สัญญาเลขที่ RDG5840015

รายงานวิจัยฉบับสมบูรณ์

การพัฒนาโปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

A Program Development of Education Institution Information Technology Security Assessment Model

ผู้วิจัย

ดร.จุมพฏ กาญจนกำธร

สังกัด

บริษัท เจเอ็มเคเนทเวริ์ค จำกัด

กิตติกรรมประกาศ

คณะผู้วิจัยขอขอบคุณสำนักงานกองทุนสนับสนุนการวิจัย สำนักงานคณะกรรมการวิจัยแห่งชาติ ที่ให้การสนับสนุนเงินทุนวิจัย ตลอดโครงการวิจัย ขอขอบพระคุณ สถาบันการศึกษา มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏสวนสุนันทา ที่เอื้อเฟื้อข้อมูล รวมถึงความอนุเคราะห์บุคลากร ขอบขอบพระคุณผู้เชี่ยวชาญ ที่มาช่วยกันพัฒนาโปรแกรมประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นเครื่องมือในการประเมิน ตรวจสอบ เพื่อการวางแผน พัฒนาระบบสารสนเทศของสถาบันการศึกษาให้มีความมั่นคงปลอดภัยและยั่งยืนต่อไป

บทคัดย่อไทย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาสถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา 2) เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา 3) เพื่อพัฒนาโปรแกรมเพื่อประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กลุ่มตัวอย่างในการวิจัยครั้งนี้เป็นการกำหนดแบบเจาะจงได้แก่ ผู้เชี่ยวชาญด้านบริหารและดูแลระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา 3 แห่ง ได้แก่ มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา และมหาวิทยาลัยราชภัฏสวนสุนันทา เครื่องมือที่ใช้ได้แก่แบบสัมภาษณ์ สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ค่าร้อยละ

ผลการวิจัยพบว่า

1. ผู้บริหารสถาบันการศึกษา ให้ความสำคัญด้านมีนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและนโยบายสิ่งแวดล้อม ด้านงบประมาณ ด้านบุคลากร และผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับมากถึงมากที่สุด แต่ปัจจุบันสถาบันการศึกษาส่วนใหญ่ ยังไม่มี นโยบายความมั่นคงปลอดภัยตามมาตรฐานสากล และนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร อีกทั้งงบประมาณที่ได้รับเพื่อบริหารระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับมหาวิทยาลัยบางแห่งยังไม่เพียงพอ มีสถาบันการศึกษา ระดับความรู้ความเข้าใจของบุคลากรและผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับปานกลาง

2. รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เรียกว่า “Education Security Assessment Model” หรือ Ed-SAM เป็นเครื่องมือบริหารเพื่อสร้างนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีตัวบ่งชี้ด้านความมั่นคง 11 ด้าน 105 ตัวบ่งชี้ สามารถนำไปใช้งานและเรียนรู้ง่าย ประหยัดเวลาและค่าใช้จ่าย สามารถดำเนินการได้ด้วยตนเอง มีประสิทธิภาพดีสอดคล้องกับรูปแบบการประเมินตามมาตรฐานสากล

3. โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

คำสำคัญ : โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

ABSTRACT

The Objectives of this research were to study the current state of the security system of Education Institution and to develop assessment a security system for Education Institution. The population and sample were Information Technology security management experts and Information Technology security administrators. Data were collected from in-depth interviews and analyzed by the use of average percentage.

The findings were as follows:

1. The current status of the security system in the Education Institution regarding **policy aspects** the administrators rated Information Technology security management and IT environmental security system at the most level, **personnel aspects** the administrators provided significance for persons associated with the security system and the users' behavior at the high level, **budget aspects** the administrators provide significant for the Information Technology security system budget at the highest level. However, at present Most of Education Institution have no international standard of Information Technology security system and Information Technology environmental security system and not enough budget. Moreover, the persons' Information Technology knowledge and understanding and Information Technology security system users were at the medium level.

2. The Program of Education Institution Security Assessment Model (ED-SAM) was developed for self-assessment information security including 11 mains items and 105 indicators that indicates the security system. The outstanding benefits were as follows: 1) assess a simple, easy to learn and to use 2) save time and cost done manually 3) can be self-assessment to all agencies and 5) be effective correspond to international standard.

Keywords: Security Information Technology, Assessment Model, Education Institution, Technology Management

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญอย่างยิ่ง เทคโนโลยีสารสนเทศหมายถึง เทคโนโลยีสองสาขาหลักที่ประกอบด้วยเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีสื่อสารโทรคมนาคมที่ผนวกเข้าด้วยกัน เพื่อใช้ในกระบวนการจัดหา จัดเก็บ พัฒนา และเผยแพร่สารสนเทศในรูปต่าง ๆ ไม่ว่าจะเป็นเสียง ภาพนิ่ง ภาพเคลื่อนไหว ข้อความ หรือตัวอักษร เพื่อเพิ่มประสิทธิภาพ ความถูกต้อง ความแม่นยำ และ ความรวดเร็วให้ทันต่อการนำไปใช้ประโยชน์ (สุขุม เฉลยทรัพย์, 2551 น.2)

ในการบริหารจัดการและการเรียนรู้ในสถาบันการศึกษา ปัจจุบันได้มีการนำเทคโนโลยีสารสนเทศมาใช้มากขึ้นในด้าน การบริหาร การเรียนการสอนและให้บริหารชุมชนซึ่งระบบสารสนเทศที่ดีจะต้องมีกระบวนการทำงานอย่างต่อเนื่อง มีบุคลกรที่มีความรู้ความสามารถ ฮาร์ดแวร์และซอฟท์แวร์ต้องมีประสิทธิภาพและทำงานได้อย่างต่อเนื่อง ข้อมูลต้องมีความมั่นคงปลอดภัย โดยต้องมีสภาพพร้อมใช้งาน มีความถูกต้องแม่นยำ มีความเป็นส่วนตัวและควบคุมความลับได้อย่างมีประสิทธิภาพ แต่ในขณะที่หน่วยงานต่าง ๆ ได้มีการจัดหาและลงทุนด้วยงบประมาณจำนวนมากกับระบบสารสนเทศที่มีอยู่จำกัด

ปัจจุบันภัยคุกคามต่าง ๆ ต่อระบบเทคโนโลยีสารสนเทศมีมากขึ้น ดังนั้นหากไม่ให้ความสำคัญในการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแล้ว ย่อมก่อให้เกิดความเสียหายอย่างมากต่อผู้บริหาร อาจารย์ เจ้าหน้าที่ นักศึกษา ผู้รับบริการและผู้ให้บริการ

สิ่งสำคัญที่สุดในการบริหารในปัจจุบันคือระบบเทคโนโลยีสารสนเทศ สร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศในสถาบันการศึกษาได้มากเท่าใด ประสิทธิภาพในการบริหารงานก็จะสูงเท่านั้น ปัจจัยที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ นโยบายความมั่นคง งบประมาณด้านความมั่นคง สิ่งแวดล้อมที่เกี่ยวข้องกับความมั่นคง บุคลากรและพฤติกรรมผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังนั้นการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ผู้บริหาร มีความจำเป็น

ต้องนำระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศมาใช้ มี 2 ทางเลือก ทางเลือกที่ 1 คือ การนำระบบสากล (ISO 27001) ต้องใช้งบประมาณสูงมาก (มากกว่า 1 ล้านบาท) บุคลากรทางด้าน IT Security มีน้อย การสื่อสารเอกสารและผู้รับดำเนินงานส่วนใหญ่ใช้ภาษาอังกฤษ ในสถานการณ์ปัจจุบัน สถาบันการศึกษาส่วนใหญ่ มีงบประมาณจำกัด ไม่สามารถนำระบบมาตรฐานสากล (ISO 27001) มาใช้ได้ ทางเลือกที่ 2 คือ การพัฒนาขึ้นมาใช้เอง โดยอ้างอิงระบบสากลและปรับใช้สำหรับมหาวิทยาลัย ใช้การสื่อสารภาษาไทย สามารถดำเนินการตรวจประเมินได้เอง ประหยัดงบประมาณ จึงจำเป็นต้องทำการวิจัยเพื่อพัฒนาโปรแกรมประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษานี้

ปัญหาต่างๆ เหล่านี้เกิดขึ้นจากผู้บริหารไม่มีข้อมูลสภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา ไม่ทราบว่าการบริหารระบบเทคโนโลยีสารสนเทศมีเรื่องใดที่ต้องดำเนินการ รวมถึงไม่ทราบสภาพความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในปัจจุบันมีอะไรและเป็นอย่างไร ทำให้การตัดสินใจในการบริหารด้านที่เกี่ยวข้อง ขาดข้อมูลที่เพียงพอ ส่งผลต่อคุณภาพของสถาบันการศึกษา ตามมาตรา 48 แห่งพระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2545 ระบุว่า “ให้หน่วยงานต้นสังกัดและสถาบันการศึกษาจัดให้มีระบบการประกันคุณภาพภายในสถาบันการศึกษาและให้ถือว่าการประกันคุณภาพภายในเป็นส่วนหนึ่งของกระบวนการบริหารการศึกษาที่ต้องดำเนินการอย่างต่อเนื่อง” ถ้าผู้บริหารสถาบันการศึกษามีเครื่องมือที่ใช้สำหรับการตรวจสอบและประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศย่อมทำให้ผู้บริหารได้ทราบแนวทางการวางนโยบายและสถานภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และสามารถนำผลจากรูปแบบการประเมินความมั่นคงปลอดภัยนี้ไปวางนโยบายแผนพัฒนาระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยและประสิทธิภาพในการบริหารสถาบันการศึกษาดียิ่งขึ้น สามารถพัฒนาภาพลักษณ์ที่ดีของสถาบันการศึกษาให้สอดคล้องกับ พระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2545 และรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้เป็นอย่างดี การได้มาซึ่งระบบการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา มี 2 ทางเลือก ผู้วิจัยมีแนวคิดว่า ทางเลือกที่ 2 คือ พัฒนาขึ้นมาใช้เอง โดยอ้างอิงระบบสากลและปรับใช้สำหรับสถาบันการศึกษาของประเทศไทย ทำให้สามารถสื่อสารเป็นภาษาไทย ประหยัดงบประมาณ และสะดวกและง่ายในการใช้ จะเป็นประโยชน์อย่างยิ่งกับสถาบันการศึกษาของประเทศไทย

ดังนั้นการวิจัยครั้งนี้จึงมีวัตถุประสงค์เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

วัตถุประสงค์ของการวิจัย

1.เพื่อศึกษาสถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา

2.เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

3.เพื่อพัฒนาโปรแกรมคอมพิวเตอร์ประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

ขอบเขตของการวิจัย

ขอบเขตด้านพื้นที่

พื้นที่ศึกษารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นมหาวิทยาลัยราชภัฏที่อยู่ในเขตกรุงเทพมหานคร รวม 3 แห่ง ได้แก่ มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มหาวิทยาลัยราชภัฏสวนสุนันทา

ขอบเขตด้านประชากร

การวิจัยนี้เป็นการวิจัยรูปแบบการวิจัยและพัฒนา (The Research and Development) ประชากรที่ใช้ในการวิจัยครั้งนี้ ประกอบด้วย ผู้เชี่ยวชาญความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏ เป็นผู้ที่มีประสบการณ์ตรง เป็นผู้รับผิดชอบในการจัดการด้านความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศในมหาวิทยาลัยราชภัฏในเขตกรุงเทพมหานครจำนวน 3 แห่ง มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มหาวิทยาลัยราชภัฏสวนสุนันทา ประกอบด้วย

1. กลุ่มผู้กำหนดนโยบายบริหารระบบเทคโนโลยีของมหาวิทยาลัยราชภัฏ จำนวน 3 แห่ง รวม 3 คน
2. กลุ่มผู้ดูแลด้านเทคนิค ระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏ จำนวน 3 แห่ง 3 คน

