแวดล้อมต่างๆ ที่เกี่ยวข้องเพื่อให้ระบบมีความปลอดภัยยิ่งขึ้น | 3 | 2 | 6 |
| A.14.2.8 | การทดสอบด้านความมั่นคงปลอดภัยของระบบ | มีการดำเนินการบ้างแต่ไม่ต่อเนื่องและไม่สามารถทำได้ครอบคลุม | 5 | 3 | 15 |

ตารางที่ 4.3 (ต่อ)

| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | | | | | |
|---|---|---|---|---|---|
| A.16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.16.1.5 | การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | เริ่มมีแนวคิดในการจัดทำขั้นตอนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | 5 | 3 | 15 |
| A.16.1.6 | การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | ผู้ดูแลระบบของสำนักงานจังหวัดให้ความสำคัญกับการจดบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและมีระบบรักษาความปลอดภัยที่ได้ติดตั้งคอยรายงานผลสนับสนุนการปฏิบัติงานเพิ่มขึ้น | 5 | 2 | 10 |

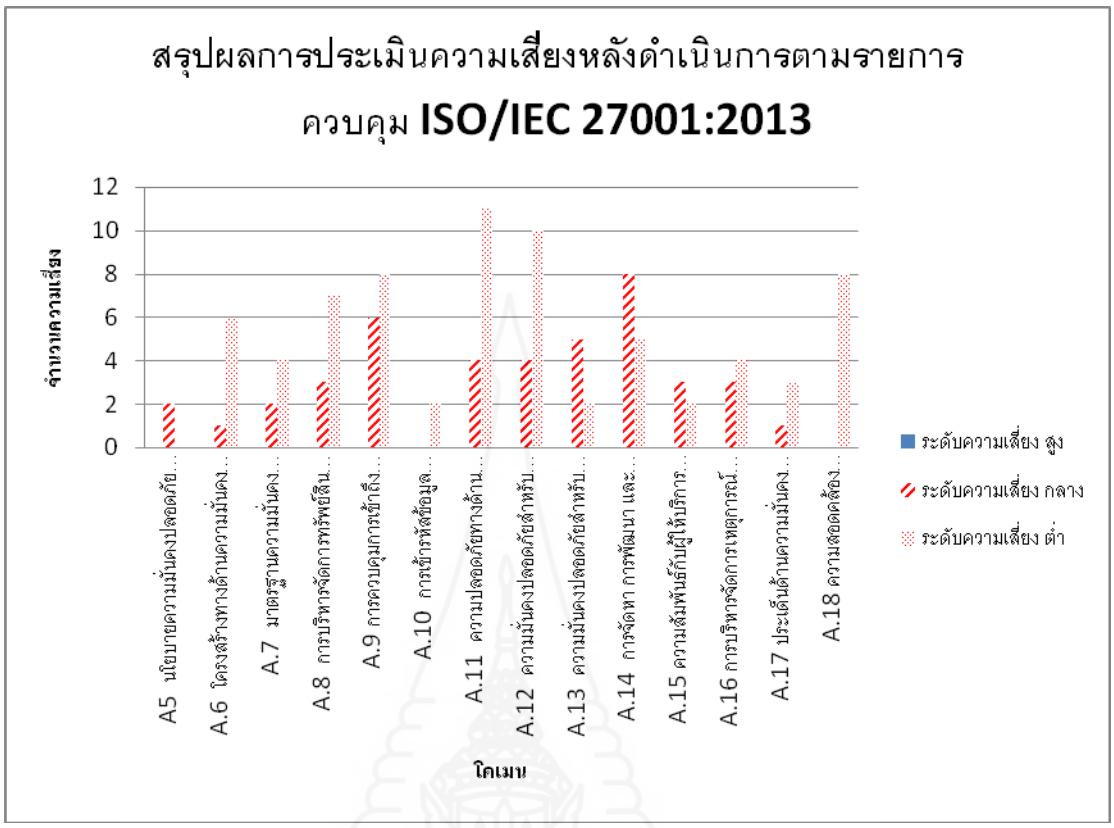
ตารางที่ 4.3 (ต่อ)

| A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) | | | | | |
|---|---|---|---|---|---|
| A.17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | | | | | |
| ข้อ | มาตรการจัดการความปลอดภัยระบบสารสนเทศที่ควรมีตามมาตรฐาน ISO/IEC 27001:2013 | สถานะปัจจุบัน | ผลกระทบ | โอกาส | ระดับความเสี่ยง |
| A.17.1.2 | การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | เจ้าหน้าที่มีการเตรียมการกำหนดขั้นตอนปฏิบัติ เพื่อความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | 4 | 3 | 12 |
| A.17.1.3 | การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ | ผู้ดูแลระบบของสำนักงานจังหวัดมีเครื่องมือในการช่วยตรวจสอบการทำงานของระบบเพื่อสร้างความต่อเนื่องให้กับการใช้งานระบบ | 2 | 2 | 4 |

หลังดำเนินการโครงการ และแก้ไขประเด็นความเสี่ยงที่ตรวจพบแล้วนั้น ผู้จัดทำได้ประเมินความเสี่ยงหลังการดำเนินโครงการพบระดับความเสี่ยงตามรายการควบคุม ตามมาตรฐาน ISO/IEC 27001:2013 ตามรายการควบคุม 14 โดเมน 114 ของสำนักงานจังหวัดพัทลุง ตามตารางที่ 4.4

ตารางที่ 4.4 สรุประดับความเสี่ยงของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001 :2013 หลังดำเนินการ

| ISO/IEC27001 | ระดับความเสี่ยง | | |
|---|---|---|---|
| 14 Domian | สูง | กลาง | ต่ำ |
| A5 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) | | 2 | |
| A.6 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) | | 1 | 6 |
| A.7 มาตรฐานความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resources Security) | | 2 | 4 |
| A.8 การบริหารจัดการทรัพย์สิน (Asset Management) | | 3 | 7 |
| A.9 การควบคุมการเข้าถึง (Access Control) | | 6 | 8 |
| A.10 การเข้ารหัสข้อมูล (Cryptography) | | | 2 |
| A.11 ความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and environmental Security) | | 4 | 11 |
| A.12 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security) | | 4 | 10 |
| A.13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security) | | 5 | 2 |
| A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance) | | 8 | 5 |
| A.15 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) | | 3 | 2 |
| A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) | | 3 | 4 |
| A.17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) | | 1 | 3 |
| A.18 ความสอดคล้อง (Compliance) | | | 8 |
| รวม | | 42 | 72 |




ภาพที่ 4.15 ระดับความเสี่ยงหลังการดำเนินการ

จากภาพที่ 4.15 แสดงกราฟสรุประดับความเสี่ยงแต่ละรายการควบคุมตามมาตรฐาน ISO/IEC 27001:2013 จะเห็นได้ว่า หลังจากดำเนินการตามกรอบนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และติดตั้งอุปกรณ์ระบบรักษาความปลอดภัยแล้ว ไม่พบรายการความเสี่ยงระดับสูง ยังคงเหลือเพียงความเสี่ยงระดับกลางและระดับต่ำเท่านั้น

5.2 ประเมินการใช้งานระบบเครือข่ายและการรับรู้นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง

ผู้วิจัยได้ออกแบบสอบถามความพึงพอใจการใช้งานระบบเครือข่ายและการรับรู้ของบุคลากรภายในสำนักงานจังหวัดพัทลุงด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง เพื่อนำผลการประเมินที่ได้มาวางแผนและหาแนวทางปรับปรุงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ในลำดับต่อไป

โดยแบ่งคำถามของแบบสอบถามออกเป็น 4 ส่วน ได้แก่ ข้อมูลทั่วไป ความพึงพอใจด้านการให้บริการเครือข่าย การรับรู้ของบุคลากร และข้อเสนอแนะ

กำหนดเกณฑ์การประเมินดังนี้

4.51-5.00 มากที่สุด

3.51-4.50 มาก

2.51-3.50 ปานกลาง

1.51-2.50 น้อย

1.00-1.50 น้อยที่สุด

โดยได้สอบถามผู้บริหารสำนักงานจังหวัดพัทลุง (หัวหน้าสำนักงานจังหวัด, ผู้อำนวยการกลุ่มงาน) ผู้ดูแลระบบ บุคลากรของสำนักงานจังหวัดพัทลุง ซึ่งเป็นผู้ใช้งานระบบเครือข่ายของสำนักงานจังหวัดพัทลุง และสอบถามจากเจ้าหน้าที่จากส่วนราชการอื่นๆ ภายในจังหวัดพัทลุงที่ขอใช้บริการระบบเครือข่ายอินเทอร์เน็ตของสำนักงานจังหวัดพัทลุง จำนวน 53 ราย ผลการประเมินความพึงพอใจมีรายละเอียดดังต่อไปนี้

### *6.2.1 ข้อมูลทั่วไปผู้ประเมิน*

ตารางที่ 4.5 ข้อมูลทั่วไปของผู้ใช้งานระบบเครือข่าย

| รายการ | รายละเอียด |
|---|---|
| 1. เพศ | ชาย จำนวน 13 คน หญิง จำนวน 40 คน |
| 2. อายุ | 21-30 ปี จำนวน 17 คน<br>31-40 ปี จำนวน 11 คน<br>41-50 ปี จำนวน 16 คน<br>51-60 ปี จำนวน 9 คน |
| 3. ระดับการศึกษา | ต่ำกว่าปริญญาตรี จำนวน 5 คน, ปริญญาตรี จำนวน 37 คน<br>ปริญญาโท จำนวน 11 คน , ปริญญาเอก จำนวน – คน |
| 4. อาชีพ | ลูกจ้างชั่วคราว จำนวน 20 คน<br>ลูกจ้างประจำ จำนวน 7 คน<br>พนักงานราชการ จำนวน 4 คน<br>ข้าราชการ จำนวน 22 คน |
| 5. ประเภทผู้ใช้งาน | ผู้บริหาร จำนวน 5 คน<br>ผู้ดูแลระบบ จำนวน 3 คน<br>ผู้ใช้งานทั่วไป จำนวน 45 คน |
| 6. ความถี่ในการใช้งานระบบเครือข่าย | น้อยกว่า 1 ชม./วัน จำนวน 3 คน<br>1-3 ชม./วัน จำนวน 10 คน<br>3-6 ชม./วัน จำนวน 22 คน<br>6-9 ชม./วัน จำนวน 18 คน |
| 7. ช่วงเวลาที่ใช้บริการ | ก่อน 8.00 น. จำนวน 5 คน<br>8.00 -12.00 น. จำนวน 28 คน<br>12.00-13.00 น. จำนวน 20 คน<br>13.00-16.00 น. จำนวน 19 คน<br>หลังจาก 16.00 น. จำนวน 3 คน |
| 8. ภาพแบบการเชื่อมต่อสัญญาณเพื่อเข้าใช้ระบบเครือข่าย | แบบมีสาย (LAN) จำนวน 53 คน<br>แบบไร้สาย (wireless) จำนวน 42 คน |

### *6.2.2 สรุปผลความพึงพอใจด้านการให้บริการเครือข่าย*

ตารางที่ 4.6 แสดงความพึงพอใจด้านการให้บริการเครือข่าย

| รายการ | $\bar{X}$ | S.D. | ระดับความพึงพอใจ |
|---|---|---|---|
| 1. ความเร็วในการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของสำนักงาน | 3.74 | 0.59 | มาก |
| 2. ความสะดวกในการเข้าถึงเครือข่ายของสำนักงาน | 4.70 | 0.57 | มากที่สุด |
| 3. ความมีเสถียรภาพของระบบเครือข่าย | 3.83 | 0.91 | มาก |
| 4.ระบบเครือข่ายให้บริการได้ครอบคลุมและทั่วถึง | 3.65 | 0.691 | มาก |
| 5. ระบบเครือข่ายมีความปลอดภัยในการใช้งาน | 3.28 | 0.81 | ปานกลาง |
| 6. การกำหนดสิทธิในการเข้าใช้งานมีความปลอดภัย | 3.89 | 0.32 | มาก |
| 7. ความปลอดภัยของเครื่องคอมพิวเตอร์ที่ท่านใช้งาน | 3.12 | 0.65 | ปานกลาง |
| 8. ความพึงพอใจภาพรวมต่อการใช้งาน | 3.98 | 0.31 | มาก |
| รวม | 3.77 | 0.78 | มาก |

