การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง

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

รัตนาภรณ์ บุญสิน[1*], ขจิตพรรณ กฤตพลวิมาน[2]
Rattanaporn Boonsin[1*], Khajitpan Kritpolviman[2]

บทคัดย่อ

งานวิจัยนี้ มีวัตถุประสงค์ 1) เพื่อพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 2) เพื่อลดและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงาน งานวิจัยนี้ ได้ดำเนินการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และนำผลลัพธ์ที่ได้มาเข้าสู่ระบบบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ และทำการพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 พร้อมกับติดตั้งอุปกรณ์และระบบรักษาความมั่นคงปลอดภัย เพื่อป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อสำนักงานจังหวัดพัทลุง

เมื่อประเมินผลพบว่าการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง ทำให้หน่วยงานมีนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงลดลง

คำสำคัญ: ระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ, นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ, ISO/IEC 27001:2013

Abstract

This reseach aimed 1) to develop information technology (IT) security policy framework of governor's office of Phatthalung Province based on ISO/IEC 27001:2013. 2) to decrease and protect IT risks of governor's office of Phatthalung Province. This research has processed the IT analysis and IT risk evaluation. Then, the results were sent to the security of information systems (ISMS) process, and the IT security policy framework was developed based on ISO/IEC 27001:2013. Mutually, the device and security system were practically installed in order to prevent the IT risks possibly occur at the governor’s office of Phatthalung Province.

The performance evaluation results found that implementation of ISMS process in the governor’s office of Phatthalung Province based on ISO/IEC 27001:2013 could develop IT security policy that be able to prevent and decrease IT risks.

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

---

[1] สาขาวิชาวิทยาศาสตร์และเทคโนโลยี แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยสุโขทัยธรรมาธิราช

[2] ผู้ช่วยศาสตราจารย์ประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยสุโขทัยธรรมาธิราช

[*] **Corresponding author, E-mail:** rattanaporn.boo@mystou.ac.th

บทนำ

ปัจจุบันหน่วยงานภาครัฐได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการสนับสนุนการปฏิบัติงานและติดต่อสื่อสารในการให้บริการทั้งกับภาครัฐด้วยกันและภาคประชาชนเพิ่มขึ้น ทำให้ภาครัฐต้องเผชิญปัญหาภัยคุกคามทางคอมพิวเตอร์ เช่น การโจมตีเว็บไซต์ ไวรัสทำลายระบบ และการขโมยข้อมูล เป็นต้น ซึ่งได้ทวีความรุนแรงเพิ่มขึ้นอย่างหลีกเลี่ยงไม่ได้ ดังนั้น การบริหารความมั่นคงปลอดภัยสารสนเทศจึงเป็นสิ่งสำคัญ ที่หน่วยงานต้องตระหนักรวมถึงการจัดทำนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เป็นเครื่องมือสำคัญในการรับมือกับภัยคุกคามทางระบบคอมพิวเตอร์ที่อาจจะเกิดขึ้น

สำนักงานจังหวัดพัทลุงเป็นหน่วยงานภาครัฐ สังกัดสำนักงานปลัดกระทรวงมหาดไทย ทำหน้าที่บูรณาการทุกส่วนราชการภายในจังหวัด ได้ให้บริการข้อมูลข่าวสารทุกส่วนราชการเพื่อขับเคลื่อนการจัดทำแผนพัฒนาจังหวัดผ่านทางระบบเทคโนโลยีสารสนเทศ ซึ่งปัจจุบันยังไม่มีการจัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และขาดการบริหารด้านความมั่นคงปลอดภัยระบบเครือข่ายที่เหมาะสม รวมถึงผู้วิจัยเห็นว่าหน่วยงานควรตระหนักและเล็งเห็นถึงความสำคัญของการกำหนดมาตรการหรือนโยบายการรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศดังกล่าว ทั้งนี้ เพื่อรับมือกับภัยคุกคามด้านระบบสารสนเทศที่อาจจะเกิดขึ้น และเพื่อเพิ่มศักยภาพในการรักษาระบบสารสนเทศให้มีความปลอดภัยและพร้อมใช้งาน ด้วยเหตุนี้ ผู้วิจัยจึงเห็นว่าควรพัฒนากรอบนโยบายรักษาความปลอดภัยเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐานสากล ISO/IEC 27001:2013 ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นต้นแบบนโยบายในการรักษาความปลอดภัยของระบบสารสนเทศของสำนักงานจังหวัดพัทลุงขึ้น