ขอบเขตเนื้อหา

ตัวแปรที่ศึกษา

ตัวแปรอิสระ ได้แก่ นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ งบประมาณเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สิ่งแวดล้อมเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยี

สารสนเทศ บุคลากรเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พฤติกรรมผู้ใช้สำหรับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตัวแปรตาม ได้แก่ รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้สภาพปัจจุบันด้านความมั่นปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา เพื่อเป็นข้อมูลให้ผู้บริหารนำไปใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

2. ได้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาเครื่องมือสำหรับผู้บริหารเพื่อใช้ในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา เพื่อให้ระบบทำงานได้อย่างถูกต้อง ต่อเนื่องและเก็บความลับได้อย่างมีประสิทธิภาพ

3. ได้โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาใช้เป็นเครื่องมือสำหรับผู้บริหารเพื่อใช้ในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา เพื่อให้ระบบทำงานได้อย่างถูกต้อง ต่อเนื่องและเก็บข้อมูลได้อย่างมีประสิทธิภาพ

นิยามศัพท์เฉพาะ

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง เครื่องมือของผู้บริหาร เพื่อใช้ในการตรวจสภาพความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในองค์กร เพื่อให้ระบบธำรงไว้ซึ่งความลับ ความถูกต้อง และสภาพพร้อมใช้งานของสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง การมีข้อกำหนดและปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

งบประมาณเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง งบประมาณที่จัดสรรเพื่อ การดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถาบันการศึกษา

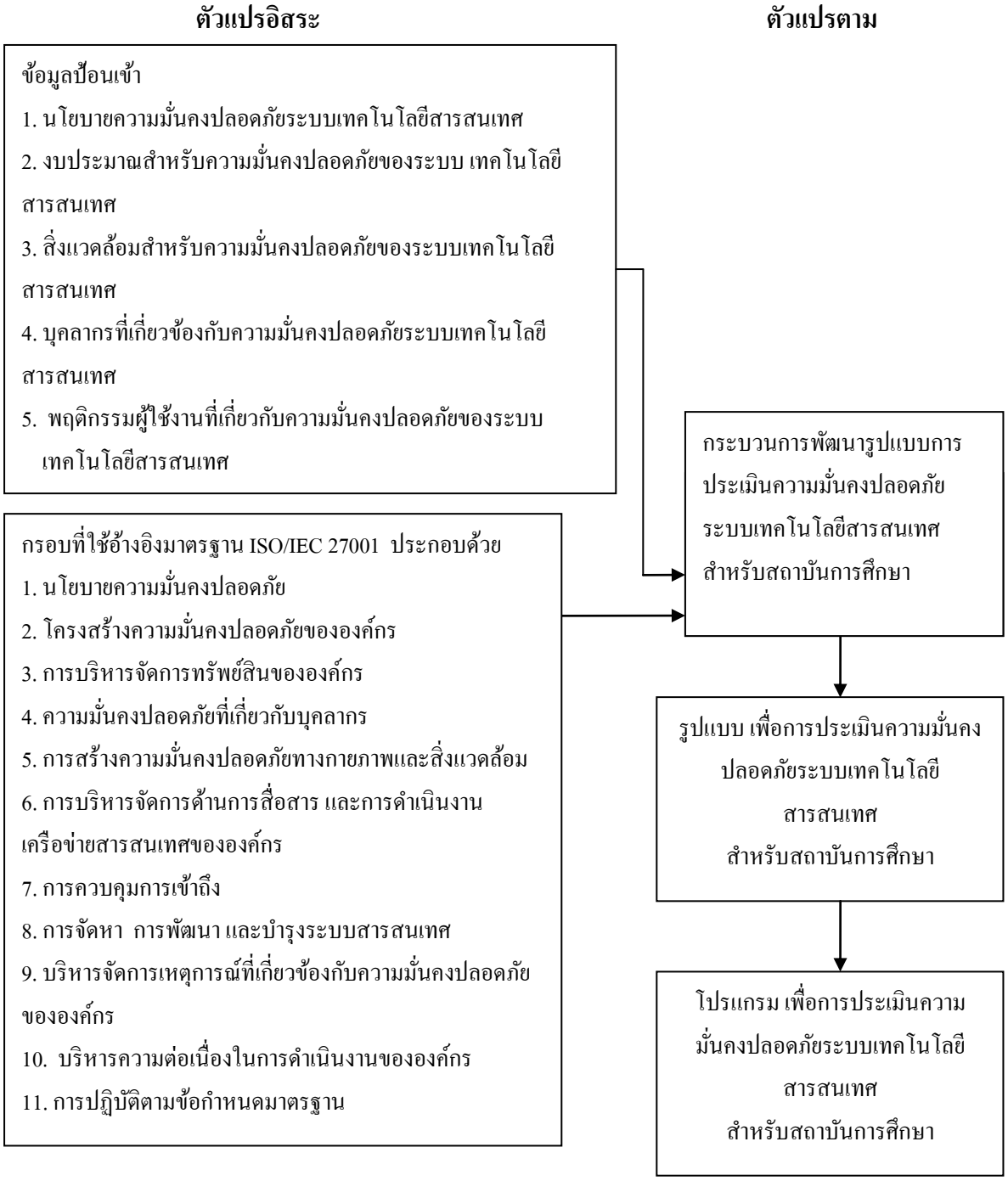
สิ่งแวดล้อมเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง การมีข้อกำหนดและปฏิบัติ เพื่อการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถาบันการศึกษา

บุคลากรเพื่อการดำเนินการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง บุคลากรที่เกี่ยวข้องกับการใช้งาน การบริหารจัดการและการบำรุงรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา

พฤติกรรมผู้ใช้สำหรับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง พฤติกรรมของผู้ใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา

กรอบแนวคิดในการวิจัย

จากการศึกษาเอกสารที่เกี่ยวข้องได้กำหนดกรอบการวิจัย รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา โดยแบ่งออกเป็น



ภาพที่ 1 กรอบแนวคิดในการวิจัย

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการวิจัยครั้งนี้ ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง และได้นำเสนอตามหัวข้อดังต่อไปนี้

1. แนวคิดการประเมิน
2. แนวคิดหลักของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
3. แนวคิด มาตรฐาน ISO/IEC 27001
4. งานวิจัยที่เกี่ยวข้อง

แนวคิดการประเมิน

การประเมิน หมายถึง การนำลักษณะของสิ่งต่าง ๆ ที่ส่วนใหญ่มักเป็นข้อมูลเชิงคุณภาพ มาศึกษาพยายามตีค่าเป็นตัวเลขให้สัมพันธ์กับสิ่งแวดล้อมขณะนั้น โดยใช้สภาวะต่าง ๆ กันเป็นเกณฑ์ จึงต้องมีการศึกษา วิเคราะห์เกณฑ์ และสิ่งแวดล้อมต่าง ๆ ไปด้วย การประเมินโดยทั่วไป จะทำในเวลาใดก็ได้ เช่นก่อน ระหว่างหรือหลังการดำเนินงานแล้ว คำที่ใช้โดยทั่วไป เช่น การประเมินตนเอง (Self Assessment) การประเมินต่างไปจากการวัดและการประเมินผล เพราะต้องมีการศึกษาข้อมูล วิเคราะห์สภาพแวดล้อมของสิ่งที่กำลังศึกษา แล้วจึงตีค่าของสิ่งนั้นออกมา โดยผลลัพธ์ที่ได้มิได้นำมาตัดสินสรุปผลเพื่อจำแนกกลุ่ม แต่ต้องการตีค่าให้เห็นย้อนกลับ ของสิ่งนั้น ๆ เพื่อจะได้นำไปพัฒนาสิ่งสิ่งนั้นในอนาคต

ปัจจุบันกระบวนการดำเนินงานของโครงการต่างๆ นิยมใช้กระบวนการ “PDCA” (Plan-Do-Check-Act) ต้องมีการควบคุมคุณภาพของการดำเนินการทุกขั้นตอนเพื่อให้โครงการนั้น ๆ

ประสบผลสำเร็จอย่างจริงจัง การประเมินจึงเข้ามาเกี่ยวข้องเพื่อที่จะได้ทราบข้อมูลย้อมกลับว่าต้องปรับปรุงในขั้นตอนใดของโครงการนั้น

กระบวนการประเมิน มีขั้นตอน การประชาสัมพันธ์ เพื่อสร้างความตระหนัก และเป็นการเตรียมความพร้อมของหน่วยของโครงการให้มีความเข้าใจถึงความสำคัญของการประเมิน ซึ่งจะทำให้ข้อมูลที่ได้รับในการประเมินใกล้เคียงกับความจริงมากที่สุด เพราะความเข้าใจถึงความสำคัญของการประเมินจะทำให้ผู้เกี่ยวข้องกับการประเมินออกความเห็นได้เต็มที่และตรงกับความเป็นจริง (ยุวดี เปรมวิชัย, 2550, น.31-39)

ขั้นตอน การวางแผนการประเมิน ประกอบด้วย การสร้างเครื่องมือในการประเมิน ในการดำเนินการของโครงการใด ๆ ย่อมมีจุดประสงค์หรือวัตถุประสงค์ของโครงการต่าง ๆ กัน ความสำเร็จของโครงการวัดจากความตรงตามจุดประสงค์หรือวัตถุประสงค์ที่ตั้งไว้ และการวัดว่าการดำเนินการตรงจุดประสงค์หรือวัตถุประสงค์เพียงใดนั้นต้องมีการกำหนด ตัวชีวิ หรือตัวบ่งชี้ หรือดัชนี ที่ตรงกับจุดประสงค์หรือวัตถุประสงค์ ตัวชี้วัด หรือตัวบ่งชี้ หรือดัชนี หมายถึงลักษณะที่สำคัญที่สามารถแสดงได้ว่าโครงการได้ดำเนินมาตรงตามวัตถุประสงค์เพียงใด การกำหนดตัวบ่งชี้ทำได้โดยการศึกษาของผู้เชี่ยวชาญในโครงการนั้น ๆ เมื่อศึกษาแล้วจึงกำหนดลักษณะที่คาดว่าจะทำให้โครงการนั้น ๆ บรรลุตามวัตถุประสงค์ขึ้นมาหลายๆ ลักษณะ ตัวบ่งชี้แบ่งได้ 2 ประเภท คือ ตัวบ่งชี้เชิงปริมาณ และตัวบ่งชี้เชิงคุณภาพ ตัวบ่งชี้เชิงปริมาณได้แก่ จำนวนร้อยละ เป็นต้น ตัวบ่งชี้เชิงคุณภาพ ได้แก่ ความพึงพอใจของผู้ใช้บริการ ความคิดเห็นของพนักงานต่อผู้บริหาร ไม่สามารถหาคุณภาพที่แท้จริงได้ จึงต้องกำหนด “ระดับคะแนน (Rating scale)” ให้เป็นค่าตัวแทนของตัวบ่งชี้ประเภทนี้ ทั้งตัวบ่งชี้ และระดับคะแนน จะถูกนำมาสร้างเป็นเครื่องมือการประเมิน อยู่ในรูปแบบฟอร์มการประเมิน หรือแบบสอบถามความคิดเห็น ที่ครอบคลุมเนื้อหาครบถ้วนทุกลักษณะของโครงการที่กำลังดำเนินการอยู่ มีความชัดเจน มีลักษณะความเป็นเครื่องมือการประเมิน เครื่องมือวัดความคิดเห็นที่ดี โดยคุณสมบัติของการเป็นเครื่องมือ ได้แก่ มีความถูกต้องหรือเที่ยงตรงตามเนื้อหา คือสามารถวัดได้ครอบคลุมเนื้อหาหรือจุดประสงค์ที่ต้องการได้ครบถ้วน มีความเชื่อถือได้ คือไม่เปลี่ยนแปลง ไม่ว่าจะวัดกี่ครั้ง เมื่อไร ที่ไหน ก็ ได้ผลอย่างเดิมเสมอ มีประสิทธิภาพ เช่นใช้คำถามเข้าใจง่าย ใช้เวลาตอบน้อย มีอำนาจจำแนก คือ มีความแตกต่างกันในแต่ละข้อถาม