จากตารางที่ 4.6 สามารถอธิบายได้ว่าความพึงใจด้านการให้บริการเครือข่ายของผู้ใช้งานโดยรวมมีค่าเฉลี่ยอยู่ที่ 3.77 ค่าเบี่ยงเบนมาตรฐานอยู่ที่ 0.78 เมื่อเทียบกับเกณฑ์ความพึงพอใจจะอยู่ในระดับมาก อย่างไรก็ตาม เมื่อดูในรายละเอียดแต่ละรายการพบว่า ระดับความพึงพอใจด้านความปลอดภัยในการใช้งานระบบเครือข่าย และความปลอดภัยของเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ในระดับปานกลาง ทำให้มีนัยสำคัญว่า ถึงแม้จะมีการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแล้วก็ตาม แต่บุคลากรยังรู้สึกได้ว่ายังมีความปลอดภัยในการใช้งานเพียงระดับปานกลางเท่านั้น ซึ่งสำนักงานจังหวัดพัทลุงต้องนำข้อมูลที่ได้จากแบบสำรวจเหล่านี้ไปปรับปรุงพัฒนาระบบเครือข่ายให้มีความมั่นคงปลอดภัยต่อไป เนื่องจากงานบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานต้องดำเนินการอย่างต่อเนื่องตามหลักการของกระบวนการบริหารด้านความมั่นคงปลอดภัยนั่นเอง

### *6.2.3 สรุปการรับรู้ของบุคลากรในหน่วยงาน*

ตารางที่ 4.7 การรับรู้ของบุคลากร

| รายการ | $\overline{X}$ | S.D. | ระดับความพึงพอใจ |
|---|---|---|---|
| 1. มีการเผยแพร่นโยบายความมั่นคงปลอดภัยขององค์กร | 2.45 | 0.90 | น้อย |
| 2. มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย | 2.50 | 0.92 | น้อย |
| 3. การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน | 2.10 | 0.66 | น้อย |
| 4.มีการจัดทำบัญชีทรัพย์สิน | 2.810 | 0.97 | ปานกลาง |
| 5. มีการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย | 4.13 | 0.48 | มาก |
| 6. มีนโยบายการใช้มาตรการเข้ารหัสข้อมูล | 1.74 | 0.89 | น้อย |
| 7. มีการควบคุมการเข้าออกห้องสารสนเทศและระบบเครือข่าย | 3.94 | 0.23 | มาก |
| 8. มีขั้นตอนบริหารจัดการการเปลี่ยนแปลง | 2.70 | 0.90 | ปานกลาง |
| 9.มีขั้นตอนการปฏิบัติในการเข้าถึงสารสนเทศของหน่วยงาน | 3.50 | 0.90 | ปานกลาง |
| 10. มีการกำหนดแนวทางการจัดหา การพัฒนาและการบำรุงรักษาระบบ | 2.62 | 0.68 | ปานกลาง |
| 11.มีการกำหนดแนวทางความสัมพันธ์กับผู้ให้บริการภายนอก | 2.11 | 0.42 | น้อย |
| 12. มีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | 2.96 | 0.75 | ปานกลาง |
| 13. มีการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ | 3.11 | 0.94 | มาก |
| 14. มีการทบทวนความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงาน | 2.04 | 0.61 | น้อย |
| รวม | 2.76 | 1.03 | ปานกลาง |

จากตารางที่ 4.7 แสดงให้เห็นระดับการรับรู้ของผู้ใช้งานถึงนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัด โดยรวมมีค่าเฉลี่ยอยู่ที่ 2.76 ค่าเบี่ยงเบนมาตรฐานอยู่ที่ 1.03 เมื่อเทียบกับเกณฑ์ความพึงพอใจจะอยู่ในระดับปานกลาง เมื่อพิจารณาในรายละเอียดจะพบว่า ยังมีการเผยแพร่ การสร้างความตระหนักรู้และการทบทวนนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ในระดับน้อย ซึ่งมีนัยสำคัญที่สำนักงานจังหวัดพัทลุงต้องดำเนินการเร่งด่วน สำหรับประเด็นที่มีการรับรู้ระดับน้อย แต่มีความเสี่ยงระดับต่ำ อภิปรายได้ดังนี้

- ประเด็นนโยบายการเข้ารหัสข้อมูลมีการรับรู้ระดับน้อย เนื่องจากสำนักงานจังหวัดยังไม่มีงานบริการที่ต้องเข้าและถอดรหัสกุญแจเพื่อให้บริการรักษาความปลอดภัย เช่น ไม่มีการติดตั้ง Public Cert (SSL) เพื่อเข้ารหัสการส่งข้อมูลผ่านเว็บ มีเพียงการเข้ารหัส (encode) สำหรับรหัสผ่านการเข้าใช้งานระบบฐานข้อมูล ซึ่งผู้ใช้งานไม่ทราบในส่วนนี้ และผู้ใช้งานยังขาดความรู้ความเข้าใจถึงการใช้งานรหัสกุญแจทำให้การรับรู้นโยบายการเข้ารหัสข้อมูลอยู่ในระดับน้อย และผู้ใช้งานยังขาดความรู้ความเข้าใจถึงการใช้งานรหัสกุญแจ

- ประเด็นการกำหนดแนวทางความสัมพันธ์กับผู้ให้บริการมีการรับรู้ระดับน้อย เนื่องจากผู้ใช้งานทั่วไปไม่ได้มีหน้าที่ติดต่อกับหน่วยงานผู้ให้บริการเครือข่าย ผู้ดูแลระบบกับผู้บริหารเท่านั้นที่จะมีการติดต่อสัมพันธ์กับผู้ให้บริการดังกล่าว จึงทำให้ประเด็นดังกล่าวมีการรับรู้ในระดับน้อย จึงต้องมีการสื่อสารให้บุคลากรในสำนักงานทราบอย่างแพร่หลาย

- ประเด็นการทบทวนความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงานมีการรับรู้ระดับน้อย เนื่องจากการทบทวนความมั่นคงปลอดภัยสารสนเทศเป็นหน้าที่ของเจ้าหน้าที่ดูแลระบบและผู้บริหาร ผู้ใช้งานไม่ทราบถึงการดำเนินงานดังกล่าวทำให้ระดับการรับรู้ในประเด็นนี้น้อย จึงต้องมีการสื่อสารให้บุคลากรในสำนักงานทราบอย่างเป็นทางการ

### *6.2.4 สรุปการรับรู้ของผู้บริหารและผู้ดูแลระบบของหน่วยงาน*

ตารางที่ 4.8 การรับรู้ของผู้บริหารและผู้ดูแลระบบ

| รายการ | $\overline{X}$ | S.D. | ระดับความพึงพอใจ |
|---|---|---|---|
| 1. มีการเผยแพร่นโยบายความมั่นคงปลอดภัยขององค์กร | 3.14 | 0.83 | ปานกลาง |
| 2. มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย | 3.57 | 0.90 | มาก |
| 3. การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน | 2.71 | 0.45 | ปานกลาง |
| 4.มีการจัดทำรายการครุภัณฑ์และอุปกรณ์ระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร | 3.57 | 0.73 | มาก |
| 5. มีการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย | 4.57 | 0.49 | มากที่สุด |
| 6. มีนโยบายการเข้ารหัส (encode) รหัสผ่านระบบฐานข้อมูล หรือมีการกำหนดให้มีการใช้งานเว็บไซต์ที่ปลอดภัย (SSL) ทำธุรกรรมต่างๆ เพื่อเข้ารหัสการส่งข้อมูลผ่านเว็บ https หรือมีการเข้าและถอดรหัสกุญแจข้อมูล | 3.28 | 0.45 | ปานกลาง |
| 7. มีการควบคุมการเข้าออกห้องสารสนเทศ | 3.71 | 0.45 | มาก |
| 8. มีการกำหนดความมั่นคงปลอดภัยในการดำเนินงาน เช่น มีขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรเพื่อบริหารจัดการการเปลี่ยนแปลง | 3.57 | 0.90 | มาก |
| 9.มีการรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เช่นมีการกำหนดชั้นความลับ มีขั้นตอนการปฏิบัติในการเข้าถึงสารสนเทศของหน่วยงาน | 4.71 | 0.45 | มากที่สุด |
| 10. มีการกำหนดแนวทางการจัดหา การพัฒนาและการบำรุงรักษาระบบ | 3.71 | 0.45 | มาก |
| 11.มีการกำหนดและตกลงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ | 2.86 | 0.35 | ปานกลาง |

ตารางที่ 4.8 (ต่อ)

| รายการ | $\overline{X}$ | S.D. | ระดับความพึงพอใจ |
|---|---|---|---|
| 12. มีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | 4.00 | 0.53 | มาก |
| 13. มีการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ | 4.00 | 0.76 | มาก |
| 14. มีการทบทวนความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงาน | 3.43 | 0.73 | ปานกลาง |
| รวม | 3.63 | 0.84 | มาก |

จากตารางที่ 4.8 จะเห็นได้ว่าระดับการรับรู้ของผู้บริหารและผู้ดูแลระดับถึงนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสำนักงานจังหวัด โดยรวมมีค่าเฉลี่ยอยู่ที่ 3.63 ค่าเบี่ยงเบนมาตรฐานอยู่ที่ 0.84 เมื่อเทียบกับเกณฑ์ความพึงพอใจจะอยู่ในระดับมากแสดงถึงว่าการรับรู้ส่วนใหญ่จะอยู่ในระดับผู้บริหารและเจ้าหน้าที่ผู้ปฏิบัติงานด้านนี้โดยเฉพาะ

จากการประเมินจากแบบสอบถามดังกล่าว ทำให้ทราบว่าผู้ใช้งานยังขาดการรับรู้ถึงนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน ดังนั้น ผู้บริหารของสำนักงานจังหวัดพัทลุง (หัวหน้าสำนักงานจังหวัด) จึงควรสร้างการรับรู้ สร้างความตระหนักรู้ให้กับผู้ใช้งานเพิ่มขึ้น โดยให้การสนับสนุนให้มีการเผยแพร่และสร้างความตระหนักรู้นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงด้วย

# บทที่ 5
# สรุปการวิจัย อภิปรายผล และข้อเสนอแนะ

## 1. สรุปการวิจัย

การพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 มีวัตถุประสงค์เพื่อพัฒนากรอบนโยบายรักษาความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศให้กับหน่วยงานให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 รวมทั้งลดและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงาน ในการนี้ผู้วิจัยจึงขอสรุปผลการวิจัยเพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย ดังนี้

1.1 การพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013

จากการพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุงถือว่าเป็นจุดเริ่มต้นที่ดีในการบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงานทำให้ผู้ดูแลระบบสารสนเทศของสำนักงานจังหวัดพัทลุงมีแนวทางในการปฏิบัติงานเพิ่มมากขึ้น โดยการนำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานมาเป็นแนวทางในการกำหนดและควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน และทำให้เจ้าหน้าที่ของสำนักงานจังหวัดและผู้รับบริการจากส่วนราชการอื่นๆ มีแนวปฏิบัติในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

จากการประเมินแบบสอบถามความพึงพอใจด้านการใช้งานระบบเครือข่าย แม้ว่าผู้ใช้งานมีระดับความพึงพอใจด้านความปลอดภัยในการใช้งานระบบเครือข่าย และความปลอดภัยของเครื่องคอมพิวเตอร์ที่ใช้งาน อยู่ในระดับปานกลาง แต่ในภาพรวม ผู้ใช้งานระบบเครือข่ายของสำนักงานจังหวัดพัทลุงมีความพึงพอใจด้านประสิทธิภาพการใช้งานระบบเครือข่ายอยู่ในระดับพอใจมาก ซึ่งถือเป็นแนวโน้มที่ดีในการพัฒนาประสิทธิภาพการให้บริการระบบเทคโนโลยีสารสนเทศของหน่วยงาน อย่างไรก็ตามการบริหารด้านความมั่นคงปลอดภัยจะต้องมีการทบทวน

และพัฒนาต่อไป เพื่อให้ผู้ใช้งานเกิดความมั่นใจในความปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดมากยิ่งขึ้น

จากการประเมินแบบสอบถามด้านการรับรู้ในการสร้างความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013 แม้ว่าผู้ใช้งานจะรับรู้ถึงการเผยแพร่ การสร้างความตระหนักรู้และการทบทวนนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในระดับน้อย แต่ในภาพรวมของการรับรู้อยู่ระดับปานกลาง ทำให้ทราบว่า สำนักงานจังหวัดพัทลุงต้องเร่งดำเนินการสร้างการรับรู้ด้านนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานให้เกิดมากขึ้น

1.2 เปรียบเทียบการประเมินความเสี่ยงก่อน-หลังดำเนินการกรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013

ผู้วิจัยได้ดำเนินการประเมินค่าความเสี่ยงก่อน-หลังดำเนินการกรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 โดยมีผลการดำเนินการ ดังนี้

ตารางที่ 5.1 สรุปจำนวนความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนการดำเนินงาน

