กรอบงานสำหรับพอร์ทัลข้อมูลเรื่องความมั่นคงของเว็บไซต์สำหรับเจ้าของกิจการขนาดกลางและขนาดย่อมของไทย

นายเอกฉันท์ รัตนเลิศนุสรณ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2554

FRAMEWORK FOR INFORMATION PORTAL ON WEBSITE SECURITY FOR OWNER OF THAI SMALL AND MEDIUM ENTERPRISES

Mr. Ekkachan Rattanalerdnusorn

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2011

หัวข้อวิทยานิพนธ์	กรอบงานสำหรับพอร์ทัลข้อมูลเรื่องความมั่นคงของเว็บไซต์สำหรับเจ้าของกิจการขนาดกลางและขนาดย่อมของไทย
โดย	นาย เอกฉันท์ รัตนเลิศนุสรณ์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ มัณฑนา ปราการสมุทร)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร. โกเมน พิบูลย์โรจน์)

เอกฉันท์ รัตนเลิศนุสรณ์ : กรอบงานสำหรับพอร์ทัลข้อมูลเรื่องความมั่นคงของเว็บไซต์สำหรับเจ้าของกิจการขนาดกลางและขนาดย่อมของไทย. (FRAMEWORK FOR INFORMATION PORTAL ON WEBSITE SECURITY FOR OWNER OF THAI SMALL AND MEDIUM ENTERPRISES) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: อ. ดร.ยรรยง เต็งอำนวย, 77 หน้า.

ปัจจุบันเว็บไซต์ของบริษัทขนาดกลางและขนาดย่อมของไทย (เอสเอ็มอี - SME) มีจำนวนมาก ซึ่งบริษัทเอสเอ็มอีเหล่านี้มีข้อจำกัดในเรื่องบุคลากร งบประมาณ และการรับรู้ข้อมูลข่าวสาร แม้ความรู้เกี่ยวกับความมั่นคงของเว็บไซต์มีอยู่มากแต่ก็มีความซับซ้อนเข้าใจยาก จึงมีแนวคิดในการนำความรู้ทางด้านความมั่นคงสำหรับเว็บไซต์มานำเสนอในรูปแบบสร้างเป็นเว็บพอร์ทัลในรูปแบบที่เข้าใจได้ง่ายเหมาะกับเจ้าของกิจการ ซึ่งจะช่วยในการกำกับดูแลเจ้าหน้าที่เทคนิคของบริษัทในการทำให้เว็บไซต์มีความมั่นคงในระดับพื้นฐานได้โดยเสียค่าใช้จ่ายต่ำ

งานวิจัยนี้ มุ่งเน้นการจัดหมวดหมู่เนื้อหาด้านความมั่นคงเว็บไซต์ และนำเสนอเนื้อหาความรู้พื้นฐานในเว็บไซต์ พร้อมทั้งสำรวจและสอบถามความคิดเห็นของเจ้าของกิจการเอสเอ็มอีที่ได้อ่านเนื้อหาในเว็บไซต์

ภาควิชา…วิศวกรรมคอมพิวเตอร์…… ลายมือชื่อนิสิต……

สาขาวิชา…วิทยาศาสตร์คอมพิวเตอร์….. ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์……

ปีการศึกษา…2554……..

5170538321 : MAJOR COMPUTER SCIENCE
KEYWORDS : WEB SECURITY / SME OWNER / EASE OF USE

EKKACHAN RATTANALERDNUSORN : FRAMEWORK FOR INFORMATION PORTAL ON WEBSITE SECURITY FOR OWNER OF THAI SMALL AND MEDIUM ENTERPRISES. ADVISOR : YUNYONG TENG-AMNUAY, Ph.D, 77 pp.

Today, the number of websites of Thai small and medium enterprises (SME) increases rapidly. Although there are many knowledge resources for building secure web, SMEs lack the adequate knowledge to secure their website because information is too technical. Budget restrictions, limited personnel, and inattention of owner also add to this. This research suggests a framework for information portal on web security for SMEs owners to supervise technical staff to secure their website appropriately and inexpensively.

This thesis focuses on classifying the various topics of computer security and modifies the necessary contents for easy understanding. Furthermore, a questionnaire was made collect opinions and comments from SMEs owners.

Department: Computer Engineering. Student's Signature…….
Field of Study: Computer Science… Advisor's Signature……..……..
Academic Year:..2011……..

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งจาก อ.ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษา ซึ่งท่านได้ให้คำแนะนำและให้ข้อคิดเห็นต่างๆที่เป็นประโยชน์อย่างยิ่งต่อการวิจัย และช่วยตรวจแก้ไขในส่วนที่บกพร่องต่างๆ ทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วง

ขอขอบพระคุณ รองศาสตราจารย์ มัณฑนา ปราการสมุทร ดร. โกเมน พิบูลย์โรจน์ ประธานกรรมการและกรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำแนะนำในการแก้ไขวิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น และขอขอบพระคุณ คุณภาณุภณ พสุชัยกุล คุณวโรรส โรจนะ คุณธันยวัชร ผลดี คุณสุพจน์ พฤกษะวัน คุณทรงเกียรติ หลิ่มศิริ คุณกมลวรรณ เอี้ยวซิโป คุณภัสสราภรณ์ สลักคำ คุณทิวากร แตงอ่อน คุณทรงศักดิ์ ประสิทธิวิริยะกุล คุณไตรยุทธ ไตรเมศวร์ คุณปฏิญญา อักษร รวมถึงสมาคมศิษย์เก่าวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยและสถาบันพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมที่ช่วยเหลือให้งานวิจัยนี้ผ่านไปได้ด้วยดี

ท้ายนี้ผู้วิจัยกราบขอบพระคุณ บิดา มารดา ที่สนับสนุนและให้กำลังใจตลอดมา หากมีข้อผิดพลาดประการใด ผู้วิจัยขออภัยมา ณ ที่นี้ด้วย

สารบัญ

หน้า

บทที่ หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเว็บไซต์สำหรับบริษัทขนาดกลางและขนาดย่อมมีจำนวนมากขึ้นโดยในหลักการแล้วบริษัทขนาดเล็กเหล่านี้ เมื่อมีเว็บไซต์ของตัวเองจะเป็นหนึ่งไซต์หรือหนึ่งหน้าจอเทียบเท่ากับบริษัทขนาดใหญ่ ดังนั้นแม้ความเสียหายต่อไซต์จะไม่มากแต่จำนวนไซต์อันมหาศาลจะก่อให้เกิดปัญหาด้านความมั่นคงและเป็นปัจจัยเสี่ยงต่อธุรกิจพาณิชย์อิเล็กทรอนิกส์ของประเทศได้เป็นอย่างมาก ซึ่งบริษัทเหล่านี้ไม่มีกำลังมากเพียงพอในการจ้างผู้เชี่ยวชาญโดยตรงทางด้านความมั่นคงเพื่อการดูแลและอาจมีเจ้าหน้าที่ทางเทคนิคที่มีความรู้คอมพิวเตอร์อยู่บ้างแต่ไม่เชี่ยวชาญด้านความมั่นคง อีกทั้งค่าใช้จ่ายเหล่านี้มีราคาสูง ดังนั้นจึงควรมีที่ให้คำปรึกษาแก่เจ้าของกิจการเพื่อให้เขาตระหนักและสามารถกำกับดูแลด้านความมั่นคงได้ด้วยตนเอง

เจ้าของบริษัทขนาดกลางและขนาดย่อมที่ดำเนินกิจการมานาน โดยทั่วไปเป็นผู้ที่มีอายุมากและไม่ใช่นักคอมพิวเตอร์ ดังนั้นจึงเป็นเรื่องยากที่จะปรับตัวศึกษาทำความเข้าใจและสามารถกำกับดูแลให้พนักงานคอมพิวเตอร์ในบริษัทรักษาความมั่นคงของเว็บไซต์ของตนเองได้

ความรู้เกี่ยวกับความมั่นคงของเว็บไซต์มีอยู่มากมาย แต่ความรู้เหล่านั้นมีคำศัพท์เทคนิคจำนวนมากและเนื้อหามีความซับซ้อนเข้าใจยาก ดังนั้นจึงควรมีกรอบวิธีในการกลั่นกรองความรู้ในด้านความมั่นคงของเว็บไซต์ให้เหมาะสมกับเจ้าของกิจการ

ด้วยเหตุดังกล่าวเหล่านี้ จึงมีแนวคิดว่าควรนำความรู้ทางด้านความมั่นคงสำหรับเว็บไซต์มานำเสนอในรูปแบบเว็บพอร์ทัลในรูปแบบที่เข้าใจได้ง่าย หากมีพอร์ทัลที่เจ้าของบริษัทใช้หาความรู้ได้จะทำให้เจ้าของกิจการสามารถกำกับดูแลเจ้าหน้าที่เทคนิคของบริษัทในการทำให้เว็บไซต์ของทางบริษัทมีความมั่นคงในระดับพื้นฐานได้โดยเสียค่าใช้จ่ายต่ำ

1.2 วัตถุประสงค์ของงานวิจัย

เพื่อกำหนดกรอบวิธีในการกลั่นกรองและการนำเสนอความรู้ในด้านความมั่นคงปลอดภัยของเว็บไซต์ขึ้นเป็นพอร์ทัลข้อมูลให้เข้าใจได้ง่ายเหมาะกับเจ้าของกิจการธุรกิจขนาดกลางและขนาดย่อม

1.3 ขอบเขตการวิจัย

1) นำเสนอและจัดหมวดหมู่เรียบเรียงประเด็นการรักษาความมั่นคงของเว็บไซต์ที่มีอยู่ในปัจจุบันในรูปแบบซึ่งสามารถเข้าใจได้อย่างง่ายๆ โดยอาศัยแนวทางจากแหล่งข้อมูล
   - เว็บไซต์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของเว็บไซต์โดยตรงเช่น www.sans.org , www.cert.org , www.owasp.org เป็นต้น
   - หนังสือเกี่ยวกับการรักษาความปลอดภัยของเว็บไซต์
   - การประชุมวิชาการและวารสารที่เกี่ยวข้อง
2) ศึกษาเกี่ยวกับความมั่นคงในส่วนของเว็บไซต์เท่านั้น ซึ่งจะเน้นกลุ่มวิสาหกิจขนาดกลางและขนาดย่อมที่ได้ดำเนินกิจการมานาน โดยกลุ่มวิสาหกิจเหล่านี้มีเว็บเซิร์ฟเวอร์เป็นของตนเองและยังคงประสบปัญหาเกี่ยวกับความมั่นคงเว็บไซต์
3) นำเสนอวิธีการแสดงผลผ่านต้นแบบ (เว็บไซต์) ซึ่งไม่ได้เน้นในด้าน ความสวยงามของเว็บไซต์แต่เน้นในด้านเนื้อหาที่เข้าใจได้ง่ายและการนำเสนอให้เหมาะกับเจ้าของบริษัทขนาดกลางและขนาดย่อม และเจ้าหน้าที่คอมพิวเตอร์ของบริษัท

1.4 ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

1) มีกรอบงานในการกลั่นกรองความรู้ด้านความมั่นคงเว็บไซต์ในรูปแบบเข้าใจง่ายสำหรับเจ้าของกิจการ และบุคคลที่ไม่มีพื้นฐานทางด้านเทคโนโลยีสารสนเทศ
2) ได้ต้นแบบเว็บพอร์ทัลด้านความมั่นคงเว็บไซต์ให้กับเจ้าของบริษัทขนาดกลางและขนาดย่อม
3) ช่วยลดปัญหาด้านความมั่นคงเว็บไซต์ของบริษัทขนาดเล็กที่มีอยู่จำนวนมากให้น้อยลงและลดความเสี่ยงต่อธุรกรรมอิเล็กทรอนิกส์ของประเทศ

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ลักษณะสมบัติของกิจการขนาดกลางและขนาดย่อม

ในปัจจุบันจำนวนวิสาหกิจขนาดกลางและขนาดย่อมมีจำนวนเพิ่มขึ้นทุกปี จากบทความของ "รายงานสถานการณ์วิสาหกิจขนาดกลางและขนาดย่อม ประจำปี 2553" ของสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว) [1] พบว่าสัดส่วนของจำนวนวิสาหกิจขนาดกลางและขนาดย่อมมีจำนวนทั้งสิ้นถึงร้อยละ 99.6 จากจำนวนวิสาหกิจทั้งหมด

จากข้อมูลของ Institute for Small and Medium Enterprises Development [2] พบว่าวิสาหกิจขนาดกลางและขนาดย่อมมีข้อจำกัดในเรื่องบุคลากร เรื่องงบประมาณและการรับรู้ข่าวสารข้อมูล เมื่อแรงงานมีฝีมือและมีความชำนาญมากขึ้นจะย้ายออกไปทำงานในวิสาหกิจที่มีขนาดใหญ่ขึ้นและผลตอบแทนที่ดีกว่า และส่วนใหญ่ใช้เทคนิคการผลิตไม่ซับซ้อนเนื่องจากการลงทุนต่ำและผู้ประกอบการและพนักงานขาดความรู้พื้นฐานที่รองรับเทคนิควิชาที่ทันสมัย

สอดคล้องกับบทความ "SMEs and Knowledge Requirements for Operating Hacker and Security Tools" [3] ที่พบว่าวิสาหกิจขนาดกลางและขนาดย่อมสนใจเรื่องการประกอบการธุรกิจมากกว่าจะคำนึงถึงความมั่นคงของข้อมูล และวิสาหกิจเหล่านั้นไม่มีพนักงานและเวลาเพียงพอที่จะทำงานในส่วนนี้ อีกทั้งพนักงานยังขาดการอบรมความรู้และการแสวงหาความรู้หรือเทคโนโลยีเกี่ยวกับความปลอดภัย โดยวิสาหกิจส่วนมากไม่รู้ว่าจะเริ่มต้นอย่างไรเพื่อให้เกิดความมั่นคงในเทคโนโลยีสารสนเทศและคิดว่าวิสาหกิจขนาดกลางและขนาดย่อมไม่ได้เป็นเป้าหมายของการจู่โจมของเหล่านักเจาะระบบ

การใช้บริการของหน่วยงานภายนอกที่มีความเชี่ยวชาญในด้านความมั่นคงในเทคโนโลยีสารสนเทศหรือที่เรียกว่า outsourcing แม้หน่วยงานเหล่านั้นจะมีเครื่องมือ มีความพร้อมและความเชี่ยวชาญสูงแต่ค่าใช้จ่ายในการให้บริการสูงเช่นกันและควรที่จะกำหนดขอบเขตการดำเนินงานของหน่วยงานเหล่านั้นให้ชัดเจน ซึ่งบทความ "OUTSOURCING ICT SECURITY TO MSSP: ISSUES AND CHALLENGES FOR THE DEVELOPING WORLD" [4] และ "Information Security Management Outsourcing" [5] ได้กล่าวถึงข้อดีและข้อเสียเกี่ยวกับการใช้บริการหน่วยงานภายนอกในการดูแลระบบความมั่นคงทางด้านเทคโนโลยีสารสนเทศ ซึ่งข้อดีในการเลือกใช้บริการของหน่วยงานภายนอกเหล่านั้นมีดังนี้

1) หน่วยงานภายนอกเหล่านั้นจะมีเครื่องมือ มีความพร้อมและความเชี่ยวชาญที่มากกว่า
2) หากไม่ใช้บริการจากหน่วยงานภายนอกแล้วบริษัทต้องจัดทีมในการดูแลความมั่นคงในด้านเทคโนโลยีสารสนเทศ ซึ่งจำเป็นต้องมีการอบรมความรู้ให้กับพนักงานในด้านนี้
3) ไม่จำเป็นต้องจ้างพนักงานที่เชี่ยวชาญด้านความมั่นคงเกี่ยวกับเทคโนโลยีสารสนเทศ ซึ่งบริษัทจะต้องจ่ายค่าตอบแทนที่สูงและเหมาะสมให้กับพนักงานเหล่านั้น

สำหรับข้อควรระวังเกี่ยวกับการใช้บริการหน่วยงานภายนอกคือ

1) ข้อมูลไปตกกับมือของคนภายนอก
2) พึ่งพาหน่วยงานภายนอกมากเกินไป
3) ขอบเขตการทำงาน (service-level agreement) มักไม่ชัดเจน
4) มีค่าใช้จ่ายสูง

2.2 ลักษณะการโจมตีเว็บไซต์

ข้อมูลจาก Web Application Security Consortium [6] จำแนกต้นเหตุการจู่โจมของเว็บไซต์มาจาก 6 ส่วนคือ การยืนยันตัวบุคคล (Authentication) การให้สิทธิใช้งาน (Authorization) การจู่โจมทางฝั่งลูกข่าย (Client-side Attacks) การประมวลผลของคำสั่ง (Command Execution) การเปิดเผยข้อมูล (Information Disclosure) และ การโจมตีแบบลอจิคอล (Logical Attacks) โดยช่องโหว่ที่ถูกพบบ่อยมาจากเทคนิค Injection, Cross-Site Scripting และ Broken Authentication and Session Management เช่นเดียวกับ OWASP [7] ได้วิเคราะห์ช่องโหว่ของเว็บแอพลิเคชันที่พบในปี 2010 จาก "MITRE Vulnerability Trends" โดยรูปที่ 2-1 แสดงถึงช่องโหว่ 10 อันดับแรก สำหรับเทคนิค Security Misconfiguration และ Unvalidated Redirects and Forwards เป็นลักษณะการโจมตีที่ผู้บุกรุกได้อาศัยช่องโหว่จากความผิดพลาดของการกำหนดค่าเริ่มต้นในเซอร์ฟเวอร์และการส่งต่อที่หน้าเว็บ ซึ่งแนวโน้มการคุกคามนี้จะมีสูงมากขึ้น จึงถูกจัดให้เป็นภัยคุกคามอันดับที่ 6 และ 10

OWASP Top 10 – 2010 (New)
A1 – Injection
A2 – Cross-Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross-Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
A10 – Unvalidated Redirects and Forwards (NEW)

รูปที่ 2-1 แสดงช่องโหว่ของเว็บแอพลิเคชันที่ถูกพบในปี 2010

โดยข้อมูลจากเว็บ www.zone-h.org [8] มีการเปิดเผยว่าเว็บไซต์ของบริษัทฯในประเทศไทยถูกโจมตีสำเร็จทั้งสิ้น 1,153 ครั้ง นับตั้งแต่เดือนตุลาคม ปี 2008 ถึงปี 2010 และจากข้อมูลของบริษัทโกลบอลเทคโนโลยีอินทิเกรเทด [9] พบว่ามีเว็บไซต์ของไทยที่ถูกโจมตีถึงปัจจุบันแล้วทั้งสิ้น 12,360 เว็บไซต์ เป็นเว็บไซต์ของหน่วยงานราชการ (.go.th) มากที่สุดถึง 5,190 เว็บไซต์ คิดเป็น 41.99% รองลงมาคือ เว็บไซต์ของสถานศึกษา (.ac.th) จำนวน 2,659 เว็บไซต์ คิดเป็น 21.51% และ เว็บไซต์ขององค์กรเอกชน (.co.th) จำนวน 2,536 โดเมน (20.52%)

HACK NOTES Web Security Portable Reference [10] และบทความ "Guidelines on Securing Public Web Servers" ของ National Institute of Standards and Technology [11] ได้กล่าวว่าเว็บไซต์จะมีความมั่นคงจำเป็นต้องมีโครงสร้างของระบบเครือข่ายที่มีกลไกการป้องกันการโจมตีจากภายนอกและในส่วนของเว็บเซอร์ฟเวอร์ต้องเก็บรวบรวมรายละเอียดต่างๆ ของระบบปฏิบัติการและซอฟท์แวร์และปรับปรุงช่องโหว่ที่เกิดขึ้น รวมทั้งต้องป้องกันการโจมตีที่เกิดขึ้นในส่วนเนื้อหาเว็บไซต์ และต้องหมั่นตรวจสอบอย่างสม่ำเสมอ

2.3 การทำเว็บไซต์สำหรับผู้สูงอายุ

การที่เจ้าของกิจการเป็นผู้มีอายุ บทความของ เคอร์เนียวาน และ ซาฟีรีส [12] ได้เสนอแนวทางการทำเว็บไซต์ให้เหมาะกับผู้สูงอายุ โดยได้รวบรวม guidelines จำนวนหลายร้อยบทความ เพื่อทำการจัดกลุ่มของกฎเกณฑ์เป็นหมวดหมู่ใหม่ซึ่งมีความชัดเจนเข้าใจได้ง่ายและไม่สับสน โดยได้ทดสอบหมวดหมู่ของกฎเกณฑ์เหล่านั้นกับเว็บไซต์สองเว็บซึ่งเป็นเว็บที่ออกแบบให้กับผู้สูงอายุใช้งาน คือเว็บ www.elderhostel.org/welcome/home.asp และ www.nsclc.org ซึ่งรูปที่ 2-2 เป็นหน้าแรกของ www.nsclc.org

รูปที่ 2-2 แสดงหน้าจอของเว็บ www.nsclc.org

โดยในบทต่อไปจะกล่าวถึงแนวทางการวิจัยซึ่งแสดงภาพรวมและขั้นตอนในการวิจัย ซึ่งแสดงกรรมวิธีเพื่อจัดเนื้อหาที่เหมาะกับเจ้าของกิจการ/บริษัท พร้อมทั้งการนำแนวทางการทำเว็บไซต์ผู้สูงอายุมาประยุกต์เพื่อทำเว็บพอร์ทัลและแนวทางออกแบบคำถามในแบบสอบถามเพื่อให้เจ้าของกิจการ/บริษัทอ่านและประเมินการใช้งานเว็บพอร์ทัล