ขั้นตอนการดำเนินการประเมิน การดำเนินการประเมินเปรียบเทียบได้กับวิธีการทางสถิติในขึ้น เก็บรวบรวมข้อมูลและวิเคราะห์หรือตีความหมายข้อมูล เพราะเมื่อนำเครื่องมือที่สร้างขึ้นหรือเรียกว่าแบบประเมิน ไปให้ผู้ประเมินกรอกข้อมูลแล้ว ข้อมูลที่ได้จะถูกรวบรวมเรียกข้อมูลที่รวบรวมแล้วว่า “คะแนนการประเมิน” ค่าคะแนนการประเมินที่ได้มาจะถูกนำมาตีความหมายว่า

คะแนนการประเมินแต่ละค่าหมายถึงลักษณะของโครงการนั้น ๆ เป็นอย่างไร การตีความหมายดังกล่าว จึงต้องมีการกำหนด “เกณฑ์การประเมิน” ขึ้น โดยเกณฑ์การประเมินหมายถึง ค่าที่ใช้กำหนดระดับคุณภาพของสิ่งที่ถูกประเมิน เป็นองค์ประกอบที่สำคัญในการพิจารณาลักษณะของโครงการ เกณฑ์การประเมินกำหนดขึ้นมาเพื่อให้เกิดความชัดเจนและยุติธรรมในการประเมิน และทำให้เห็นทิศทางในการพัฒนาให้โครงการนั้น ๆ เป็นไปตามเป้าหมายหรือวัตถุประสงค์ของโครงการที่กำลังถูกประเมิน เกณฑ์การประเมินมีความสัมพันธ์อย่างใกล้ชิดมากกับตัวบ่งชี้ที่กำหนดไว้ในตอนสร้างเครื่องมือการประเมิน เกณฑ์การประเมินแสดงได้หลายลักษณะ โดยเกณฑ์การประเมินของตัวบ่งชี้เชิงปริมาณจะแสดงตรงตามข้อมูลจริง มีทั้งเมื่อได้ข้อมูลจริงของตัวบ่งชี้เชิงปริมาณแล้วนำมากำหนดเกณฑ์การประเมินแสดงเป็นค่าคะแนนรวม แต่เกณฑ์การประเมินของตัวบ่งชี้เชิงคุณภาพ ไม่สามารถแสดงจาข้อมูลจริงได้ เช่นตัวบ่งชี้เป็นความพึงพอใจของผู้ใช้บริการ จึงนิยมแสดงเกณฑ์การประเมินของตัวบ่งชี้เชิงคุณภาพในรูปค่าเฉลี่ยถ่วงน้ำหนัก หรือ ค่าร้อยละถ่วงน้ำหนัก

ขั้นตอนการเขียน รายงานและการเผยแพร่ การเขียนรายงานการประเมินใช้หลักการเขียนเช่นเดียวกับการเขียนรายงานวิจัย

ขั้นตอนการนำผลการประเมินไปใช้ เนื่องจากการประเมินต้องถูกกระทำซ้ำ ๆ กันอยู่ตามช่วงเวลาที่เหมาะสม ตลอดเวลาที่โครงการหรือหน่วยงานหรือองค์กรนั้น ๆ ยังมีอยู่ การประเมินจึงต้องมีการบันทึกผล และนำไปใช้เปรียบเทียบกับผลงานแรก ๆ เพื่อใช้เป็นข้อมูลย้อนกลับ บอกให้ทราบข้อบกพร่องของการปฏิบัติ ให้เกิดการพัฒนาในโครงการนั้น ๆ อย่างต่อเนื่อง ผลของการประเมินจึงนำไปใช้ในความหมายเพื่อให้ทราบถึงข้อมูลย้อนกลับ สำหรับใช้เป็นทิศทางในการพัฒนาให้โครงการนั้น ๆ เป็นไปตามเป้าหมายหรือวัตถุประสงค์ของโครงการที่กำหนดไว้

ปัญหาหรือข้อผิดพลาดที่เกิดจากการประเมิน ปัญหาทั่วไปที่เกิดจากการประเมินและมีผลทำให้กระบวนการประเมินของโครงการใด ๆ มีความน่าเชื่อถือน้อยลง หรือทางสถิติเรียกว่าเกิดข้อผิดพลาด มักพบในขั้นตอนการดำเนินการประเมิน ซึ่งส่วนใหญ่เป็นปัญหาตั้งแต่การเก็บรวบรวมข้อมูล มีทั้งปัญหาเนื่องมาจากผู้ประเมินและผู้ถูกประเมิน เช่น ผู้ประเมินไม่ประเมินหรือประเมินอย่างเสียไม่ได้ ผู้ประเมินมีคติในด้านต่าง ๆ ผู้ประเมินจำแนกผู้ถูกประเมินไม่ได้ เพราะผู้ประเมินไม่ใกล้ชิดผู้ถูกประเมินพอที่จะสังเกตพฤติกรรมของผู้ถูกประเมิน กรณีที่เป็นการประเมินพฤติกรรมเชิงคุณธรรมต้องใช้เวลาสังเกตที่นานมาก ทั้งปัญหาและข้อผิดพลาดเหล่านี้เป็นสิ่งที่ต้องเกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ ทุกครั้งที่มีการเก็บรวบรวมและวิเคราะห์ข้อมูล การประเมินทำได้โดยพยายามให้เกิดปัญหาและข้อผิดพลาดเหล่านี้ให้น้อยที่สุดเท่าที่จะเป็นไปได้

จากแนวคิดการประเมิน ผู้วิจัยได้สรุปแนวคิดและรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อหาคำตอบว่ามีปัจจัยใดบ้างที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อย่างไร และมีความสำคัญระดับใด เพื่อเป็นแนวทางในการป้องกันแก้ไขเพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงยิ่งขึ้น ดังนั้นรูปแบบการประเมินควรมีกระบวนการเป็นลำดับ และมีเกณฑ์ในการแปลผลอย่างมีระบบ

แนวคิดการประกันคุณภาพภายใน

มีการพัฒนากันอยู่ในขณะนี้ แนวคิดเพื่อส่งเสริมและเสนอแนวทางเกี่ยวกับการพัฒนาคุณภาพทางการศึกษา โดยมีการดำเนินงาน 3 ขั้นตอน ดังนี้

1. การควบคุมคุณภาพ เป็นการกำหนดมาตรฐานคุณภาพ การพัฒนาสถานศึกษาให้เข้าสู่มาตรฐาน
2. การตรวจสอบคุณภาพ เป็นการตรวจสอบและติดตามผลการดำเนินงาน
3. การประเมินคุณภาพ เป็นการประเมินคุณภาพของสถานศึกษา โดยหน่วยงานที่กำกับดูแลในเขตพื้นที่

ตามหลักการบริหาร การประกันคุณภาพภายใน เป็นกระบวนการบริหารจัดการเพื่อให้บรรลุเป้าหมายในการพัฒนาคุณภาพเป็นไปตามเป้าหมาย ต้องช่วยกันคิดและช่วยกันวางแผน (Plan) ช่วยกันทำ (Do) ช่วยกันตรวจสอบ (Check) ปรับปรุงแก้ไขข้อบกพร่อง (Action) เพื่อให้บรรลุตามเป้าหมายกำหนดอย่างต่อเนื่อง เพื่อพัฒนาปรับปรุงคุณภาพให้ดีขึ้น โดยร่วมกันทำงานเป็นทีม การควบคุมคุณภาพ และการตรวจสอบคุณภาพเป็น กระบวนการบริหารเพื่อพัฒนาคุณภาพตามหลักการบริหาร โดยการควบคุมคุณภาพ สถานศึกษาต้องร่วมกันวางแผน และดำเนินการตามแผน เพื่อพัฒนาสถานศึกษาให้มีคุณภาพตามเป้าหมายมาตรฐานการศึกษา ส่วนการตรวจสอบคุณภาพ คือการที่สถานศึกษาร่วมกันตรวจสอบ เพื่อพัฒนาปรับปรุงคุณภาพให้เป็นไปตามเป้าหมาย หลักการสำคัญการประกันคุณภาพภายในของสถานศึกษาตามแนวคิดข้างต้น
คือ จุดมุ่งหมายของการประกันคุณภาพภายใน คือ การที่สถานศึกษาร่วมกันพัฒนาปรับปรุงคุณภาพให้เป็นไปตามมาตรฐานการศึกษา ดำเนินการให้บรรลุเป้าหมาย ต้องทำให้การประกันคุณภาพการศึกษาเป็นส่วนหนึ่งของกระบวนการบริหารจัดการและ การทำงานของบุคลากรทุกคนในสถานศึกษา มีการประกันคุณภาพเป็นหน้าที่ของบุคลากรทุกคนในสถานศึกษา ไม่ว่าจะเป็นผู้บริหาร ครู – อาจารย์ และบุคลากรอื่น ๆ ในสถานศึกษา

แนวคิดหลักของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

องค์ประกอบหลักของความปลอดภัยระบบเทคโนโลยีสารสนเทศ วิเคราะห์คุณสมบัติ 3 ด้าน คือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีอยู่ครบหรือไม่ ความลับหมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ความถูกต้อง หมายถึง การรักษาความคงสภาพข้อมูลจากแหล่งที่มา หรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต ความพร้อมใช้งาน ให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ (จตุชัย แพงจันทร์,2553, น.8-9)

ความเป็นส่วนตัว (Privacy) คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กรจะต้องถูกใช้ในวัตถุประสงค์ที่เป็นเจ้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศมิฉะนั้น จะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ (พนิดา พานิชกุล, 2553, น. 6-8)

ระบบสารสนเทศมีส่วนประกอบสำคัญ 5 ส่วน ได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล (Data) บุคลากรทางคอมพิวเตอร์ (People ware) กระบวนการทำงาน (Procedures) (โอภาส เอี่ยมสิริวงศ์, 2551, น. 212-213)

คุณสมบัติของสารสนเทศที่ดี

1. ตรงกับความต้องการ (Relevance) สารสนเทศที่ดีจะต้องสอดคล้องกับความต้องการของผู้ที่นำไปใช้งาน ดังนั้นหากสารสนเทศที่นำเสนอแม้จะมีความถูกต้อง แต่สาระสำคัญของเนื้อหาไม่ตรงกับสิ่งที่ต้องการเลย ก็ถือว่าเป็นสารสนเทศที่ไม่มีประโยชน์ ไม่สามารถนำมาใช้เพื่อประกอบการตัดสินใจของผู้บริหารได้

2. ทันเวลาต่อการนำไปใช้ให้เกิดประโยชน์ (Timeliness) รูปแบบธุรกิจบางอย่างจำเป็นต้องได้รับสารสนเทศอย่างรวดเร็ว ทันต่อเหตุการณ์ เช่น เกี่ยวกับการค้าหลักทรัพย์ หรือตลาดหุ้น แต่อย่างไรก็ตามก็ใช่ว่าธุรกิจทุกประเภทจะต้องได้รับสารสนเทศอย่างรวดเร็วในช่วงระยะเวลาสั้น ๆ ดังนั้น คำว่า ทันเวลาต่อการนำไปใช้ให้เกิดประโยชน์นั้น จึงหมายความว่าสารสนเทศต้องทันต่อเหตุการณ์ ไม่ล้าสมัยขณะที่นำไปใช้ประโยชน์ ซึ่งหากสารสนเทศที่นำเสนอไป ไม่ทันเวลาหรือไม่ทันต่อความต้องการ สารสนเทศนั้นอาจล้าสมัยได้ในทันที คุณประโยชน์ที่ควรได้รับก็อาจลดน้อยลงไป หรืออาจไม่สามารถนำไปใช้ประโยชน์ได้เลยก็เป็นได้

3. มีความเที่ยงตรง (Accurate) สารสนเทศที่ดีต้องมีความเที่ยงตรง แม่นยำ ปราศจากการคลาดเคลื่อนในข้อมูลที่นำเสนอ ดังนั้นผลลัพธ์ของสารสนเทศที่มีความเที่ยงตรง ก็ขึ้นอยู่กับข้อมูลที่ป้อนเข้าไปในระบบด้วย ดังนั้น คำว่าเที่ยงตรงในที่นี้จึงหมายรวมถึงความถูกต้อง ความสมบูรณ์และความปลอดภัย