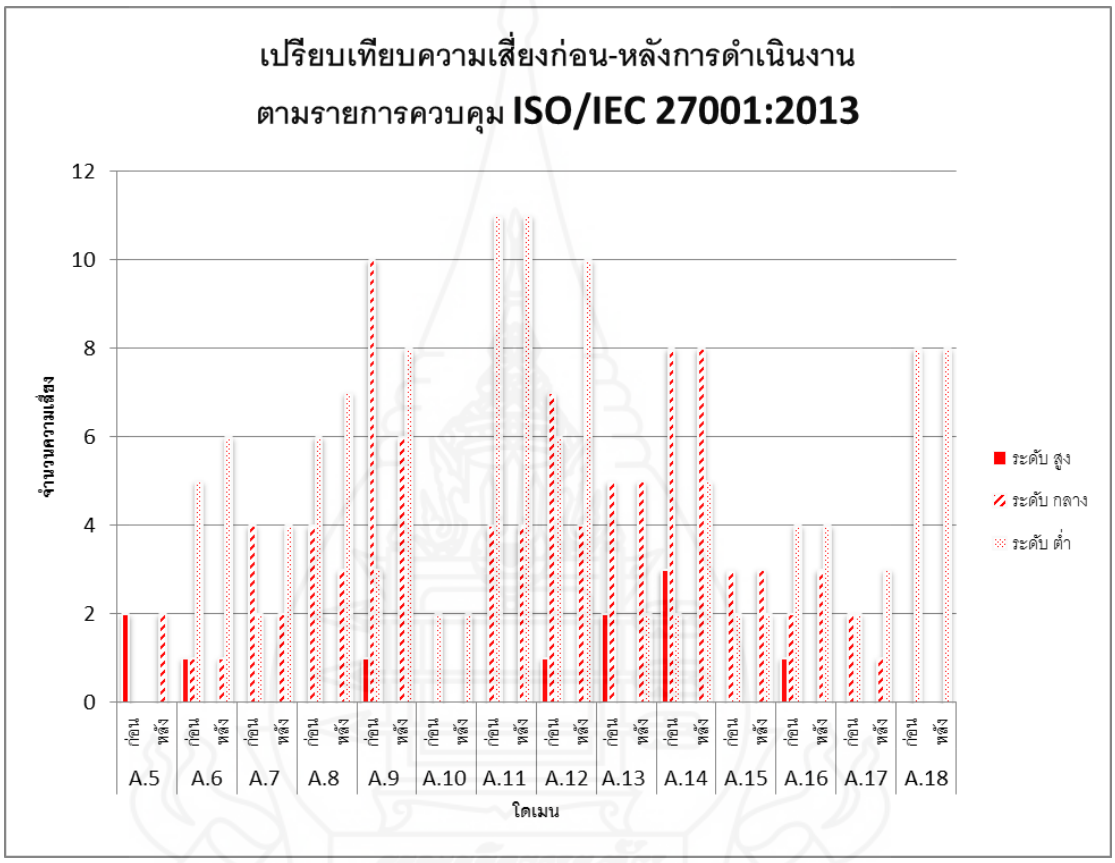
| | ระดับความเสี่ยงสูง | ระดับความเสี่ยงปานกลาง | ระดับความเสี่ยงต่ำ |
|---|---|---|---|
| จำนวน | 11 | 50 | 53 |

จากตารางที่ 5.1 แสดงการประเมินค่าความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 ก่อนดำเนินการ พบว่า หน่วยงานมีจำนวนความเสี่ยงระดับสูง 11 รายการ จำนวนความเสี่ยงระดับปานกลาง 50 รายการ และจำนวนความเสี่ยงระดับต่ำ 53 รายการ

ตารางที่ 5.2 สรุปจำนวนความเสี่ยงด้านเทคโนโลยีสารสนเทศหลังการดำเนินงาน

| | ระดับความเสี่ยงสูง | ระดับความเสี่ยงปานกลาง | ระดับความเสี่ยงต่ำ |
|---|---|---|---|
| จำนวน | 0 | 42 | 72 |

จากตารางที่ 5.2 แสดงการประเมินค่าความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 หลังดำเนินการ พบว่า ไม่พบรายการความเสี่ยงระดับสูง มีจำนวนความเสี่ยงระดับปานกลาง 42 รายการ และจำนวนความเสี่ยงระดับต่ำ 72 รายการ เปรียบเทียบการประเมินความเสี่ยงก่อน-หลังดำเนินการกรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013




ภาพที่ 5.1 เปรียบเทียบระดับความเสี่ยงก่อน-หลังดำเนินการ

จากภาพที่ 5.1 จะเห็นได้ว่าหลังจากดำเนินการตามกรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงและบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตาม ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง พบว่า หลังจากดำเนินการติดตั้งอุปกรณ์และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามนโยบายที่กำหนดขึ้น สำนักงานจังหวัดพัทลุงมีระดับความเสี่ยงสูงลดลง เหลือเพียงระดับความเสี่ยงปานกลางและต่ำเท่านั้น

## 2. อภิปรายผล

การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง ได้มีการวิเคราะห์และประเมินความเสี่ยง แล้วนำมาพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องและผู้ใช้งานให้เป็นไปในแนวทางเดียวกัน และได้ติดตั้งอุปกรณ์และระบบรักษามั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อให้สามารถป้องกันและลดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมกับหน่วยงานได้ ซึ่งจากการประเมินความเสี่ยงหลังจากดำเนินการบริหารจัดการด้านความมั่นคงปลอดภัยดังกล่าว พบว่า ความเสี่ยงที่เกิดกับระบบเทคโนโลยีสารสนเทศของหน่วยงานลดลง รวมทั้งหน่วยงานสามารถบริหารจัดการเครือข่ายได้ด้วยตนเองมากขึ้น สอดคล้องตามแนวทางมาตรฐานสากล ISO/IEC 27001:2013 ผลการประเมินความพึงพอใจของผู้ใช้งานระบบเครือข่ายด้านประสิทธิภาพการใช้งานอยู่ในระดับมาก ด้านการรับรู้ตามมาตรฐาน ISO/IEC 27001:2013 อยู่ในระดับปานกลาง ซึ่งจะต้องปรับปรุงให้บุคลากรในหน่วยงานตระหนักและรับรู้แนวทางการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงานให้เพิ่มขึ้น

จึงสรุปได้ว่า การบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง ทำให้หน่วยงานมีนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศใช้เป็นแนวทางปฏิบัติในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของหน่วยงานได้มากขึ้น และสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงลดลง

## 3. ข้อเสนอแนะ

จะเห็นได้ว่าการพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยของสำนักงานจังหวัดพัทลุง ตามมาตรฐาน ISO/IEC 27001:2013 ทำให้หน่วยงานสามารถลดระดับความเสี่ยงจากภัยคุกคามระบบสารสนเทศที่จะเกิดกับหน่วยงานได้ ซึ่งงานวิจัยนี้สามารถนำไปใช้เป็นกรณีศึกษาถึงแนวทางของการบริหารจัดการด้านความมั่นคงปลอดภัยในเชิงการนำไปปฏิบัติให้เกิดผลเพื่อรองรับสถานการณ์ที่จะเกิดขึ้นทั้งในปัจจุบันและอนาคต เนื่องจากแนวโน้มสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเพิ่มสูงขึ้น และเกิดขึ้นในรูปแบบใหม่ตลอดเวลา ดังนั้น หน่วยงานทั้งภาครัฐและภาคเอกชนจะต้องเตรียมรับมือกับเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่

คาดไม่ถึง ต้องเน้นให้บุคลากรในหน่วยงานตระหนักถึงความสำคัญในการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างจริงจัง โดยเฉพาะผู้บริหารหน่วยงานจะต้องมีวิสัยทัศน์ในการหาแนวทางป้องกันและรับมือกับภัยคุกคามด้านเทคโนโลยีสารสนเทศที่จะเกิดขึ้น โดยต้องให้ความสำคัญในการจัดทำนโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ และจะต้องทำอย่างต่อเนื่องตามกระบวนการการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ เนื่องจากความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามระบบสารสนเทศเกิดขึ้นในรูปแบบใหม่ตลอดเวลา ผู้วิจัยจึงได้เสนอแนวทางการดำเนินการลดความเสี่ยงให้เหลือน้อยที่สุดเท่าที่จะสามารถดำเนินการได้ดังนี้

1) ผู้บริหารของหน่วยงานต้องประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน อย่างเป็นทางการ

2) สำนักงานต้องจัดอบรมชี้แจงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน

3) สำนักงานต้องทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างต่อเนื่องรองรับสถานการณ์ภัยคุกคามที่คาดไม่ถึง เนื่องจากว่าภัยคุกคามที่จะเกิดขึ้นสามารถเปลี่ยนแปลงภาพแบบและความรุนแรงได้ตลอดเวลา

# บรรณานุกรม

# บรรณานุกรม


กรกฎ สราญสุทธิ์. (2556). การพัฒนานโยบายด้านความปลอดภัย ภายใต้มาตรฐาน ISO27001. สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

จุติชัย ทองกระจาย. (2557). ระบบตรวจจับการบุกรุกเครือข่ายกรณีศึกษา บริษัท เวนด้า ซอฟแวร์ ดีเวลอปเมนท์ จำกัด. (สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร: กรุงเทพฯ.

จตุชัย แพงจันทร์. (2550). Master in Security. นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.

จตุพร แพงจันทร์ และอนุโชต วุฒิพรพงษ์. (2555). เจาะระบบ Network. นนทบุรี: บริษัท ไอดีซี พรีเมียร์จำกัด.

เฉลิม สุวรรณ. (2554). การรักษาความมั่นคงปลอดภัยสารสนเทศ: กรณีศึกษาศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี. (สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร: กรุงเทพฯ.

บรรจง หะรังษี.(2554). หัวใจหลักของกระบวนการบริหารด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 (online). http://www.tnetsecurity.com/content_audit/pdca_def.pdf

บริษัท ที-เน็ต จำกัด. (2556).มาตรฐาน ISO/IEC 27001:2013 (online). http://www.tnetsecurity.com/ content_audit/27001-2013.pdf

ประกิจ อินทรักษ์ (2556).การพัฒนานโยบายด้านความมั่นคงปลอดภัยภายใต้มาตรฐาน ISO 27001:2005 กรณีศึกษาสาหรับสถาบันวิจัยแห่งหนึ่ง. (สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร: กรุงเทพฯ.

ไพศาล จันทร์เลื่อน. (2557). การพัฒนาความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศภายใต้มาตรฐาน ISO 27001 : กรณีศึกษา ศูนย์พัฒนาและบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพระนคร. (สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร: กรุงเทพฯ.

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ. (2550). มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น2.5). กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

Dell Inc.(2014).SonicOS 6.2.1 Administrator
Guide(online).https://support.software.dell.com/sonicwall-supermassive-9000-series/release-notes-guides.

# ภาคผนวก

# ภาคผนวก ก

กรอบนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ของสำนักงานจังหวัดพัทลุงที่พัฒนาขึ้น

# กรอบนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงที่พัฒนาขึ้น

## 1. ที่มา

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชกฤษฎีการว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสเทศของหน่วยงานของรัฐ ประกอบกับกระทรวงมหาดไทยได้จัดทำโครงการพัฒนาระบบรักษาความปลอดภัยด้านสารสนเทศและการสื่อสารเพื่อสนับสนุนให้มีการใช้งานและเชื่อมโยงเครือข่ายสื่อสารข้อมูลภาครัฐ (GIN) ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเพิ่มประสิทธิภาพในการใช้งานระบบเครือข่ายของสำนักงานจังหวัดพัทลุงให้มีความมั่นคงปลอดภัยและเชื่อถือได้ ในการนี้ สำนักงานจังหวัดจึงต้องกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสเทศของสำนักงานจังหวัดพัทลุง ขึ้นให้รองรับมาตรฐานสากล โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001:2013

## 2. วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดมีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง ตลอดจนสามารถรับมือกับภัยคุกคามต่างๆ ที่จะส่งผลให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของสำนักงาน จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง โดยมีวัตถุประสงค์ดังนี้

2.1 กำหนดขอบเขตการบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001 :2013

2.2 จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง เพื่อให้เกิดความมั่นคงปลอดภัยของหน่วยงาน ให้หน่วยงานดำเนินงานระบบเครือข่ายได้อย่างมีประสิทธิภาพและประสิทธิผล

2.3 กำหนดแนวทางและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ ที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญของการรักษาความปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงานและปฏิบัติตามอย่างเคร่งครัด

**3. องค์ประกอบของนโยบาย**

คำนิยาม

องค์กร หมายถึง สำนักงานจังหวัดพัทลุง

ผู้ใช้งาน หมายถึง ผู้ที่ได้รับอนุญาตให้สามารถเข้าใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ต่างกันตามที่องค์กรกำหนดได้แก่

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร ในที่นี้ ได้แก่ หัวหน้าสำนักงานจังหวัด

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอก ที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ขององค์กร ตามที่องค์กรกำหนด

ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ต่างๆ

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

**4. นโยบาย**

**4.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)**

ผู้บริหาร

- ต้องสนับสนุนให้จัดทำนโยบายความมั่นคงปลอดภัยอย่างเป็นทางการ และประกาศใช้ให้บุคลากรและหน่วยงานภายนอกที่เกี่ยวข้องทราบ และกำหนดให้มีการทบทวนนโยบายอย่างต่อเนื่องเป็นประจำทุกๆ ปี

**4.2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)**

ผู้บริหาร

- กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและแบ่งหน้าที่และงานที่รับผิดชอบให้ชัดเจนเพื่อลดข้อขัดแย้งในการปฏิบัติงาน