บทที่ 3

แนวทางการวิจัย

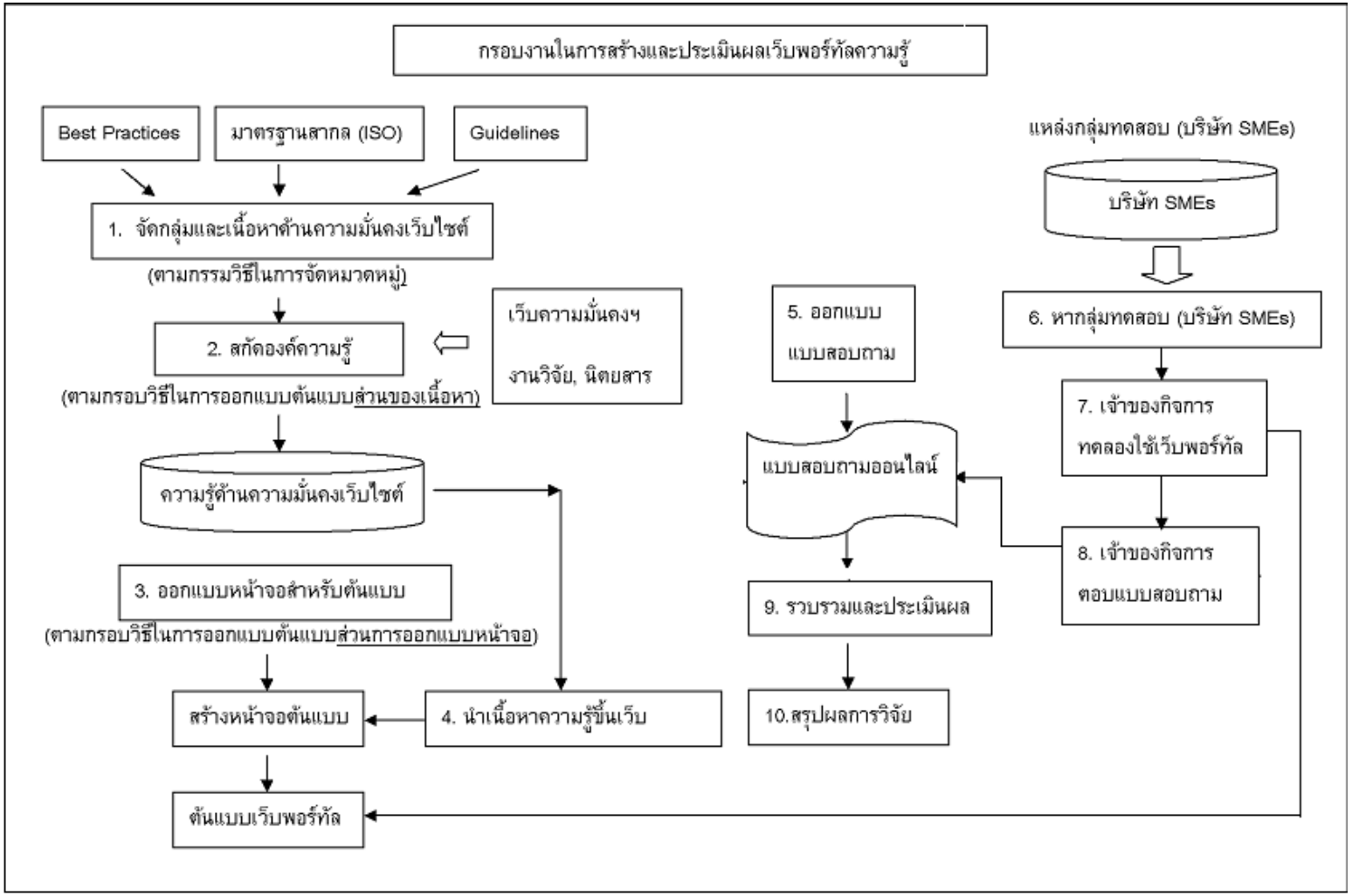
สำหรับกรอบงานในการสร้างและประเมินผลเว็บพอร์ทัลสำหรับให้ความรู้กับเจ้าของกิจการหรือบริษัทขนาดกลางและขนาดย่อมของไทย รูปที่ 3-1 แสดงภาพรวมของการวิจัยโดยมีขั้นตอนในการวิจัย 9 ขั้นตอน โดยเริ่มตั้งแต่การจัดกลุ่มหัวข้อเนื้อหา การออกแบบและสร้างเว็บต้นแบบ การออกแบบแบบสอบถาม การหากลุ่มทดสอบ และการประเมินผล ซึ่งในแต่ละขั้นตอนมีรายละเอียดดังตารางที่ 3-1

ตารางที่ 3-1 แสดงรายละเอียดการดำเนินการวิจัย

ขั้นที่	การดำเนินงาน	รายละเอียดแต่ละขั้นตอน
1	จัดกลุ่มและเนื้อหาด้านความมั่นคงเว็บไซต์	● หาแหล่งอ้างอิงมาตรฐานสากลและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับเจ้าของกิจการ (หรือผู้บริหารระดับสูง) ● นำข้อแนะนำและมาตรการที่สอดคล้องกันมาจัดหมวดหมู่ใหม่ให้เหมาะกับเจ้าของกิจการตามกรรมวิธีในการจัดหมวดหมู่ (ในหัวข้อ 3.1)
2	สกัดองค์ความรู้	● นำเนื้อหาความรู้เกี่ยวกับความมั่นคงปลอดภัยของเว็บไซต์ที่ตรงตามหมวดหมู่ที่ได้จากขั้นตอนแรก มาถอดความหมายที่เข้าใจได้ง่ายตามแนวทางปฏิบัติในการออกแบบเว็บต้นแบบในส่วนของเนื้อหา (ในหัวข้อ 3.2.2)
3	ออกแบบหน้าจอสำหรับต้นแบบ (ในรายละเอียดการออกแบบเว็บต้นแบบ จะกล่าวเพิ่มเติมในบทที่ 4 ต่อไป)	● เลือกใช้โปรแกรมระบบจัดการเนื้อหาเพื่อสร้างเว็บต้นแบบโดยอาศัยกรอบวิธีและแนวทางปฏิบัติในการออกแบบระบบต้นแบบในส่วนการออกแบบหน้าจอ (ในหัวข้อ 3.2.1) ● ออกแบบโครงสร้างรวมของเว็บไซต์ (sitemap)

ตารางที่ 3-1 แสดงรายละเอียดการดำเนินการวิจัย (ต่อ)

ขั้นที่	การดำเนินงาน	รายละเอียดแต่ละขั้นตอน
4	นำเนื้อหาความรู้ขึ้นเว็บต้นแบบ	● การนำเนื้อหาความรู้ขึ้นสู่เว็บไซต์ได้ใช้ความสามารถของโปรแกรมระบบจัดการเนื้อหา (content management system) ในการควบคุมและจัดการเนื้อหาเข้าสู่เว็บไซต์
5	ออกแบบแบบสอบถาม	● อาศัยกรรมวิธีในการออกแบบ แบบสอบถาม ซึ่งได้อธิบายขั้นตอนในการออกแบบและการสำรวจในบทที่ 5 (ในหัวข้อ 5.1 การออกแบบสอบถามออนไลน์)
6	หากลุ่มทดสอบ	● โดยงานวิจัยนี้ได้รับความช่วยเหลือจากสถาบันพัฒนาวิสาหกิจขนาดกลางและขนาดย่อม และสมาคมศิษย์เก่าคณะวิศวกรรมศาสตร์จุฬาลงกรณ์มหาวิทยาลัยในการติดต่อประชาสัมพันธ์ให้กับเจ้าของกิจการ/บริษัทให้เข้าชมเว็บและร่วมประเมินเว็บต้นแบบ
7	เจ้าของกิจการทดลองใช้เว็บพอร์ทัล	● โดยใช้เวลาประมาณสองเดือนเพื่อให้เจ้าของกิจการ/บริษัทเข้าชมและร่วมทำแบบประเมินเว็บต้นแบบ
8	เจ้าของกิจการตอบแบบสอบถาม	● โดยใช้เวลาประมาณสองเดือนเพื่อให้เจ้าของกิจการ/บริษัทเข้าชมและร่วมทำแบบประเมินเว็บต้นแบบ
9	รวบรวมและประเมินผล	● เก็บรวบรวมข้อมูลของกลุ่มตัวอย่างจากฐานข้อมูลของเว็บไซต์ ● ตรวจสอบความสมบูรณ์ของข้อมูลก่อนนำมาวิเคราะห์ข้อมูลโดยหาค่าเฉลี่ยและแสดงออกเป็นกราฟแนวโน้มและสัดส่วนของระดับคะแนน (ผลของการวิจัยแสดงในบทที่ 6)



รูปที่ 3-1 แสดงกรอบงานในการวิจัย

3.1 กรรมวิธีในการจัดหมวดหมู่

ภาพรวมของกรรมวิธีในการจัดหมวดหมู่ได้แสดงไว้ในรูปที่ 3-2 โดยหัวข้อที่ 3.1.1 ได้กล่าวถึงแหล่งอ้างอิงมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงเว็บไซต์ในงานวิจัยนี้ และในหัวข้อที่ 3.1.2 ได้กล่าวถึงการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์

3.1.1 แหล่งอ้างอิงมาตรฐานความมั่นคงเว็บไซต์

แหล่งอ้างอิงมาตรฐานสากลและแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับเจ้าของกิจการ (หรือผู้บริหารระดับสูง) มีดังนี้

1) มาตรฐานในการบริหารการรักษาความมั่นคงปลอดภัย (มาตรฐาน ISO/IEC 27001:2005) [13, 14] เพื่อให้กลุ่มหมวดหมู่ที่พัฒนาขึ้นสอดคล้องกับมาตรฐานสากล ซึ่งมาตรฐานดังกล่าวได้มีการกำหนดมาตรการควบคุม 133 รายการในหัวข้อหลัก 11 ข้อ
2) เอกสารเผยแพร่ “แนวทางปฏิบัติด้านความมั่นคงบนเว็บไซต์” ของ National Institute of Standards and Technology (U.S. Department of Commerce) Version 2 [11]
3) เอกสารเผยแพร่ “แนวทางปฏิบัติด้านความมั่นคงบนเว็บไซต์” (Web Server Security Guidelines) ของ Indian Computer Emergency Response Team (CERT-In) [15]
4) เอกสารเผยแพร่ “แนวทางปฏิบัติด้านความมั่นคงสำหรับผู้จัดการระดับสูง” (COMMON SENSE GUIDE FOR SENIOR MANAGERS) ของ Internet Security Alliance Officers [16]

3.1.2 เปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์

1) นำมาตรการควบคุมในการบริหารการรักษาความมั่นคงปลอดภัย (มาตรฐาน ISO/IEC 27001:2005) ทั้งหมด 133 รายการใน 11 ข้อ มาเปรียบเทียบกับแนวทางด้านความมั่นคงเว็บไซต์ และแนวทางปฏิบัติด้านความมั่นคงสำหรับผู้จัดการระดับสูงโดยคัดเลือกเฉพาะมาตรการที่ถูกกล่าวถึงในแนวทางปฏิบัติด้านความมั่นคงเว็บไซต์หรือด้านความมั่นคงสำหรับผู้จัดการระดับสูงอย่างน้อยหนึ่งแนวทางปฏิบัติ จึงทำให้ได้ 6 กลุ่มหัวข้อมาตรการความมั่นคง ซึ่งประกอบด้วย 28 มาตรการควบคุม (ตามภาคผนวก ก.) สำหรับหัวข้อหลักในมาตรฐาน ISO27001 มีดังนี้

1.1) นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Security Policy)

1.2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organizational of Information Security)

1.3) การบริหารจัดการทรัพย์สินขององค์กร (Assets management)

1.4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

1.5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

1.6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and operations management)

1.7) การควบคุมการเข้าถึง (Access control)

1.8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

1.9) การบริหารจัดการสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

1.10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

1.11) การปฏิบัติตามข้อกำหนด (Compliance)

2) นำมาตรการควบคุมมาจัดกลุ่มหัวข้อใหม่ โดยยุบหมวดหมู่ที่ไม่มีมาตรการควบคุมและรวมมาตรการที่เหลือในบางหมวดหมู่เข้าด้วยกันเพื่อความกระชับ

3) จะได้กลุ่มหัวข้อมาตรการควบคุมที่สอดคล้องสำหรับเจ้าของกิจการ/บริษัท จำนวน 6 หัวข้อ ได้แก่

3.1) กลุ่มแผนและนโยบายการปฏิบัติด้านความมั่นคงเว็บไซต์

3.2) กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

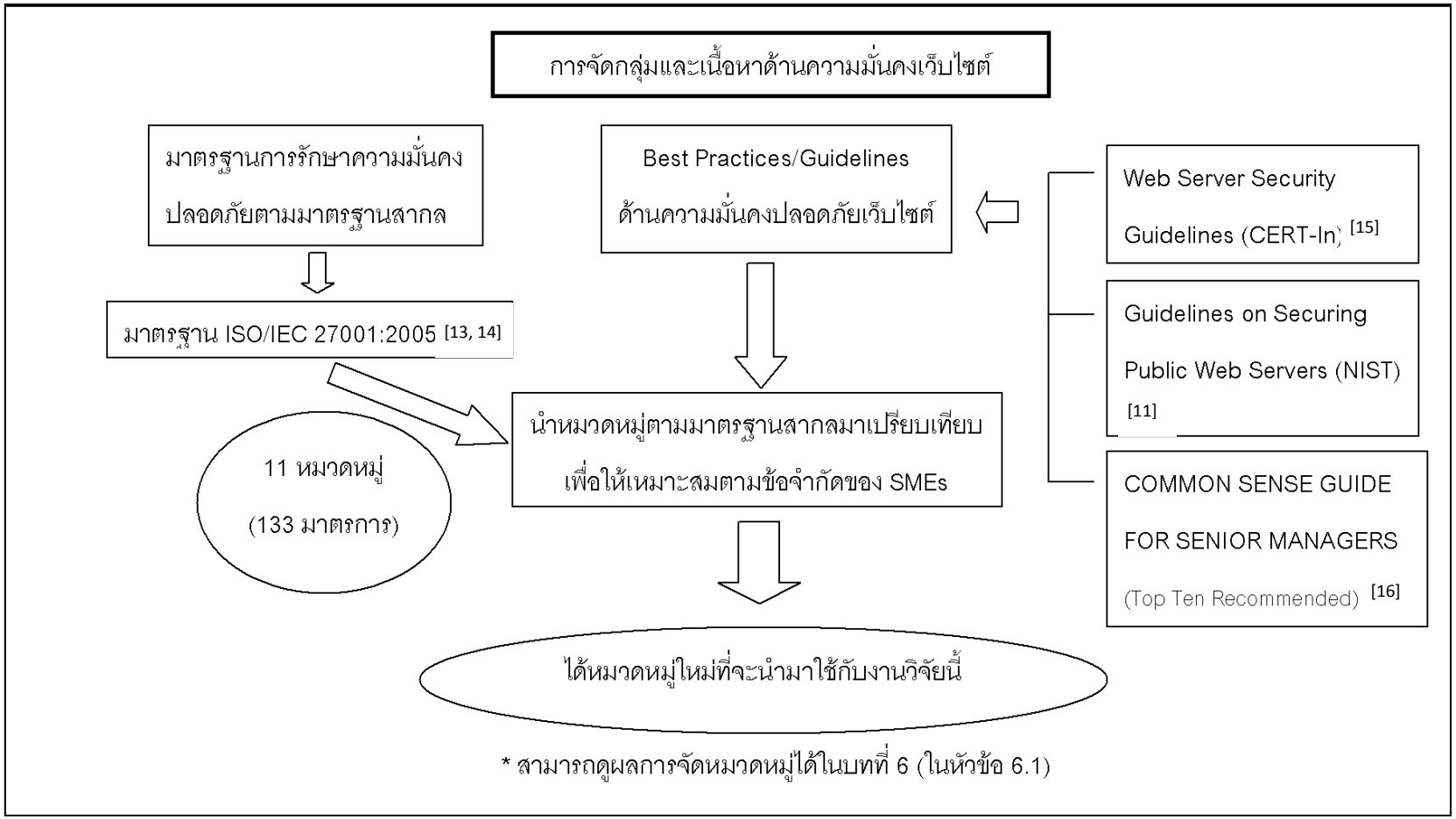
3.3) กลุ่มความมั่นคงปลอดภัยทางกายภาพอุปกรณ์และสิ่งแวดล้อม

3.4) กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงาน

3.5) กลุ่มการควบคุมการเข้าถึง

3.6) กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

โดย 6 กลุ่มหัวข้อมาตรการควบคุมใหม่ ประกอบด้วยมาตรการทั้งหมด 28 มาตรการ ซึ่งได้แสดงในบทที่ 6 (ในหัวเรื่องที่ 6.1 ผลการจัดหมวดหมู่)



รูปที่ 3-2 แสดงกรรมวิธีในการจัดหมวดหมู่

3.2 กรอบวิธีและแนวทางปฏิบัติในการออกแบบระบบต้นแบบ

ในการออกแบบระบบต้นแบบจะคำนึงถึง 2 แนวทางด้วยกัน คือ การออกแบบหน้าจอและการกำหนดเนื้อหา ดังนี้

3.2.1 แนวทางปฏิบัติในการออกแบบหน้าจอ (Interface Design) [12, 17, 18, 19, 20]

1) การใช้รูปภาพ
   - หลีกเลี่ยงรูปภาพหรือลูกเล่นที่ไม่เกี่ยวกับเนื้อหา รวมถึงโฆษณาประชาสัมพันธ์ต่างๆ
   - ไม่ควรใช้ภาพเคลื่อนไหว (animation) ในการนำเสนอ รวมถึงไม่ควรพึ่งการติดตั้ง software อื่นๆ เพิ่มเติม เช่น Flash หรือ Adobe Acrobat Reader
   - การแสดงรูปภาพควรมีกำหนด ALT Tag
   - ถ้าใช้ Icon ควรเป็นแบบพื้นฐานและสื่อความหมาย
2) การกำหนด Navigation
   - บอกถึงตำแหน่งของหน้าเว็บปัจจุบันใน Navigation
   - หลีกเลี่ยง Navigation ที่เป็น pull down หรือต้องใช้ความคล่องแคล่วของมือและนิ้ว เช่น hold and drag
   - ไม่ควรจัดลำดับชั้นลึกจนเกินไป
   - ควรสร้างปุ่มสำหรับดูหน้าถัดไป (Next Page) หรือหน้าที่แล้ว (Previous Page)
3) กำหนดลักษณะของ Browser
   - ขนาดของหน้าจอที่เหมาะสมคือ 1024×768 พิกเซล
   - ไม่ควรมีเมนูที่เยิ่นเย้อและไม่ควรทำเมนูแบบ Drop-Down นอกจากนี้ควรเปลี่ยนสีเมื่อเคลื่อนเมาส์มายังเมนูเหล่านั้น
   - เว็บเพจไม่ควรยาวเกินไปและควรหลีกเลี่ยงการใช้ Scroll bar
   - พยายามหลีกเลี่ยงการทำ Pop-up หรือสร้างหน้าต่างใหม่ (open window)
4) การวางเนื้อหา
   - เนื้อหาสำคัญควรอยู่บริเวณตรงกลางของหน้าจอหรือบริเวณพื้นที่ส่วนใหญ่
   - ข้อความสำคัญที่ต้องการสื่อความหมายต้องเน้นหรือทำ highlight
   - รูปแบบของหน้าจอ และ Navigation ที่ใช้จะต้องเรียบง่ายและต้องเหมือนกันในทุกหน้าเพื่อไม่ให้สับสน

5) การกำหนดเกี่ยวกับ Link
   - ควรจะแสดงสีและข้อความของลิงค์ให้ชัดเจนเพื่อผู้ใช้จะเห็นได้สะดุดตาและเห็นความแตกต่างระหว่างเนื้อหาทั่วไปกับลิงค์นั้น ทั้งนี้อาจแสดงเมื่อมี mouse over เป็นการขีดเส้นของลิงค์หรือแสดงสีของลิงค์ที่เปลี่ยนไป
   - ต้องสามารถแยกได้ว่าลิงค์ใดได้เข้าไปดูแล้วและลิงค์ใดยังไม่ได้เข้าไปดูได้อย่างชัดเจน (ไม่สับสนระหว่าง visited กับ unvisited links)
6) การใช้สีและการกำหนดสีพื้น
   - ควรหลีกเลี่ยงการใช้สีเหลือง เขียว และสีน้ำเงิน
   - พื้นหลังของเว็บไม่ควรเป็นสีขาวทั้งหมดหรือทำให้เกิดความสว่างมากจนเกินไป
   - ควรให้เกิดความแตกต่างระหว่างพื้นหน้าและพื้นหลังของเว็บอย่างชัดเจน
   - การใช้สีของข้อความกับสีของพื้นควรต้องระมัดระวังในการใช้
   - เนื้อหาไม่ควรใช้เพียงสีเดียว แต่ห้ามใช้หลายสีเกินไป
7) การกำหนดเกี่ยวกับข้อความ
   - หลีกเลี่ยงข้อความที่เคลื่อนไหว
   - การจัดข้อความควรจัดแบบชิดซ้าย
   - ควรมีช่องว่างระหว่างบรรทัดอย่างชัดเจน
   - ควรจะเว้นช่องไฟให้กว้างเป็น 2 ช่อง
   - ส่วนของเนื้อหาตรงกลางไม่ควรใช้ตัวอักษรพิมพ์ใหญ่ทั้งหมด
   - ควรเลือกใช้ฟอนต์ Sans Serif เช่น Helvetica และ Arial โดยหลีกเลี่ยงการใช้ฟอนต์ที่ดูเป็นลูกเล่น (Fancy)
   - ควรเลือกฟอนต์แบบ medium หรือ normal และมีขนาดไม่ต่ำกว่า 16
8) การกำหนดอื่นๆ
   - ควรจัดให้มีแผนผังเว็บไซต์ (Sitemap)
   - ไม่ควรจัดหน้าเว็บเพจให้ซับซ้อนและสามารถเข้าถึงเนื้อหาได้เร็ว โดยไม่ต้องคลิกเมาส์หลายครั้ง