วัตถุประสงค์ของการวิจัย

1. พัฒนากรอบนโยบายรักษาความมั่งคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานตามมาตรฐาน ISO/IEC 27001:2013
2. ลดและป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงาน

แนวคิด ทฤษฎี กรอบแนวคิด

การรักษาความปลอดภัยมีจุดประสงค์ เพื่อรักษาความลับ (Confidentiality) ป้องกันการเปลี่ยนแปลงข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) เป็นกระบวนการวิเคราะห์และบริหารความเสี่ยง เฝ้าระวังเหตุการณ์ที่เกิดจากภัยคุกคาม และช่องโหว่หรือจุดอ่อนขององค์การ การติดตั้งระบบรักษาความปลอดภัยให้เหมาะสมกับหน่วยงาน รวมถึงกำหนดนโยบายการรักษาความปลอดภัย การบังคับใช้นโยบาย หรือการหาวิธีปฏิบัติที่เหมาะสมที่สุดสำหรับการรักษาความปลอดภัยข้อมูลขององค์การ (จตุชัย แพงจันทร์และอนุโชต วุฒิพรพงษ์, 2555)

ISO/IEC 27001 เป็นมาตรฐานสากลที่ได้กำหนดแนวทางดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงาน ปัจจุบัน ISO/IEC 27001:2013 มีข้อกำหนดหลักที่ต้องปฏิบัติ 14 โดเมน 114 รายการ (บริษัท ที-เน็ต จำกัด, 2556)

โดยระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) นั้น ประกอบด้วยกระบวนการ PDCA (Plan, Do, Check, Act) ได้แก่ กระบวนการวางแผน (Plan) เป็นการกำหนดรายการควบคุม การประเมินความเสี่ยงตามรายการควบคุม และกำหนดเป็นนโยบายความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยระบบสารสนเทศ กระบวนการลงมือปฏิบัติ (Do) เป็นการลงมือปฏิบัติตามระบบบริหารจัดการความมั่นคงปลอดภัยที่ได้ประเมินไว้เพื่อลดช่องโหว่ที่จะเกิดขึ้น กระบวนการการตรวจสอบ (Check) การประเมินผล ทบทวนสิ่งที่ได้ดำเนินการบริหารจัดการความมั่นคงปลอดภัยไว้ ทบทวนนโยบายด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ ว่าครบถ้วนครอบคลุมทันสมัยกับภัยคุกคามใหม่ ๆ หรือไม่ และการปรับปรุงแก้ไข (Act) ระบบบริหารความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน เป็นการนำผลที่ได้จากการตรวจสอบ มาปรับปรุงให้ดีขึ้น (บรรจง หะรังษี, 2554)

กรกฎ สราญสุทธิ์ (2556) ได้พัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO 27001 ของกรมทรัพยากรน้ำบาดาล พร้อมประเมินความเสี่ยงและจัดทำรายงานผลกระทบ รายงานวิธีการจัดการกับความเสี่ยง โดยดำเนินการวิเคราะห์และประเมินความเสี่ยงระบบความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศของศูนย์ข้อมูล และจัดการความเสี่ยง โดยจัดทำนโยบายด้านความมั่นคงปลอดภัยมาตรฐาน ISO 27001 ปรับปรุงระบบฮาร์ดแวร์และซอฟต์แวร์ และอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยให้ผู้ใช้งาน หลังจากประเมินความเสี่ยงพบว่าหน่วยงานมีความเสี่ยงลดลง และมีข้อเสนอแนะตรวจสอบ ทบทวน และปรับปรุงระบบอยู่เสมอ เพื่อลดความเสี่ยง ช่องโหว่ และโอกาสที่จะถูกโจมตีต่อภัยคุกคามต่าง ๆ