4. ประหยัด (Economy) สารสนเทศที่ดีจะต้องมีการนำทรัพยากรที่เหมาะสมมาใช้งานได้อย่างคุ้มค่าที่สุด สารสนเทศที่ใช้ทรัพยากรสูง ย่อมก่อให้เกิดค่าใช้จ่ายสูงตามมา ซึ่งสามารถ

เปรียบเทียบง่าย ๆ เช่น หากคุณภาพของสารสนเทศออกมาเหมือนกัน โดยที่ระบบหนึ่งใช้ทรัพยากรสูง ในขณะที่อีกระบบหนึ่งใช้ทรัพยากรที่ต่ำกว่า ผลลัพธ์ในสารสนเทศที่มาจากระบบที่ใช้ทรัพยากรน้อยกว่าย่อมดีกว่า เมื่อเทียบกับคุณภาพที่ทัดเทียมกัน

5. มีประสิทธิภาพ (effective) สารสนเทศที่ดีต้องมีประสิทธิภาพ คำว่าประสิทธิภาพ ความจริงสามารถวัดได้หลายแนวทางด้วยกัน สารสนเทศนี้นำเสนอได้อย่างเที่ยงตรง และรวดเร็วมาก อีกทั้งยังใช้ทรัพยากรน้อยด้วย ก็จัดได้ว่าเป็นสารสนเทศที่มีประสิทธิภาพ (โอภาส เอี่ยมสิริวงศ์, 2551, น. 212-213)

การใช้ระบบเทคโนโลยีสารสนเทศจะเป็นที่น่าพอใจเป็นที่ยอมรับของผู้ใช้เพียงใด จะต้องมีคุณสมบัติหรือมีเกณฑ์ชี้วัดอยู่ 4 ตัว ดังนี้ คือ 1) ตรงกับกรณี (Relevance) 2) ความครบถ้วน (Completeness) 3) ทันเวลา (Timeliness) และ 4) การใช้ประโยชน์ (Verifiability) ในการตัดสินใจนั้นระบบเทคโนโลยีสารสนเทศจะต้องสมบูรณ์และจำเป็นต้องรู้เกี่ยวกับสถานะที่แน่นอนเพื่อตัดสินใจในการปฏิบัติการ ดังนั้นการให้บริการระบบแก้ผู้ที่ต้องการใช้ จึงควรคำนึงถึงหลักการให้บริการและคุณภาพ

การวัดความสำเร็จของระบบเทคโนโลยีสารสนเทศสามารถใช้ค่าตัวแปรต่าง ๆ ดังต่อไปนี้

1. ระดับการใช้งาน (Utilization) ซึ่งหมายถึงทั้งปริมาณและคุณภาพของการใช้งานด้านปริมาณ ได้แก่ ความถี่ในการใช้งานต่อสัปดาห์ จำนวนผู้ใช้ และจำนวนรายงานที่นำไปใช้งาน ส่วนด้านคุณภาพ ได้แก่ การนำระบบไปใช้ในการปฏิบัติงานประจำ

2. ความพึงพอใจของผู้ใช้ต่อระบบ (User Satisfaction) ได้แก่ ความพึงพอใจของผู้ใช้ต่อระบบการป้อนข้อมูล การประมวลผล รายงาน และคุณภาพของการบริการ ตลอดจนการกำหนดเวลาในการปฏิบัติงาน รวมถึงความพึงพอใจของผู้บริหาร (Ives et al., 1984)

3. ประสิทธิผล (Effectiveness) คือ ระดับความสามารถในการตอบสนองต่อวัตถุประสงค์ของหน่วยงานหรือความสามารถในการบรรลุวัตถุประสงค์ของโครงการ

4. ประสิทธิภาพ (Efficiency) คือ ความคุ้มค่าในการใช้ทรัพยากรหรือการเปรียบเทียบอินพุตหรือต้นทุนที่ใส่เข้าไปในระบบเทียบกับผลผลิตที่ได้รับ (พงศักดิ์ ผกามาศ, 2553, น. 369-370)

สรุปแนวคิดของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ระบบสารสนเทศที่ดีประกอบด้วย กระบวนการทำงานอย่างต่อเนื่อง บุคลกรในองค์กรมีความรู้ความสามารถด้านสารสนเทศที่ดี ฮาร์ดแวร์และซอฟท์แวร์ มีประสิทธิภาพและข้อมูลจะต้อง

มีความมั่นคงปลอดภัย ซึ่งความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องมีสภาพพร้อมใช้งาน มีความถูกต้องแม่นยำ มีความเป็นส่วนตัวและมีความลับที่เชื่อถือได้

1 . แนวคิด มาตรฐาน ISO/IEC 27001

ปัจจุบันมีแม่บท หรือมาตรฐานของการบริหารความปลอดภัยข้อมูลมากมาย มาตรฐานที่ได้รับความนิยมมาก คือ BS 7799 ซึ่งเป็นมาตรฐานที่พัฒนาโดยประเทศอังกฤษ (British Standard : BS) ปัจจุบันได้ปรับเปลี่ยนไปเป็น มาตรฐาน ISO/IEC 27000 ซึ่งเป็นชุดมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศ (จตุชัย แพงจันทร์, 2550, น.38-42) ประกอบด้วย

ISO 27000 มีวัตถุประสงค์เพื่อแสดงศัพท์นิยาม ที่ใช้ในชุดมาตรฐานนี้ คือศัพท์บัญญัติทั้งหลายที่ใช้มาตรฐานการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Standards-ISMS)

ISO 27001 คือ มาตรฐานที่จำเป็นของ ISMS ได้แก่ คุณลักษณะเฉพาะ (Specification) ซึ่งองค์กรทั้งหลายจะต้องขอรับใบรับรอง (Certificate) จากหน่วยงานภายนอกว่าได้มีการปฏิบัติตามข้อกำหนด (Compliance) เหล่านั้นอย่างเป็นทางการ

มาตรฐาน ISO/IEC 27001:2005-Infomaiton Security Management System (ISMS) เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูล ซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยสถาบันนานาชาติ ISO (The International Organization for Standardization) และ IEC (International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจดำเนินไปอย่างต่อเนื่อง ช่วยป้องกันกระบวนจากภัยคุกคามต่าง ๆ เป็นมาตรฐานเกี่ยวกับการบริหารการรักษาความปลอดภัยข้อมูล เป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยข้อมูลโดยใช้รูปแบบการบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการสร้างและพัฒนาระบบการรักษาความปลอดภัย เป็นพื้นฐานเพื่อที่จะสร้างระบบควบคุมเพื่อให้การบริหารองค์กรบรรลุภารกิจในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และเพื่อให้แน่ใจว่าระบบนั้นควรได้รับการปรับปรุงเมื่อถึงเวลา โดยมีระบบการจัดการความปลอดภัยของข้อมูล 3 ด้าน ประกอบด้วย ความลับ (Confidentiality) เพื่อให้แน่ใจว่าข้อมูลต่าง ๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิเท่านั้น ความถูกต้อง (Integrity) เพื่อปกป้องให้ข้อมูลมีความถูกต้องและความสมบูรณ์ และแก้ไขได้เฉพาะผู้มีสิทธิ์เท่านั้น ความพร้อมใช้งาน (Availability) เพื่อแน่ใจว่าผู้ที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้เมื่อมีความต้องการ

ISO/IEC27001 เป็นกระบวนการสำหรับการวางแผน การลงมือทำ การปฏิบัติการ การเฝ้าระวัง การทบทวน การดูแลรักษา และการปรับปรุงระบบ ISMS โดยองค์กรต้องกำหนดแผนการ

ปฏิบัติหลายอย่างเพื่อให้เป็นผลสำเร็จ ซึ่งการจะทำให้เป็นผลสำเร็จนั้น จำเป็นต้องทำเป็นกระบวนการ โดยมี 4 ขั้นตอนหลักคือ

1. การทำความเข้าใจเกี่ยวกับความสำคัญของการรักษาความปลอดภัยข้อมูลขององค์กรและความจำเป็นในการกำหนดนโยบายเกี่ยวกับการรักษาความปลอดภัยข้อมูล

2. การลงมือปฏิบัติและการควบคุมเพื่อบริหารความเสี่ยงด้านการรักษาความปลอดภัยข้อมูล

3. การเฝ้าระวังและวัดประสิทธิภาพและประสิทธิผลของระบบ ISMS

4. การปรับปรุงระบบอย่างต่อเนื่อง

หลักการของการออกแบบโครงสร้างจะใช้อ้างอิงรูปแบบ PDCA ซึ่งเป็นหลักการบริหารเดียวกับมาตรฐานสากลอื่น ที่นิยมใช้กันทั่วโลก เช่น ระบบการจัดการคุณภาพ (ISO 9001:2000) ระบบการจัดการสิ่งแวดล้อม (ISO14001:2004) ระบบการจัดการคุณภาพสำหรับอุตสาหกรรมรถยนต์ (ISO/TS 16949) ระบบการจัดการคุณภาพสำหรับอุตสาหกรรมอาหาร (ISO 21001)

ขั้นตอนการปฏิบัติ PDCA จัดทำ ISMS

Plan วางแผนจัดทำ ดำเนินการ โดยการ กำหนดขอบเขตการจัดทำ กำหนดนโยบาย กำหนดรูปแบบและวิธีการประเมินความเสี่ยง ระบุความเสี่ยง วิเคราะห์และประเมินความเสี่ยง วิเคราะห์และประเมินหนทางในการลดความเสี่ยง กำหนดวัตถุประสงค์และมาตรการในการควบคุมเพื่อลดความเสี่ยง ขออนุมัติผู้บริหารเกี่ยวกับความเสี่ยงที่ไม่มีมาตรการเพื่อควบคุม ขออนุมัติผู้บริหารเกี่ยวกับการทำระบบ จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้

Do ดำเนินการตามแผน ดำเนินการ โดยการ กำหนดแผนการกำจัดความเสี่ยง ซึ่งประกอบด้วยแนวทางในการปฏิบัติสำหรับผู้บริหาร ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม ฝึกอบรมและกระตุ้นให้ตระหนักเกี่ยวกับการรักษาความปลอดภัย บริหารการปฏิบัติการ บริหารทรัพยากร กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

Check ดำเนินการโดย การเฝ้าระวังและตรวจสอบ ดำเนินการ โดยการ เฝ้าระวังและตรวจจับข้อผิดพลาดต่าง ๆ และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ ตรวจพิจารณาว่า ระบบมีประสิทธิภาพเพียงพอหรือไม่ ประเมินเป็นประจำว่า ความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ ตรวจสอบภายในระบบ ตรวจสอบและประเมินว่าระบบทำงานตามขอบเขตที่กำหนด

หรือไม่ ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดต่าง ๆ ที่ตรวจพบ บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของระบบ

Act รักษาและปรับปรุง ดำเนินการโดย การเพิ่มเติมเพื่อปรับปรุงระบบ แก้ไขปัญหาที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นอีก สื่อสารให้ผู้เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงระบบ ทำให้แน่ใจว่า การปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

ต่อจากนั้นต้องมีการกำหนดเกี่ยวกับการจัดทำเอกสารเพื่อจะชี้ให้เห็นชัดว่านโยบายที่กำหนดนั้นจะนำไปปฏิบัติจริง โดยเอกสารที่ต้องจัดทำประกอบด้วย

1. แถลงการณ์เกี่ยวกับวัตถุประสงค์และนโยบายของระบบ
2. ของเขตการทำงานของระบบ
3. ข้ออธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง
4. รายงานเกี่ยวกับการประเมินความเสี่ยง
5. กำหนดแผนเพื่อลดความเสี่ยง
6. กำหนดแนวทางการปฏิบัติสำหรับองค์กรเพื่อให้สามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ และกำหนดแนวทางในการวัดประสิทธิภาพของมาตรการควบคุมต่าง ๆ
7. การเก็บรักษาเอกสารต่าง ๆ ที่ทำตามมาตรฐานนี้
8. แถลงการณ์ของการประยุกต์ใช้งาน