3.2.2 **แนวทางปฏิบัติในเนื้อหา** (Content Design)

1) เน้นเนื้อหาเป็นภาษาไทยเพื่อให้เกิดความเข้าใจได้ง่าย
2) ใช้ภาษาสุภาพ อ่านง่าย

3) หลีกเลี่ยงภาษาที่ซับซ้อนหรือใช้คำศัพท์วิชาการชั้นสูง และควรพยายามหาคำขยายความอย่างง่ายๆ มาใช้แทน เช่น “การกำหนดระดับการเข้าถึงของ User” ควรเปลี่ยนเป็น “ใครบ้างสามารถใช้งานได้ และใช้งานอะไรได้บ้าง”
4) เนื้อหานำเสนอควรเหมาะสำหรับบุคคลสูงอายุ ไม่มีเวลามากนัก และไม่มีทักษะเกี่ยวกับการใช้งานคอมพิวเตอร์ รวมไปถึงบุคคลทั่วไปที่สนใจในเรื่องความมั่นคงของเว็บไซต์

3.3 หลักการและข้อกำหนดในการสร้างเว็บไซต์สำหรับเจ้าของกิจการ SME

จากกรอบวิธีและแนวทางปฏิบัติในการออกแบบเว็บไซต์ต้นแบบในหัวข้อที่ 3.2 เพื่อให้สามารถสร้างเว็บไซต์ให้เหมาะกับเจ้าของกิจการเอสเอ็มอี ซึ่งส่วนใหญ่เป็นผู้ที่มีอายุ จึงได้กำหนดข้อปฏิบัติในการสร้างเว็บไซต์และข้อห้ามในการสร้างเว็บไซต์ไว้ดังนี้

3.3.1 ข้อปฏิบัติในการสร้างเว็บไซต์สำหรับเจ้าของกิจการ SME

1) ควรบอกถึงตำแหน่งของหน้าเว็บในปัจจุบัน เพื่อไม่ให้สับสนในการเข้าถึงเว็บไซต์
2) ควรสร้างปุ่มสำหรับดูหน้าถัดไป (next page) หรือหน้าที่แล้ว (previous page) เพื่อให้สามารถอ่านต่อหรือย้อนกลับไปดูได้ง่าย
3) ควรแสดงสีและข้อความของลิงค์ให้ชัดเจนเพื่อให้สะดุดตาและเห็นถึงความแตกต่างระหว่างเนื้อหาทั่วไปกับลิงค์นั้น
4) เนื้อหาสำคัญควรเน้นอยู่บริเวณตรงกลางของหน้าจอหรือบริเวณพื้นที่ส่วนใหญ่ เพื่อให้เนื้อหามีความเด่นและมีพื้นที่ในการนำเสนอได้มาก
5) รูปแบบของหน้าจอต้องเรียบง่ายและเหมือนกันในทุกหน้า เพื่อไม่ให้สับสน
6) ข้อความสำคัญที่ต้องการสื่อความหมายต้องเน้นหรือทำ highlight
7) ควรเลือกใช้ฟอนต์ขนาดไม่ต่ำกว่า 16

3.3.2 ข้อห้ามในการสร้างเว็บไซต์สำหรับเจ้าของกิจการ SME

1) ไม่ควรจัดหน้าเว็บเพจให้ซับซ้อน ซึ่งทำให้เข้าถึงเนื้อหาที่ต้องการอ่านได้ยาก
2) ไม่ควรใช้ภาพเคลื่อนไหว (animation) ในการนำเสนอ เพราะทำให้ผู้อ่านลายตาและเข้าไม่ถึงเนื้อหาที่ต้องการนำเสนอ
3) ไม่ควรมีเมนูที่เยิ่นเย้อและไม่ควรทำเมนูแบบ drop-down เนื่องจากผู้ใช้อาจไม่มีความชำนาญในการใช้เมาส์ ซึ่งจะทำให้ต้องเรียนรู้ในการคลิกเข้าถึงเมนู

4) เว็บเพจไม่ควรยาวเกินไปและควรหลีกเลี่ยงการใช้ scroll bar การใช้ Scroll Bar จะทำให้ผู้ใช้ที่ไม่มีความชำนาญในการใช้เมาส์พลาดโอกาสในการเลื่อน Scroll Bar เพื่อมาอ่านข้อความด้านล่างได้
5) หลีกเลี่ยงการทำ pop-up หรือสร้างหน้าต่างใหม่ (open window) ซึ่งทำให้เกิดความรำคาญในการอ่านและอาจทำให้เกิดความยุ่งยากของหน้าต่างที่เกิดขึ้นใหม่มากมาย
6) หลีกเลี่ยงการใช้สีเหลือง เขียว และสีน้ำเงิน ทำให้เกิดปัญหากับผู้ที่ตาบอดสี
7) หลีกเลี่ยงการใช้ฟอนต์ที่ดูเป็นลูกเล่น (fancy) เพราะทำให้ผู้อ่านเกิดลายตา

การวิจัยในบทนี้ได้กล่าวถึงกรรมวิธีในการจัดหมวดหมู่เนื้อหา ข้อควรปฏิบัติและข้อห้ามในการสร้างเว็บไซต์สำหรับเจ้าของกิจการ SME ซึ่งในบทต่อไปจะกล่าวถึงการเลือกใช้เครื่องมือในการพัฒนาเว็บต้นแบบ การจัดโครงสร้างของเนื้อหาในเว็บ (Sitemap) และการออกแบบหน้าจอของเว็บไซต์

บทที่ 4

การออกแบบระบบต้นแบบ

จะกล่าวถึงส่วนในการเลือกใช้เครื่องมือในการพัฒนาเว็บต้นแบบ การออกแบบหน้าจอและโครงสร้างรวมของเว็บไซต์ โดยในงานวิจัยนี้ได้เลือกใช้โปรแกรมระบบจัดการเนื้อหา (Content Management System หรือ CMS) เพราะ

1) โปรแกรมระบบจัดการเนื้อหาที่มีอยู่ในปัจจุบันมีความสามารถในการพัฒนาและควบคุมบริหารการจัดการเว็บไซต์ ซึ่งจะช่วยประหยัดเวลาในการพัฒนาและนำไปใช้งานได้ทันที
2) เป็นโปรแกรม Freeware และมีให้เลือกใช้มากมาย
3) สามารถหาคู่มือและเอกสารให้อ่านเพิ่มเติมจากอินเตอร์เน็ตหรือร้านหนังสือทั่วไป
4) เป็นโปรแกรมที่สามารถนำมาดัดแปลงแก้ไข แล้วนำมาประยุกต์ใช้งานให้เหมาะสมตามแต่รูปแบบที่ต้องการได้
5) มีส่วนในการจัดการเนื้อหาเช่น การนำเสนอบทความ (Articles) การจัดการไฟล์ในส่วนดาวน์โหลด เป็นต้น

4.1 แนวทางเลือกใช้โปรแกรมระบบจัดการเนื้อหา

ปัจจุบันมีโปรแกรมระบบจัดการเนื้อหาหลายตัวที่มีความนิยม เช่น Joomla [21] PHP-Nuke [22] Mambo [23] Drupal [24] เป็นต้น แต่ในงานวิจัยนี้ได้เลือกใช้โปรแกรม Joomla เนื่องจากโปรแกรม Joomla เป็น Freeware และมีผู้ใช้งานจำนวนมากซึ่งเป็นที่ได้รับความนิยม จึงทำให้มีหนังสือเกี่ยวกับการใช้งานโปรแกรมจำนวนมาก ซึ่งโปรแกรม Joomla นี้ได้มีส่วนในการจัดการเนื้อหา เช่น การนำเสนอบทความ (Articles) และลักษณะรูปแบบอื่นๆ (Features) ประกอบกับโดยส่วนตัวผู้วิจัยเองมีความคุ้นเคยในการออกแบบและใช้งานมาในระดับหนึ่ง ดังนั้นจึงเลือกโปรแกรม Joomla มาใช้ในการพัฒนาเว็บต้นแบบ

4.2 โครงสร้างรวมของระบบ

หลังจากที่ได้ทำการจัดหมวดหมู่หัวข้อในบทที่ 3 แล้วจะได้หมวดหมู่ความมั่นคงปลอดภัยบนเว็บไซต์ที่แสดงในภาคผนวกที่ ข จากนั้นจะนำหัวเรื่องที่จะแสดงบนเว็บพอร์ทัลตามแต่ละหมวดหมู่ใหม่มาแบ่งเนื้อหาออกเป็น 4 กลุ่ม โดยแต่ละกลุ่มมีดังนี้

1) กลุ่มเนื้อหาที่เร่งด่วนในหน้าแรก

เนื้อหาในส่วนนี้จะเน้นนำเสนอเนื้อหาที่จำเป็นสำหรับเจ้าของกิจการควรรู้และต้องทำอย่างเร่งด่วนในการป้องกันเว็บไซต์ โดยอธิบายอย่างกระชับให้เข้าใจในหนึ่งหน้าก่อนอ่านต่อเพิ่มเติมในส่วนอื่นที่ขยายความมากขึ้น

2) กลุ่มเนื้อหาส่วนป้องกันเว็บไซต์

เนื้อหาในกลุ่มนี้เป็นการให้ความรู้หรือข้อคิด รวมทั้งคำแนะนำแก่เจ้าของกิจการ/บริษัทว่าต้องทำหรือมีแนวทางอย่างไรในการป้องกันเว็บไซต์ของบริษัทก่อนที่คนร้ายจะโจมตี รวมทั้งต้องกำชับเจ้าหน้าที่เทคนิคในบริษัททำอย่างไรเพื่อป้องกันและสอดส่องเว็บไซต์ โดยเน้นการป้องกันก่อนที่จะเกิดถูกเจาะเว็บไซต์

3) กลุ่มเนื้อหาการซ่อมแซมและแก้ไข

สำหรับเนื้อหาในกลุ่มนี้เน้นขอควรปฏิบัติเมื่อเว็บไซต์ถูกบุกรุก เป็นคำแนะนำเบื้องต้นในการแก้ไขปัญหาอย่างเร่งด่วน เช่น บอกหน่วยงานที่เชี่ยวชาญด้านความมั่นคงบนเว็บไซต์เพื่อขอคำปรึกษาเกี่ยวกับปัญหาที่เกิดขึ้น จะทำอย่างไรเมื่อเว็บไซต์ถูกบุกรุก เป็นต้น

4) เนื้อหาความรู้ทั่วไป

เนื้อหาในกลุ่มนี้จะเน้นเนื้อหาความรู้ด้านความมั่นคงเว็บไซต์ทั่วไป เพื่อให้เจ้าของกิจการ/บริษัท อ่านเพิ่มเพื่อให้เสริมสร้างความรู้ความเข้าใจมากขึ้น อาจจะเป็นคำศัพท์เทคนิคบางคำ หรือ รูปแบบการโจมตีแบบต่างๆ เป็นต้น

ซึ่งเมื่อเรียบเรียงหัวเรื่องและกลุ่มของเนื้อหาแล้วจะแสดงอยู่ในภาคผนวก ค ที่บอกถึงเนื้อหาหัวข้อใดอยู่กลุ่มใดบ้าง โดยโครงสร้างโดยรวมของเว็บต้นแบบเวอร์ชั่นแรก (Sitemap) มีดังนี้

- หน้าแรก (เป็นการอธิบายอย่างกระชับให้เห็นเข้าใจในหน้าเดียว)
- การป้องกันเว็บไซต์เบื้องต้น
  - การดูแลสอดส่อง
  - คำแนะนำในการปฏิบัติของเจ้าหน้าที่คอมฯ
  - โปรแกรมหาช่องโหว่
  - การป้องกันเว็บเบื้องต้น
  - ความปลอดภัยในที่จัดวางเว็บไซต์
  - ข้อคิดในการดูแลเว็บ
  - สร้างเว็บอย่างไรให้ปลอดภัย

- การซ่อมแซมและแก้ไข
  - หน่วยงานที่ปรึกษาด้านความมั่นคงเว็บไซต์
  - รู้ได้อย่างไรว่าเว็บเราถูกเจาะ
  - เมื่อไฟล์สำคัญในเว็บถูกเปลี่ยน
  - ทำอย่างไรเมื่อเว็บเราถูกล่วงละเมิด
- ห้องความรู้ทั่วไป
  - รหัสผ่านคืออะไร
  - แนวทางการตั้งรหัสผ่าน
  - แนวคิดการป้องกันเว็บ
  - ไฟร์วอลล์คืออะไร
  - ช่องโหว่มาจากที่ไหน
  - คนร้ายเจาะเว็บอย่างไร
  - ทำไมต้องสำเนาข้อมูล
  - การขโมยข้อมูลบนเน็ต
  - การโจมตีผ่านช่องโหว่ของโปรแกรม
  - การโจมตีโดยการใส่ข้อมูลที่ไม่ถูกต้อง
  - การโจมตีก่อกวนให้ทำงานไม่ได้
  - การหลอกถามหรือโทรศัพท์เพื่อหาข้อมูล
  - ทดสอบเว็บอย่างง่ายโดยการใส่ข้อมูลแปลกๆ
- แบบสอบถาม
- เกี่ยวกับผู้จัดทำ

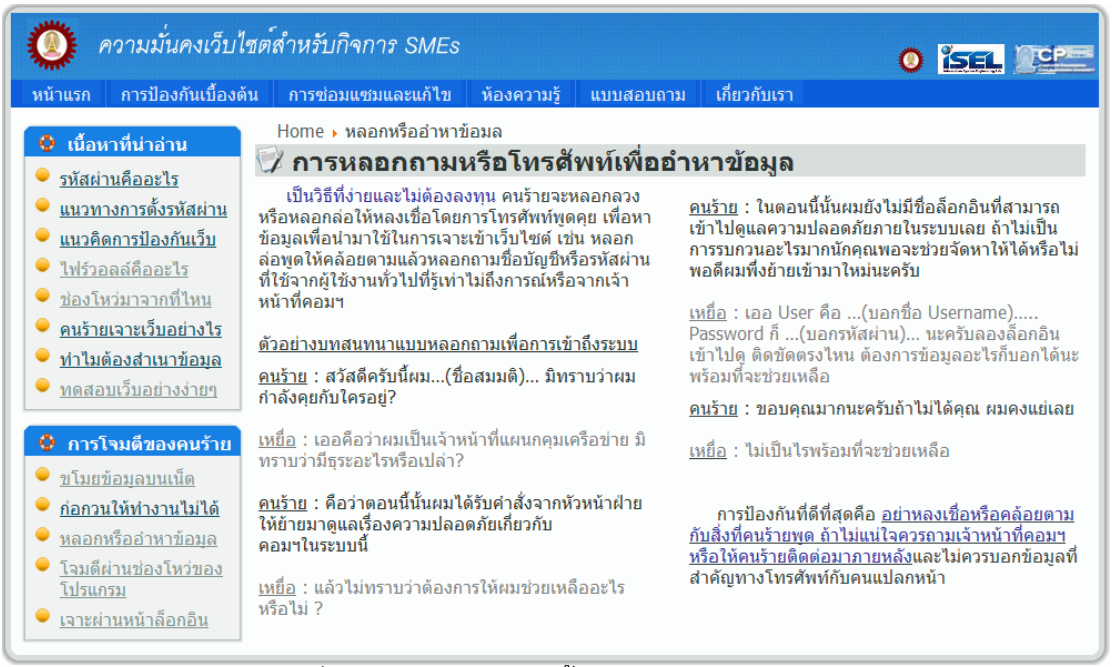
4.3 **การออกแบบหน้าจอของเว็บไซต์**

ผู้วิจัยได้เลือกโปรแกรม Joomla มาใช้พัฒนาเว็บไซต์ต้นแบบ โดยใช้ข้อกำหนดในการสร้างเว็บไซต์สำหรับเจ้าของกิจการ SME (ในหัวข้อ 3.3) และกรอบวิธีในการออกแบบระบบต้นแบบในส่วนการออกแบบหน้าจอ (ในหัวข้อ 3.2.1) ทั้งนี้ผู้วิจัยได้กำหนดขนาดหน้าจอของเว็บไซต์เป็น 1024x768 เพื่อให้เหมาะสมกับหน้าจอของคอมพิวเตอร์ในปัจจุบัน โดยเน้นพื้นสีขาว ตัวอักษรที่ใช้เป็นสีดำขนาด 16 และเน้นใช้โลโกและเมนูสีฟ้าเพื่อให้ดูสบายตา

สำหรับหน้าแรกของเว็บต้นแบบจะเน้นความกระชับในการนำเสนอเนื้อหาที่ควรรู้และสิ่งที่ต้องทำอย่างเร่งด่วนเพื่อป้องกันเว็บไซต์ของตนเอง รูปที่ 4-1 แสดงหน้าแรกของเว็บไซต์ต้นแบบ โดยแนวทางการสร้างเว็บต้นแบบมีดังนี้

1) ลดความสูงของ Logo Header ลงเพื่อเน้นแสดงจุดเด่นที่ส่วนของเนื้อหาบริเวณตรงกลางของหน้าจอ
2) นำส่วนของ Footer ออก เพื่อให้เนื้อหาที่แสดงในเว็บครบถ้วนในเพจเดียวโดยไม่ต้องใช้ Scroll Bar
3) แสดงสีและข้อความของลิงค์เป็นสีน้ำเงินเข้ม และเมื่อลิงค์ถูกเมาส์ลากผ่าน (mouse over) ข้อความลิงค์จะถูกขีดเส้นใต้ เพื่อให้ผู้ใช้สะดุดตาและเห็นถึงความแตกต่างระหว่างเนื้อหาทั่วไปกับลิงค์นั้น
4) เมนูที่ใช้มีอยู่สองส่วน คือ เมนูด้านบน (Top Menu) และเมนูด้านซ้าย (Left Menu)
    - เมนูด้านบน (Top Menu) ไว้ใช้แสดงและเชื่อมต่อกลุ่มเนื้อหาหลักของเว็บ เช่น หน้าแรก เนื้อหาในการป้องกันเว็บไซต์ เนื้อหาในการซ่อมแซมและแก้ไข เนื้อหาความรู้ทั่วไป รวมทั้งแบบสอบถามออนไลน์ เป็นต้น งดการใช้เมนูด้านบนแบบ Drop-Down แต่ได้ใช้เมนูด้านซ้ายของหน้าจอแทน
    - เมนูด้านซ้าย (Left Menu) ไว้แสดงหัวเรื่องในแต่กลุ่มเนื้อหา เช่น รหัสผ่านคืออะไร แนวทางการตั้งรหัสผ่าน แนวคิดการป้องกันเว็บไซต์ เป็นต้น ซึ่งเมนูด้านซ้ายได้ถูกแสดงในหน้าอื่นที่ไม่ใช่หน้าแรกดังรูปที่ 4-2
5) ใช้ Icon ขนาดเล็ก ไม่ใช้รูปภาพขนาดใหญ่จนเกินไปหรือลูกเล่นที่ไม่เกี่ยวกับเนื้อหา ทำให้ผู้ใช้เปิดเข้าหน้าเว็บเพจได้เร็ว

รูปที่ 4-1 แสดงหน้าแรกของเว็บไซต์ต้นแบบ



รูปที่ 4-2 แสดงหน้าเพจเนื้อหาในเว็บไซต์ต้นแบบ

หลังจากเลือกใช้โปรแกรมระบบจัดการเนื้อหา ออกแบบหน้าจอเว็บไซต์ และนำเนื้อหาขึ้นบนเว็บเรียบร้อยแล้ว ขั้นตอนต่อไปจะเป็นแนวทางการออกแบบแบบสอบถามและขั้นตอนการประเมินผลเว็บต้นแบบ โดยบทต่อไปจะกล่าวถึงวิธีการสร้างแบบสอบถามและขั้นตอนในการสำรวจแบบสอบถาม

บทที่ 5

การออกแบบ แบบสอบถามออนไลน์ และ การประเมินผลระบบต้นแบบ

การออกแบบคำถามเพื่อประเมินผลระบบต้นแบบใช้แบบสอบถามออนไลน์ โดยมีขั้นตอนในการทำดังนี้

5.1 การออกแบบ แบบสอบถามออนไลน์

ในการวิจัยนี้ใช้แบบสอบถามออนไลน์ ซึ่งทำให้อาสาสมัครสามารถตอบแบบสอบถามได้ทันทีหลังจากทดสอบการใช้เว็บต้นแบบแล้ว