เฉลิม สุวรรณ (2554) ได้จัดทำกรอบนโยบบายด้านความมั่นคงปลอดภัยอ้างอิงตามมาตรฐานสากล ISO/IEC 27001 ของศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี และดำเนินการจัดการความเสี่ยงให้กับระบบสารสนเทศของหน่วยงาน มีแนวทางดำเนินงานคือ ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่ใช้อยู่ปัจจุบัน กับมาตรฐานและข้อกำหนดด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 จากนั้นจัดทำนโยบายความมั่นคงปลอดภัยให้กับหน่วยงาน พร้อมแก้ไข ควบคุมความเสี่ยง โดยการปรับปรุงระบบเครือข่าย เปลี่ยนอุปกรณ์สวิตช์ อุปกรณ์กระจายสัญญาณ ระบบไฟฟ้าสำรอง และติดตั้งโปรแกรมแอนตี้ไวรัส พร้อมทดสอบระบบ และสุดท้ายประเมินความเสี่ยงหลังจากดำเนินโครงการพบว่า ร่างนโยบายความมั่นคงปลอดภัยที่จัดทำขึ้นและการแก้ไขช่องโหว่ต่าง ๆ ทำให้ความเสี่ยงลดลงอยู่ในระดับกลางและต่ำ และมีข้อเสนอแนะให้หน่วยงานขอใบรับรองมาตรฐาน ISO 27001 เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัยน่าเชื่อถือ และให้บริการผู้ป่วยได้อย่างรวดเร็วและมีประสิทธิภาพ

จากการศึกษาแนวคิดการรักษาความปลอดภัยของข้อมูล หลักการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 และแนวทางควบคุมความเสี่ยงโดยเน้นการปรับปรุงระบบและอุปกรณ์ที่เกี่ยวข้องให้มีประสิทธิภาพเพิ่มขึ้นนั้น ผู้วิจัยจึงได้นำหลักการและแนวคิดดังกล่าวมาพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001: 2013 ซึ่งได้ปรับปรุงล่าสุด รวมทั้งติดตั้งอุปกรณ์และระบบรักษาความปลอดภัยเพื่อควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของหน่วยงาน

วิธีดำเนินการวิจัย

งานวิจัยการพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง มีขั้นตอนและวิธีการดำเนินงาน ดังนี้

1. ศึกษาเอกสารต่าง ๆ ที่เกี่ยวข้อง

ศึกษามาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ ISO/IEC 27001:2013 ข้อกฎหมาย พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ศึกษาระบบโครงสร้างเครือข่ายที่มีอยู่เพื่อหาความเสี่ยงด้านความมั่นคงปลอดภัย ตลอดจนศึกษาความรู้ด้านเทคโนโลยีด้านความมั่นคงปลอดภัยระบบเครือข่าย

2. วิเคราะห์และประเมินความเสี่ยง

นำรายการ 14 โดเมน 114 รายการ ตามมาตรฐาน ISO/IEC 27001:2013 มาพิจารณาประเมินหาโอกาสและผลกระทบที่จะเกิดขึ้นกับหน่วยงาน เพื่อนำผลที่ได้ไปประกอบจัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง

จากการประเมินค่าความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 พบว่าหน่วยงานมีจำนวนความเสี่ยงระดับสูง 11 รายการ จำนวนความเสี่ยงระดับปานกลาง 50 รายการ และจำนวนความเสี่ยงระดับต่ำ 53 รายการ ดังแสดงในตารางที่ 1

ตารางที่ 1 สรุปความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนการดำเนินงาน

	ระดับความเสี่ยงสูง	ระดับความเสี่ยงปานกลาง	ระดับความเสี่ยงต่ำ
จำนวน	11	50	53

จากระดับความเสี่ยงดังกล่าวสามารถสรุปผลได้ ดังนี้

1) หน่วยงานขาดนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2) หน่วยงานขาดการกำหนดบทบาทและหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3) หน่วยงานขาดการควบคุมการใช้งานระบบเครือข่ายและสารสนเทศ

4) หน่วยงานขาดการจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

5) หน่วยงานขาดการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับบุคลากร

3. ดำเนินการบริหารจัดการความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27001:2013

เพื่อให้สำนักงานสามารถรับมือกับภัยคุกคามที่จะเกิดขึ้น ผู้วิจัยจึงได้ดำเนินการพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และใช้เป็นแนวทางปฏิบัติให้กับเจ้าหน้าที่ในหน่วยงานเพื่อรักษาความมั่นคงปลอดภัย โดยนำผลลัพธ์ที่ได้จาก ขั้นตอนที่ 1 และ 2 มาเข้าสู่กระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดังนี้

3.1 กระบวนการวางแผน : พัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

กำหนดนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุง ประกอบด้วย การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security) การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control) การควบคุมการใช้งานอินเทอร์เน็ต (Use of the Internet) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