- พิจารณาอนุมัติให้ผู้ใช้งานนำอุปกรณ์คอมพิวเตอร์แบบพกพามาปฏิบัติงาน

- กำหนดนโยบายการปฏิบัติงานระยะไกล

ผู้ดูแลระบบ

- จัดทำรายชื่อสำหรับติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน เช่น กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และในการบริหารโครงการจะต้องระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

- ควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบ หากทำการเปิดพอร์ตควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอและอนุมัติจากผู้บริหารเท่านั้น

**4.3 การควบคุมการเข้าถึง (Access Control)**

ผู้บริหาร

- พิจารณาอนุมัติการลงทะเบียนผู้ใช้ใหม่ และยกเลิกสิทธิการใช้งานของผู้ใช้ในสำนักงาน

ผู้ดูแลระบบ

- บริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่อย่างรัดกุม

- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของแต่ละระดับความสำคัญของข้อมูล

- ออกแบบระบบเครือข่ายตามกลุ่ม (Zone) ของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

- กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall,IPS/IDS เป็นต้น

- จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาต หรือในเวลาที่กำหนด เท่านั้น

- ติดตั้งระบบตรวจจับการบุกรุก เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

- ป้องกันหมายเลขเครื่องคอมพิวเตอร์ของระบบงานเครือข่ายภายในขององค์กรไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

- จำกัดสิทธิการเข้าถึงเครือข่ายอินเทอร์เน็ตขององค์กรได้ตามความเหมาะสมที่ได้รับอนุมัติจากหัวหน้าสำนักงานจังหวัด เช่น การจำกัดสิทธิการเล่นเฟสบุคในเวลาทำงาน การเข้าเว็บไซต์ที่ไม่เหมาะสม

ผู้ใช้งาน

- ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

- ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

- ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

- ห้ามไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

- ต้องดูแล ป้องกันและรักษารหัสผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น หรือให้ผู้อื่นทราบ รวมถึงต้องมีการเปลี่ยนรหัสอย่างสม่ำเสมอ

**4.4 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)**

ผู้ดูแลระบบ

- ต้องติดตาม ปรับปรุงการใช้งานของทรัพยากรระบบเครือข่ายอย่างสม่ำเสมอ เพื่อให้เกิดประสิทธิภาพสูงสุดในการใช้งานระบบ

- ติดตั้งอุปกรณ์ตรวจจับการบุกรุก โปรแกรมที่ไม่พึงประสงค์ ไวรัส และอัพเดตให้ทันสมัยอย่างเสมอ

- สำรองข้อมูลและทดสอบการสำรองข้อมูลอย่างสม่ำเสมอตามกรอบระยะเวลาที่กำหนด

- บันทึกข้อมูลล็อคแสดงเหตุการณ์การใช้งานระบบ และให้เข้าถึงข้อมูลล็อคเฉพาะผู้ได้รับอนุญาตเท่านั้น

ผู้ใช้งาน

- ห้ามไม่ให้ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ของสำนักงาน ซึ่งถือเป็นสิ่งจำเป็นต่อการทำงาน

- ให้ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การอัพเดทโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

**4.5 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)**

ผู้ดูแลระบบ

- จัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน ได้แก่ ส่วนของระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone)

- จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- กำหนดระดับความสำคัญหรือชั้นความลับของข้อมูลและทบทวนอย่างสม่ำเสมอ

ผู้ใช้งาน

- ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต เช่น อีเมล์ หรือโพสต์ในเว็บต่างๆ

- การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

- ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ

**4.6 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (Systems acquisition, development and maintenance)**

ผู้บริหาร

- สนับสนุนให้มีการกำหนดขอบเขตงานในการพัฒนาระบบโดยเน้นความมั่นคงปลอดภัยอย่างเป็นทางการ

ผู้ดูแลระบบ

- ต้องนำหลักวิศวะกรรมระบบด้านความมั่นคงปลอดภัยมาใช้ในการปฏิบัติงาน

- มีการทดสอบ เพื่อหาแนวทางป้องกันความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ

**4.7 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)**

ผู้บริหาร

- สนับสนุนให้มีการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อ เตรียมความพร้อมกรณีฉุกเฉินตอบสนองต่อสถานการณ์ความไม่มั่นคงปลอดภัยสารสนเทศ

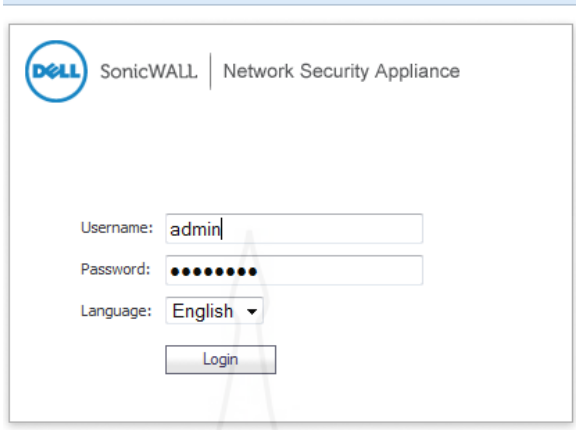
ผู้ดูแลระบบ

- จัดทำขั้นตอนการปฏิบัติงาน เช่น การสำรองข้อมูล ไว้เป็นลายลักษณ์อักษร
- รายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

**ภาคผนวก ข**

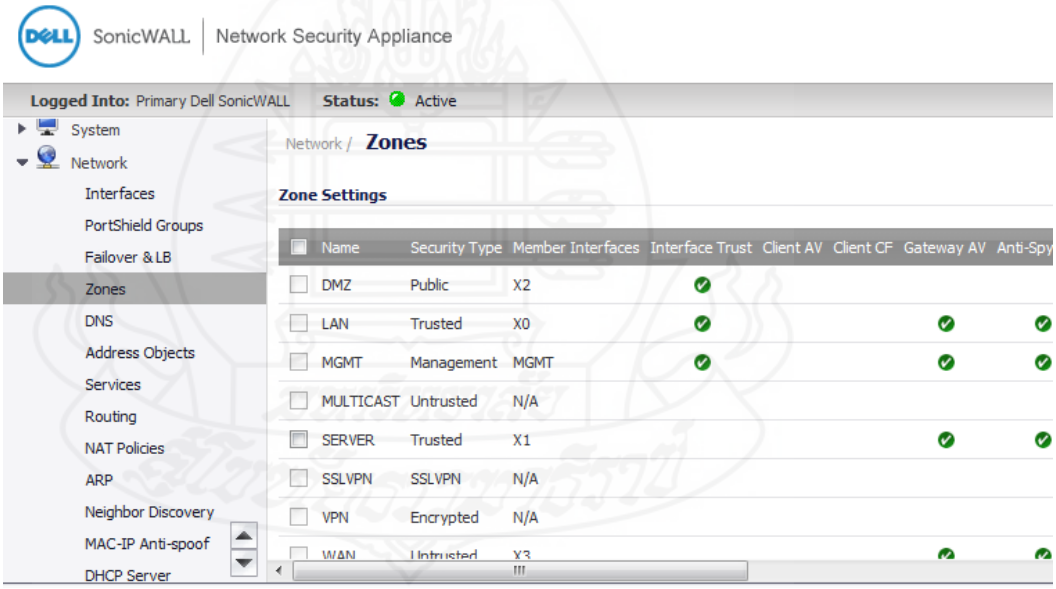
การกำหนดค่าระบบรักษาความปลอดภัย
บนอุปกรณ์ไฟร์วอลล์และอุปกรณ์ป้องกันการบุกรุก

1. เข้าผ่านทางหน้าบริหารจัดการ ทาง https

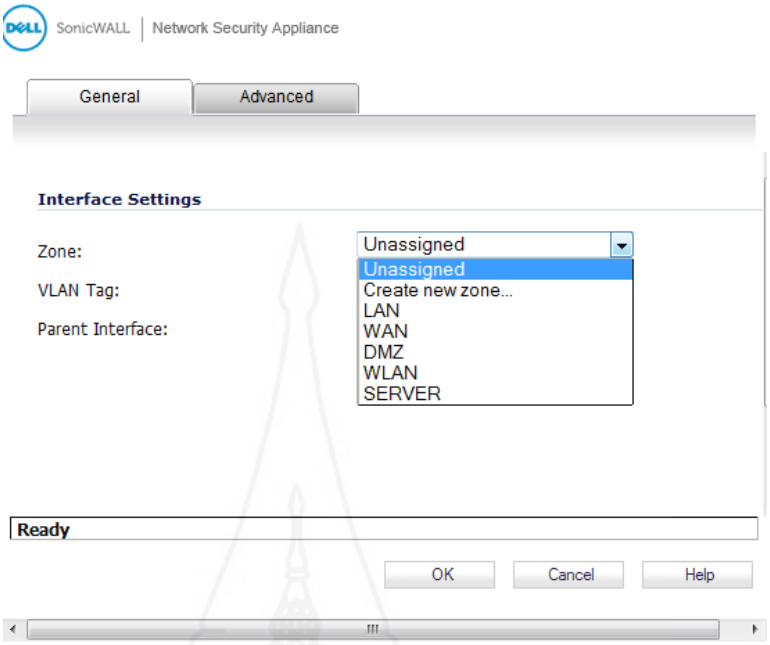


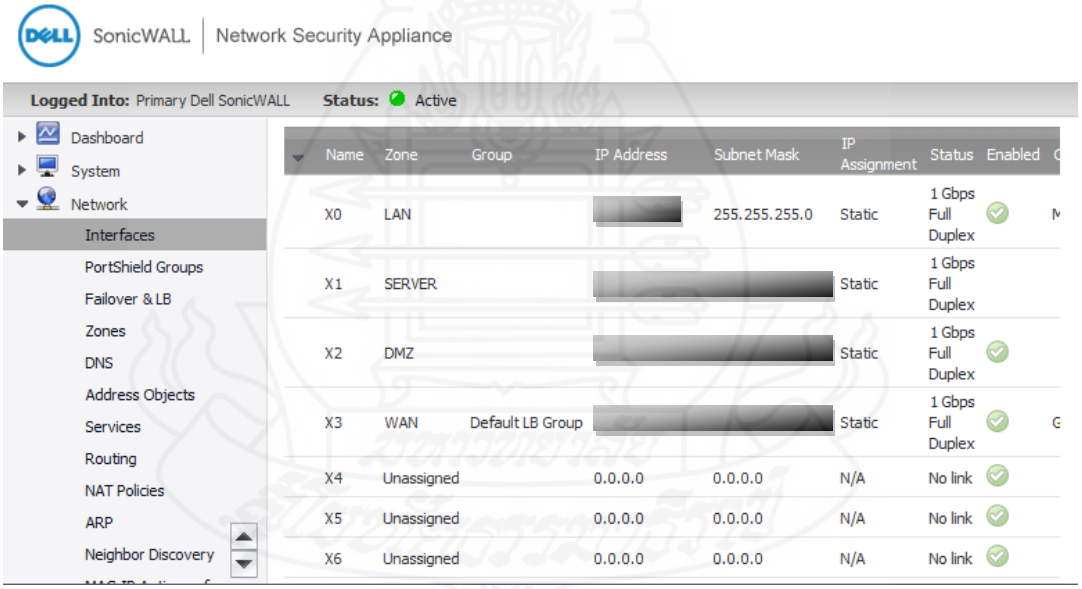

2. กำหนดค่าให้กับอุปกรณ์ไฟล์วอล (Configure) ตามที่ออกแบบไว้

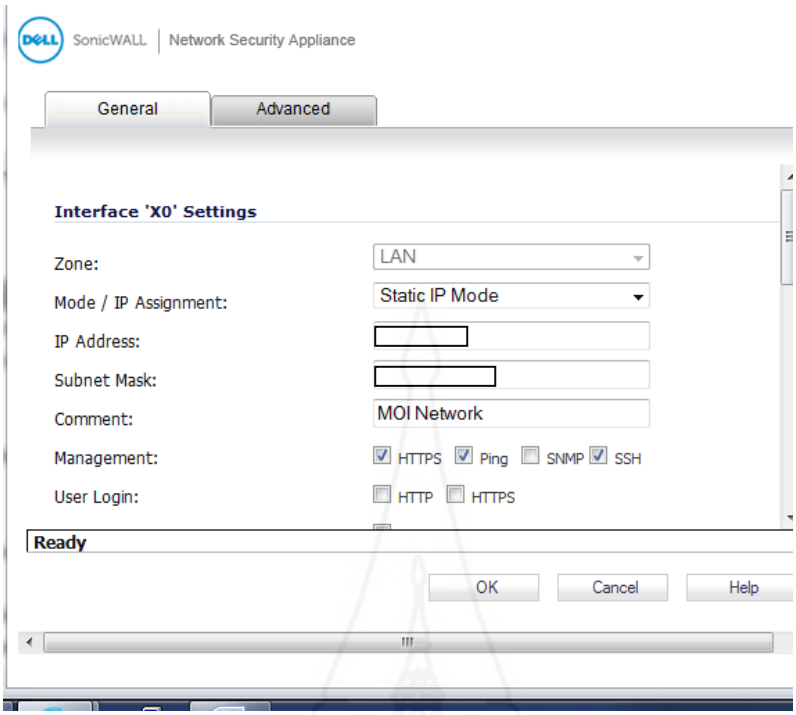
2.1 กำหนดค่า Networking ตั้งค่า Security Zone (Network-> Zone) โดยเลือกเพิ่มโซนใหม่บน ไฟล์วอล กำหนดค่าต่างๆ