ขั้นตอนการนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ในองค์กร มีขั้นตอนดังนี้

1. จัดตั้งคณะทำงานเฉพาะเรื่องมาตรฐานฯ เพื่อศึกษาตัวมาตรฐานโดยละเอียดและหาแนวทางนำมาปรับปรุงประยุกต์ใช้ในองค์กร โดยคณะนี้ควรจัดฝึกอบรม ทำความเข้าใจในส่วนของข้อกำหนดทั้ง 11 โดเมน เพื่อจะทำให้ทีมงานได้เข้าใจแนวทางของการตรวจสอบตามสากลจากตัวต้นฉบับที่เป็นภาษาอังกฤษ และศึกษาแนวทางในการปฏิบัติจากมาตรฐานฯ ด้วย เพื่อที่จะได้รายละเอียดในการประยุกต์ใช้เพิ่มมากขึ้น เพราะในส่วนภาคผนวกของมาตรฐานฯ นั้นจะเป็นแบบเช็คลิสต์ หรือข้อกำหนดพื้นฐานที่ทางผู้ตรวจสอบความมั่งปลอดภัยระบบเทคโนโลยีสารสนเทศจะใช้ในการตรวจสอบระบบเท่านั้น แต่ไม่ได้มีคำอธิบายแนวทางปฏิบัติที่ละเอียดไว้ในตัวมาตรฐาน แต่มาตรฐานฯ จะเน้นไปที่แนวทางปฏิบัติ ที่สามารถนำมาอ้างอิงถึงเป็นแนวทางในการปฏิบัติ รวมทั้งมีการยกตัวอย่างประกอบความเข้าใจ

2. จัดประเมินระบบในภาพรวมเพื่อหาว่า ระบบในองค์กรยังไม่ได้ปฏิบัติตามข้อกำหนดใดในมาตรฐานและมีความแตกต่างจาก “สิ่งที่ควรจะเป็น” หรือ “สิ่งที่ควรจะต้องทำ” ตามนโยบายอย่างไร โดยนำเทคนิค “Gap Analysis” มาใช้ กล่าวคือ นำมาตรฐานควบคุมที่อยู่ในภาคผนวก A

ของมาตรฐานฯ มาทำเป็นแบบสอบถาม เพื่อใช้ในการสัมภาษณ์ผู้ที่เกี่ยวข้องในองค์กร โดยพยายามให้ทุกคนสามารถเข้ามามีส่วนร่วมในการตอบคำถามและให้ความเห็น หลังจากได้ข้อมูลก็สรุปเป็นรายงานเพื่อนำเสนอให้ผู้บริหารระดับสูงขององค์กรได้ทราบถึงสถานะล่าสุดขององค์กร และความแตกต่างกับข้อกำหนดในมาตรฐาน นอกจากนี้ยังช่วยทำให้ผู้บริหารเกิดความเข้าใจในปัญหาที่เกิดขึ้น เพื่อจะทำให้ผู้บริหารระดับสูงตัดสินใจให้การสนับสนุนในการปฏิบัติตามมาตรฐานฯ และดำเนินการแก้ไขข้อบกพร่องจากการที่องค์กรยังไม่ได้ปฏิบัติตามมาตรฐานดังกล่าวอย่างเป็นรูปธรรม

3. หลังจากได้รับความเห็นชอบจากผู้บริหารแล้ว ขั้นตอนต่อไป คือ การลงรายละเอียดการปฏิบัติ โดยการทำกระบวนการบริหารความเสี่ยงในสามมุมมอง คือ มุมมองด้านบุคลากร ด้านกระบวนการ และด้านเทคโนโลยี เพื่อที่จะได้ประเมินความเสี่ยงของระบบ และจัดทำแผนปฏิบัติการเพื่อลดความเสี่ยง เพื่อปฏิบัติตามข้อกำหนดของมาตรฐานฯ และเป็นการปฏิบัติตาม พ.ร.บ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์อีกด้วย

4. สุดท้ายก็ควรมีการทบทวนและการเฝ้าระวังเพื่อเปรียบเทียบความเปลี่ยนแปลงระหว่างก่อนการปฏิบัติตามมาตรฐาน และหลังจากปฏิบัติตามมาตรฐาน ซึ่งควรจะเห็นผลลัพธ์ในเชิงบวกเป็นรูปธรรมชัดเจนและควรเฝ้าระวังระบบอย่างต่อเนื่อง เพื่อที่จะได้แน่ใจว่าระบบสามารถทำงานได้ปกติโดยไม่เกิดผลกระทบจากการค้นพบช่องโหว่ใหม่ ๆ และภัยใหม่ ๆ และสามารถปรับตัวแก้ไขปัญหาได้อย่างทันท่วงที

การได้รับรองมาตรฐานสากลนี้ จะทำให้ภาพลักษณ์ขององค์กรต่อสาธารณะชน ตลอดจนผู้ใช้บริการเกิดความมั่นใจในการรักษาความมั่นคงปลอดภัยระบบขององค์กรที่ได้ตามมาตรฐานสากล ดั้งนั้น ผู้บริหารระดับสูงจึงควรมีวิสัยทัศน์ในเรื่องการนำมาตรฐานฯ มาประยุกต์ใช้ในองค์กร เพื่อเพิ่มความมั่นคงปลอดภัยแก่ระบบขององค์กร เพื่อความยั่งยืนขององค์กรต่อไปในอนาคต

มาตรฐาน ISO 27001 ได้มีการกำหนดมาตรการในการบริหารการรักษาความมั่นคงปลอดภัยเป็น 11 หัวข้อหลัก หรือ โดเมน 39 วัตถุประสงค์การควบคุม และ 133 มาตรการควบคุม ดังนี้

1. นโยบายการรักษาความปลอดภัย เป็นสิ่งแรกที่สำคัญ และจำเป็นสำหรับองค์กรที่ต้องมีเพื่อเป็นแนวทางและสนับสนุนการรักษาความปลอดภัยของข้อมูล

1.1 นโยบายการรักษาความปลอดภัยสารสนเทศ เพื่อกำหนดทิศทางการดำเนินการด้านการรักษาความปลอดภัยสำหรับสารสนเทศขององค์กร และเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ผู้บริหารต้องจัดทำนโยบายการ

รักษาความปลอดภัยสารสนเทศขององค์กรเป็นลายลักษณ์อักษร และมีการเผยแพร่ให้พนักงานและหน่วยงานภายนอกรับรู้ มีการทบทวนนโยบายเก่าที่มีอยู่ และปรับเปลี่ยนให้ทันสมัยตามระยะเวลา

2. การจัดโครงสร้างของการรักษาความปลอดภัย มีจุดประสงค์เพื่อบริหารความปลอดภัยของข้อมูลภายในองค์กรและดูแลควบคุมระบบการรักษาความปลอดภัยของข้อมูลและระบบที่ต้องมีการเข้าถึงจากภายนอกองค์กร

2.1 โครงสร้างภายในองค์กร (Internal Organization)

2.2 กระบวนการที่เกี่ยวข้องกับหน่วยงานหรือบุคคลภายนอก

3. การจัดการทรัพย์สิน เพื่อแบ่งแยกความรับผิดชอบในทรัพย์สินต่าง ๆ ที่มีในองค์กรประกอบด้วย

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน

3.2 การจัดหมวดหมู่สารสนเทศ

4. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ มีจุดมุ่งหมายเพื่อลดความเสี่ยงที่อาจเกิดขึ้นเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกง หรือหลอกลวง และการใช้งานระบบในทางที่ผิด เพื่อทำให้มั่นใจว่าผู้ใช้มีความระมัดระวังเกี่ยวกับภัยคุกคามต่อการรักษาความปลอดภัยข้อมูลและมีระบบป้องกันและรองรับนโยบายการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน และลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์การทำงานที่ผิดพลาดของระบบและเรียนรู้จากบทเรียนต่าง ๆ

4.1 การตรวจสอบบุคลากรก่อนรับเข้าทำงาน

4.2 การตรวจสอบบุคคลระหว่างการจ้างงาน

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน

5. การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม มีจุดมุ่งหมายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อทำลาย หรือขัดขวางการดำเนินธุรกิจขององค์กร ป้องกันการสูญเสีย และป้องกันการขโมยข้อมูลและการใช้ทรัพยากรขององค์กร

5.1 การกำหนดพื้นที่ที่ต้องมีการรักษาความปลอดภัยเป็นพิเศษ

5.2 การรักษาความปลอดภัยอุปกรณ์หรือเครื่องมือ

6. การบริหารการสื่อสารและการปฏิบัติงาน มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่าระบบจัดการข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย ลดความเสี่ยงในการที่จะล่ม รักษาความถูกต้อง ความมั่นคงของซอฟต์แวร์และข้อมูล เพื่อรักษาความถูกต้องและความพร้อมใช้งานของระบบสื่อสารข้อมูลและระบบการจัดการข้อมูล เพื่อป้องกันรักษาความปลอดภัยข้อมูลบนเครือข่ายและการป้องกันโครงสร้างของระบบ ป้องกันการสูญเสียต่อทรัพย์สินและการขัดขวางต่อการดำเนินธุรกิจ

ป้องกันการสูญเสียการดัดแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดเมื่อต้องมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร

6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน

6.2 การจัดการการส่งมอบระบบงานจากหน่วยงานภายนอก

6.3 การวางแผนและการตรวจรับระบบใหม่ ๆ

6.4 การป้องกันโปรแกรมประสงค์ร้าย

6.5 การสำรองข้อมูล

6.6 การบริหารการรักษาความปลอดภัยภายในเครือข่าย

6.7 การจัดการสื่อบันทึกข้อมูล

6.8 การแลกเปลี่ยนสารสนเทศ

6.9 การให้บริการด้านพาณิชย์อิเล็คทรอนิคส์

6.10 การเฝ้าระวังและติดตาม

7. การควบคุมการเข้าถึงระบบ มีจุดมุ่งหมายเพื่อควบคุมการเข้าถึงข้อมูล ป้องกันการเจ้าถึงระบบโดยไม่ได้รับอนุญาต ป้องกันการให้บริการทางเครือข่าย ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาต รักษาความปลอดภัยเมื่อใช้อุปกรณ์เคลื่อนที่และการใช้งานการสื่อสารโทรคมนาคม

7.1 ข้อกำหนดทางธุรกิจสำหรับควบคุมการเข้าถึง

7.2 การจัดการการเข้าถึงของผู้ใช้

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน

7.4 การควบคุมการเข้าถึงเครือข่าย

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ

7.6 การเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

7.7 การควบคุมอุปกรณ์ประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

8. การดูแลและพัฒนาระบบ มีวัตถุประสงค์เพื่อให้แน่ใจว่า ระบบที่พัฒนาหรือสร้างนั้นมีความปลอดภัยเพียงพอสำหรับการใช้งานจริง ป้องกันการสูญเสีย เปลี่ยนแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดในโปรแกรมสำเร็จรูป ป้องกันความลับ การพิสูจน์ทราบตัวตน และความถูกต้องของข้อมูล ทำให้แน่ใจว่าโครงการต่าง ๆ นั้นให้ความสำคัญกับการรักษาความปลอดภัย ดูแลรักษาความปลอดภัยของโปรแกรมสำเร็จรูปและข้อมูล

8.1 ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศ

8.2 การประมวลผลที่ถูกต้องสารสนเทศในโปรแกรมประยุกต์

8.3 มาตรการการเข้ารหัสข้อมูล

8.4 การรักษาความปลอดระบบไฟล์

8.5 การรักษาความปลอดภัยในกระบวนการพัฒนาและดูแลระบบ

8.6. การบริหารช่องโหว่ทางเทคนิค

9. การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย ซึ่งมีมาตรการ 2 ส่วน คือ การรายงานเหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัย และการบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัยให้มีความรวดเร็วและมีประสิทธิภาพ