3.2 กระบวนการลงมือปฏิบัติ : ลงมือปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ได้กำหนดไว้ ติดตั้งระบบรักษาความปลอดภัยและกำหนดค่าให้กับอุปกรณ์ พร้อมทดสอบการทำงาน ดังตารางที่ 2

ตารางที่ 2 ความสัมพันธ์นโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศกับการติดตั้งระบบรักษาความปลอดภัย

นโยบาย / การรักษาความปลอดภัย	การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ	การควบคุมการใช้งานอินเทอร์เน็ต	การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
กำหนดโซนบริหารจัดการระบบเครือข่าย	×	×		
จัดทำแผนผังระบบเครือข่าย	×	×		
กำหนดช่องทาง (Port) การเชื่อมต่อ		×		
ป้องกัน IP ภายในจากการมองเห็นของหน่วยงานภายนอก		×		
บริหารจัดการการเข้าถึง		×	×	×
จำกัดสิทธิการเชื่อมต่อ		×	×	×
บันทึกการเข้าออกระบบ		×	×	×
จำกัดปริมาณการใช้งาน		×	×	×
กำหนดการตรวจจับการโจมตี		×	×	×

3.2.1) ปรับปรุงระบบเครือข่าย โดยสำนักงานปลัดกระทรวงมหาดไทยหน่วยงานต้นสังกัดของสำนักงานจังหวัดพัทลุงได้จัดสรรอุปกรณ์ป้องกันและรักษาความปลอดภัยมาติดตั้งให้กับหน่วยงาน ซึ่งผู้วิจัยได้ร่วมดำเนินการปรับปรุงระบบเครือข่ายและกำหนดค่าอุปกรณ์ เพื่อรักษาความปลอดภัยให้กับสำนักงานจังหวัด ดังนี้

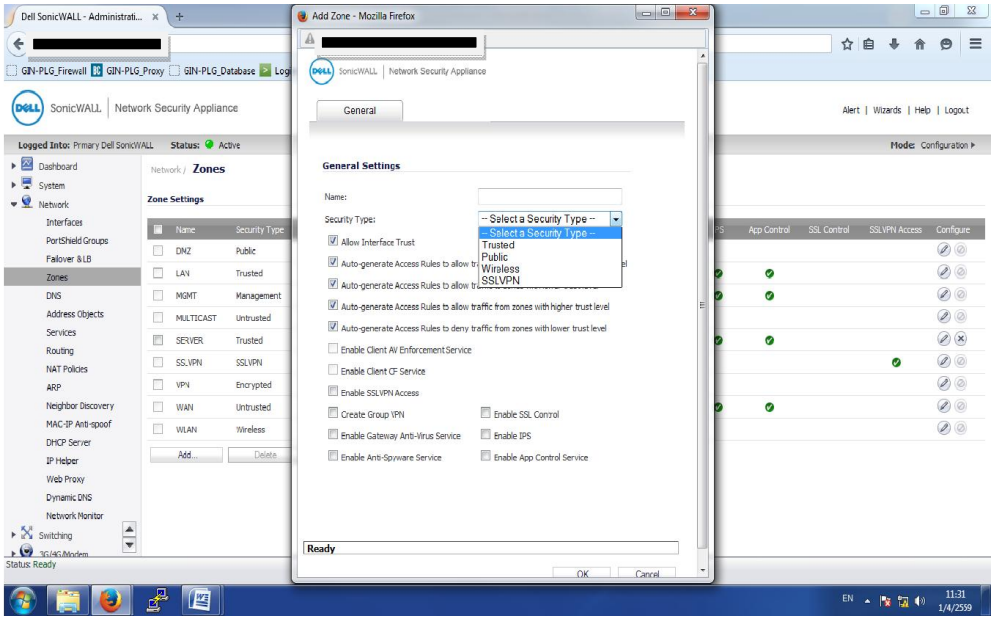
1) ออกแบบระบบเครือข่ายใหม่

2) เพิ่มช่องทางการใช้งานระบบเครือข่ายอินเทอร์เน็ตและเพิ่มความเร็วในการให้บริการอินเทอร์เน็ต จาก 10 Mbps เป็น 50 Mbps

3) ติดตั้งอุปกรณ์และระบบรักษาความปลอดภัยเพิ่มเติม 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