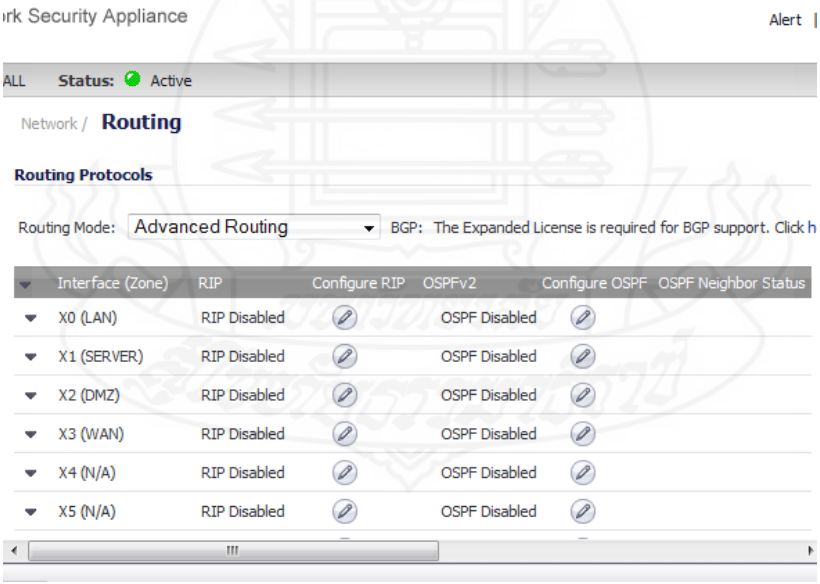
2.2 ตั้งค่า Interface (Network-> Interface-> Configuration) เป็นการระบุโซน สำหรับอินเทอร์เฟส

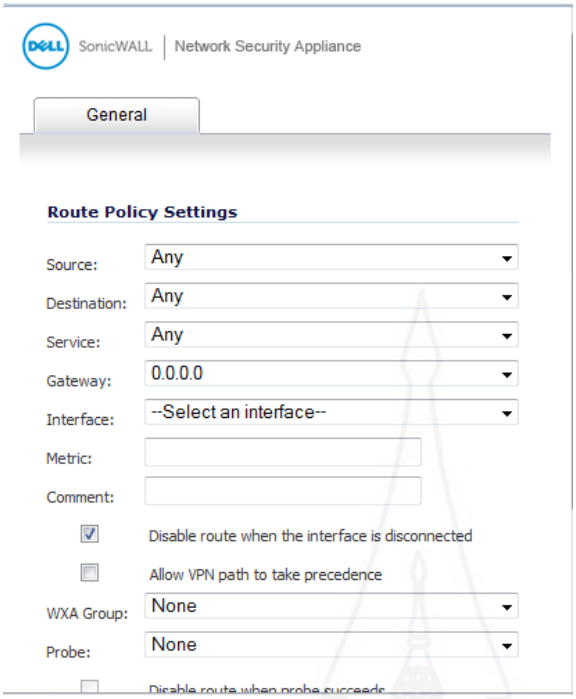


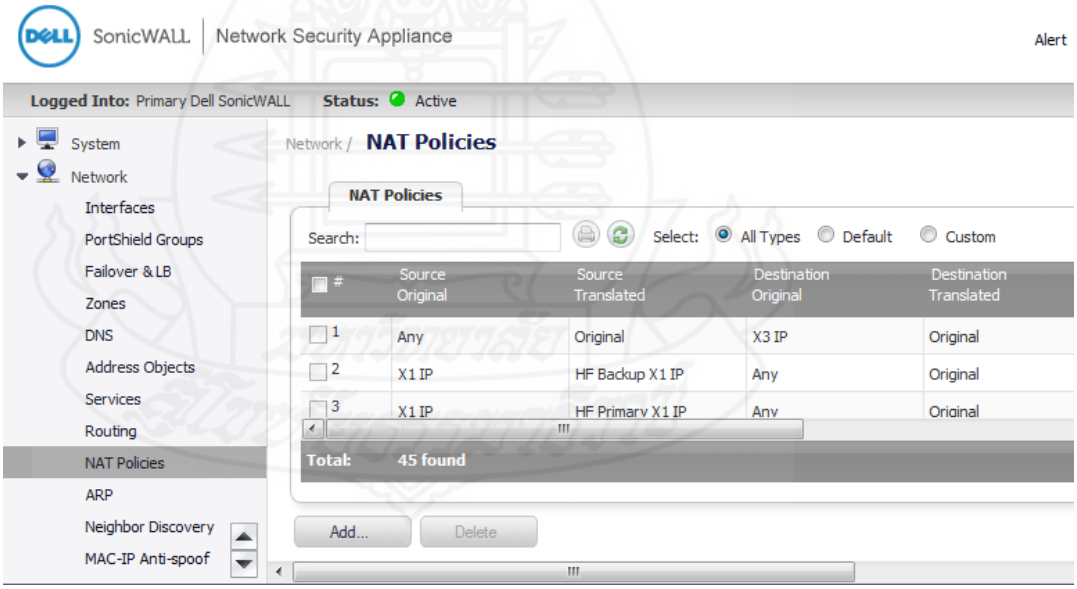


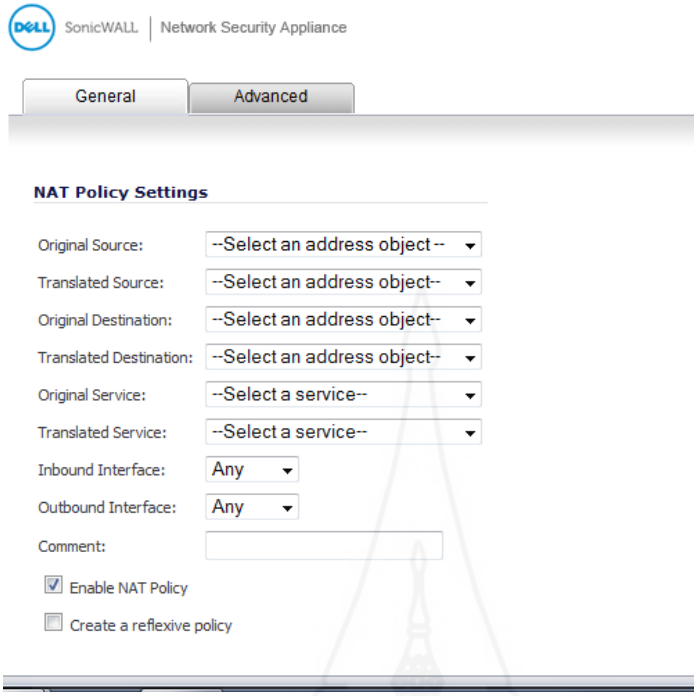

2.3 ตั้งค่า Routing (Network->routing)



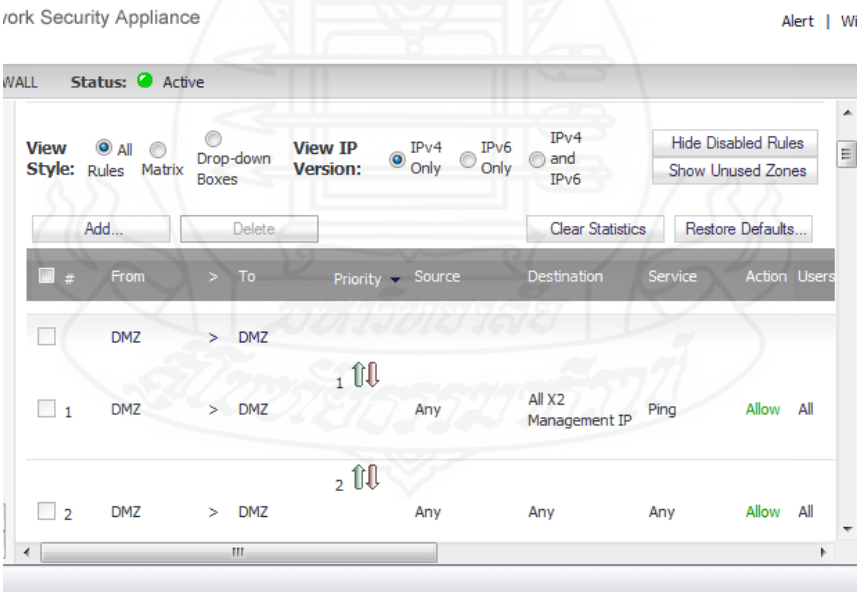


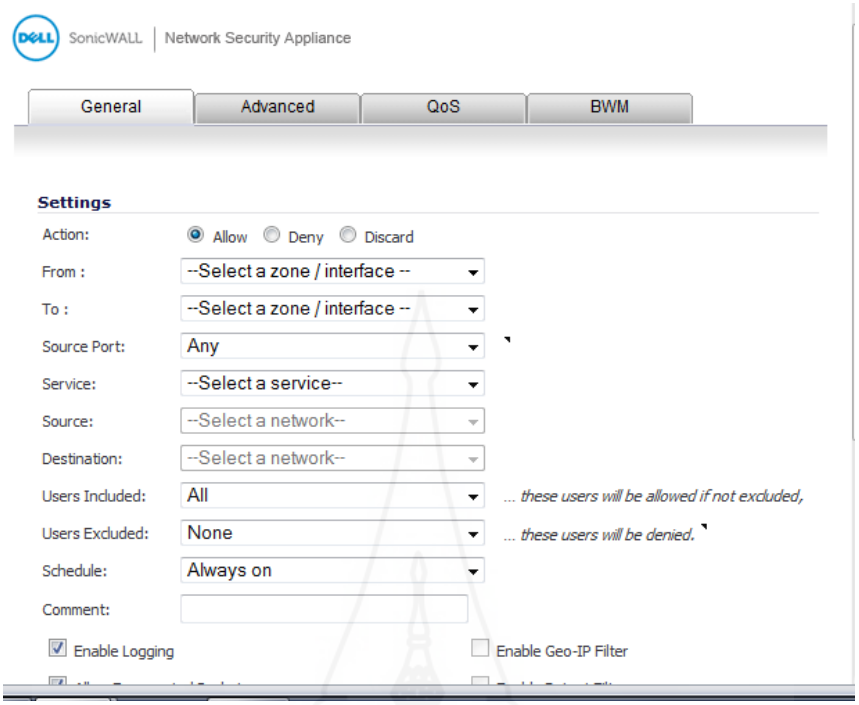

2.4 ตั้งค่า NAT Policies (Network-> NAT Policies-> Add)