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

10. การบริหารเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง ป้องกันเหตุการณ์ที่จะขัดขวางการดำเนินธุรกิจจากเหตุการณ์ล้มเหลวขนาดใหญ่หรือภัยธรรมชาติ

10.1 การบริหารธุรกิจอย่างต่อเนื่องในประเด็นที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล

11. การปฏิบัติตามข้อกำหนดของกฎหมาย มีวัตถุประสงค์เพื่อป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่าง ๆ เพื่อทำให้แน่ใจว่า ระบบนั้นไม่ขัดต่อนโยบายการรักษาความปลอดภัยขององค์กรหรือมาตรฐาน เพื่อให้เพิ่มประสิทธิภาพของระบบตรวจสอบ และลดการรบกวนต่อการปฏิบัติงานปกติ

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย

11.2 การปฏิบัติตามนโยบาย มาตรฐานการรักษาความปลอดภัยและข้อกำหนดทางเทคนิค

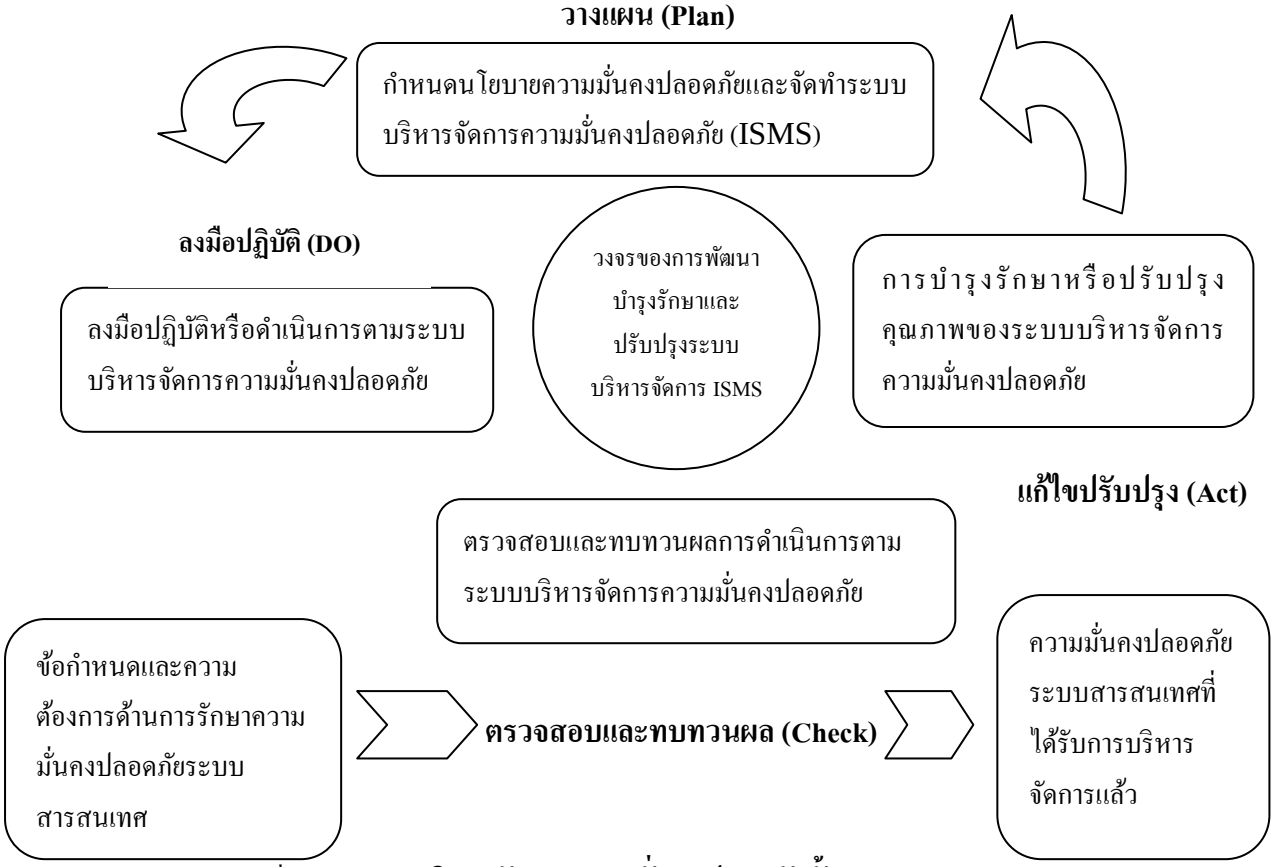
11.3 ข้อพิจารณาในการตรวจสอบระบบสารสนเทศ

2. กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ อ้างอิงข้อกำหนดตามมาตรฐาน ISO/IEC 27001 ประกอบไปด้วย 5 ข้อคือ (1) ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (2) หน้าที่ความรับผิดชอบของผู้บริหาร (3) การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย (4) การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร (5) การปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

2. 1. ข้อกำหนดทั่วไป ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

ข้อกำหนดทั่วไป องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการทางธุรกิจต่างๆ รวมทั้งความเสี่ยงที่เกี่ยวข้องกับแนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A



ภาพที่ 2 วงจรการบริหารจัดการความมั่นคงปลอดภัยขั้นตอน Plan-Do-Check-Act

2.2 กำหนดและบริหารจัดการ ระบบบริหารจัดการความมั่นคงปลอดภัย กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) องค์กรจะต้องปฏิบัติดังนี้ กำหนดขอบเขตบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สินและเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัย

2.3 กำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้งทรัพย์สินและเทคโนโลยี นโยบายความมั่นคงปลอดภัยจะต้องมีองค์ประกอบกรอบในการดำเนินการ ทิศทางและหลักการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับ

สารสนเทศ ข้อกำหนดทางธุรกิจ ข้อกำหนดในสัญญาต่างๆ ระบบปฏิบัติ ข้อบังคับ รวมทั้งกฎหมายของประเทศ การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ในระดับองค์กร เกณฑ์ในการประเมินความเสี่ยง และการได้รับการอนุมัติจากผู้บริหาร

2.4 กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยขององค์กร โดยกำหนดเกณฑ์ในการยอมรับความเสี่ยง และระบุระดับความเสี่ยงที่ยอมรับได้ ซึ่งระบบความเสี่ยง เช่น (1) ระบุทรัพย์สินที่อยู่ในขอบเขตของระบบบริหารจัดการ (2) ระบุภัยคุกคามที่มีต่อทรัพย์สินเหล่านั้น (3) ระบุจุดอ่อนที่ภัยคุกคามอาจจะใช้ให้เป็นประโยชน์ (4) ระบุผลกระทบที่ก่อให้เกิดความสูญเสียทางด้านความลับความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

สำหรับการวิเคราะห์และประเมินความเสี่ยงมีดังนี้ (1) ประเมินผลกระทบที่มีต่อธุรกิจซึ่งอาจเป็นผลจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย โดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น (2) กำหนดความน่าจะเป็นของความเสี่ยงอันเกิดจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย โดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น (3) กำหนดระดับความเสี่ยง (4) กำหนดว่าความเสี่ยงเหล่านั้น สามารถยอมรับได้หรือไม่ โดยใช้เกณฑ์ในการยอมรับความเสี่ยง (ชนม์ชนก วีรวรรณ, 2541)

การระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ อาจรวมถึงใช้มาตรการที่เหมาะสม ยอมรับความเสี่ยงเหล่านั้นโดยมีเงื่อนไขว่า ความเสี่ยงเหล่านั้น จะต้องอยู่ภายในเกณฑ์ในการยอมรับความเสี่ยงที่ยอมรับได้เพื่อหลีกเลี่ยงความเสี่ยงเหล่านั้น และโอนย้ายความเสี่ยงเหล่านั้นไปสู่ผู้อื่น

เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัย เพื่อจัดการกับความเสี่ยง วัตถุประสงค์และมาตรการดังกล่าว สามารถเลือกมาจากมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ในตอนท้ายของมาตรฐานฉบับนี้

ขออนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรการตามที่แสดงไว้ในส่วนของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ เอกสารดังกล่าว มีองค์ประกอบดังนี้ (1) วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยตามที่ได้เลือกไว้ รวมทั้งเหตุผลการใช้งาน (2) วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยที่ได้ใช้งานอยู่ในปัจจุบัน และ (3) วัตถุประสงค์และมาตรการความมั่นคงปลอดภัยที่ไม่มีการใช้งานรวมทั้งเหตุผลที่ไม่มีการใช้งาน

2.5 ลงปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยองค์กร ควรปฏิบัติดังนี้

2.5.1 จัดทำแผนการจัดการความเสี่ยง ซึ่งกล่าวถึงการดำเนินการเชิงบริหารจัดการทรัพยากรที่จำเป็น หน้าที่ความรับผิดชอบ และลำดับการดำเนินการเพื่อบริหารจัดการความเสี่ยงที่พบ

2.5.2 ลงมือปฏิบัติตามแผนการจัดการความเสี่ยง เพื่อบรรลุในวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

2.5.3 ลงมือปฏิบัติตามมาตรการที่เลือกไว้ เพื่อบรรลุวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยของมาตรการดังกล่าว

2.5.4 กำหนดวิธีการในการวัดความสัมฤทธิ์ผลของมาตรการที่เลือกมาใช้งาน การวัดดังกล่าว จะต้องสามารถสร้างผลลัพธ์ที่สามารถเปรียบเทียบได้ รวมทั้งสามารถสร้างผลลัพธ์เดิมขึ้นมาอีกครั้งหนึ่งได้

2.5.5 จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก

2.5.6 บริหารการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

2.5.7 บริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

2.5.8 จัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตาการณ์ทางด้านความมั่นคงปลอดภัย

2.6 เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ดำเนินการทบทวน ความสัมฤทธิผลของระบบการบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยนำสิ่งต่างๆ ต่อไปนี้มาพิจารณาร่วมด้วยได้แก่ ผลการปลอดภัยอย่างสม่ำเสมอ โดยนำสิ่งต่างๆ ต่อไปนี้มาพิจารณาร่วมด้วยได้แก่ ผลการตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่

เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือหน่วยงานที่เกี่ยวข้อง เป็นต้น วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับ ระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ โดยพิจารณาการเปลี่ยนแปลงของสิ่งต่อไปนี้ ประกอบด้วย องค์กร เทคโนโลยี วัตถุประสงค์และกระบวนการทางธุรกิจ ภัยคุกคามที่ระบุไว้ก่อนหน้านี้ กับสภาพการเปลี่ยนแปลงปัจจุบัน ความสัมฤทธิผลของมาตรการที่ได้ลงมือปฏิบัติไปแล้ว เหตุการณ์ภายนอกได้แก่ การเปลี่ยนแปลงที่มีต่อกฎระเบียบกฎหมาย ข้อกำหนดในสัญญาที่ทำไว้ หรือข้อกำหนดอื่นๆ และการเปลี่ยนแปลงทางสังคม เป็นต้น (ชัยยศ สันติวงศ์ และนิตยา เจริยงประเสริฐ, 2546)

2.7 การบำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย องค์กรควรปฏิบัติ โดยการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ ใช้มาตรการเชิงแก้ไขและป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่นมาช่วยในการปรับปรุงให้ดีขึ้น แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

3. หน้าที่ความรับผิดชอบของผู้บริหาร

3.1 การให้ความสำคัญในการบริหารจัดการ ผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย โดยกำหนดนโยบายความมั่นคงปลอดภัย กำหนดวัตถุประสงค์และแผนสำหรับระบบบริหารจัดการ กำหนดบทบาทและหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย แจ้งทุกหน่วยภายในองค์กรได้รับทราบถึงความสำคัญของการรักษาความมั่นคงปลอดภัยและการปฏิบัติตามนโยบายความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบภายใต้กฎหมายของประเทศ รวมทั้งการยกระดับด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง จัดสรรทรัพยากรอย่างเพียงพอสำหรับการกำหนด การลงมือปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษา และการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ จัดให้มีการ

ตรวจสอบภายในสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย

3.2 การบริหารจัดการทรัพยากร

3.2.1 การจัดทรัพยากร องค์กรจะต้อง จัดสรรทรัพยากรที่จำเป็น เพื่อกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย ให้มีการดำเนินการตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัย ให้สามารถระบุข้อกำหนดที่เกี่ยวข้องกับกฎหมายและระเบียบปฏิบัติ รวมถึงข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้ในสัญญา ให้สามารถบำรุงรักษาความมั่นคงปลอดภัยอย่างพอเพียง โดยการเลือกใช้มาตรการทางด้านความมั่นคงปลอดภัยที่ถูกต้องและเหมาะสม ให้มีการดำเนินการทบทวนตามความจำเป็นรวมถึงมีการดำเนินการเพิ่มเติมอย่างเหมาะสมต่อผลของการทบทวนนั้น และให้สามารถปรับปรุงความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัย

3.2.2 การอบรม การสร้างความตระหนัก และการเพิ่มขีดความสามารถ องค์กรจะต้องดำเนินการเพื่อให้บุคคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่ความรับผิดชอบตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย บุคลากรเหล่านั้น ควรมีขีดความสามารถที่จะปฏิบัติงานตามที่กำหนดไว้ ดังนี้ (1) กำหนดความรู้ความสามารถที่จำเป็นสำหรับบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัย (2) จัดการอบรมหรือใช้วิธีการอื่นๆ (เช่น ว่าจ้างบุคลากรที่มีความสามารถ) เพื่อเป็นการเสริมความรู้ความสามารถ (3) ประเมินความสัมฤทธิผลของการดำเนินการ (4) เก็บรักษาบันทึกข้อมูลที่เกี่ยวข้องกับการศึกษา การฝึกอบรมทักษะประสบการณ์และคุณสมบัติของบุคคลากรขององค์กร องค์กรจะต้องดำเนินการให้บุคลากรที่เกี่ยวข้อง มีความตระหนักถึงความเกี่ยวข้องและความสำคัญของกิจกรรมทางด้านความมั่นคงปลอดภัยที่บุคคลเหล่านี้เป็นส่วนหนึ่งและมีผลต่อความสำเร็จของระบบบริหารจัดการความมั่นคงปลอดภัย

4. การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย

องค์กรควรดำเนินการตรวจสอบภายในตามรอบระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนการปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัย สอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้ และกฎหมาย ระเบียบ ข้อบังคับหรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องหรือไม่ สอดคล้องกับข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ได้

กำหนดไว้หรือไม่ ได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิผลหรือไม่ และเป็นไปตามที่คาดหมายไว้หรือไม่

องค์กรจะต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่างๆ ที่จะได้รับการตรวจสอบ รวมทั้งผลการตรวจสอบจากครั้งต่างๆ ที่ผ่านมา องค์กรจะต้องกำหนดเกณฑ์ในการตรวจสอบ ขอบเขต ความถี่ และวิธีการที่ใช้ในการตรวจสอบ การคัดเลือกผู้ตรวจสอบ และการดำเนินการตรวจสอบจะต้องคำนึงถึงหลักฐานตามความเป็นจริง และความเที่ยงธรรมของผู้ตรวจสอบ รวมทั้งผู้ตรวจสอบจะต้องไม่ตรวจสอบงานของตนเอง

องค์กรต้องระบุหน้าที่ ความรับผิดชอบและข้อกำหนดต่างๆ ในการวางแผนและดำเนินการตรวจสอบ รวมทั้งลายการจัดทำรายงานผลการตรวจสอบ และบำรุงรักษาบันทึกข้อมูลที่เกี่ยวข้องกับการตรวจสอบนั้น อย่างเป็นลักษณ์อักษร

ผู้บริหารที่รับผิดชอบในส่วนที่ได้รับการตรวจสอบจะต้องควบคุมให้การดำเนินการแก้ไข เพื่อกำจัดความไม่สอดคล้องและสาเหตุที่เกี่ยวข้องได้รับการดำเนินการโดยปราศจากความล่าช้าที่เกินควร รวมทั้งจะต้องควบคุมให้มีกิจกรรมการติดตามเพื่อตรวจสอบการดำเนินการที่ได้ดำเนินการไปแล้ว และมีการจัดทำรายงานผลการตรวจสอบนั้น

5. การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร

5.1 ข้อกำหนดทั่วไป ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่น ปีละ 1 ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิผล การทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งหมายรวมถึงนโยบายความมั่นคงปลอดภัยและวัตถุประสงค์ทางด้านความมั่นคงปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนจะต้องได้รับการบำรุงรักษาไว้ (พรพิไล เลิศวิชา, 2541)

5.2 ข้อมูลนำเข้าที่ใช้ในการทบทวน ข้อมูลนำเข้าที่ใช้ในการทบทวนโดยผู้บริหารจะรวมถึง ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยและผลการทบทวน ผลตอบกลับจากทุกหน่วยที่เกี่ยวข้อง เทคนิค ผลิตภัณฑ์ หรือขั้นตอนการปฏิบัติซึ่งสามารถใช้ในการปรับปรุงประสิทธิภาพและความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย สถานภาพของการดำเนินการเชิงป้องกันและการดำเนินการเชิงแก้ไข จุดอ่อนหรือภัยคุกคามที่ยังไม่ได้รับการกล่าวถึงในรายงานการประเมินความเสี่ยงครั้งที่ผ่านมา ผลของการวัดความสัมฤทธิ์ผล การดำเนินการติดตามจากผลการทบทวนครั้งต่างๆ ที่ผ่านมา การเปลี่ยนแปลงแก้ไขที่อาจมีผลต่อระบบบริหารจัดการความมั่นคงปลอดภัย ข้อเสนอแนะในการปรับปรุงแก้ไข

5.3 ผลจากการทบทวน ผลจากการทบทวนโดยผู้บริหารจะรวมถึงการตัดสินใจและการดำเนินการต่างๆ ดังนี้ (1) การปรับปรุงทางด้านความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย (2) การปรับปรุงด้านการประเมินความเสี่ยงและปรับปรุงแผนการจัดการกับความเสี่ยง (3) การแก้ไขขั้นตอนปฏิบัติและมาตรการที่มีผลต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ การแก้ไขดังกล่าว อาจเป็นผลมาจากการเปลี่ยนแปลง ข้อกำหนดทางธุรกิจ ข้อกำหนดทางด้านความมั่นคงปลอดภัย กระบวนการทางธุรกิจที่มีผลต่อข้อกำหนดทางธุรกิจที่มีอยู่ในปัจจุบัน ข้อกำหนดที่เกี่ยวข้องกับกฎ ระเบียบหรือกฎหมาย ข้อกำหนดที่ระบุไว้ในสัญญา และระดับของความเสี่ยง และ/หรือ เกณฑ์สำหรับการยอมรับความเสี่ยง ความต้องการด้านทรัพยากร การปรับปรุงวิธีการวัดความสัมฤทธิผลของมาตรการที่ใช้

6. การดำเนินการเพื่อบำรุงรักษาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

6.1 การปรับปรุงอย่างต่อเนื่อง องค์กรจะต้องปรับปรุงความสัมฤทธิผลของระบบบริหารความมั่นคงปลอดภัยอย่างต่อเนื่อง โดยใช้นโยบายความมั่นคงปลอดภัย วัตถุประสงค์ทางด้านความมั่นคงปลอดภัย ผลการตรวจสอบความมั่นคงปลอดภัย ผลการวิเคราะห์เหตุการณ์ที่ได้รับการเฝ้าระวัง การดำเนินการเชิงแก้ไขและป้องกัน การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร

6.2 การดำเนินการเชิงแก้ไข องค์กรจะดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนดสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อป้องกันการเกิดขึ้นอีก ขั้นตอนปฏิบัติสำหรับการดำเนินการเชิงแก้ไขที่เป็นลายลักษณ์อักษร จะต้องพิจารณาถึงการระบุความไม่สอดคล้อง การระบุสาเหตุของความไม่สอดคล้อง การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันไม่ให้ความไม่สอดคล้องนั้นเกิดขึ้นอีก การลงมือปฏิบัติการดำเนินการเชิงแก้ไขตามความจำเป็น การบันทึกข้อมูลผลการดำเนินการ การทบทวนการดำเนินการเชิงแก้ไขที่ได้ปฏิบัติแล้ว (เยาวดี รางชัยกูล, 2542)

6.3 การดำเนินการเชิงป้องกัน องค์กรจะต้องดำเนินการกำจัดสาเหตุความไม่สอดคล้องกับข้อกำหนดสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยที่มีโอกาสเกิดขึ้นเพื่อป้องกันกรเกิดขึ้น การดำเนินการเชิงป้องกันจะต้องเหมาะสมกับผลกระทบของปัญหาที่มีโอกาสเกิดขึ้น ขั้นตอนการปฏิบัติสำหรับการดำเนินการเชิงป้องกันที่เป็นลายลักษณ์อักษร จะต้องพิจารณา

ถึงการระบุความไม่สอดคล้องที่มีโอกาสเกิดขึ้นและสาเหตุของความไม่ถูกต้อง การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้อง การลงมือปฏิบัติการดำเนินการเชิงป้องกันตามความจำเป็น การบันทึกข้อมูลผลการดำเนินการ และการทบทวนการดำเนินการเชิงป้องกันที่ได้ปฏิบัติไปแล้ว

องค์กรจะต้องระบุความเสี่ยงที่แปรเปลี่ยนไปและกำหนดการดำเนินการเชิงป้องกัน โดยให้ความสำคัญกับความเสี่ยงที่มีระดับสูง รวมทั้งกำหนดลำดับความสำคัญของการดำเนินเชิงป้องกัน โดยพิจารณาจากผลของการประเมินความเสี่ยง

มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

การจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ อ้างอิงตามมาตรฐาน ISO/IEC 27001 Annex A และศึกษารายละเอียดวิธีปฏิบัติทางเทคนิคจาก ISO/IEC 17799:2005 มีดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy) นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

วัตถุประสงค์ เพื่อกำหนดทิศทางการดำเนินการด้านการรักษาความปลอดภัยสำหรับสารสนเทศขององค์กร และเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ผู้บริหารต้องจัดทำนโยบายการรักษาความปลอดภัยสารสนเทศขององค์กรเป็นลายลักษณ์อักษร และมีการเผยแพร่ให้พนักงานและหน่วยงานภายนอกรับรู้ มีการทบทวนนโยบายเก่าที่มีอยู่ และปรับเปลี่ยนให้ทันสมัยตามระยะเวลา ประกอบด้วย

1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร ผู้บริหารองค์กรต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมด ที่เกี่ยวข้องได้รับทราบ

1.2 การทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

วัตถุประสงค์ เพื่อบริหารความปลอดภัยของข้อมูลภายในองค์กรและดูแลควบคุมระบบการรักษาความปลอดภัยของข้อมูลและระบบที่ต้องมีการเข้าถึงจากภายนอกองค์กร ประกอบด้วย

2.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย ผู้บริหารองค์กรต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจน และการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร ผู้บริหารสารสนเทศต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงาน หรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้น จะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย ผู้บริหารสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัย สำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

2.4 กระบวนการในการอนุมัติการใช้งาน อุปกรณ์ประมวลผลสารสนเทศ ผู้บริหารสารสนเทศต้องกำหนดกระบวนการในการอนุมัติกรใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

2.5 การลงนามมิให้เปิดเผยความลับองค์กร หัวหน้างานบุคคลต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไปเปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

2.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่นๆ ผู้บริหารสารสนเทศต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการ

อินเทอร์เน็ต ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

2.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน ผู้บริหารองค์กรและหัวหน้างานสารสนเทศต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม

2.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ ผู้บริหารสารสนเทศต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

3. โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

3.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก หัวหน้างานสารสนเทศต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

3.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร หัวหน้างานสารสนเทศต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