5.1.1 กรรมวิธีในการออกแบบ แบบสอบถาม

ซึ่งแนวทางในการออกแบบสอบถาม [25, 26] มีดังนี้

1) กำหนดวัตถุประสงค์
2) กำหนดกลุ่มเป้าหมายในการสอบถาม
3) ตั้งคำถามเพื่อตรวจสอบบุคคลที่ตอบแบบสอบถามมีลักษณะใกล้เคียงกับกลุ่มเป้าหมาย
4) จัดเรียงคำถามอย่างเป็นเหตุเป็นผลในแต่ละตอน
5) ลดความยุ่งยากสำหรับผู้ตอบแบบสอบถาม เพื่อให้ได้รับความร่วมมือจากผู้ตอบ
6) ใช้คำสั้นๆ เข้าใจง่าย และคำถามไม่ควรจะยาวเกินไป
7) หลีกเลี่ยงคำถามที่ยากและมีคลุมเครือ ตีความหมายยาก
8) หลีกเลี่ยงคำถามที่โน้มเอียงหรือจูงใจให้ตอบ
9) ใช้ถ้อยคำที่ง่าย เข้าใจง่าย และเป็นภาษาสุภาพ
10) เลี่ยงคำถามที่ทำให้ผู้ตอบเสียศักดิ์ศรี ซึ่งจะทำให้ได้คำตอบที่ไม่เป็นความจริง
11) หลีกเลี่ยงการบังคับให้ตอบ (เดา) ควรให้มีทางเลือกอื่นในการตอบ เช่น ไม่รู้จัก ไม่ทราบ เป็นต้น
12) แบบสอบถามไม่ควรยาวจนเกินไป

5.1.2 วัตถุประสงค์ในการออกแบบ แบบสอบถาม

เพื่อใช้ประเมินประโยชน์ที่เจ้าของกิจการ/บริษัทจะได้รับจากเว็บพอร์ทัล เช่น การนำความรู้ที่ได้ไปใช้ในการตัดสินใจเบื้องต้นและสามารถกำกับดูแลเจ้าหน้าที่เทคนิคของบริษัทเพื่อทำให้เว็บไซต์ของบริษัทมีความมั่นคงในระดับเริ่มต้นได้

5.1.3 กำหนดกลุ่มเป้าหมาย

กลุ่มเป้าหมายในการทำแบบสอบถามเป็นเจ้าของวิสาหกิจขนาดกลางและขนาดย่อม โดยเน้นกลุ่มที่มีเว็บไซต์เป็นของตนเอง เพื่อร่วมประเมินเว็บต้นแบบความรู้เรื่องการป้องกันการโจมตีเว็บไซต์

5.1.4 การจัดลำดับคำถาม

สำหรับคำถามในแบบสอบถามได้อาศัยแนวทางในการสร้างคำถามซึ่งกล่าวไว้ในบทที่ 3 โดยเน้นถามในเรื่องความพึงพอใจในการใช้งานเว็บพอร์ทัลและการตอบรับของเจ้าของกิจการ/บริษัท แสดงไว้ในภาคผนวก ง. ซึ่งมีจำนวนคำถาม 22 ข้อ โดยแบ่งคำถามออกเป็น 4 กลุ่ม คือ

1) คำถามที่เกี่ยวกับข้อมูลผู้กรอกแบบสอบถามและบริษัท มีจำนวน 7 ข้อ

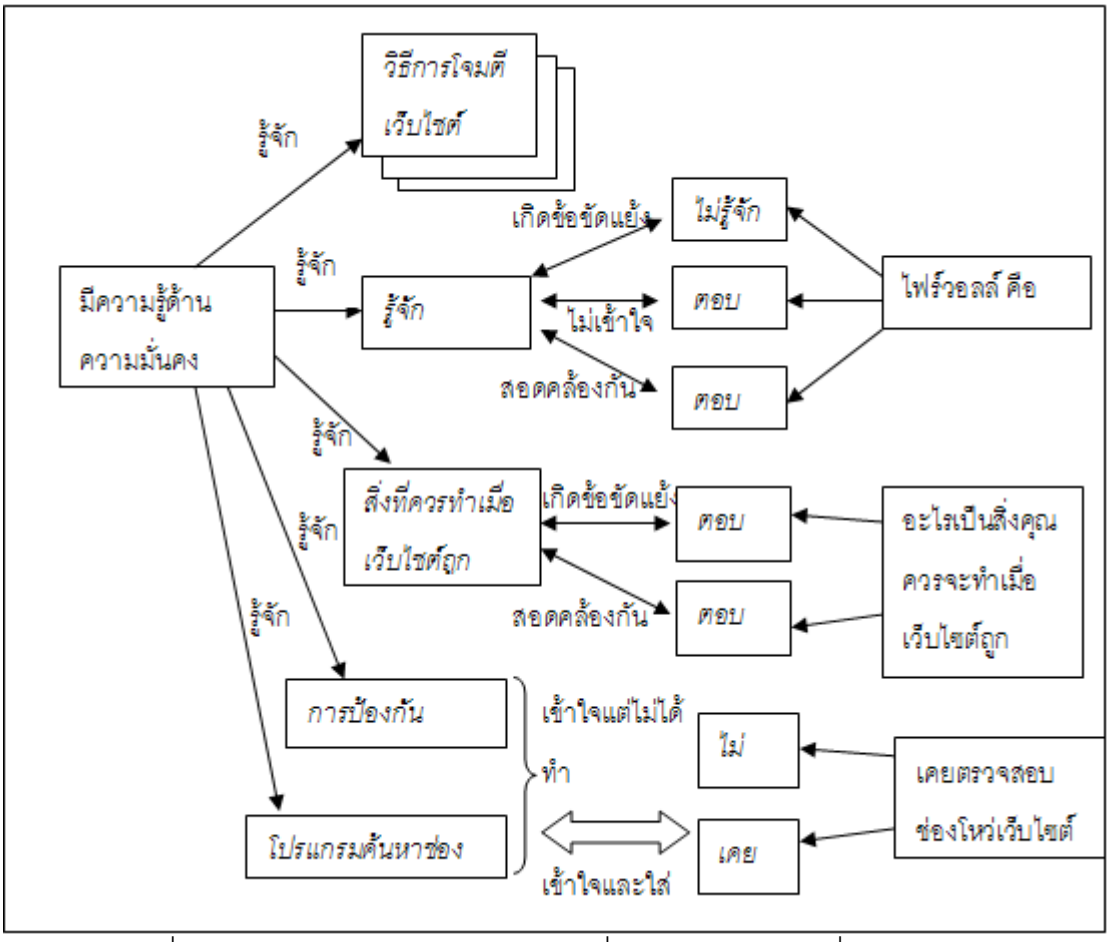
โดยคำถามในกลุ่มนี้ใช้เก็บข้อมูลสำหรับไว้อ้างอิง เช่น ข้อมูลชื่อผู้กรอกแบบสอบถาม เบอร์โทรศัพท์ หรืออีเมล์ที่ใช้ติดต่อ จำนวนพนักงาน หรือข้อมูลที่จำเป็นเพื่อระบุกลุ่มเป้าหมาย เช่น ถามว่าบริษัทมีเว็บไซต์หรือไม่ เป็นต้น

2) คำถามเกี่ยวกับความเข้าใจในเนื้อหาบนเว็บพอร์ทัล มีจำนวน 7 ข้อ

คำถามในกลุ่มนี้ได้แบ่งคำถามเป็น 2 ลักษณะ คือ ลักษณะคำถามที่เกี่ยวกับความเข้าใจและความคิดเห็นของเจ้าของกิจการ/บริษัท กับลักษณะคำถามที่วัดระดับความพึงพอใจในเนื้อหาบนเว็บ เช่น การนำมาประยุกต์ใช้ในบริษัท เพื่อนำไปสรุปผลความพึงพอใจในเว็บพอร์ทัล โดยคำถามในลักษณะที่สองนี้ จะมีการแบ่งระดับความพอใจออกเป็น 5 ระดับ คือ

ระดับ 5 หมายถึง มีความพอใจอยู่ในระดับมาก
ระดับ 4 หมายถึง มีความพอใจอยู่ในระดับค่อนข้างมาก
ระดับ 3 หมายถึง มีความพอใจอยู่ในระดับปานกลาง
ระดับ 2 หมายถึง มีความพอใจอยู่ในระดับค่อนข้างน้อย
ระดับ 1 หมายถึง มีความพอใจอยู่ในระดับน้อย

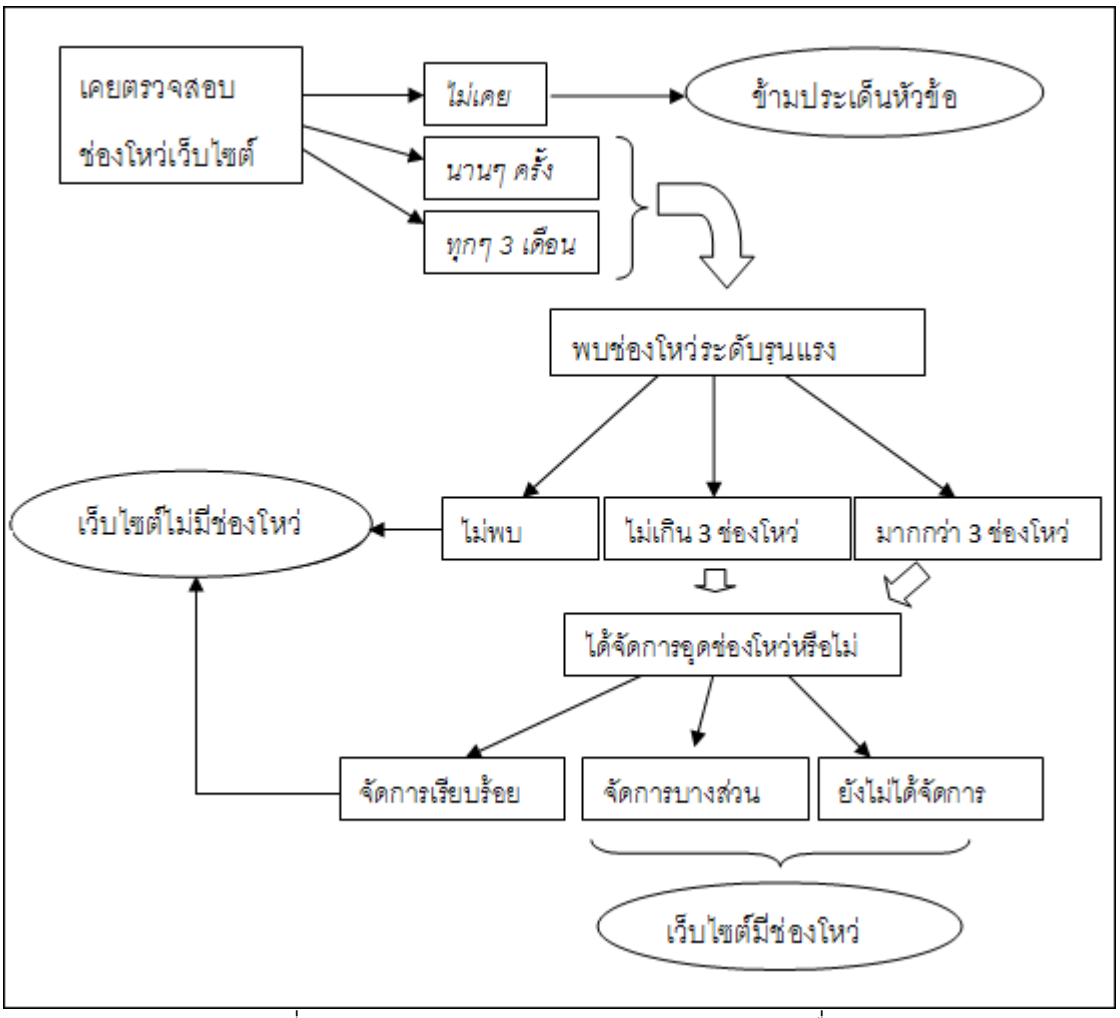
เพื่อนำระดับคะแนนมาใช้วิเคราะห์หาเฉลี่ยเพื่อประเมินความพึงพอใจของเนื้อหาบนเว็บพอร์ทัล นอกจากนี้ในแบบสอบถามจะเป็นการหยิบยกคำถามในเรื่องต่างๆมาถามเพื่อทดสอบความเข้าใจ เช่น รู้จักไฟร์วอลล์หรือไม่ ไฟร์วอลล์คืออะไร อะไรคือสิ่งที่ควรทำเมื่อเว็บไซต์ถูกเจาะ เป็นต้น ซึ่งในแบบสอบถามจะออกแบบเพื่อทดสอบความขัดแย้งและความสอดคล้องกันของการตอบ เพื่อจะได้คำตอบที่มีความถูกต้องและแม่นยำ โดยแสดงในรูปที่ 5-1



รูปที่ 5–1 แสดงความสัมพันธ์ของคำถามเกี่ยวกับความรู้ความมั่นคงเว็บไซต์

3) คำถามเกี่ยวกับแนวทางการป้องกันเว็บไซต์ของบริษัท มีจำนวน 6 ข้อ

คำถามในกลุ่มนี้ใช้ถามเกี่ยวกับความสนใจติดตามข่าวสารด้านความมั่นคงเว็บไซต์ ความตื่นตัวของเจ้าของกิจการในการนำไปประยุกต์ใช้ เช่น มีการติดตั้งและใช้งานไฟร์วอลล์หรือไม่ มีการตรวจสอบช่องโหว่อย่างสม่ำเสมอหรือไม่ มีการกำหนดรหัสผ่านให้เหมาะสมหรือไม่ เป็นต้น และถามเกี่ยวกับแนวทางการตรวจสอบช่องโหว่ของเว็บไซต์ ซึ่งลักษณะของคำถามเป็นคำถามแบบต่อเนื่อง โดยแสดงในรูปที่ 5-2



รูปที่ 5–2 แสดงความสัมพันธ์ของคำถามแบบต่อเนื่อง

4) คำถามอื่นๆ มีจำนวน 2 ข้อ

คำถามในกลุ่มนี้เป็นคำถามปลายเปิดเพื่อให้ผู้กรอกได้แสดงความคิดเห็น ข้อเสนอแนะ รวมทั้งคำแนะนำที่มีเกี่ยวกับงานวิจัยนี้ทั้งในส่วนของภาพรวมของเนื้อหาบนเว็บ และส่วนของแบบสอบถาม

5.2 ขั้นตอนในการสำรวจโดยใช้แบบสอบถาม

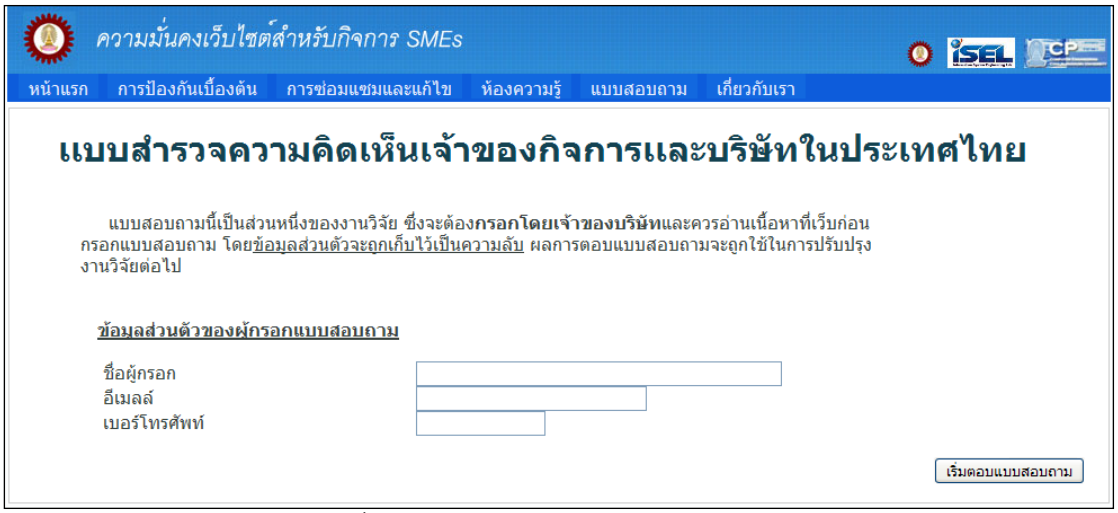
ขั้นตอนในการสำรวจแบ่งเป็น 4 ขั้นคือ เตรียมการสำรวจ ดำเนินการสำรวจ ประเมินเว็บต้นแบบ วิเคราะห์ข้อมูล ดังนี้

5.2.1 เตรียมการสำรวจโดยใช้แบบสอบถามและทดสอบแบบสอบถาม

หลังจากที่กำหนดกลุ่มเป้าหมายและลำดับขั้นของคำถามเรียบร้อยแล้ว ขั้นตอนหลังจากนี้คือ เลือกวิธีในการสำรวจความคิดเห็นเพื่อความสะดวกในการติดต่อกับกิจการหรือบริษัท ในงานวิจัยนี้จึงเลือกทำการสำรวจผ่านทางเว็บ โดยนำคำถามทั้งหมดที่ได้ในหัวข้อ 5.1 (การออกแบบสอบถามออนไลน์) มาสร้างแบบสอบถามบนเว็บไซต์ แล้วการทดสอบแบบสอบถามออนไลน์ โดยมีเจ้าของบริษัทเอสเอ็มอี และพนักงานคอมพิวเตอร์ของบริษัท จำนวน 9 คน ร่วมกับผู้เชียวชาญด้านความมั่นคงอีกจำนวน 3 คน รวมเป็น 12 คนในทำการทดสอบ โดยผู้ทดสอบได้แนะนำให้ควรลดจำนวนหน้าของแบบสอบถามลงจากเดิม 9 หน้า ให้เหลือเพียง 3 หน้า คือ หน้าที่ใช้เก็บข้อมูลส่วนตัวของผู้กรอกก่อนเริ่มตอบแบบสอบถาม หน้าที่แรกในการถามตอบแบบสอบถาม และ หน้าที่สองเพื่อใช้ถามตอบความคิดเห็นทั่วไปจำนวนสองข้อ ทั้งนี้เมื่อปรับแบบสอบถามออนไลน์ใหม่แล้วจะทำให้เกิด Scroll Bar ในหน้าแรกของการถามตอบแบบสอบถาม แต่เพื่อช่วยลดความซับซ้อนและช่วยทำให้ผู้ตอบสามารถตอบแบบสอบถามได้จนเสร็จ สำหรับหน้าจอของเว็บแบบสอบถามออนไลน์ ได้แสดงในรูปที่ 5-3 ซึ่งเป็นเว็บเพจที่ใช้เก็บข้อมูลส่วนตัวของผู้กรอกแบบสอบถาม โดยเมื่อผู้กรอกกดปุ่ม “เริ่มตอบแบบสอบถาม” โปรแกรมจะทำการบันทึกลงบนฐานข้อมูล พร้อมทั้งสร้าง Cookie session เอาไว้ เมื่อผู้กรอกที่กรอกไม่เสร็จ (ไม่ครบทุกหน้า) โปรแกรมจะนำ Cookie Session ในเครื่องผู้กรอกไปดึงข้อมูลในฐานข้อมูลกลับขึ้นมาแสดงที่หน้าเว็บอีกครั้งทำให้ผู้กรอกไม่ต้องกรอกข้อมูลเดิมซ้ำ

5.2.2 การดำเนินการสำรวจ

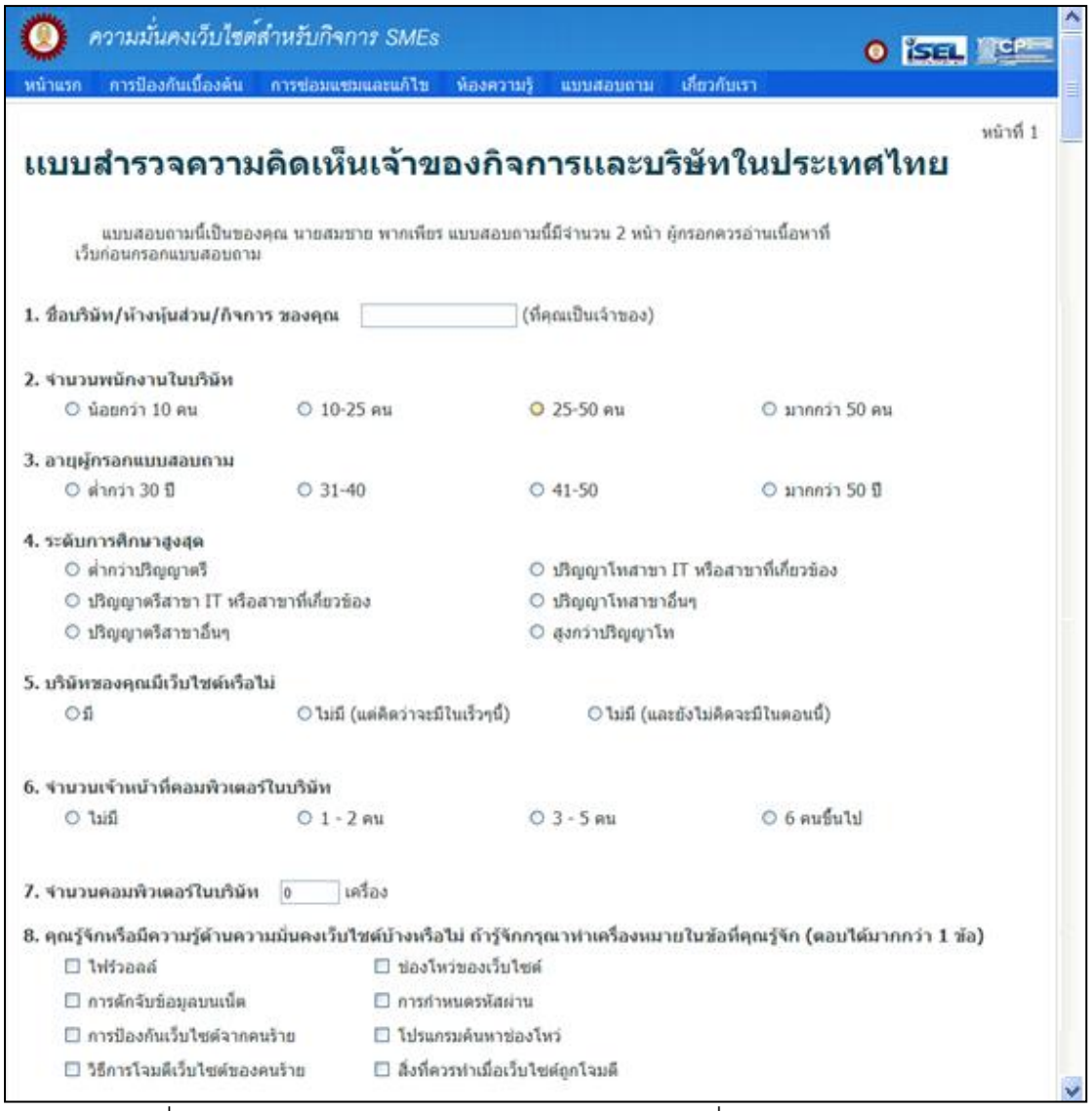
เมื่อสร้างเว็บแบบสอบถามเสร็จสมบูรณ์แล้วขั้นตอนต่อไปคือ ประชาสัมพันธ์ให้เจ้าของกิจการ/บริษัทให้เข้าชมและอ่านเนื้อหาในเว็บไซต์ต้นแบบและร่วมตอบแบบประเมินเว็บต้นแบบ ซึ่งในงานวิจัยนี้ได้รับความช่วยเหลือจากสถาบันพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมในการติดต่อประสานงานกับเจ้าของกิจการ/บริษัท กับสมาคมศิษย์เก่าคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย โดยใช้เวลาประมาณสองเดือนเพื่อให้เจ้าของกิจการ/บริษัทเข้าชมและร่วมทำแบบประเมินเว็บต้นแบบ