2.5 กำหนดค่า Firewall ตั้งค่า Access Rule

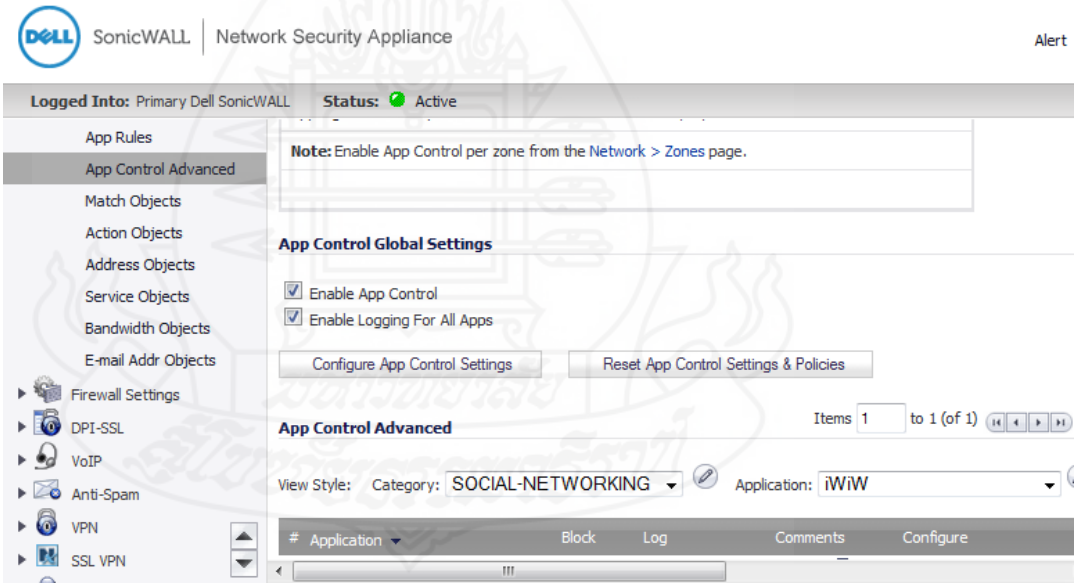


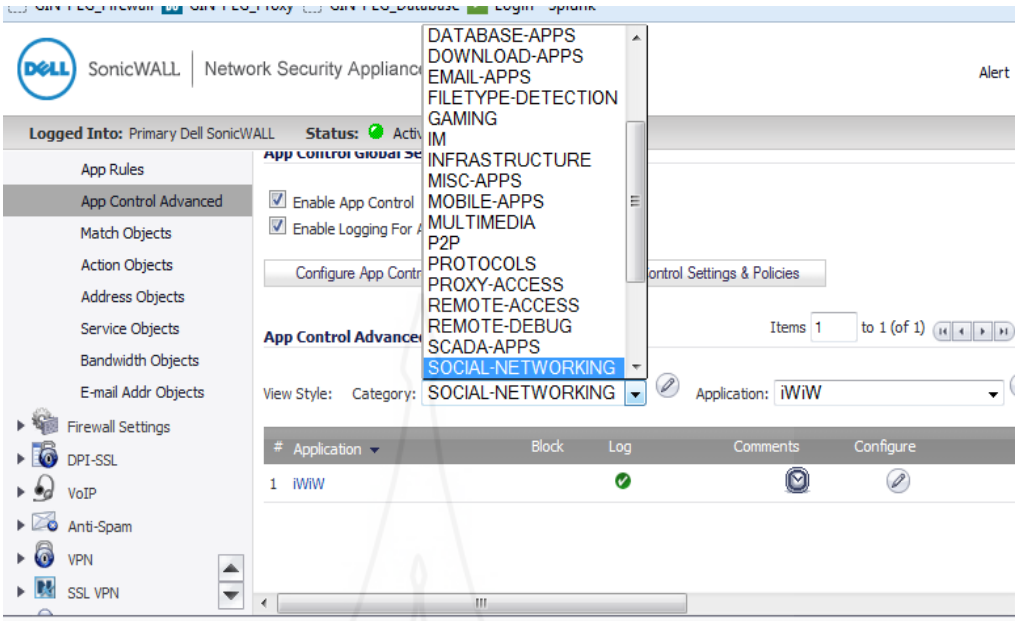


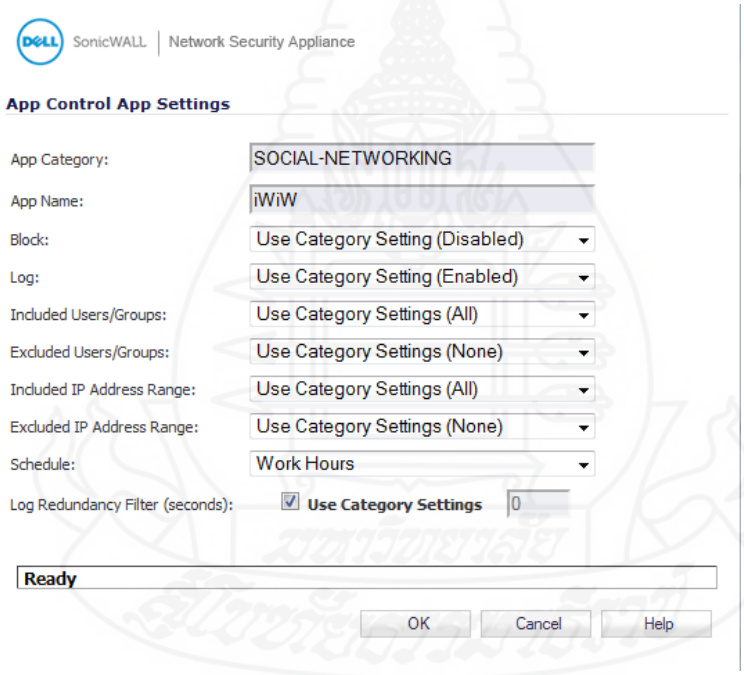

2.6 กำหนดค่า Firewall ตั้งค่า Control Application จะระดับ Global ซึ่งสามารถเลือก Control ได้ตาม Category ของ Application ดังนี้

| | |
|---|---|
| 1 | APP-UPDATE |
| 2 | BACKUP-APPS |
| 3 | BROWSING-PRIVACY |
| 4 | BUSINESS-APPS |
| 5 | DATABASE-APPS |
| 6 | DOWNLOAD-APPS |
| 7 | EMAIL-APPS |
| 8 | FILETYPE-DETECTION |
| 9 | GAMING |
| 10 | IM |
| 11 | INFRASTRUCTURE |
| 12 | MISC-APPS |
| 13 | MOBILE-APPS |
| 14 | MULTIMEDIA |

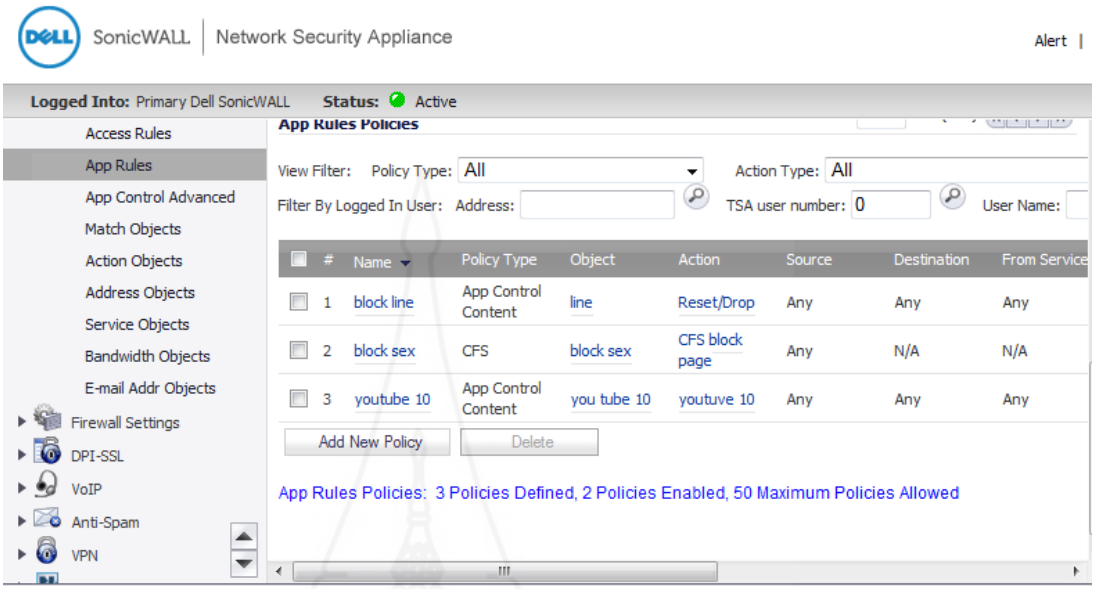
| | |
|---|---|
| 15 | P2P |
| 16 | PROTOCOLS |
| 17 | PROXY-ACCESS |
| 18 | REMOTE-ACCESS |
| 19 | REMOTE-DEBUG |
| 20 | SCADA-APPS |
| 21 | SOCIAL-NETWORKING |
| 22 | SRC-CRTL-APPS |
| 23 | STOCK-TRADING |
| 24 | VoIP-APPS |
| 25 | WEB-BROWSER |
| 26 | WEB-CONFERENCING |
| 27 | WEBMAIL |

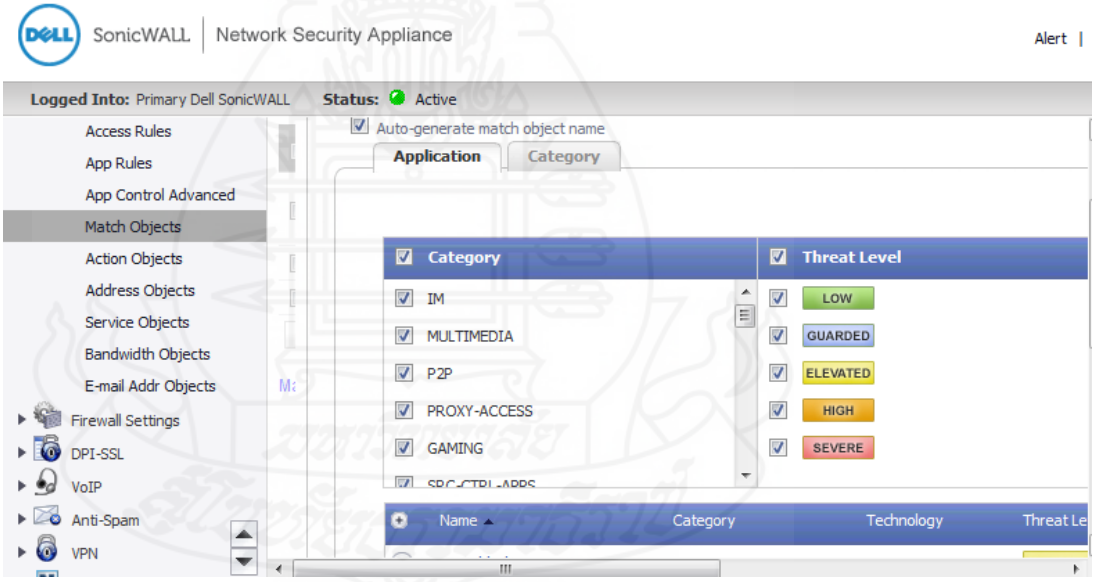



SonicWALL | Network Security Appliance
Alert
Logged Into: Primary Dell SonicWALL
Status:
App Rules
App Control Advanced
Match Objects
Action Objects
Address Objects
Service Objects
Bandwidth Objects
E-mail Addr Objects
Firewall Settings
DPI-SSL
VoIP
Anti-Spam
VPN
SSL VPN
Enable App Control
Enable Logging For
Configure App Contr
ontrol Settings & Policies
App Control Advance
Items 1 to 1 (of 1)
View Style:
Category: SOCIAL-NETWORKING
Application: iWiW
# Application
Block
Log
Comments
Configure
1 iWiW
DATABASE-APPS
DOWNLOAD-APPS
EMAIL-APPS
FILETYPE-DETECTION
GAMING
IM
INFRASTRUCTURE
MISC-APPS
MOBILE-APPS
MULTIMEDIA
P2P
PROTOCOLS
PROXY-ACCESS
REMOTE-ACCESS
REMOTE-DEBUG
SCADA-APPS
SOCIAL-NETWORKING

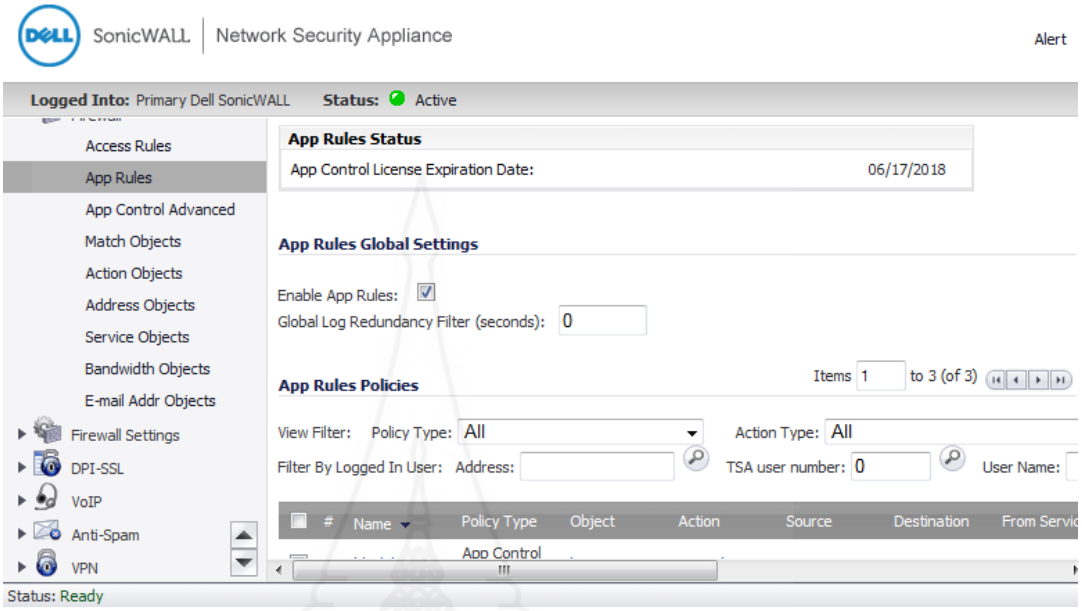

SonicWALL | Network Security Appliance
App Control App Settings
App Category: SOCIAL-NETWORKING
App Name: iWiW
Block: Use Category Setting (Disabled)
Log: Use Category Setting (Enabled)
Included Users/Groups: Use Category Settings (All)
Excluded Users/Groups: Use Category Settings (None)
Included IP Address Range: Use Category Settings (All)
Excluded IP Address Range: Use Category Settings (None)
Schedule: Work Hours
Log Redundancy Filter (seconds): Use Category Settings 0
Ready
OK
Cancel
Help