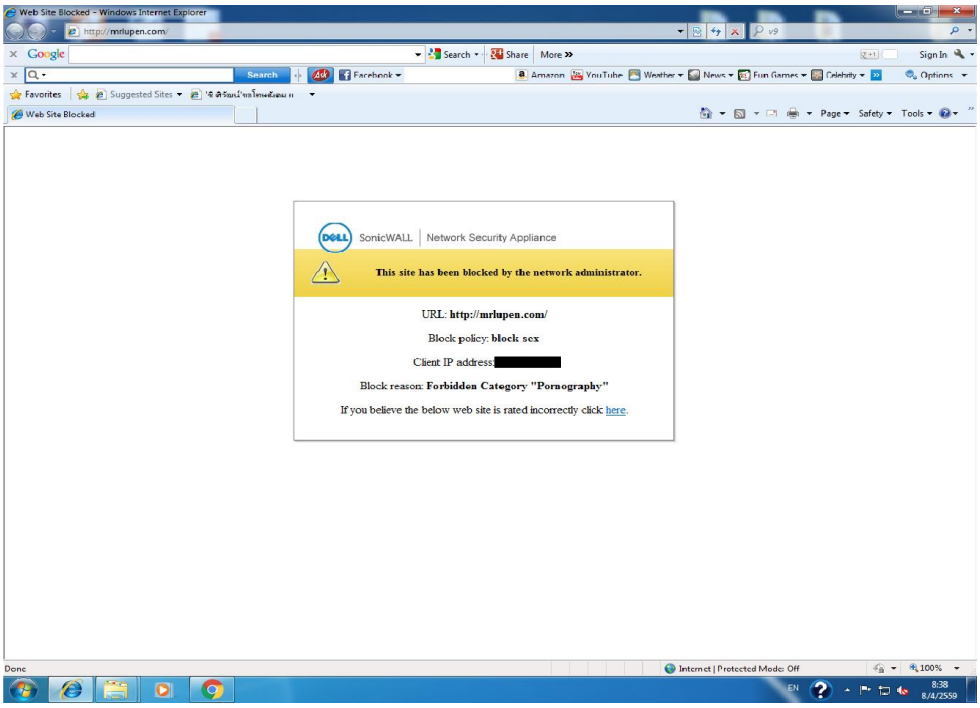
3.2.2) การบริหารจัดการอุปกรณ์ กำหนดค่าการทำงานให้กับอุปกรณ์ป้องกันรักษาความปลอดภัยตามนโยบายที่กำหนด (Dell Inc.,2014) และทดสอบการใช้งาน รายละเอียดดังนี้

1) กำหนดค่าการทำงานให้กับอุปกรณ์ไฟร์วอลล์ อุปกรณ์ตรวจจับการบุกรุกให้สอดคล้องตามนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศที่ได้กำหนดไว้ ได้แก่ การกำหนดค่าการจัดแบ่งโซน การกำหนดการจ่ายไอพี การกำหนดการเข้าถึงเว็บไซต์และแอปพลิเคชัน ฯลฯ ตัวอย่างดังภาพที่ 1



ภาพที่ 1 การกำหนดค่าการแบ่งโซนให้กับระบบเครือข่าย

2) ทดสอบการใช้งาน ประกอบด้วย การทดสอบระบบพิสูจน์ตัวจริง (Authentication) ระบบการรักษาความปลอดภัยในการใช้งานอินเทอร์เน็ต การเข้าถึงเว็บไซต์และแอปพลิเคชันที่กำหนด เพื่อให้มั่นใจว่าเป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้ ตัวอย่างดังภาพที่ 2



ภาพที่ 2 การทำงานของอุปกรณ์ไฟร์วอลล์ในการบล็อกเว็บ

3.3 กระบวนการตรวจสอบ : ประเมินผลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ได้กำหนดไว้

เมื่อวิเคราะห์ค่าความเสี่ยงหลังจากดำเนินการตามนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและติดตั้งอุปกรณ์ระบบรักษาความปลอดภัย ของหน่วยงานตามรายการควบคุม 14 โดเมน ของ ISO/IEC 27001:2013 แล้ว พบว่า ไม่พบรายการความเสี่ยงระดับสูง จำนวนความเสี่ยงระดับปานกลาง 42 รายการ และจำนวนความเสี่ยงระดับต่ำ 72 รายการ ดังแสดงในตารางที่ 3