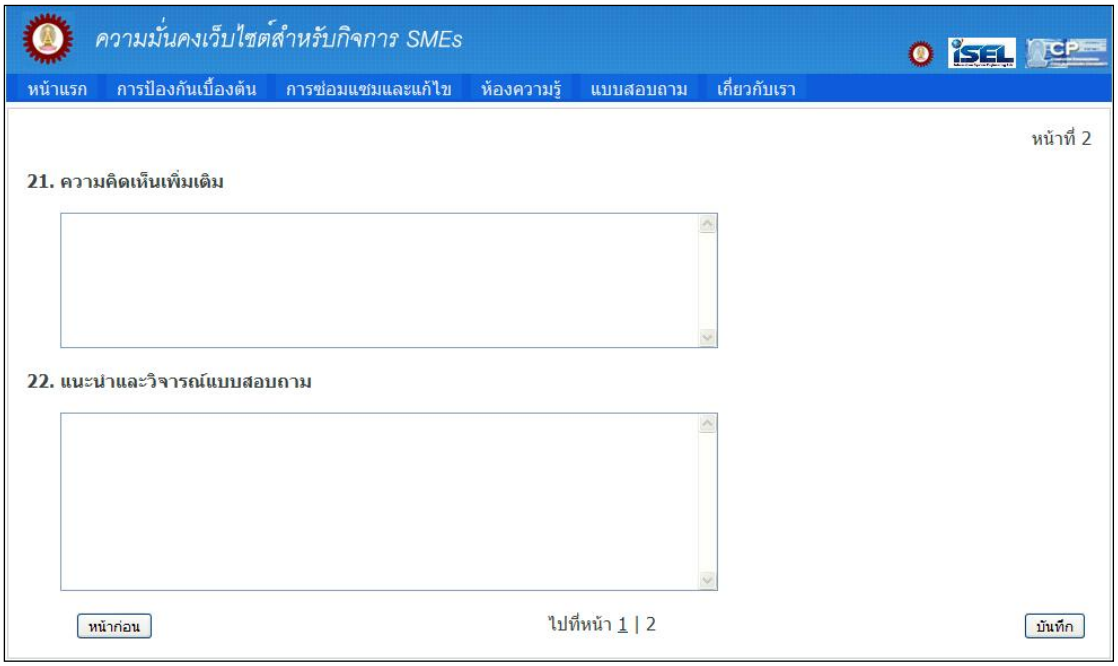
รูปที่ 5–3 แสดงเว็บแบบสอบถามออนไลน์

5.2.3 การประเมินเว็บต้นแบบ

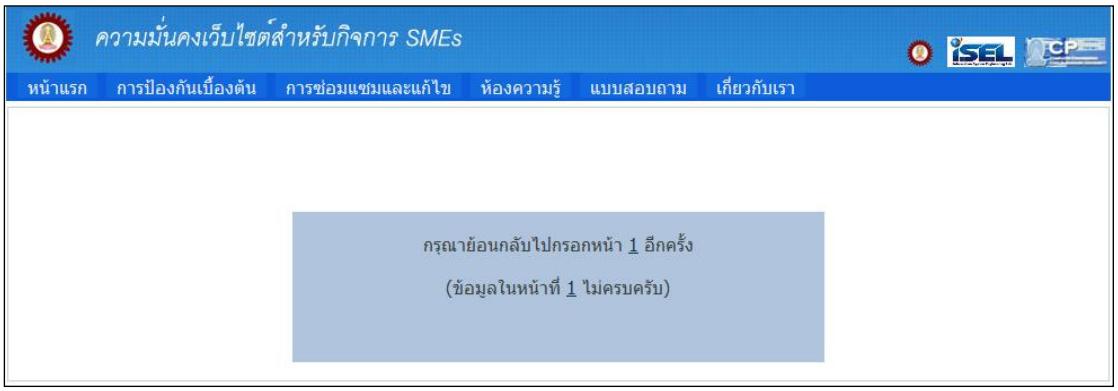
หลังจากเจ้าของกิจการ/บริษัทได้ใส่ชื่อและรายละเอียดสำหรับติดต่อกลับในรูปที่ 5-3 แล้ว รูปที่ 5-4 เป็นหน้าจอที่เริ่มเก็บข้อมูลและผลการประเมิน ซึ่งเก็บผลสำรวจจำนวนสองหน้า โดยหน้าแรกประกอบด้วยคำถามแบบเลือกตอบทั่วไปจำนวน 20 ข้อ และในหน้าที่สองเป็นคำถามแบบปลายเปิดจำนวน 2 ข้อ (แสดงในรูปที่ 5-5) โดยเมื่อผู้กรอกกดปุ่ม “Next” ในหน้าแรกโปรแกรมจะบันทึกข้อมูลไว้ที่ฐานข้อมูลและเมื่อผู้กรอกย้อนกลับมากรอกหน้าเดิมใหม่ โปรแกรมจะดึงข้อมูลที่ได้กรอกเหล่านั้นกลับคืนมา สำหรับผลการประเมินจะเสร็จสมบูรณ์เมื่อผู้กรอกต้องกรอกข้อมูลทั้งสองหน้านี้ให้ครบถ้วน (สำหรับคำถามปลายเปิดในหน้าที่สองสามารถเว้นว่างไว้ได้) เมื่อกดปุ่ม “บันทึก” แล้วถ้าผู้กรอกยังกรอกแบบสอบถามไม่ครบโปรแกรมจะขึ้นเตือนให้ผู้กรอกกลับไปกรอกในหน้านั้นอีกครั้งหนึ่ง ดังรูปที่ 5-6 และเมื่อกรอกครบถ้วนเรียบร้อยแล้วโปรแกรมจะแสดงหน้าจอขอบคุณดังรูปที่ 5-7 ถ้ายังต้องการเปลี่ยนคำตอบอีกครั้งในวันหลังให้เลือกกดที่ปุ่ม “กรอกต่อวันหลัง” และถ้ายืนยันส่งแบบสอบถามให้เลือกกดปุ่ม “ยื่นแบบสอบถาม”



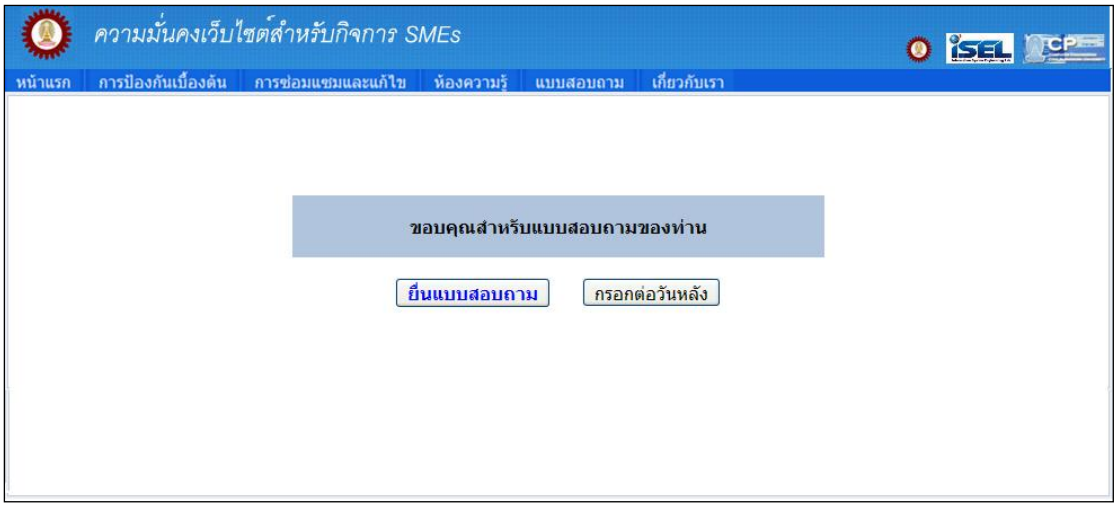
รูปที่ 5-4 แสดงหน้าจอแบบสอบถามออนไลน์ในหน้าเริ่มเก็บผลการประเมิน



รูปที่ 5-5 แสดงหน้าจอแบบสอบถามออนไลน์ในหน้าสุดท้าย



รูปที่ 5-6 แสดงหน้าจอแจ้งเตือนเมื่อผู้กรอกกรอกข้อมูลไม่ครบ



รูปที่ 5-7 แสดงหน้าจอเมื่อผู้กรอกกรอกข้อมูลเสร็จสมบูรณ์

5.2.4 การวิเคราะห์ข้อมูล

การวัดผลจะใช้เว็บแบบสอบถามในเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง และนำข้อมูลที่ได้เหล่านั้นมาตรวจสอบความสมบูรณ์ของข้อมูลและวิเคราะห์ข้อมูลโดยใช้ค่าสถิติ คือ ร้อยละ ความถี่ และ ค่าเฉลี่ย ก่อนสรุปผลการทดลองและนำเสนอในรูปกราฟ หรือ ตาราง เช่น

1) วิเคราะห์ลักษณะของกลุ่มกิจการ/บริษัท เช่น ดูจากจำนวนพนักงานในบริษัท มีเว็บไซต์ของบริษัทหรือไม่ เป็นต้น
2) วิเคราะห์ความรู้พื้นฐานของเจ้าของกิจการ/บริษัท โดยวิเคราะห์จากผลการตอบแบบสอบถาม ซึ่งมีการทดสอบหาข้อขัดแย้งและความสอดคล้องกันของคำตอบ เพื่อจะได้คำตอบที่มีความถูกต้องและแม่นยำมากที่สุด
3) นำคะแนนที่ได้จากการตอบของผู้ประเมินมาสรุปหาค่าเฉลี่ยและนำมาแสดงเป็นกราฟบอกสัดส่วนของระดับคะแนน เช่น ระดับความเข้าใจง่ายในเนื้อหาของเว็บ เพื่อแสดงให้เห็นแนวโน้มอยู่ในระดับใด เป็นต้น

หลังจากเจ้าของกิจการได้อ่านเนื้อหาในเว็บต้นแบบและตอบแบบสอบถามออนไลน์เรียบร้อยแล้ว ข้อมูลทั้งหมดจะถูกบันทึกลงในฐานข้อมูลบนเว็บไซต์ ซึ่งการวิเคราะห์ผลการประเมินจะใช้คำสั่ง SQL ในการดึงข้อมูลและสรุปจำนวนของข้อมูลที่ตอบในแต่ละข้อ โดยผู้วิจัยได้เขียนโปรแกรมบนเว็บไซต์โดยใช้ภาษา PHP ในการติดต่อไปยังฐานข้อมูลบนเว็บไซต์ (MySQL) โดยใช้คำสั่ง SELECT ในการค้นหาผลตอบแบบสอบถามที่ตอบเสร็จแล้ว ดังบรรทัดด้านล่าง

```
SELECT * FROM evaluate_table WHERE status='OK'
```

จากนั้นเขียนโปรแกรมเพื่อนับจำนวนผู้ตอบในแต่ระดับความพอใจตั้งแต่ระดับน้อย (มีค่าเป็น 1) ถึงระดับมาก (มีค่าเป็น 5) และนำมาคำนวณหาค่าเฉลี่ยของแต่ละเกณฑ์คำถาม ยกตัวอย่างเช่น การวิเคราะห์ข้อมูลของ “การนำไปประยุกต์ใช้งานในบริษัท" จะใช้คำสั่ง SELECT แบบ AVG เพื่อหาค่าเฉลี่ยดังบรรทัดด้านล่าง

SELECT AVG(ApplyInSMEs) FROM evaluate_table WHERE status='OK'

และใช้คำสั่ง SQL ด้านล่าง ในการรวมความถี่ที่ตอบในแต่ละระดับความพอใจ

SELECT COUNT(*) FROM evaluate_table WHERE status='OK' and ApplyInSMEs = '1';

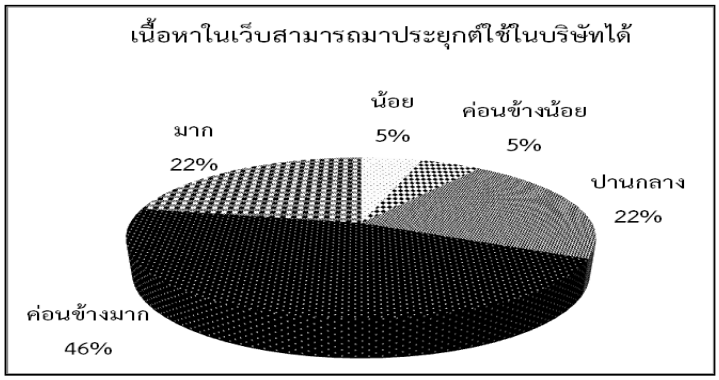
SELECT COUNT(*) FROM evaluate_table WHERE status='OK' and ApplyInSMEs = '2';

SELECT COUNT(*) FROM evaluate_table WHERE status='OK' and ApplyInSMEs = '3';

SELECT COUNT(*) FROM evaluate_table WHERE status='OK' and ApplyInSMEs = '4';

SELECT COUNT(*) FROM evaluate_table WHERE status='OK' and ApplyInSMEs = '5';

จากนั้นนำจำนวนความถี่ในแต่ละระดับมาสร้างเป็นกราฟรูปวงกลม ซึ่งในงานนี้ได้เขียนโปรแกรม PHP โดยใช้ Library ของ jpgraph เพื่อสร้างกราฟแสดงผลบนเว็บไซต์ โดยผลของระดับความพอใจของการนำไปประยุกต์ใช้งานในบริษัท แสดงดังรูปที่ 5-8



รูปที่ 5-8 ผลของระดับความพอใจในการนำไปประยุกต์ใช้

ซึ่งในบทต่อไปจะกล่าวถึงผลการวิจัยในส่วนของเนื้อหา ผลของการจัดหมวดหมู่เนื้อหาด้านความมั่นคงเว็บไซต์สำหรับเจ้าของกิจการ และผลการวัดระดับความพึงพอใจในส่วนอื่น เช่น ความรู้และความเข้าใจเกี่ยวกับไฟร์วอลล์ ความรู้ในการกำหนดรหัสผ่านให้เหมาะสม การตรวจสอบและปรับปรุงช่องโหว่ ความรู้ในการป้องกันเว็บไซต์และการแก้ไขปัญหา เป็นต้น

บทที่ 6

ผลการวิจัย

สำหรับผลการวิจัยแสดงไว้ใน 3 หัวข้อคือ การจัดหมวดหมู่ การเปรียบเทียบเว็บต้นแบบการออกแบบเว็บไซต์ ความพึงพอใจในส่วนของเนื้อหาความรู้ โดยมีรายละเอียดดังนี้

6.1 ผลการจัดหมวดหมู่

หลังจากการเปรียบเทียบมาตรการควบคุมของการบริหารการรักษาความมั่นคงปลอดภัย (ISO/IEC 27001:2005) [14] ที่สอดคล้องกับแนวทางด้านความมั่นคงเว็บไซต์ [11, 15] และแนวทางปฏิบัติด้านความมั่นคงสำหรับผู้จัดการระดับสูง [16] โดยคัดเลือกเฉพาะมาตรการที่ตรงกับแนวทางปฏิบัติอย่างน้อยหนึ่งแนวทางปฏิบัติ จึงทำให้เหลือมาตรการควบคุม 28 มาตรการจากทั้งหมด 133 มาตรการ (ตามภาคผนวก ก.) และเมื่อยุบหมวดหมู่ที่ไม่มีมาตรการควบคุมและรวมมาตรการที่เหลือในบางหมวดหมู่เข้าด้วยกันเพื่อความกระชับ เช่น นำมาตรการควบคุมการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (ในหมวดหมู่การบริหารความต่อเนื่องในการดำเนินงานขององค์กร) มาไว้ในกลุ่มหมวดหมู่ของนโยบายในกลุ่มที่ 1 เพื่อให้เกิดความกระชับ ซึ่งจะเหลือ 6 หมวดหมู่ ดังนี้

1) กลุ่มแผนและนโยบายการปฏิบัติด้านความมั่นคงเว็บไซต์ (System Security Plan and Policy)
   - 1.1) เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร
   - 1.2) การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ
   - 1.3) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการป้องกันหรือแผนเมื่อเกิดเหตุไม่คาดคิด
   - 1.4) นโยบายการใช้งานบริการเครือข่าย
   - 1.5) นโยบายการใช้งานการเข้ารหัสข้อมูล
2) กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)
   - 2.1) หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย
   - 2.2) การสร้างความตระหนัก การให้ความรู้ด้านความมั่นคงปลอดภัย (Security Awareness and Training)

3) กลุ่มความมั่นคงปลอดภัยทางกายภาพอุปกรณ์และสิ่งแวดล้อม (Physical and environmental security)
   3.1) การจัดทำบริเวณล้อมรอบ
   3.2) การควบคุมการเข้าและออก
   3.3) การจัดวางและการป้องกันอุปกรณ์
   3.4) ระบบและอุปกรณ์สนับสนุนการทำงาน
4) กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communication and operations management)
   4.1) การวางแผนความต้องการทรัพยากรสารสนเทศ
   4.2) การป้องกันโปรแกรมที่ไม่พึงประสงค์
   4.3) การสำรองระบบ
   4.4) มาตรการทางเครือข่าย
   4.5) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย
   4.6) สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ
   4.7) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ
   4.8) การตรวจสอบการใช้งานระบบ
5) กลุ่มการควบคุมการเข้าถึง (Access control)
   5.1) การบริหารจัดการสิทธิ์การใช้งานระบบ
   5.2) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
   5.3) การใช้งานรหัสผ่าน
6) กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)
   6.1) การตรวจสอบข้อมูลนำเข้า
   6.2) การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล
   6.3) การตรวจสอบข้อมูลนำออก
   6.4) การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ
   6.5) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ
   6.6) มาตรการควบคุมช่องโหว่ทางเทคนิค

6.2 ผลการเปรียบเทียบเว็บต้นแบบ

เมื่อเปรียบเทียบเนื้อหาของเว็บไซต์ต้นแบบกับเว็บไซต์สารานุกรมไทยที่เป็นความรู้ทั่วไป th.wikipedia.org [27] และ เว็บไซต์เฉพาะทางเกี่ยวกับความมั่นคงของไทยที่มีเนื้อหาเข้มข้น www.thaicert.nectec.or.th [28] รูปที่ 6-1 แสดงเนื้อหาของไฟร์วอลล์ในแต่ละเว็บไซต์

รูปที่ 6-1 แสดงเนื้อหาของไฟร์วอลล์ในเว็บให้ความรู้ทั้งสามแหล่งเว็บ

โดยผลการเปรียบเทียบได้แสดงในตารางที่ 6-1 พบว่าทั้งสามแหล่งเว็บได้ออกแบบหน้าจอให้เหมาะกับความกว้างขนาด 1024 พิกเซล และเลือกใช้พื้นเว็บเป็นสีขาวและฟอนต์เป็นสีดำ ทำให้ตัวหนังสืออ่านได้ชัดเจน แต่เว็บสารานุกรมวิกิพีเดียและเว็บไทยเซิร์ทมีการเกิด Scroll bar จึงทำให้ผู้อ่านดูข้อมูลที่สนใจได้ช้าลง และเมื่อพิจารณาในเนื้อหา ทั้งสามเว็บมีเนื้อหาที่กระชับใกล้เคียงกัน (จากข้อที่ 6 ที่มีจำนวนบรรทัดที่ใช้อธิบายประมาณ 4 -5 บรรทัด) แต่ถ้านับจำนวนคำศัพท์เทคนิคพบว่า เว็บต้นแบบมีจำนวนคำศัพท์เทคนิคเพียง 1 คำเท่านั้น และปรากฏในเนื้อหาเพียง 3 ครั้ง ซึ่งมีความถี่ของคำศัพท์เทคนิคที่ปรากฏในหนึ่งบรรทัดอยู่ที่ประมาณ 0.75 คำต่อบรรทัด ซึ่งมีค่าน้อยที่สุด จึงทำให้ผู้อ่านเนื้อหาในเว็บไซต์สามารถอ่านข้อมูลได้เร็วโดยไม่ต้องติด