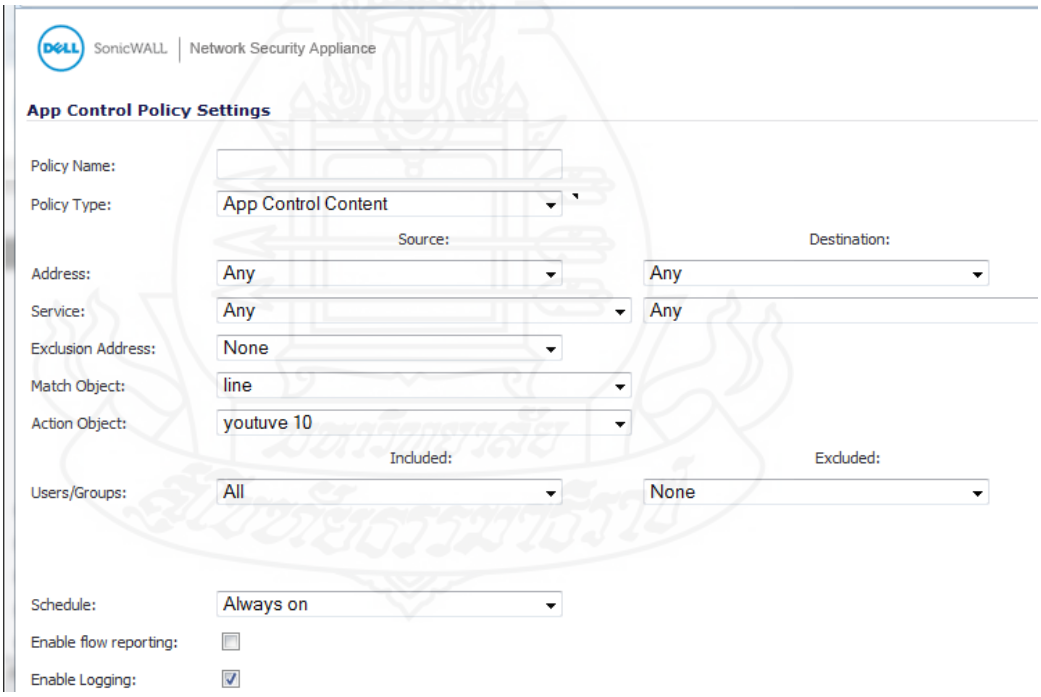
2.7 กำหนดค่า Firewall ตั้งค่า App Rules



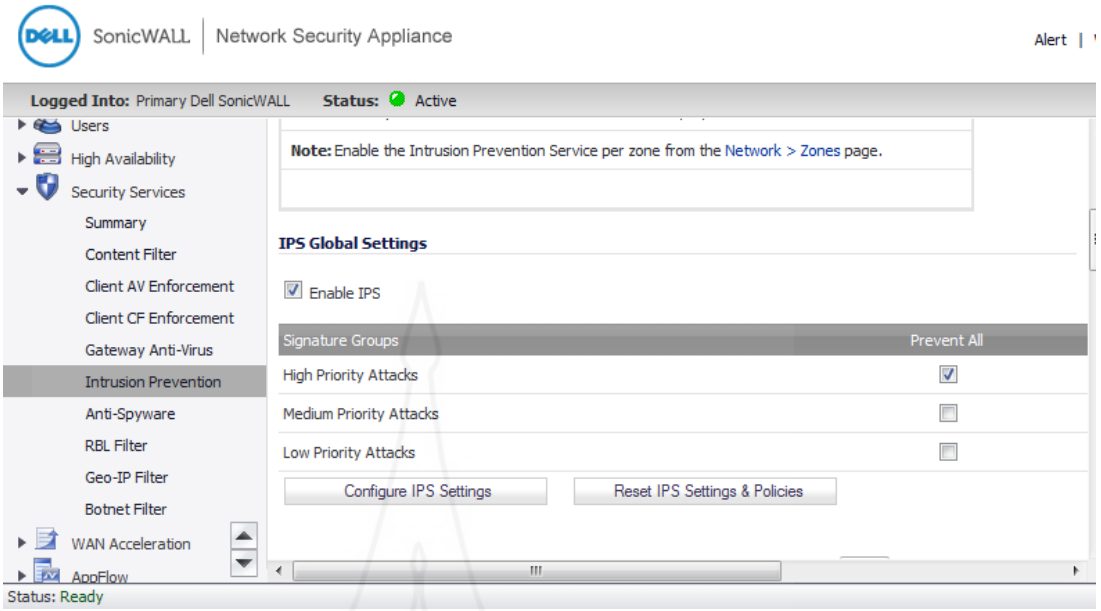
2.8 กำหนดค่า Firewall ตั้งค่า App Rules Policies

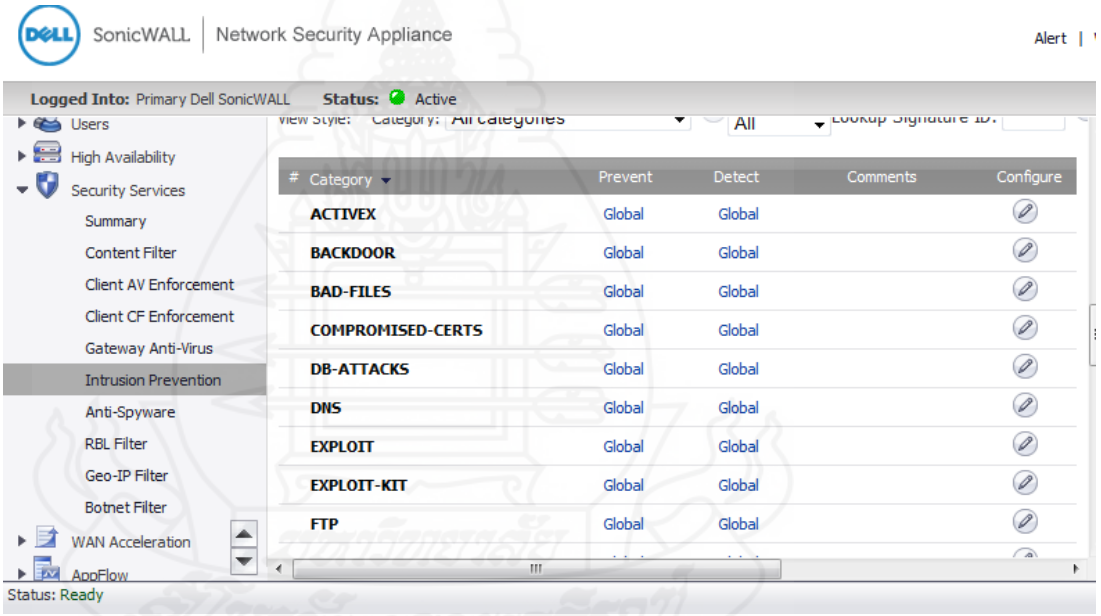


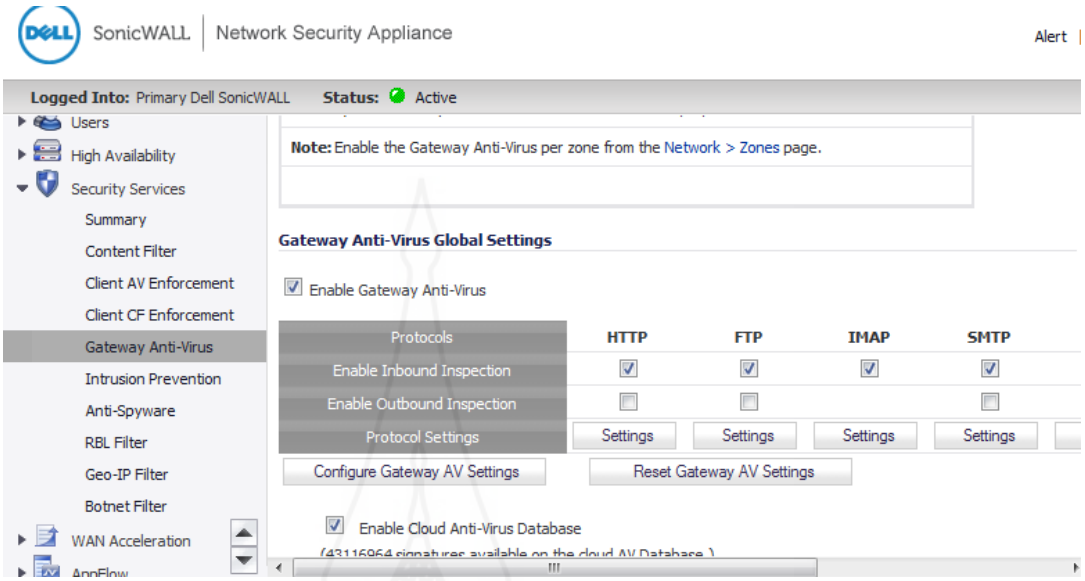
2.9 กำหนดค่า Firewall ตั้งค่า Security services (IPS,Gateway,Anti-Virus,Anti-Spyware) ตั้งค่า Intrustion Prevention (IPS) โดยมี IPS Signature list ดังตาราง และรูปตามลำดับ

| | |
|---|---|
| 1 | APP-UPDATE |
| 2 | BACKUP-APPS |
| 3 | BROWSING-PRIVACY |
| 4 | BUSINESS-APPS |
| 5 | DATABASE-APPS |
| 6 | DOWNLOAD-APPS |
| 7 | EMAIL-APPS |
| 8 | FILETYPE-DETECTION |
| 9 | GAMING |
| 10 | IM |
| 11 | INFRASTRUCTURE |
| 12 | MISC-APPS |
| 13 | MOBILE-APPS |
| 14 | MULTIMEDIA |
| 15 | P2P |
| 16 | PROTOCOLS |
| 17 | PROXY-ACCESS |
| 18 | REMOTE-ACCESS |
| 19 | REMOTE-DEBUG |
| 20 | SCADA-APPS |
| 21 | SOCIAL-NETWORKING |
| 22 | SRC-CRTL-APPS |
| 23 | STOCK-TRADING |
| 24 | VoIP-APPS |
| 25 | WEB-BROWSER |
| 26 | WEB-CONFERENCING |
| 27 | WEBMAIL |

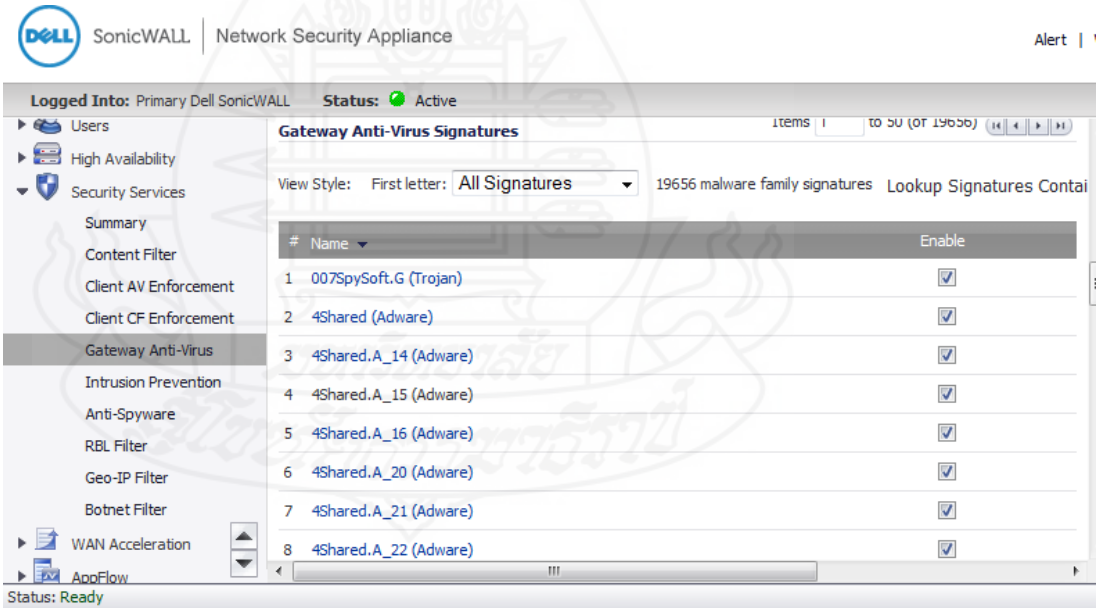

SonicWALL | Network Security Appliance
Alert
Logged Into: Primary Dell SonicWALL
Status: Active
Users
High Availability
Security Services
Summary
Content Filter
Client AV Enforcement
Client CF Enforcement
Gateway Anti-Virus
Intrusion Prevention
Anti-Spyware
RBL Filter
Geo-IP Filter
Botnet Filter
WAN Acceleration
AppFlow
Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.
IPS Global Settings
Enable IPS
Signature Groups
Prevent All
High Priority Attacks
Medium Priority Attacks
Low Priority Attacks
Configure IPS Settings
Reset IPS Settings & Policies
Status: Ready