ตารางที่ 3 สรุปความเสี่ยงด้านเทคโนโลยีสารสนเทศหลังการดำเนินงาน

	ระดับความเสี่ยงสูง	ระดับความเสี่ยงปานกลาง	ระดับความเสี่ยงต่ำ
จำนวน	0	42	72

จากตารางที่ 3 พบว่าความเสี่ยงเหลือเพียงระดับกลางและระดับต่ำ เนื่องจากหลังดำเนินโครงการได้ควบคุมความเสี่ยงระดับสูงให้ลดเหลือระดับกลางและต่ำ โดยการกำหนดกรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศข้างต้น ซึ่งแสดงว่าหน่วยงานสามารถบริหารจัดการเครือข่ายเพื่อป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศได้มากขึ้น

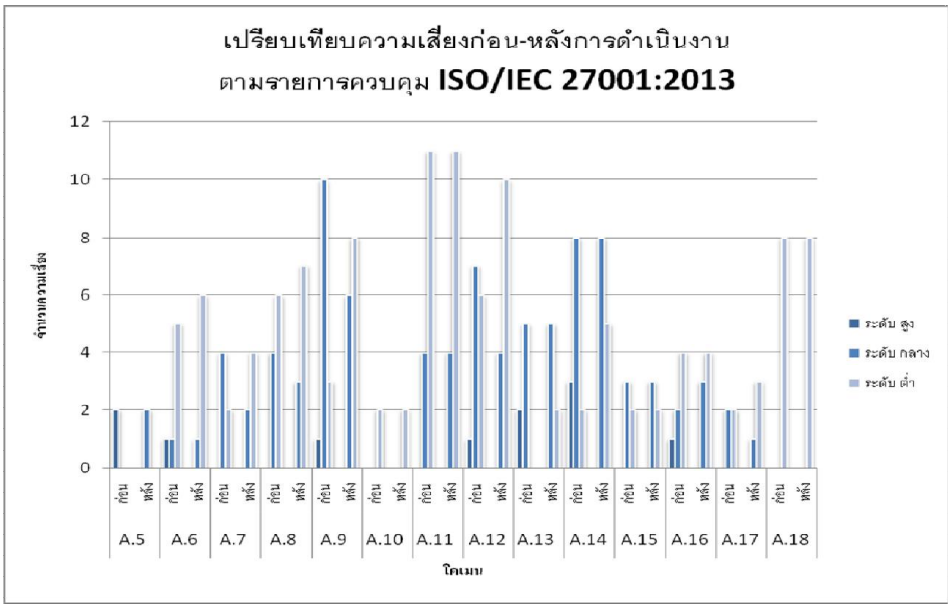
3.4 การปรับปรุงแก้ไข : การปรับปรุงแก้ไขนโยบายความมั่นคงปลอดภัย

จากการประเมินพบว่า เมื่อเปรียบเทียบระดับความเสี่ยงก่อนและหลังดำเนินการ หน่วยงานยังคงมีจำนวนระดับความเสี่ยงปานกลางและต่ำจำนวนมากดังภาพที่ 3 ดังนั้น ผู้วิจัยจึงได้เสนอแนวทางการดำเนินการลดความเสี่ยงให้เหลือน้อยที่สุดเท่าที่จะสามารถดำเนินการได้ดังนี้

1) ผู้บริหารของหน่วยงานต้องประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างเป็นทางการ

2) สำนักงานต้องจัดอบรมชี้แจงนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน

3) สำนักงานต้องทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างต่อเนื่องเพื่อรองรับสถานการณ์ภัยคุกคามที่คาดไม่ถึง เนื่องจากว่าภัยคุกคามที่จะเกิดขึ้นสามารถเปลี่ยนแปลงรูปแบบและความรุนแรงได้ตลอดเวลา



ภาพที่ 3 การเปรียบเทียบผลก่อน-หลังดำเนินการบริหารจัดการด้านความมั่นคงปลอดภัย

สรุปผลการวิจัย

จากการวิเคราะห์และประเมินความเสี่ยงหลังจากดำเนินการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตาม ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง พบว่า การดำเนินการตามกรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงที่พัฒนาขึ้น ทำให้มีแนวทางในการปฏิบัติงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศชัดเจนมากขึ้น รวมทั้งหลังจากการติดตั้งอุปกรณ์และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามนโยบายที่กำหนดขึ้นมาแล้วประเมินและปรับปรุงแก้ไข พบว่า ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศหลังดำเนินโครงการลดลง

อภิปรายผลการวิจัย

การพัฒนากรอบนโยบายและการบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 กรณีศึกษา สำนักงานจังหวัดพัทลุง ได้มีการวิเคราะห์และประเมินความเสี่ยงแล้วพัฒนากรอบนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งถือเป็นมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องและผู้ใช้งานให้เป็นไปในแนวทางเดียวกัน รวมถึงได้ดำเนินการตามแนวคิดการรักษาความปลอดภัยของข้อมูลและหลักการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยได้ติดตั้งอุปกรณ์ไฟร์วอลล์ อุปกรณ์ป้องกันการตรวจจับการบุกรุก เพื่อรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน ให้หน่วยงานสามารถป้องกันความเสี่ยงระบบเทคโนโลยีสารสนเทศได้ ซึ่งจากการประเมินความเสี่ยงหลังจากดำเนินการบริหารจัดการด้านความมั่นคงปลอดภัยดังกล่าว พบว่า ความเสี่ยงที่จะเกิดกับระบบเทคโนโลยีสารสนเทศของหน่วยงานลดลง รวมทั้งหน่วยงานสามารถบริหารจัดการเครือข่ายได้ด้วยตนเองมากขึ้น สอดคล้องตามแนวทางมาตรฐานสากล ISO/IEC 27001:2013 จึงสรุปได้ว่า การบริหารด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานจังหวัดพัทลุง ทำให้

หน่วยงานมีนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานจังหวัดพัทลุงลดลง

ข้อเสนอแนะและการนำผลการวิจัยไปใช้ประโยชน์

จากงานวิจัยนี้ จะเห็นได้ว่าการพัฒนากรอบบริหารความมั่นคงปลอดภัยของสำนักงานจังหวัดพัทลุงตามมาตรฐาน ISO/IEC 27001:2013 ทำให้หน่วยงานสามารถลดความเสี่ยงจากภัยคุกคามระบบสารสนเทศที่จะเกิดกับหน่วยงานได้ ซึ่งงานวิจัยนี้สามารถนำไปใช้เป็นกรณีศึกษาถึงแนวทางของการบริหารจัดการด้านความมั่นคงปลอดภัยในเชิงการนำไปปฏิบัติให้เกิดผล เพื่อรองรับสถานการณ์ที่จะเกิดขึ้นทั้งในปัจจุบันและอนาคต เนื่องจากแนวโน้มสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเพิ่มสูงขึ้น และเกิดขึ้นในรูปแบบใหม่ตลอดเวลา ดังนั้น หน่วยงานทั้งภาครัฐและภาคเอกชนจะต้องเตรียมรับมือกับเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่คาดไม่ถึง ต้องตระหนักถึงความสำคัญในการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างจริงจัง โดยเฉพาะผู้บริหารหน่วยงานจะต้องมีวิสัยทัศน์ในการหาแนวทางป้องกันและรับมือกับภัยคุกคามด้านเทคโนโลยีสารสนเทศที่จะเกิดขึ้น โดยต้องให้ความสำคัญในการจัดทำนโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ และจะต้องทำอย่างต่อเนื่องตามกระบวนการการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ เนื่องจากความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือภัยคุกคามระบบสารสนเทศเกิดขึ้นในรูปแบบใหม่ตลอดเวลา

เอกสารอ้างอิง

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

จตุพร แพงจันทร์ และอนุโชต วุฒิพรพงษ์. (2555). **เจาะระบบ Network.** นนทบุรี: บริษัท ไอดีซี พรีเมียร์ จำกัด.

เฉลิม สุวรรณ. (2554). **การรักษาความมั่นคงปลอดภัยสารสนเทศ: กรณีศึกษาศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี.** สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมเครือข่าย มหาวิทยาลัยเทคโนโลยีมหานคร.

บรรจง หะรังษี.(2554). **หัวใจหลักของกระบวนการบริหารด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001** (online). http://www.tnetsecurity.com/content_audit/pdca_def.pdf, 5 ธันวาคม 2558

บริษัท ที-เน็ต จำกัด .(2556).**มาตรฐาน ISO/IEC 27001:2013** (online). http://www.tnetsecurity.com/content_audit/27001-2013.pdf , 30 ธันวาคม 2558

Dell Inc.(2014). **SonicOS 6.2.1 Administrator Guide(online).** https://support.software.dell.com/sonicwall-supermassive-9000-series/release-notes-guides, 1 ตุลาคม 2558