กับความหมายของศัพท์เทคนิค และการใช้ฟอนต์ที่มีขนาดใหญ่จึงทำให้ผู้อ่านสามารถอ่านเนื้อหาได้เร็วยิ่งขึ้น

ตารางที่ 6-1 เปรียบเทียบเว็บเพจที่อธิบายความหมายของไฟร์วอลล์

	เว็บเพจต้นแบบ	เว็บไซต์ที่ 2	เว็บไซต์ที่ 1
1. ความกว้างหน้าจอมีขนาดเหมาะสม	√	√	√
2. พื้นสีของเว็บไซต์	ขาว	ขาว	ขาว
3. สีของฟอนต์	ดำ	ดำ	ดำ
4. ขนาดฟอนต์	16	12	14-16
5. มี Scroll bar	ไม่มี	มี	มี
6. จำนวนบรรทัดที่ใช้อธิบาย	4	4	5
7. จำนวนคำศัพท์เทคนิค	1	6	5
8. จำนวนครั้งที่พบคำศัพท์เทคนิค	3	11	14
9. ความถี่ของศัพท์เทคนิคต่อบรรทัด	0.75	2.75	2.8
10. จำนวนบรรทัดในเว็บเพจ	5	> 20	> 20

เมื่อเปรียบเทียบความถี่ของศัพท์เทคนิครวมกับเว็บไซต์อื่นอีก 5 เว็บไซต์ที่ได้จากการค้นหาด้วยคำว่า "ไฟร์วอลล์ คืออะไร" ในเว็บไซต์ Google [29] พบว่าจำนวนสัดส่วนความถี่ที่พบคำศัพท์เทคนิคในเว็บต้นแบบ (หมายเลข 9) มีค่าน้อยที่สุดเช่นกัน แสดงในตารางที่ 6-2

ตารางที่ 6-2 เปรียบเทียบความถี่ของศัพท์เทคนิคในแต่ละเว็บไซต์

รายชื่อเว็บไซต์	ความถี่ที่พบ
1. http://windows.microsoft.com	2.4
2. http://www.microsoft.com	2
3. http://thaicert.nectec.or.th	2.8
4. http://th.wikipedia.org	2.75
5.http://www.it-guides.com	1.6
6. http://www.viruscom2.com	1.7
7. http://www.thaiall.com	1.8
8. http://www.th-sme-security.com	0.75

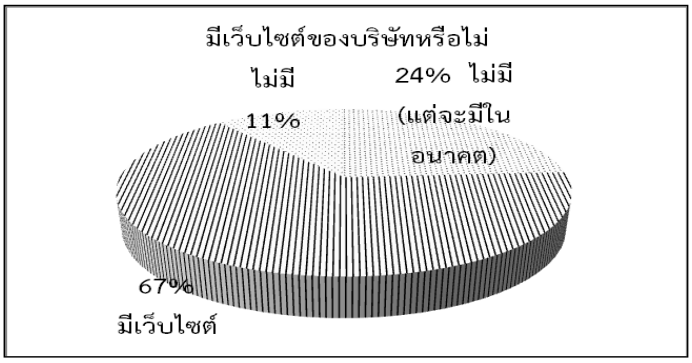
6.3 ผลของความพอใจในการออกแบบเว็บไซต์

โดยข้อสรุปของความคิดเห็นผู้ตอบแบบสอบถามในส่วนของรูปแบบของเว็บไซต์ มีดังนี้

1) ขนาดหน้าเว็บไซต์พอดีกับหน้าจอสามารถอ่านได้ในหน้าเดียว ไม่อึดอัด โทนสีสบายตาดี
2) ขนาดฟอนต์อ่านง่าย แต่ไม่ควรเลือกใช้ฟอนต์ตัวใหญ่ปนตัวเล็กเพื่อเน้นข้อความ เพราะจะทำให้ดูไม่สม่ำเสมอ แต่ควรใช้เปลี่ยนสีฟอนต์เป็นสีอื่นหรือเลือกใส่สีพื้นหลังแทน
3) ไม่ควรแบ่งคอลัมน์มากเกินไปจะทำให้ลายตา และควรเว้นช่องไฟให้มากขึ้นจะทำให้อ่านง่ายยิ่งขึ้น
4) ควรเน้นข้อความในโลโก้ด้านบนเพื่อบอกให้รู้จุดประสงค์ของเว็บไซต์

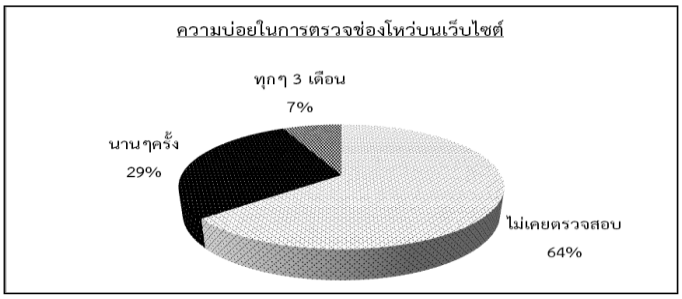
6.4 ผลของความพึงพอใจในส่วนของเนื้อหาความรู้

จากการสำรวจแบบสอบถามของเจ้าของบริษัทเอสเอ็มอี เจ้าของร้านค้าขายของบนอินเตอร์เน็ต และพนักงานคอมพิวเตอร์ของบริษัท(ซึ่งเป็นผู้ได้รับมอบอำนาจจากเจ้าของบริษัท) จำนวน 100 คน มีผู้ตอบกลับแบบสอบถามจำนวน 37 คน โดยส่วนใหญ่ร้อยละ 67 มีเว็บไซต์ของบริษัทหรือร้านค้า ซึ่งแสดงดังรูปที่ 6-2



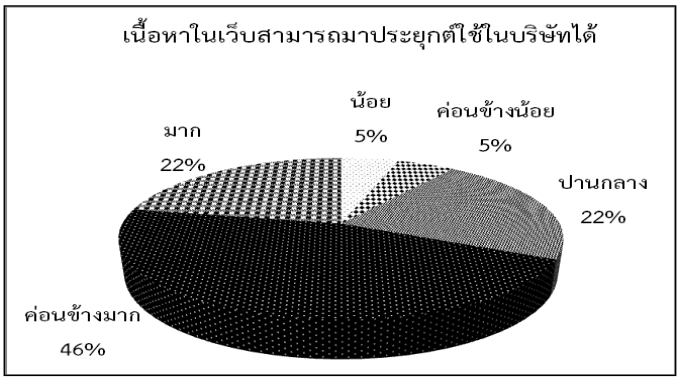
รูปที่ 6-2 สัดส่วนของจำนวนบริษัทที่มีเว็บไซต์และไม่มีเว็บไซต์

ร้อยละ 64 ของกลุ่มตัวอย่างที่มีเว็บไซต์ไม่เคยทำการตรวจสอบช่องโหว่ของเว็บไซต์เลย มีเพียงร้อยละ 7 เท่านั้นที่ตรวจสอบทุกๆสามเดือน ดังรูปที่ 6-3



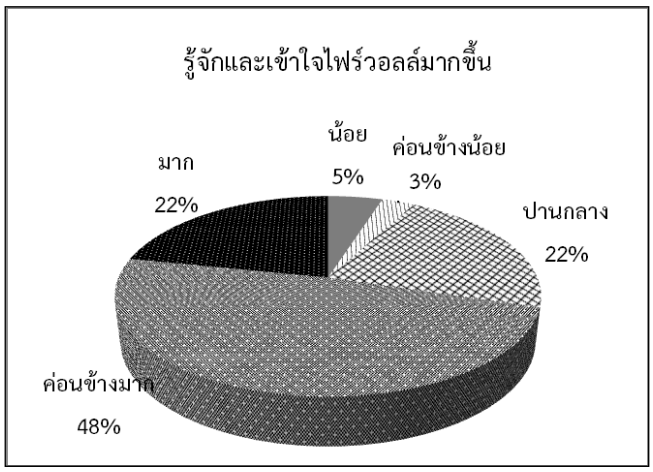
รูปที่ 6-3 ความถี่ในการตรวจสอบช่องโหว่

จากผลตอบแบบสอบถาม พบว่าผู้ตอบส่วนใหญ่คิดว่าเนื้อหาในเว็บสามารถนำไปประยุกต์ใช้ในบริษัทได้ดี โดยมีส่วนน้อยที่คิดว่าอาจจะนำไปใช้งานได้น้อยและค่อนข้างน้อย รูปที่ 6-4 แสดงระดับความพอใจในการนำไปประยุกต์ใช้ในบริษัท



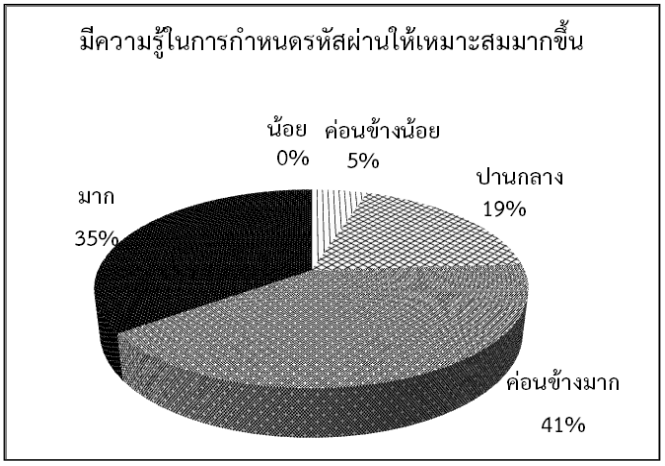
รูปที่ 6-4 สัดส่วนของความพอใจในการประยุกต์ใช้งานในบริษัท

ส่วนใหญ่ผู้ตอบเมื่ออ่านเนื้อหาบนเว็บแล้วมีความรู้และเข้าใจไฟร์วอลล์ตั้งแต่ระดับปานกลางถึงมาก พบว่ามีเพียง 8 เปอร์เซ็นต์ที่คิดว่าเข้าใจได้น้อยหรือค่อนข้างน้อย ดังรูปที่ 6-5



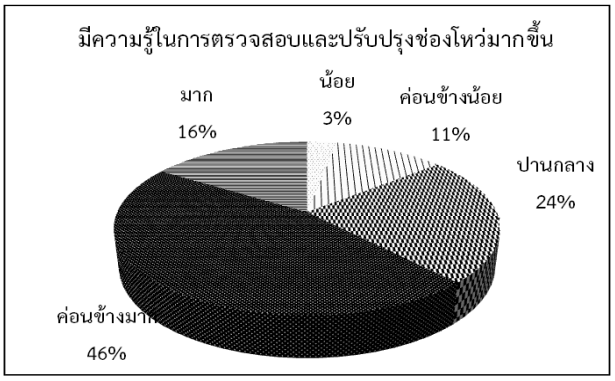
รูปที่ 6-5 สัดส่วนของระดับความเข้าใจในไฟร์วอลล์

ผู้ตอบถึงร้อยละ 95 คิดว่าได้รับความรู้ในการกำหนดรหัสผ่านให้เหมาะสม (ตั้งแต่ระดับปานกลางขึ้นไป) มีเพียงร้อยละ 5 เท่านั้นที่คิดว่าได้รับความรู้ค่อนข้างน้อย ซึ่งแสดงในรูปที่ 6-6



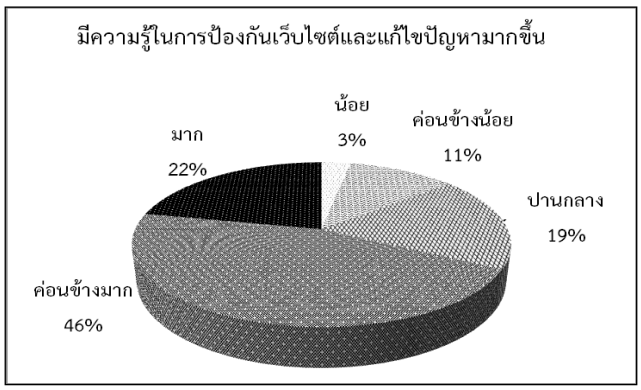
รูปที่ 6-6 สัดส่วนของระดับความเข้าใจในการกำหนดรหัสผ่านให้เหมาะสม

ผู้ตอบส่วนใหญ่ถึงร้อยละ 46 คิดว่าได้ความรู้ในการตรวจสอบและปรับปรุงช่องโหว่ค่อนข้างมาก และมีเพียง 3 เปอร์เซ็นต์ที่คิดว่าได้รับความรู้ในส่วนนี้ได้น้อย ซึ่งดังรูปที่ 6-7



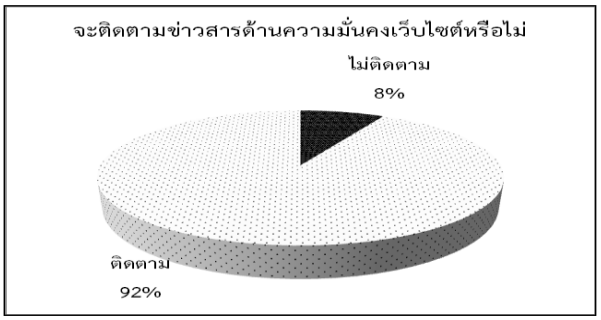
รูปที่ 6-7 สัดส่วนของระดับความเข้าใจในการตรวจสอบและปรับปรุงช่องโหว่

ส่วนใหญ่เมื่ออ่านแล้ว มีความรู้ในการจัดการเว็บไซต์มากขึ้น มีเพียงร้อยละ 3 และ 11 เท่านั้นที่คิดว่าได้รับความรู้น้อยและค่อนข้างน้อย แสดงในรูปที่ 6-8



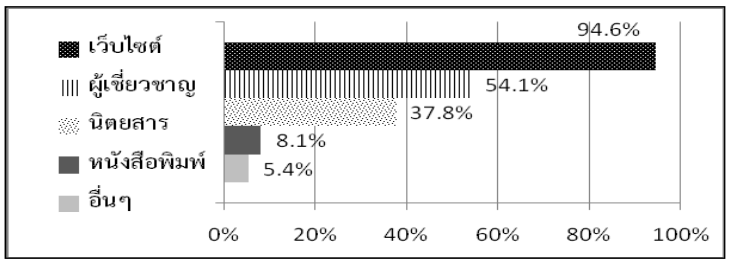
รูปที่ 6-8 สัดส่วนของระดับความเข้าใจในการป้องกันเว็บไซต์และจัดการปัญหา

ความสนใจที่ผู้ตอบจะติดตามข่าวสารด้านความมั่นคงเว็บไซต์ต่อไปนั้น พบว่าร้อยละ 92 คิดว่าจะติดตามข่าวสารด้านความมั่นคงเว็บไซต์ต่อไป ดังรูปที่ 6-9



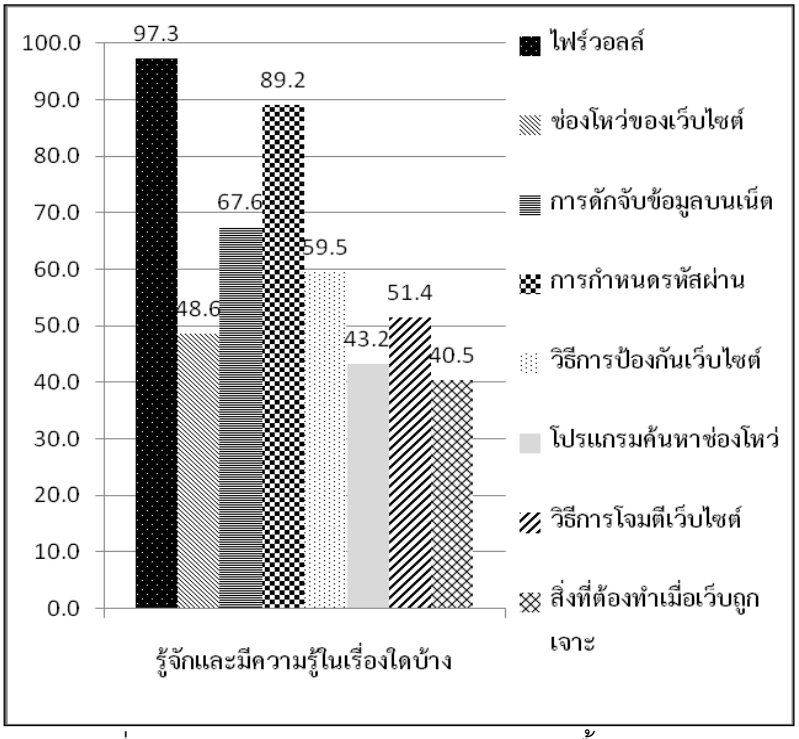
รูปที่ 6-9 สัดส่วนของจำนวนผู้ที่จะติดตามข่าวสารด้านความมั่นคงต่อไป

และส่วนใหญ่นิยมติดตามข่าวสารจากเว็บไซต์ และรองลงไปคือ ปรึกษาจากผู้เชี่ยวชาญ หรืออ่านจากนิตยสาร



รูปที่ 6-10 จำนวนเปอร์เซ็นต์ของแหล่งข่าวสารที่เจ้าของกิจการจะติดตาม

เมื่อเจ้าของกิจการได้อ่านเนื้อหาแล้ว ส่วนใหญ่มีความรู้และความเข้าใจในเรื่องไฟร์วอลล์ และการกำหนดรหัสผ่านมากเป็นสองอันดับแรก ดังรูปที่ 6-11 สำหรับเจ้าของกิจการที่ไม่ได้จบด้านไอทีส่วนใหญ่จะมีความเข้าใจในเรื่องไฟร์วอลล์ และการกำหนดรหัสผ่าน และมีส่วนน้อยที่มีความเข้าใจในเรื่องช่องโหว่ของเว็บไซต์ การป้องกันเว็บไซต์ และมีส่วนน้อยมากที่มีความรู้และความเข้าใจว่าจะต้องทำอย่างไรเมื่อเว็บไซต์ถูกเจาะ



รูปที่ 6-11 สัดส่วนของความเข้าใจในแต่ละเนื้อหาความรู้

ส่วนเรื่องความสนใจที่จะป้องกันเว็บไซต์ของตนเอง เจ้าของกิจการ/บริษัทส่วนใหญ่ได้ให้ความสำคัญในการจัดการรหัสผ่านเป็นอันดับแรก รองลงไปคือดูแลและป้องกันโดยการใช้งานไฟร์วอลล์ รวมทั้งการตรวจสอบช่องโหว่และติดตามข่าวสารอย่างสม่ำเสมอ ดังตารางที่ 6-3

ตารางที่ 6-3 ร้อยละของสิ่งที่บริษัทได้ทำเพื่อป้องกันเว็บไซต์ของตนเอง

อันดับที่	**บริษัท SMEs ได้ทำสิ่งใดแล้วบ้าง**	**จำนวนร้อยละ**
1	กำหนดรหัสผ่านให้เหมาะสม	91.9
2	ติดตั้งและใช้งานไฟร์วอลล์	64.9
3	ติดตามข่าวสารด้านความมั่นคงเว็บไซต์	54.1
4	ตรวจสอบช่องโหว่อย่างสม่ำเสมอ	40.5
5	ปรับปรุงช่องโหว่ในทันที	29.7
6	ใช้โปรแกรมถ่ายโอนที่เข้ารหัส	29.7

โดยในบทสุดท้ายจะสรุปผลการวิจัย ทั้งในส่วนของการสร้างเว็บไซต์ต้นแบบ รวมถึงข้อเสนอแนะและปัญหาที่เกิดขึ้นจากการวิจัยนี้

บทที่ 7

สรุปผลการวิจัยและข้อเสนอแนะ

ในบทก่อนได้แสดงผลการเปรียบเทียบเว็บต้นแบบกับเว็บให้ความรู้อื่น รวมทั้งผลของการประเมินเว็บไซต์ต้นแบบทั้งในส่วนของการออกแบบและส่วนของเนื้อหาความรู้ ซึ่งผลตอบแบบสอบถามทำให้ทราบถึงแนวทางการป้องกันเว็บไซต์ของแต่ละบริษัท ความใส่ใจในการป้องกันเว็บไซต์ โดยผลสรุปของการวิจัย ข้อเสนอแนะ และปัญหาที่เกิดขึ้นในการวิจัยมีดังนี้

7.1 สรุปผลการวิจัย

จากการวิจัยนี้ ทำให้เห็นถึงภาพรวมในการสร้างเว็บไซต์ทั้งในส่วนของการออกแบบเว็บไซต์ การนำเสนอเนื้อหาความรู้ในเว็บไซต์ ซึ่งได้มาจากความพึงพอใจในแบบสอบถามของเจ้าของกิจการ SME ทั้งนี้จากการวิจัยทำให้สามารถสรุปกรอบวิธีในการออกแบบสร้างเว็บไซต์ต้นแบบสำหรับเจ้าของกิจการ SME โดยผลสรุปการวิจัยมีดังนี้

5.1.5 สรุปผลการสร้างเว็บไซต์ต้นแบบสำหรับเจ้าของกิจการ SME

สำหรับการสร้างเว็บไซต์ต้นแบบโดยรวมเป็นที่น่าพอใจ แม้มีบางจุดที่ต้องปรับปรุงแต่ก็เป็นส่วนน้อยเช่น ความสม่ำเสมอของฟอนต์ในบางหน้าและการเพิ่มขนาดช่องไฟเพื่อให้อ่านได้ง่ายขึ้น