SonicWALL | Network Security Appliance
Alert
Logged Into: Primary Dell SonicWALL
Status: Active
Users
High Availability
Security Services
Summary
Content Filter
Client AV Enforcement
Client CF Enforcement
Gateway Anti-Virus
Intrusion Prevention
Anti-Spyware
RBL Filter
Geo-IP Filter
Botnet Filter
WAN Acceleration
AppFlow
# Category
Prevent
Detect
Comments
Configure
ACTIVEX Global Global
BACKDOOR Global Global
BAD-FILES Global Global
COMPROMISED-CERTS Global Global
DB-ATTACKS Global Global
DNS Global Global
EXPLOIT Global Global
EXPLOIT-KIT Global Global
FTP Global Global
Status: Ready

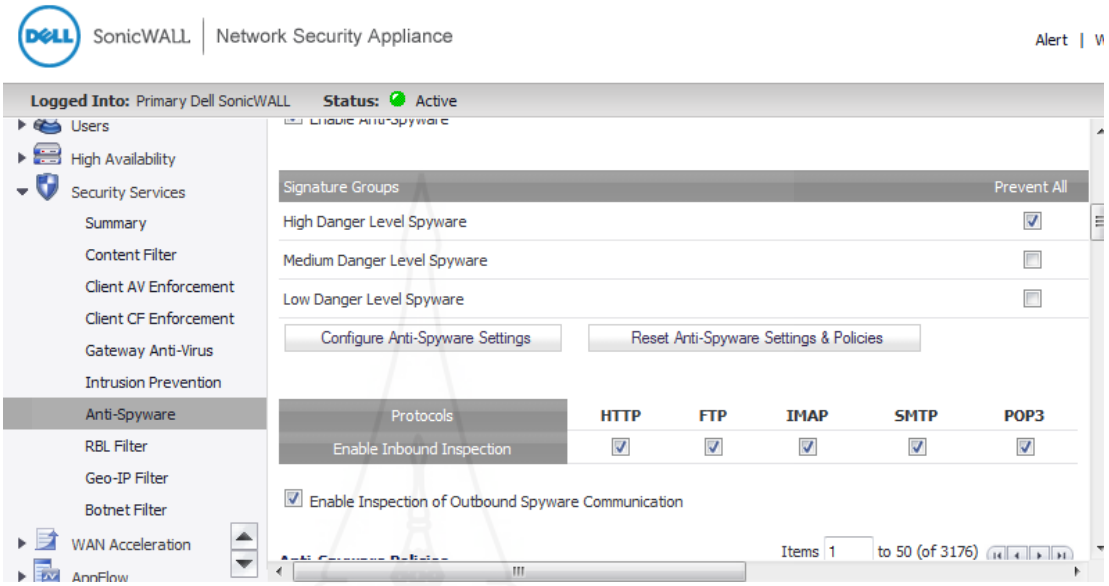
2.10 กำหนดค่า Firewall ตั้งค่า Gateway Anti-Virus

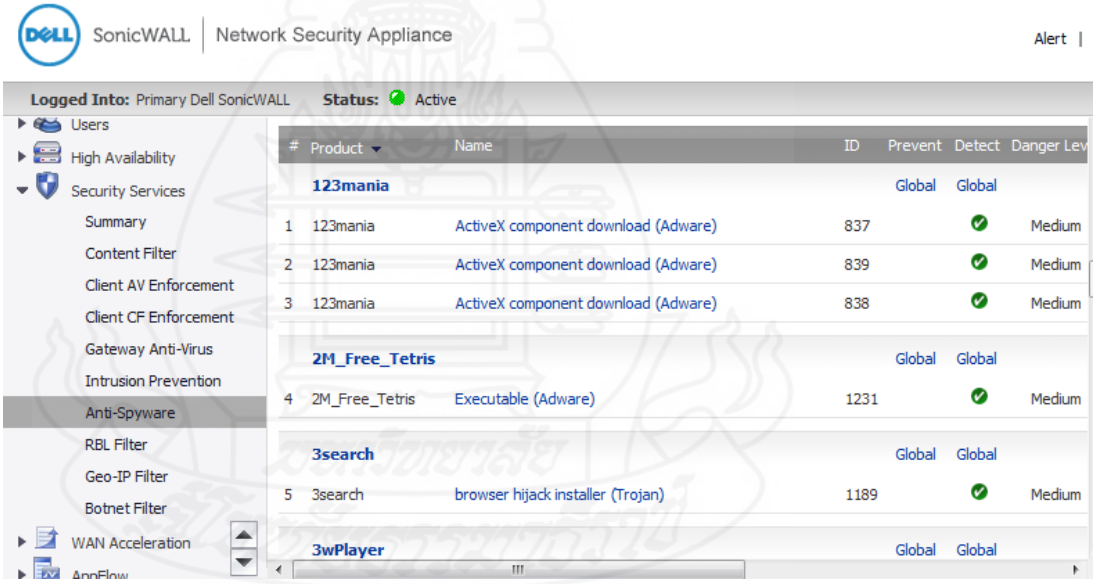



2.11 กำหนดค่า Firewall ตั้งค่า Gateway Anti-Virus Global setting



2.12 กำหนดค่า Firewall ตั้งค่า Anti-Spyware ดังรูป



# ภาคผนวก ค

แบบสอบถามความพึงพอใจ

แบบสอบถามความพึงพอใจของผู้ใช้บริการระบบเครือข่ายสำนักงานจังหวัดพัทลุง

คำชี้แจง

แบบสอบถามนี้จัดทำขึ้นเพื่อประเมินความพึงพอใจการใช้บริการระบบเครือข่ายของสำนักงานจังหวัดพัทลุง เพื่อนำผลการประเมินมาปรับปรุงระบบเครือข่ายให้มีประสิทธิภาพมากยิ่งขึ้นตามมาตรฐาน ISO/IEC 27001:2013

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบสอบถามความพึงพอใจการให้บริการระบบเครือข่าย

ตอนที่ 3 ข้อเสนอแนะ

<u>ตอนที่ 1 ข้อมูลทั่วไป</u>

1. เพศ

   ○ ชาย ○ หญิง

2. อายุ

   ○ ต่ำกว่า 20 ปี ○ 21-30 ปี ○ 31-40 ปี ○ 41-50 ปี ○ 51-60 ปี ○ 60 ปีขึ้นไป

3. ระดับการศึกษา

   ○ ต่ำกว่าปริญญาตรี ○ ปริญญาตรี ○ ปริญญาโท ○ ปริญญาเอก

4. อาชีพ

   ○ ลูกจ้างชั่วคราว ○ ลูกจ้างประจำ ○ พนักงานราชการ ○ ข้าราชการ

   ○ อื่นๆ ระบุ.....

5. ประเภทผู้ใช้งาน

   ○ ผู้ใช้งานทั่วไป (user) ○ ผู้ดูแลระบบ (admin) ○ อื่นๆ ระบุ.....

6. ความถี่ในการใช้งานระบบเครือข่าย

   ○ น้อยกว่า 1 ชม./วัน ○ 1-3 ชม./วัน ○ 3-6 ชม./วัน ○ 6-9 ชม./วัน

   ○ มากกว่า 9 ชม./วัน

7. ช่วงเวลาที่ใช้บริการ (เลือกได้มากกว่า 1 ข้อ)

   ○ ก่อน 8.00 น. ○ 8.00 -12.00 น. ○ 12.00-13.00 น. ○ 13.00-16.00 น.

   ○ หลังจาก 16.00 น.

8. รูปแบบการเชื่อมต่อสัญญาณเพื่อเข้าใช้ระบบเครือข่าย (เลือกได้มากกว่า 1 ข้อ)

   ○ แบบมีสาย (LAN) ○ แบบไร้สาย (wireless) ○ อื่นๆ ระบุ.....

ตอนที่ 2 แบบสอบถามความพึงพอใจการให้บริการระบบเครือข่าย

| การบริการ | ระดับความพึงพอใจในการบริการที่ได้รับ | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 1. ความเร็วในการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของสำนักงาน | | | | | |
| 2. ความสะดวกในการเข้าถึงเครือข่ายของสำนักงาน | | | | | |
| 3. ความมีเสถียรภาพของระบบเครือข่าย | | | | | |
| 4. ระบบเครือข่ายให้บริการได้ครอบคลุมและทั่วถึง | | | | | |
| 5. ระบบเครือข่ายมีความปลอดภัยในการใช้งาน | | | | | |
| 6. การกำหนดสิทธิในการเข้าใช้งานมีความปลอดภัย | | | | | |
| 7. ความปลอดภัยของเครื่องคอมพิวเตอร์ที่ท่านใช้งาน | | | | | |
| 8. ความพึงพอใจภาพรวมต่อการใช้งาน | | | | | |

ตอนที่ 3 แบบสอบถามการรับรู้ของบุคลากรในหน่วยงาน

| รายการ | ระดับความพึงพอใจในการบริการที่ได้รับ | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 1. มีการเผยแพร่นโยบายความมั่นคงปลอดภัยของหน่วยงาน | | | | | |
| 2. มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย | | | | | |
| 3. การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดให้แก่พนักงาน | | | | | |
| 4.มีการการจัดทำบัญชีทรัพย์สิน | | | | | |
| 5. มีการควบคุมการเข้าถึงระบบสารสนเทศ และระบบ | | | | | |

| รายการ | ระดับความพึงพอใจในการบริการที่ได้รับ | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| เครือข่าย | | | | | |
| 6. มีนโยบายการใช้มาตรการเข้ารหัสข้อมูล | | | | | |
| 7. มีการควบคุมการเข้าออกห้องสารสนเทศและการสื่อสาร | | | | | |
| 8. มีขั้นตอนการบริหารจัดการการเปลี่ยนแปลง | | | | | |
| 9. มีขั้นตอนปฏิบัติในการเข้าถึงสารสนเทศของหน่วยงาน | | | | | |
| 10. มีการกำหนดแนวทางการจัดหา การพัฒนา และการบำรุงรักษาระบบ | | | | | |
| 11. มีการกำหนดแนวทางความสัมพันธ์กับผู้ให้บริการภายนอก | | | | | |
| 12. มีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | | | | | |
| 13. มีการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ | | | | | |
| 14. มีการทบทวนความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงาน | | | | | |

ตอนที่ 4 ข้อเสนอแนะ

……..…

……..…

……..…

……..…

แบบสอบถามการรับรู้ของผู้บริหารและเจ้าหน้าที่ดูแลระบบ

| รายการ | ระดับความพึงพอใจในการบริการที่ได้รับ | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 1. มีการเผยแพร่นโยบายความมั่นคงปลอดภัยของหน่วยงาน | | | | | |
| 2. มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย | | | | | |
| 3. การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดให้แก่พนักงาน | | | | | |
| 4.มีการจัดทำรายการครุภัณฑ์และอุปกรณ์ระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร | | | | | |
| 5. มีการควบคุมการเข้าถึงระบบสารสนเทศ และระบบเครือข่าย | | | | | |
| 6. มีนโยบายการเข้ารหัส (encode) รหัสผ่านระบบฐานข้อมูลหรือมีการกำหนดให้มีการใช้งานเว็บไซต์ที่ปลอดภัย (SSL) ทำธุรกรรมต่างๆ เพื่อเข้ารหัสการส่งข้อมูลผ่านเว็บ https หรือมีการเข้าและถอดรหัสกุญแจข้อมูล | | | | | |
| 7. มีการควบคุมการเข้าออกห้องสารสนเทศและการสื่อสาร | | | | | |
| 8. มีการกำหนดความมั่นคงปลอดภัยในการดำเนินงาน เช่น มีขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษรเพื่อบริหารจัดการการเปลี่ยนแปลง | | | | | |
| 9.มีการรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เช่นมีการกำหนดชั้นความลับ มีขั้นตอนการปฏิบัติในการเข้าถึงสารสนเทศของหน่วยงาน | | | | | |
| 10. มีการกำหนดแนวทางการจัดหา การพัฒนาและการบำรุงรักษาระบบ | | | | | |

| รายการ | ระดับความพึงพอใจในการบริการที่ได้รับ | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 11.มีการกำหนดและตกลงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ | | | | | |
| 12. มีการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ | | | | | |
| 13. มีการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ | | | | | |
| 14. มีการทบทวนความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงาน | | | | | |

# ประวัติผู้ศึกษา

| | |
|---|---|
| **ชื่อ** | นางสาวรัตนาภรณ์ บุญสิน |
| **วัน เดือน ปีเกิด** | 13 เมษายน 2526 |
| **สถานที่เกิด** | จังหวัดนครศรีธรรมราช |
| **ประวัติการศึกษา** | พ.ศ. 2545 มัธยมศึกษาตอนปลาย โรงเรียนเบญจมราชูทิศ นครศรีธรรมราช |
| | พ.ศ. 2549 วิทยาศาสตรบัณฑิต มหาวิทยาลัยสงขลานครินทร์ |
| **สถานที่ทำงาน** | สำนักงานจังหวัดพัทลุง |
| **ตำแหน่ง** | นักวิชาการคอมพิวเตอร์ |