สำหรับส่วนของเนื้อหาความรู้บนเว็บไซต์ แม้เนื้อหาในเว็บเป็นเนื้อหาเฉพาะทางแต่ผู้ทดสอบก็สามารถอ่านได้เข้าใจและสามารถตอบคำถามในแบบสอบถามได้อย่างถูกต้อง อีกทั้งผลตอบรับเกี่ยวกับเนื้อหาในเว็บไซต์เป็นที่น่าพอใจโดยดูจากผลตอบในแบบสอบถาม ซึ่งผู้ตอบส่วนใหญ่อ่านแล้วได้ประโยชน์และสามารถนำความรู้ไปประยุกต์ใช้กับบริษัทของตนเองได้ โดย

สำหรับผลตอบแบบสอบถามพบว่า บริษัทส่วนใหญ่ไม่ค่อยให้ความสนใจในการตรวจหาช่องโหว่ของเว็บไซต์ เป็นเพราะบริษัทส่วนใหญ่ยังขาดความรู้ในการจัดการปัญหาด้านความมั่นคงของเว็บไซต์ ซึ่งมีเพียงส่วนน้อยเท่านั้นที่นานครั้งจะตรวจสอบเว็บไซต์ของตนเอง แต่เจ้าของบริษัทส่วนใหญ่มีความสนใจที่จะติดตามข้อมูลข่าวสารด้านความมั่นคงบนเว็บไซต์ และนิยมที่จะศึกษาความรู้จากเว็บไซต์

5.1.6 สรุปกรอบวิธีในการสร้างเว็บไซต์ต้นแบบสำหรับเจ้าของกิจการ SME

จากการวิจัยนี้ทำให้ได้ข้อสรุปเกี่ยวกับกรอบวิธีในการสร้างเว็บไซต์ให้เหมาะกับเจ้าของกิจการเอสเอ็มอี ดังในตารางที่ 7-1

ตารางที่ 7-1 สรุปกรอบวิธีในการสร้างเว็บไซต์ให้เหมาะกับเจ้าของกิจการ

ข้อที่	รายละเอียดของกรอบวิธีในการสร้างเว็บไซต์
1	กำหนดความกว้างของเว็บเป็น 1024 พิกเซล เพื่อให้เหมาะกับขนาดหน้าจอคอมพิวเตอร์ปัจจุบัน
2	เน้นโทนสีฟ้าเพื่อให้ดูสบายตา พื้นเว็บเป็นสีขาว เน้นตัวอักษรสีดำขนาดไม่ต่ำกว่า 16 พิกเซล สำหรับการกำหนดพื้นสีของเว็บเป็นสีขาว แม้มีประเด็นเรื่องการสิ้นเปลืองพลังงาน แต่เนื่องจากเป็นการล้อเลียนเอกสารกระดาษที่เป็นตัวดำพื้นขาว ซึ่งจะเหมาะกับผู้สูงอายุที่คุ้นเคยกับการอ่านกระดาษ
3	เลือกใช้ฟอนต์ Tahoma Microsoft San Sarif และ Thonburi ซึ่งสามารถเข้าชมเว็บได้จากหลายแพลตฟอร์มทั้ง Windows Linux และ Macintosh
4	ไม่ควรแบ่งหน้าเว็บเกินสองคอลัมน์ และเลือกใช้การเปลี่ยนสีฟอนด์หรือเลือกใส่สีพื้นหลังแทน เพื่อเน้นเนื้อหาที่ต้องการให้รู้
5	ลดความสูงของโลโก้ด้านบนและตัดส่วนของ Footer ออก เพื่อเลี่ยงการเกิด Scroll Bar และเพิ่มพื้นที่เนื้อหาบริเวณตรงกลางของหน้าจอ
6	ใช้สีของลิงค์เป็นสีน้ำเงินเข้มและเมื่อเมาส์ลากผ่านข้อความของลิงค์จะถูกขีดเส้นใต้ เพื่อให้ผู้ใช้สะดุดตาและเห็นถึงความแตกต่างระหว่างเนื้อหาทั่วไปกับลิงค์นั้น
7	ใช้เมนูด้านบน (Top Menu) แสดงกลุ่มของเนื้อหาในเว็บ โดยเลี่ยงการใช้เมนูแบบ Drop-Down และใช้เมนูด้านซ้าย (Left Menu) แทนการแสดงหัวเรื่องในแต่ละกลุ่มของเนื้อหา
8	ใช้ Icon ขนาดเล็ก ไม่ใช้รูปภาพขนาดใหญ่หรือลูกเล่นที่ไม่เกี่ยวกับเนื้อหา ทำให้เข้าถึงเว็บเพจได้เร็ว
9	สร้างเนื้อหาความรู้เป็นภาษาไทยที่อ่านเข้าใจได้ง่าย หลีกเลี่ยงภาษาที่ซับซ้อน เน้นหาคำขยายความอย่างง่าย แทนการใช้คำศัพท์วิชาการหรือศัพท์เทคนิค

7.2 ปัญหาและอุปสรรค

1) ความซับซ้อนเกี่ยวกับเนื้อหาเกี่ยวกับความมั่นคงเว็บไซต์ จึงต้องนำมาจัดหมวดหมู่เนื้อหาที่เหมาะสมก่อน
2) การนำเสนอเนื้อหาให้เหมาะสมกับเจ้าของเอสเอ็มอี ซึ่งจะต้องอ่านเข้าใจได้ง่าย สบายตาและนำไปประยุกต์ใช้งานได้
3) ความยากลำบากในการประชาสัมพันธ์และเชิญชวนให้เจ้าของกิจการและบริษัทเนื่องจากไม่สามารถติดต่อกับเจ้าของกิจการและบริษัทได้โดยตรง รวมทั้งเจ้าของกิจการหรือบริษัทเองไม่มีเวลามากนัก จึงทำให้มีจำนวนผู้มาทดลองใช้งานเว็บต้นแบบและตอบแบบประเมินมีไม่มากนัก

7.3 ข้อเสนอแนะในการพัฒนาระบบต่อไป

เว็บต้นแบบนี้สร้างขึ้นเพื่อให้ความรู้ด้านความมั่นคงเว็บไซต์ให้กับเจ้าของกิจการหรือบริษัทที่ไม่มีความรู้มากนัก (ซึ่งรวมไปถึงผู้ที่เริ่มต้นสนใจในความรู้ด้านนี้) เพื่อให้เกิดความตระหนักถึงภัยคุกคามซึ่งมีผลต่อองค์กร อย่างไรก็ดีเนื้อหาในเว็บต้นแบบนี้เป็นเพียงส่วนหนึ่งของความรู้ด้านความมั่นคงเว็บไซต์ และเป็นเพียงระดับเริ่มต้นเท่านั้น ดังนั้นในการพัฒนาต่อไปควรที่จะมีการเพิ่มเนื้อหาความรู้ให้มีความเข้มข้นมากขึ้น นอกจากนี้จะปรับปรุงในส่วนของแบบสอบถามให้มีความกระชับ โดยควรลดจำนวนคำถามลง (เลือกคำถามเฉพาะที่สำคัญ) เพื่อหลีกเลี่ยงการเกิด Scroll Bar ทั้งนี้ในแบบสอบถามควรให้ผู้ทดสอบได้เสนอแนะเนื้อหาความรู้ที่ต้องการทราบเพื่อให้เกิดประโยชน์กับผู้ทดสอบต่อไป รวมถึงจำนวนคำถามของแบบสอบถามที่ผู้ตอบคิดว่าเหมาะสม เพื่อนำไปใช้ประยุกต์ในงานวิจัยอื่น และจำนวนเวลาหรือจำนวนเงินที่ลงทุนในการป้องกันเว็บไซต์ เพื่อจะได้ทราบว่าภาพรวมการลงทุนในเรื่องนี้ประมาณเท่าไร ซึ่งจะได้ช่วยในการตัดสินใจถึงความคุ้มทุนในการจัดการ ซึ่งถ้าไม่คุ้มกับการลงทุน กิจการหรือบริษัทขนาดกลางและขนาดย่อม (SMEs) อาจจะเลือกใช้บริการรับฝากเว็บไซต์ที่มีความชำนาญเข้ามาจัดการแทน

รายการอ้างอิง

[1] The Office of Small and Medium Enterprise Promotion (OSMEP). รายงานสถานการณ์วิสาหกิจขนาดกลางและขนาดย่อมปี 2553 และแนวโน้มปี 2554: จำนวนและการจ้างงานวิสาหกิจขนาดกลางและขนาดย่อมปี 2553 [ออนไลน์]. แหล่งที่มา: http://www.sme.go.th/Documents/2554/whitepaper-2553/chapter-4-edit.pdf [2554, กันยายน 27]

[2] Institute for Small and Medium Enterprises Development. นิยาม SMEs [ออนไลน์]. แหล่งที่มา: http://www.ismed.or.th/SME/src/bin/controller.php?view=generalContents.GeneralContent&form=&rule=generalContents.FMGeneralContent.bctrl_Id=273 [2552, เมษายน 16]

[3] M.E. Jennex and T. Addo. SMEs and Knowledge Requirements for Operating Hacker and Security Tools. *Proceedings of Information Resources Management Association International Conference (IRMA 2004)*, 2004.

[4] J.K. Bakari, C. Magnusson, C.N. Tarimo and L. Yngström. Outsourcing ICT security to MSSP: Issues and Challenges for the developing world. *Proceedings of Information Security South Africa (ISSA)*, 2006.

[5] P. Hom-anek. Information Security Management Outsourcing เหตุผล และมุมมองการวิเคราะห์ข้อดี /ข้อเสีย ในการบริหารระบบความปลอดภัยคอมพิวเตอร์ [ออนไลน์]. แหล่งที่มา: http://acisonline.net/article_prinya_eleader_010847.htm [2552, มีนาคม 12]

[6] Web Application Security Consortium. Web application security statistics project 2007 [Online]. Available from: http://www.webappsec.org/projects/statistics/wasc_wass_2007.pdf [2009, May 20]

[7] Open Web Application Security Project. OWASP Top 10 2010 [Online]. Available from: http://owasptop10.googlecode.com/files/OWASP Top 10 - 2010.pdf [2011, May 6]

[8] Zone-h.org. Zone-H's list of hacked sites to find websites whose security status makes them vulnerable [Online]. Available from: http://www.zone-h.org [2010, Dec 15]

[9] Global Technology Integrated Co. ภาพรวมเว็บไทยที่ถูกโจมตี ตั้งแต่ปี 1999 - 2011 [ออนไลน์]. แหล่งที่มา: http://who.sran.org/audit [2554, ตุลาคม 4]

[10] M. Shema. *HackNotes Network Security Portable Reference*. California: Osborne/McGraw-Hill, 2003.

[11] National Institute of Standards and Technology. Guidelines on Securing Public Web Servers [Online]. Available from: http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf [2009, March 5]

[12] S. Kurniawan, P. Zaphiris. Research-Derived Web Design Guidelines for Older People. *Proceedings of 7th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS'05)*, pp.129-135, 2005.

[13] The ISO 27000 Directory [Online]. Available from: http://www.27000.org/iso-27001.htm

[14] NECTEC (Thai-CERT). มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550 [ออนไลน์]. แหล่งที่มา: http://www.thaicert.nectec.or.th/paper/basic/Book_2.5_Fullversion.pdf [2552, เมษายน 19]

[15] CERT-In. Web Server Security Guidelines Checklist [Online]. Available from: http://www.cert-in.org.in/knowledgebase/guidelines/CISG-2004-04.pdf [2009, April 23]

[16] Internet Security Alliance. Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices [Online]. Available from: http://www.lansingcaninetrainingcenter.com/practices/ISABestPractices.pdf [2009, March 5]

[17] P. Gregor, A.F. Newell, and M. Zajicek. Designing for dynamic diversity – interfaces for older people. *Proceedings of the 5th International ACM*

SIGCAPH Conference on Assistive Technologies (ASSETS 2002), pp.151-156, 2002.

[18] T. Fidgeon. Usability for Older Web Users. WebCredible [Online]. Available from: http://www.webcredible.co.uk/user-friendly-resources/web-usability/older-users.shtml [2009, April 20]

[19] National Institute on Aging. Making Your Web Site Senior Friendly: A Checklist [Online]. Available from: http://www.nlm.nih.gov/pubs/checklist.pdf [2009, April 23]

[20] J. Nielsen. Usability for Senior Citizens, Jakob Nielsen's Alertbox [Online]. Available from: http://www.useit.com/alertbox/seniors.html [2009, April 20]

[21] Joomla [Online]. Available from: http://www.joomla.org [2009, April 25]

[22] PHPNuke [Online]. Available from: http://www.phpnuke.org [2009, April 26]

[23] Mambo [Online]. Available from: http://mambo-foundation.org [2009, April 24]

[24] Drupal [Online]. Available from: http://drupal.org [2009, April 25]

[25] Council of University Faculty Senate of Thailand. ขั้นตอนการพัฒนาแบบสอบถาม [ออนไลน์]. แหล่งที่มา: http://thaifacultysenate.com/Questionaing.aspx [2009, April 23]

[26] นัทธมน ธีระกุล. เอกสารการประกอบบรรยาย การออกแบบสอบถาม [ออนไลน์]. แหล่งที่มา: http://www.mcc.cmu.ac.th/agbus/data/present/Nov29_46.pdf [2552, เมษายน 23]

[27] Wikipedia. ไฟร์วอลล์ [ออนไลน์]. แหล่งที่มา: http://th.wikipedia.org/wiki/Firewall [2554, กุมภาพันธ์ 21]

[28] ThaiCERT. ความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์ (Firewall) [ออนไลน์]. แหล่งที่มา: http://www.thaicert.nectec.or.th/paper/firewall/fwbasics.php [2554, กุมภาพันธ์ 21]

[29] Google. [Online]. Available from: http://www.google.co.th [2011,Feb 20]

ภาคผนวก

ภาคผนวก ก

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.5		**นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ)Security Policy)**			
A5.1		Information Security Policy			
A.5.1.1	1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร	√	√	√
A.5.1.2	2	การทบทวนนโยบายความมั่นคงปลอดภัย			
A.6		**โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร**)Organizational of Information Security)			
		แนวปฏิบัติด้านความมั่นคงไม่ได้เน้นในส่วนของการจัดการภายในและบริษัท SMEs มีขนาดเล็กและจำนวนพนักงานไม่มาก โครงสร้างองค์กรไม่ซับซ้อน	ไม่มี	ไม่มี	ไม่มี
A.7		Assets management			
		แนวปฏิบัติด้านความมั่นคงไม่ได้เน้นในส่วนการบริหารจัดการทรัพย์สินขององค์กร เนื่องจากใช้เครื่องคอมพิวเตอร์เป็นเว็บไซต์เพียงเครื่องเดียว	ไม่มี	ไม่มี	ไม่มี
A.8		Human resources security			
A.8.1		Prior to employment			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.8.1.1	19	การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย			
A.8.1.2	20	การตรวจสอบคุณสมบัติของผู้สมัคร			
A.8.1.3	21	การกำหนดเงื่อนไขการจ้างงาน			
A.8.2.1	22	หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย	√		√
A.8.2.2	23	การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน	√		√
A.8.2.3	24	กระบวนการทางวินัยเพื่อลงโทษ			
A.8.3		Termination or change of employment			
A.8.3.1	25	การสิ้นสุดหรือการเปลี่ยนการจ้างงาน			
A.8.3.2	26	การคืนทรัพย์สินขององค์กร			
A.8.3.3	27	การถอดถอนสิทธิในการเข้าถึง			
A.9		**Physical and environmental security**			
A.9.1.1	28	การจัดทำบริเวณล้อมรอบ		√	√
A.9.1.2	29	การควบคุมการเข้าออก-		√	√
A.9.1.3	30	การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ			
A.9.1.4	31	การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม			
A.9.1.5	32	การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.9.1.6	33	การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก			
A.9.2		Equipment security			
A.9.2.1	34	การจัดวางและการป้องกันอุปกรณ์		√	√
A.9.2.2	35	ระบบและอุปกรณ์สนับสนุนการทำงาน		√	√
A.9.2.3	36	การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ			
A.9.2.4	37	การบำรุงรักษาอุปกรณ์			
A.9.2.5	38	การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน			
A.9.2.6	39	การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง			
A.9.2.7	40	การนำทรัพย์สินขององค์กรออกนอกสำนักงาน			
A.10		**Communication and operations management**			
A.10.1		Operational procedures and responsibilities			
A.10.1.1	41	ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร			
A.10.1.2	42	การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ			
A.10.1.3	43	การแบ่งหน้าที่ความรับผิดชอบ			
A.10.1.4	44	การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.10.2		Third party service delivery management			
A.10.2.1	45	การให้บริการโดยหน่วยงานภายนอก			
A.10.2.2	46	การตรวจสอบการให้บริการโดยหน่วยงานภายนอก			
A.10.2.3	47	การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ			
A.10.3		System planning and acceptance			
A.10.3.1	48	การวางแผนความต้องการทรัพยากรสารสนเทศ	√		√
A.10.3.2	49	การตรวจรับระบบ			
A.10.4		Protection against malicious and mobile code			
A.10.4.1	50	การป้องกันโปรแกรมที่ไม่ประสงค์ดี	√	√	√
A.10.4.2	51	การป้องกันโปรแกรมชนิดเคลื่อนที่			
A.10.5		Back-up			
A.10.5.1	52	การสำรองข้อมูล	√	√	√
A.10.6		Network security management			
A.10.6.1	53	มาตรการทางเครือข่าย	√	√	√
A.10.6.2	54	ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย	√	√	√
A.10.7		Media handling			
A.10.7.1	55	การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้			
A.10.7.2	56	การกำจัดสื่อบันทึกข้อมูล			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	**มาตรการที่**	**ข้อกำหนดตาม** ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.10.7.3	57	ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ			
A.10.7.4	58	การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ			
A.10.8		Exchange of information			
A.10.8.1	59	การพาณิชย์อิเล็กทรอนิกส์			
A.10.8.2	60	การทำธุรกรรมออนไลน์			
A.10.8.3	61	สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ			
A.10.8.4	62	การส่งข้อความทางอิเล็กทรอนิกส์			
A.10.8.5	63	ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน			
A.10.9		Electronic commerce Service			
A.10.9.1	64	การพาณิชย์อิเล็กทรอนิกส์			
A.10.9.2	65	การทำธุรกรรมออนไลน์			
A.10.9.3	66	สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ	√	√	
A.10.10		Monitoring			
A.10.10.1	67	การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ	√	√	√
A.10.10.2	68	การตรวจสอบการใช้งานระบบ	√	√	√
A.10.10.3	69	การป้องกันข้อมูลบันทึกเหตุการณ์			
A.10.10.4	70	บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ			
A.10.10.5	71	การบันทึกเหตุการณ์ข้อผิดพลาด			
A.10.10.6	72	การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.11		**Access Control**			
A.11.1		Business requirement for access control			
A.11.1.1	73	นโยบายการควบคุมการเข้าถึงระบบ			
A.11.2		User access management			
A.11.2.1	74	การลงทะเบียนพนักงาน			
A.11.2.2	75	การบริหารจัดการสิทธิการใช้งานระบบ			√
A.11.2.3	76	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน	√		√
A.11.2.4	77	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน			
A.11.3		User responsibilities			
A.11.3.1	78	การใช้งานรหัสผ่าน	√	√	√
A.11.3.2	79	การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล			
A.11.3.3	80	นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญ			
A.11.4		Network access control			
A.11.4.1	81	นโยบายการใช้งานบริการเครือข่าย	√	√	√
A.11.4.2	82	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร			
A.11.4.3	83	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย			
A.11.4.4	84	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ			
A.11.4.5	85	การแบ่งแยกเครือข่าย			
A.11.4.6	86	การควบคุมการเชื่อมต่อทางเครือข่าย			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.11.4.7	87	การควบคุมการกำหนดเส้นทางบนเครือข่าย			
A.11.5		Operating system access control			
A.11.5.1	88	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย			
A.11.5.2	89	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน			
A.11.5.3	90	ระบบบริหารจัดการรหัสผ่าน			
A.11.5.4	91	การใช้งานโปรแกรมประเภทยูติลิตี้			
A.11.5.5	92	การหมดเวลาการใช้งานระบบสารสนเทศ			
A.11.5.6	93	การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ			
A.11.6		Application and information access control			
A.11.6.1	94	การจำกัดการเข้าถึงสารสนเทศ			
A.11.6.2	95	การแยกระบบสารสนเทศที่มีความสำคัญสูง			
A.11.7		Mobile computing and teleworking			
A.11.7.1	96	การป้องกันอุปกรณ์สื่อสารประเภทพกพา			
A.11.7.2	97	การปฏิบัติงานจากภายนอกสำนักงาน			
A.12		**Information systems acquisition, development and maintenance**			
A.12.1		Security requirements of information systems			
A.12.1.1	98	การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.12.2		Correct processing in applications			
A.12.2.1	99	การตรวจสอบข้อมูลนำเข้า	√	√	
A.12.2.2	100	การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล	√		
A.12.2.3	101	การตรวจสอบความถูกต้องของข้อความ			
A.12.2.4	102	การตรวจสอบข้อมูลนำออก	√		
A.12.3		Crytographic controls			
A.12.3.1	103	นโยบายการใช้งานการเข้ารหัสข้อมูล	√		√
A.12.3.2	104	การบริหารจัดการกุญแจเข้ารหัสข้อมูล			
A.12.4		Security of system files			
A.12.4.1	105	การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ	√	√	
A.12.4.2	106	การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ			
A.12.4.3	107	การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ	√		
A.12.5		Security in development and support processes			
A.12.5.1	108	ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ			
A.12.5.2	109	การตรวจสอบการทำงานของโปรแกรมประยุกต์ภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ			
A.12.5.3	110	การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	มาตรการที่	ข้อกำหนดตาม ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.12.5.4	111	การป้องกันการรั่วไหลของสารสนเทศ			
A.12.5.5	112	การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก			
A.12.6		Technical Vulnerability Management			
A.12.6.1	113	มาตรการควบคุมช่องโหว่ทางเทคนิค	√	√	
A.13		Information Security Incident Management			
A.13.1		Reporting information security events and weaknesses			
A.13.1.1	114	การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย			
A.13.1.2	115	การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร			
A.13.2		Management of information security incidents and improvements			
A.13.2.1	116	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ	√		√
A.13.2.2	117	การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย			
A.13.2.3	118	การเก็บรวบรวมหลักฐาน			
A.14		Business Continuity Management			
A.14.1		Information security aspects of business continuity management			
A.14.1.1	119	กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ			

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ตารางที่ ก-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ISO-ID	**มาตรการที่**	**ข้อกำหนดตาม** ISO/IEC 27001:2005*	NIST[11]	CERT-In[15]	ISAlliance[16]
A.14.1.2	120	การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ			√
A.14.1.3	121	การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ			
A.14.1.4	122	การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ			
A.14.1.5	123	การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ			
A.15		**Compliance**			
		แนวปฏิบัติด้านความมั่นคงไม่ได้เน้นในการปฏิบัติตามข้อกำหนดของกฎหมาย	ไม่มี	ไม่มี	ไม่มี
สรุป		**28 ข้อ**	**22 ข้อ**	**17 ข้อ**	**24 ข้อ**

* ชื่อมาตรการควบคุมยึดตามมาตรฐานการรักษาความปลอดภัยของ NECTEC เวอร์ชั่น 2.5 [14]

** เครื่องหมาย √ หมายถึง เป็นมาตรการที่สอดคล้องกับ Best Practices และ Guidelines นั้น ถ้าไม่มีเครื่องหมาย √ แสดงว่าไม่ได้กล่าวถึงใน Best Practices และ Guidelines นั้น

ภาคผนวก ข

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
1	1	A5.1.1	1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร	ต้องทำแผนฯเป็นลายลักษณ์อักษรและต้องเผยแพร่ก่อนนำไปใช้งาน
2	4	A.8.2.1	2	หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย	กำหนดหน้าที่ ความรับผิดชอบที่ต้องปฏิบัติ
3	4	A.8.2.2	2	การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน	พนักงานได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายฯและขั้นตอนปฏิบัติที่พนักงานต้องรับผิดชอบด้วย
4	5	A.9.1.1	3	การจัดทำบริเวณล้อมรอบ	การจัดสรรพื้นที่กั้นบริเวณหรือจัดทำผนังหรือกำแพงล้อมรอบ

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	**ข้อกำหนดตามมาตรฐาน ISO**	**คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)**
5	5	A.9.1.2	3	การควบคุมการเข้าออก-	จัดให้มีการควบคุมการเข้าออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาติให้ผ่านเฉพาะผู้ที่ได้รับอนุญาติแล้วเท่านั้น
6	5	A.9.2.1	3	การจัดวางและการป้องกันอุปกรณ์	ต้องวางและป้องกันอุปกรณ์เพื่อลดความความเสี่ยงจากอันตรายต่างๆ รวมไปถึงลดความเสี่ยงในการเข้าถึงอุปกรณ์
7	5	A.9.2.2	3	ระบบและอุปกรณ์สนับสนุนการทำงาน	มีกลไกในการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ
8	6	A.10.3.1	4	การวางแผนความต้องการทรัพยากรสารสนเทศ	ต้องมีการวางแผนเพื่อรองรับอนาคตให้เพียงพอต่อการใช้งาน
9	6	A.10.4.1	4	การป้องกันโปรแกรมที่ไม่ประสงค์ดี	มีมาตรการป้องกันตรวจจับและกู้คืนจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องสร้างความตระหนักเกี่ยวกับผู้ใช้งานด้วย

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
10	6	A.10.5.1	4	การสำรองระบบ (Backup)	ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายสำรองข้อมูลขององค์กร
11	6	A.10.6.1	4	มาตรการทางเครือข่าย	กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆที่ส่งผ่านเครือข่าย
12	6	A.10.6.2	4	ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย	กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่ใช้บริการอยู่

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
13	6	A.10.9.3	4	สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ	ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ
14	6	A.10.10.1	4	การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ	ต้องบันทึกกิจกรรมการใช้งานของผู้ใช้ และเหตุการณ์ต่างๆเกี่ยวกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนด
15	6	A.10.10.2	4	การตรวจสอบการใช้งานระบบ	ต้องมีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่
16	7	A.11.2.2	5	การบริหารจัดการสิทธิการใช้งานระบบ	ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
17	7	A.11.2.3	5	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน	ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดหารหัสผ่านให้แก่ผู้ใช้งานเพื่อให้มีความมั่นคงปลอดภัย
18	7	A.11.3.1	5	การใช้งานรหัสผ่าน	ต้องกำหนดวิธีปฏิบัติที่ดีให้ผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน
19	7	A.11.4.1	1	นโยบายการใช้งานบริการเครือข่าย	ต้องมีการกำหนดว่าบริการใดที่อนุญาติให้สามารถใช้งานได้ และบริการใดไม่สามารถใช้งานได้
20	8	A.12.2.1	6	การตรวจสอบข้อมูลนำเข้า	ต้องกำหนดวิธีตรวจสอบข้อมูลนำเข้าของแอพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผล

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
21	8	A.12.2.2	6	การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล	ต้องกำหนดวิธีตรวจสอบข้อมูลในระหว่างการประมวลผลว่าเกิดความผิดพลาดหรือไม่
22	8	A.12.2.4	6	การตรวจสอบข้อมูลนำออก	ต้องกำหนดวิธีตรวจสอบข้อมูลนำออกจากแอพลิเคชันเพื่อให้มั่นใจว่ามีการประมวลผลไปอย่างถูกต้องและเหมาะสม
23	9	A.12.3.1	1	นโยบายการใช้งานการเข้ารหัสข้อมูล	ต้องมีนโยบายควบคุมการเข้ารหัสข้อมูลในการใช้งานและมีแผนบังคับใช้
24	9	A.12.4.1	6	การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ	ต้องมีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ เพื่อลดความเสี่ยงที่เกิดจากการทำงานผิดพลาดหรือใช้งานไม่ได้
25	9	A.12.4.3	6	การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ	ต้องจำกัดการเข้าถึงซอร์สโค๊ด เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาติ หรือไม่ได้เจตนา

ตารางที่ ข-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หมวดหมู่ ISO	ISO-ID	หมวดใหม่	ข้อกำหนดตามมาตรฐาน ISO	คำอธิบายตามมาตรฐานการรักษาความปลอดภัย เวอร์ชั่น 2.5 ปี 2550 (NECTEC)
26	9	A.12.6.1	6	มาตรการควบคุมช่องโหว่ทางเทคนิค	ต้องติดตามข่าวสารที่เกี่ยวข้องกับช่องโหว่ของระบบ ประเมินความเสี่ยงของช่องโหว่ รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว
27	10	A.13.2.1	1	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการป้องกันหรือแผนเมื่อเกิดเหตุไม่คาดคิด	กำหนดหน้าที่และขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ สามารถทำได้ด้วยความรวดเร็ว ได้ผล และเป็นระบบระเบียบที่ดี
28	11	A.14.1.2	1	การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ	

ภาคผนวก ค

ตารางที่ ค-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์

ลำดับ	หัวเรื่อง	หมวดหมู่	กลุ่มที่แสดงหน้าเว็บ			
			เร่งด่วน	ป้องกัน	ซ่อมแซม	ทั่วไป
1	ทำอย่างไรเมื่อเว็บเราถูกแฮ๊ก	1. กลุ่มแผนและนโยบายการปฏิบัติด้านความมั่นคงเว็บไซต์ (หัวข้อ 1.3)			√	
2	เมื่อไฟล์สำคัญในเว็บถูกเปลี่ยน	1. กลุ่มแผนและนโยบายการปฏิบัติด้านความมั่นคงเว็บไซต์ (หัวข้อ 1.3)			√	
3	หน่วยงานที่ปรึกษาด้านความมั่นคงเว็บไซต์	1. กลุ่มแผนและนโยบายการปฏิบัติด้านความมั่นคงเว็บไซต์ (หัวข้อ 1.3) และ 2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)			√	
4	การดูแลสอดส่อง	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.1) กับ 6. กลุ่มการจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.6)	√	√		
5	คำแนะนำในการปฏิบัติของเจ้าหน้าที่คอมฯ	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.1)		√		

ตารางที่ ค-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หัวเรื่อง	หมวดหมู่	กลุ่มที่แสดงหน้าเว็บ			
			เว็บบอร์ด	ป้องกัน	ซุ่มแฮก	อื่นๆ
6	ข้อคิดในการดูแลเว็บ	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)		√		
7	รู้ได้อย่างไรว่าเว็บเราถูกเจาะ	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)			√	
8	แนวคิดการป้องกันเว็บไซต์	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)				√
9	ช่องโหว่เว็บไซต์มาจากที่ไหน	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)				√
10	คนร้ายเจาะเว็บไซต์ได้อย่างไร	2. กลุ่มความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (หัวข้อ 2.2)				√
11	ความปลอดภัยในที่จัดวางเว็บไซต์	3. กลุ่มความมั่นคงปลอดภัยทางกายภาพอุปกรณ์และสิ่งแวดล้อม		√		

ตารางที่ ค-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หัวเรื่อง	หมวดหมู่	กลุ่มที่แสดงหน้าเว็บ			
			เร่งด่วน	ป้องกัน	สถานะ	ความรู้
12	ไฟร์วอลล์คืออะไร	3. กลุ่มความมั่นคงปลอดภัยทางกายภาพ อุปกรณ์และสิ่งแวดล้อม (หัวข้อ 3.4) กับ 4. กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (หัวข้อ 4.5)	√			√
13	ทำไมต้องสำเนาข้อมูล	4. กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (หัวข้อ 4.3)				√
14	การขโมยข้อมูลบนเน็ต	4. กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (หัวข้อ 4.4)				√
15	การโจมตีก่อกวนให้ทำงานไม่ได้	4. กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (หัวข้อ 4.4)				√

ตารางที่ ค-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หัวเรื่อง	หมวดหมู่	กลุ่มที่แสดงหน้าเว็บ			
			เว็บสาธารณะ	เว็บปิดกั้น	เว็บสมาชิก	เว็บรัฐ
16	การป้องกันเว็บเบื้องต้น	4. กลุ่มการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (หัวข้อ 4.5)		√		
17	รหัสผ่านคืออะไร	5. กลุ่มการควบคุมการเข้าถึง (หัวข้อ 5.3)				√
18	แนวทางการตั้งรหัสผ่าน	5. กลุ่มการควบคุมการเข้าถึง (หัวข้อ 5.3)	√			√
19	สร้างเว็บอย่างไรให้ปลอดภัย	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ		√		
20	การโจมตีโดยการใส่ข้อมูลที่ไม่ถูกต้อง	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.1 – 6.2)				√
21	ทดสอบเว็บอย่างง่ายๆ โดยการใส่ข้อมูลแปลกๆ	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.1 – 6.2)				√
22	การลงโปรแกรมอย่างระมัดระวัง	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.5)	√			

ตารางที่ ค-1 ผลการเปรียบเทียบหมวดหมู่ด้านความมั่นคงเว็บไซต์ (ต่อ)

ลำดับ	หัวเรื่อง	หมวดหมู่	กลุ่มที่แสดงหน้าเว็บ			
			ทั่วไป	ป้องกัน	ตอบโต้	ตรวจ
23	โปรแกรมหาช่องโหว่	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.6)		√		
24	การโจมตีผ่านช่องโหว่ของโปรแกรม	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.6)				√
25	การหลอกถามหรือโทรศัพท์เพื่ออำหาข้อมูล	6. กลุ่มการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (หัวข้อ 6.6)				√

ภาคผนวก ง

แสดงแบบประเมินเว็บความรู้เรื่องการป้องกันการโจมตีเว็บไซต์

แบบประเมินนี้เป็นส่วนหนึ่งของงานวิจัย ซึ่งจะต้องกรอกโดยเจ้าของบริษัทและควรอ่านเนื้อหาที่เว็บ http://www.th-sme-websecurity.com ก่อนกรอกแบบสอบถาม โดยข้อมูลส่วนตัวจะถูกเก็บไว้เป็นความลับ ผลการตอบแบบสอบถามจะถูกใช้ในการปรับปรุงงานวิจัยต่อไป

สามารถกรอกออนไลน์ได้ที่ http://www.th-sme-websecurity.com/questioniare/

ชื่อผู้กรอกแบบประเมิน ……..
อีเมล์ของผู้กรอกแบบประเมิน …… (ถ้ามี)
เบอร์โทรศัพท์ ……

ข้อมูลผู้ตอบแบบสอบถามและบริษัท

1. ชื่อบริษัท/ห้างหุ้นส่วน/กิจการ …… (ที่เป็นเจ้าของ)

2. จำนวนพนักงานในบริษัท

   ☐ น้อยกว่า 10 คน ☐ 10 – 25 คน ☐ 25 – 50 คน ☐ มากกว่า 50 คน

3. อายุของผู้กรอกแบบสอบถาม

   ☐ น้อยกว่า 10 คน ☐ 10 – 25 คน ☐ 25 – 50 คน ☐ มากกว่า 50 คน

4. ระดับการศึกษาสูงสุด

   ☐ ต่ำกว่าปริญญาตรี

   ☐ ปริญญาตรีสาขา IT หรือสาขาที่เกี่ยวข้อง

   ☐ ปริญญาตรีสาขาอื่นๆ

   ☐ ปริญญาโทสาขา IT หรือสาขาที่เกี่ยวข้อง

   ☐ ปริญญาโทสาขาอื่นๆ

   ☐ ปริญญาเอก

5. บริษัทของคุณมีเว็บไซต์หรือไม่

   ☐ มี

   ☐ ไม่มี (แต่คิดว่าจะมีในเร็วๆนี้)

   ☐ ไม่มี (และยังไม่คิดจะมีในตอนนี้)

6. จำนวนเจ้าหน้าที่<u>คอมพิวเตอร์</u>ทั้งหมดในบริษัท

   ☐ ไม่มี ☐ 1 – 2 คน ☐ 3 – 5 คน ☐ 6 คนขึ้นไป

7. จำนวนคอมพิวเตอร์ในบริษัท _____ เครื่อง

<u>ความเข้าใจในเนื้อหาบนเว็บ</u>

8. คุณรู้จักหรือมีความรู้ด้านความมั่นคงเว็บไซต์บ้างหรือไม่ ถ้ารู้จักกรุณาทำเครื่องหมายในข้อที่คุณรู้จัก (ตอบได้มากกว่า 1 ข้อ)

   ☐ ไฟร์วอลล์ ☐ ช่องโหว่ของเว็บไซต์

   ☐ การดักจับข้อมูลบนเน็ต ☐ การกำหนดรหัสผ่าน

   ☐ การป้องกันเว็บไซต์จากคนร้าย ☐ โปรแกรมค้นหาช่องโหว่

   ☐ วิธีการโจมตีเว็บไซต์ของคนร้าย ☐ สิ่งที่ควรทำเมื่อเว็บไซต์ถูกโจมตี

9. คุณรู้จักไฟร์วอลล์หรือไม่ ถ้ารู้จักกรุณาทำเครื่องหมายในข้อที่คุณเข้าใจว่าเป็นไฟร์วอลล์

   ☐ ไม่รู้จัก

   ☐ หาช่องโหว่ของเว็บไซต์

   ☐ กรองหรือกักข้อมูลเข้าออกเว็บไซต์ทำหน้าที่คล้ายรปภ.

10. คุณสามารถนำมาประยุกต์ใช้กับบริษัทและกำชับให้เจ้าหน้าที่คอมฯของบริษัทจัดการเกี่ยวกับความมั่นคงเว็บไซต์ได้

	1	2	3	4	5	
เห็นด้วยน้อย	O	o	o	o	o	เห็นด้วยมาก

11. เมื่อคุณอ่านเนื้อหาบนเว็บแล้วคุณมีความเข้าใจในระดับไหน (เลือกตอบตามช่องระดับความเข้าใจ)

ข้อ	คำถาม	ระดับความเข้าใจ				
		น้อย	ค่อนข้างน้อย	ปานกลาง	ค่อนข้าง มาก	มาก
11.1	รู้จักและเข้าใจไฟร์วอลล์มากขึ้น					
11.2	การกำหนดรหัสผ่านให้เหมาะสม					
11.3	การตรวจสอบและปรับปรุงช่องโหว่					
11.4	คำแนะนำในการป้องกันเว็บไซต์และการแก้ไขปัญหา					

12. คุณรู้จักหน่วยงานที่ให้คำแนะนำเกี่ยวกับความมั่นคงเว็บไซต์ (เช่น ThaiCERT) หรือไม่

- ☐ รู้จัก
- ☐ ไม่รู้จัก

13. อะไรที่ทำให้คุณคิดว่าเว็บของคุณถูกขโมย (ตอบได้มากกว่า 1 ข้อ)

- ☐ เจ้าหน้าที่ฝ่ายคอมฯมาบอก
- ☐ หน้าเว็บไซต์ของคุณถูกเปลี่ยน
- ☐ รหัสผ่านของคุณเปลี่ยนไป
- ☐ มีการเข้าใช้งานเว็บไซต์ โดยที่คุณไม่ได้ใช้งาน

14. อะไรเป็นสิ่งคุณควรจะทำเมื่อเว็บไซต์ถูกขโมย (เลือกตอบข้อที่ดีที่สุดเพียงข้อเดียว)

- ☐ ปิดเครื่องในทันที
- ☐ ตัดการเชื่อมต่อเว็บไซต์จากอินเทอร์เน็ต
- ☐ ติดต่อหน่วยงานให้ความช่วยเหลือความมั่นคงเว็บไซต์

แนวทางในการป้องกันเว็บไซต์

15. บริษัทของคุณได้ทำสิ่งใดแล้วบ้าง (ตอบได้มากกว่า 1 ข้อ)

☐ ติดตั้งและใช้งานไฟร์วอลล์ ☐ ปรับปรุงช่องโหว่ในทันที

☐ ตรวจสอบช่องโหว่อย่างสม่ำเสมอ ☐ ใช้โปรแกรมถ่ายโอนข้อมูลที่เข้ารหัส

☐ กำหนดรหัสผ่านให้เหมาะสม ☐ ติดตามข่าวสารด้านความมั่นคงเว็บไซต์

16. คุณเคยตรวจสอบช่องโหว่เว็บไซต์หรือไม่ และบ่อยแค่ไหน

☐ ไม่เคย (เลือกตอบข้อนี้ ให้ข้ามไปตอบต่อในข้อที่ 16)

☐ นานๆครั้ง

☐ ทุกๆ 3 เดือน

17. ครั้งล่าสุดที่ใช้โปรแกรมตรวจหาช่องโหว่เว็บไซต์ พบช่องโหว่ระดับรุนแรงหรือไม่ (ถ้ามี โปรดระบุจำนวนช่องโหว่)

☐ ไม่มีช่องโหว่

☐ มีน้อย ไม่เกิน 3 ช่องโหว่

☐ มีมากกว่า 3 ช่องโหว่

18. คุณได้อุดช่องโหว่ที่เกิดขึ้นตามคำแนะนำที่ได้จากโปรแกรมหาช่องโหว่หรือไม่

☐ อุดช่องโหว่เรียบร้อย

☐ อุดช่องโหว่บางส่วน

☐ ไม่ได้ทำอะไรเลย

19. คุณคิดว่าจะติดตามข่าวสารด้านความมั่นคงเว็บไซต์หรือไม่

☐ ติดตาม

☐ ไม่ติดตาม

20. คุณคิดว่าสามารถติดตามข่าวสารเกี่ยวกับความมั่นคงเว็บไซต์ได้จากที่ไหนได้บ้าง (ตอบได้มากกว่า 1 ข้อ)

☐ หนังสือพิมพ์

☐ นิตยสาร

☐ อินเทอร์เน็ต (เว็บไซต์ หรือ อีเมลล์)

☐ ผู้เชี่ยวชาญด้านความมั่นคงเว็บไซต์

☐ อื่นๆ

<u>ข้อเสนอแนะ</u>

21. ความคิดเห็นเพิ่มเติมเกี่ยวกับงานวิจัยนี้ (เกี่ยวกับเนื้อหาที่นำเสนอ ความคิดเห็นของท่านที่มีต่อความมั่นคงเว็บไซต์ของบริษัท)

.....

.....

.....

.....

.....

.....

.....

22. แนะนำและวิจารณ์แบบสอบถาม

.....

.....

.....

.....

.....

.....

.....

ประวัติผู้เขียนวิทยานิพนธ์

นายเอกฉันท์ รัตนเลิศนุสรณ์ เกิดเมื่อวันที่ 29 ตุลาคม พ.ศ. 2521 เรียนจบการศึกษาระดับปริญญาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย สำเร็จการศึกษาในปีการศึกษา 2542 เริ่มต้นทำงานในตำแหน่งวิศวกรระบบคอมพิวเตอร์เกี่ยวกับการบริการรับฝากอีเมลล์และเว็บไซต์ภาครัฐที่สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) โดยปัจจุบันทำงานเป็นตำแหน่งวิศวกรในหน่วยพัฒนานวัตกรรมและวิศวกรรม ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. (สวทช)