3.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร หัวหน้างานสารสนเทศต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัย สำหรับสารสนเทศระหว่างองค์กรและหน่วยงาน

ภายนอกเมื่อมีความจำเป็นต้องให้หน่วยงานนั้น เข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

3. การบริหารจัดการทรัพย์สินขององค์กร

วัตถุประสงค์ เพื่อแบ่งแยกความรับผิดชอบในทรัพย์สินต่าง ๆ ที่มีประกอบด้วย

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินของ มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

3.1.1 การจัดทำบัญชีทรัพย์สิน หัวหน้างานพัสดุและหัวหน้างานสารสนเทศต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน หัวหน้างานพัสดุและหัวหน้างานสารสนเทศต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน

3.1.3 การใช้งานทรัพย์สินที่เหมาะสม หัวหน้างานพัสดุและหัวหน้างานสารสนเทศจะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น

3.2 การจัดหมวดหมู่สารสนเทศ มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

3.2.1การจัดหมวดหมู่ทรัพย์สินสารสนเทศ หัวหน้างานสารสนเทศจะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ หัวหน้างานสารสนเทศจะต้องจัดให้มีขั้นตอนการปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคลากร

วัตถุประสงค์เพื่อลดความเสี่ยงที่อาจเกิดขึ้นเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกง หรือหลอกลวง และการใช้งานระบบในทางที่ผิด เพื่อทำให้มั่นใจว่าผู้ใช้มีความระมัดระวังเกี่ยวกับภัยคุกคามต่อการรักษาความปลอดภัยข้อมูลและมีระบบป้องกันและรองรับนโยบายการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน และลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์การทำงานที่ผิดพลาดของระบบและเรียนรู้จากบทเรียนต่าง ๆ
ประกอบด้วย

4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย หัวหน้างานสารสนเทศต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงานผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้างต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคล หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึงประกอบการคัดเลือกด้วย

4.1.3 การกำหนดเงื่อนไขการจ้างงาน หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้างต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญาและการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าว จะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งถึงหน้าที่รับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.2.1 หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัย ผู้บริหารองค์กรต้องกำหนดให้พนักงานที่ได้รับกานว่าจ้างตามสัญญา การจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนการปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ พนักงาน หัวหน้าพนักงานบุคคลและหัวหน้างานที่เกี่ยวข้องต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกได้รักการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

4.2.3 กระบวนการทางวินัยเพื่อลงโทษ ผู้บริหารองค์กรต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบาย หรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอก ได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

4.3.1การสิ้นสุดหรือการเปลี่ยนการจ้างงาน หัวหน้างานบุคคลต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

4.3.2 การคืนทรัพย์สินขององค์กร หัวหน้างานบุคคลและหัวหน้างานพัสดุต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือการเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

4.3.3 การถอดถอนสิทธิในการเข้าถึง หัวหน้างานสารสนเทศและหัวหน้างานอาคารต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อทำลาย หรือขัดขวางการดำเนินธุรกิจขององค์กร ป้องกันการสูญเสีย และป้องกันการขโมยข้อมูลและการใช้ทรัพยากรขององค์กร ประกอบด้วย การกำหนดพื้นที่ที่ต้องมีการรักษาความปลอดภัยเป็นพิเศษ และการรักษาความปลอดภัยอุปกรณ์หรือเครื่องมือ รายละเอียดมีดังนี้

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพ โดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

5.1.1 การจัดทำบริเวณล้อมรอบ หัวหน้างานสารสนเทศ และหัวหน้างานอาคารต้องมีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออก ที่มีการควบคุมตั้งโต๊ะทำการของ ผู้รักษาความปลอดภัยบริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร (ปทีป เมธาคุณวุฒิ, 2544)

5.1.2 การควบคุมการเข้า-ออก หัวหน้างานสารสนเทศและหัวหน้างานอาคารต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออก ได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ หัวหน้างานอาคารต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม งานอาคารต้องจัดให้มีการป้องกันภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย หัวหน้างานอาคาร ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก หัวหน้างานอาคาร และหัวหน้างานสารสนเทศต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบ ผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

5.2.1 การจัดวางและป้องกันอุปกรณ์ พนักงานต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน หัวหน้างานสารสนเทศต้องกำหนดให้มีกลไกการทำงาน การป้องกันการล้มเหลวของระบบและอุปกรณ์ สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณหรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

5.2.4 การบำรุงรักษาอุปกรณ์ หัวหน้างานสารสนเทศต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

5.2.5 การป้องกันอุปกรณ์ ที่ใช้งานอยู่นอกสำนักงาน หัวหน้างานสารสนเทศต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงาน เพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น

5.2.6 การกำจัดอุปกรณ์หรือ การนำอุปกรณ์กลับมาใช้งานอีกครั้ง พนักงานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าว ได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าว หากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน หัวหน้างานอาคารต้องไม่อนุญาตในการนำทรัพย์สินออกนอกองค์กรได้แก่ อุปกรณ์สารสนเทศหรือซอฟต์แวร์ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

วัตถุประสงค์ เพื่อทำให้แน่ใจว่าระบบจัดการข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย ลดความเสี่ยงในการที่จะล่ม รักษาความถูกต้อง ความมั่นคงของซอฟต์แวร์และข้อมูล เพื่อรักษาความถูกต้องและความพร้อมใช้งานของระบบสื่อสารข้อมูลและระบบการจัดการข้อมูล เพื่อป้องกันรักษาความปลอดภัยข้อมูลบนเครือข่ายและการป้องกันโครงสร้างของระบบ ป้องกันการสูญเสียต่อทรัพย์สินและการขัดขวางต่อการดำเนินธุรกิจ ป้องกันการสูญเสียการดัดแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดเมื่อต้องมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร ประกอบด้วย

6.1 การกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนการปฏิบัติงาน

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร หัวหน้างานสารสนเทศ ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควรและแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบ หรืออุปกรณ์ประมวลผลสารสนเทศหัวหน้างานสารสนเทศ ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

6.1.3 การแบ่งหน้าที่ความรับผิดชอบ ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือให้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน หัวหน้างานสารสนเทศต้องจัดให้มีการแยกระบบสำหรับการพัฒนากรทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่ โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

6.2.1 การให้บริการโดยหน่วยงานภายนอก หัวหน้างานสารสนเทศ ต้องกำหนดให้ผู้ให้บริการจากภายนอก ปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ

6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก หัวหน้างานสารสนเทศต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้ เป็นต้น

6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ ผู้บริหารสารสนเทศต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือ กระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงาน

ภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนการปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ หัวหน้างานสารสนเทศต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศ เพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งาน

6.3.2 การตรวจรับ หัวหน้างานสารสนเทศต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดลองก่อนที่จะได้รับระบบนั้นมาใช้งาน

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี มีจุดประสงค์เพื่อรักษาซอฟท์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี ผู้ดูแลระบบต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ ผู้ดูแลระบบ ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่ง เพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

6.5 การสำรองข้อมูล มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้งานของสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ หัวหน้างานสารสนเทศต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

6.6.1 มาตรการทางเครือข่าย ผู้ดูแลระบบต้องบริหารและจัดการเครือข่ายกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมสำเร็จรูปที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย หัวหน้างานสารสนเทศ ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการ สำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้ อาจจะเป็นบริการเครือข่ายภายในขององค์กรเอง หรือบริการที่ได้รับจากหน่วยงานภายนอก (ไอทีของภาครัฐ, 2550)

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ หัวหน้างานสารสนเทศต้องกำหนดขั้นตอนการปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

6.7.2 การกำจัดสื่อบันทึกข้อมูล หัวหน้างานสารสนเทศต้องกำหนดขั้นตอนการปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

6.7.3 ขั้นตอนการปฏิบัติสำหรับการจัดการสารสนเทศ หัวหน้างานสารสนเทศ ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ หัวหน้างานสารสนเทศต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

6.8 การแลกเปลี่ยนสารสนเทศ มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟแวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

6.8.1 นโยบายและขั้นตอนการปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ ผู้บริหารองค์กรต้องกำหนดนโยบาย ขั้นตอนการปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ หัวหน้างานสารสนเทศ ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟแวร์ระหว่างองค์กร อย่างเป็นลายลักษณ์อักษร

6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร หัวหน้างานสารสนเทศและหัวหน้างานธุรการต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน ผู้บริหารสารสนเทศต้องกำหนดนโยบายและขั้นตอนการปฏิบัติ เพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

6.9 การสร้างความมั่นคงปลอดภัยสำหรับการบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

6.9.1 การพาณิชย์อิเล็กทรอนิกส์ หัวหน้างานสารสนเทศต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ ที่มีการส่งผ่านเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

6.9.2 การทำธุรกรรมออนไลน์ หัวหน้างานสารเสนเทศต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ได้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศที่ถูกส่งไปผิดเส้นทางบน

เครือข่าย การเปลี่ยนแปลงสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ ผู้ดูแลระบบต้องกำหนดให้มีการป้องกันความถูกต้อง และความสมบูรณ์ของสารสนเทศ ที่มีการเผยแพร่ออกสู่สาธารณะ

6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ หัวหน้างานสารสนเทศต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

6.10.2 การตรวจสอบการใช้งานระบบ หัวหน้างานสารสนเทศต้องกำหนดให้มีขั้นตอนการปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ หัวหน้างานสารสนเทศต้องกำหนดให้มีมาตรการป้องกันข้อมูล บันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ หัวหน้างานสารสนเทศต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด หัวหน้างานสารสนเทศต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาด เหล่านั้น และดำเนินการแก้ไขตามสมควร

6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน ผู้ดูแลระบบต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลา หากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

7. การควบคุมการเข้าถึง

วัตถุประสงค์ เพื่อควบคุมการเข้าถึงข้อมูล ป้องกันการเจ้าถึงระบบโดยไม่ได้รับอนุญาต ป้องกันการให้บริการทางเครือข่าย ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาต รักษาความปลอดภัยเมื่อใช้อุปกรณ์เคลื่อนที่และการใช้งานการสื่อสารโทรคมนาคม ประกอบด้วย

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ นโยบายการควบคุมการเข้าถึงระบบ ผู้บริหารสารสนเทศต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึง อย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้ จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.1 การลงทะเบียนพนักงาน หัวหน้างานสารสนเทศต้องกำหนดให้มีขั้นตอนการปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนพนักงานใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้ง ขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือ เปลี่ยนแปลงตำแหน่งงานภายในองค์กร เป็นต้น

7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

7.2.3 การบริหารจัดการรหัสผ่าน สำหรับผู้ใช้งาน ผู้ดูแลระบบต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่าน สำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่าน ให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน หัวหน้างานสารสนเทศต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

7.3.1 การใช้งานรหัสผ่าน ผู้ดูแลระบบ ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล พนักงานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

7.3.3 นโยบายการควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย ผู้บริหารสารสนเทศต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นสาธารณะ หรือพบเห็นได้ง่าย เป็นต้น

7.4 การควบคุมการเข้าถึงเครือข่าย มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

7.4.1 นโยบายการใช้งานบริการเครือข่าย ผู้บริหารสารสนเทศต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่า บริการใดที่อนุญาตให้ผู้ใช้งานสารสนเทศใช้ได้ บริการใดที่ไม่สามารถใช้งานได้

7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะได้รับอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่า การเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ผู้ดูแลระบบต้องมีมาตรการป้องกันการเข้าถึงช่องทางที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพ และการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

7.4.5 การแบ่งแยกเครือข่าย ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ

7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย ผู้ดูแลระบบ ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่าง องค์กรการเชื่อมต่อ ต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้

7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย ผู้ดูแลระบบต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมโยงทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึง หรือการใช้งานระบบปฏิบัติการ

7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

7.5.3 ระบบบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดทำหรือจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่ได้กำหนดไว้ หรือมีอยู่แล้ว

7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

7.6 การควบคุมการเข้าถึงโปรแกรมสำเร็จรูปและสารสนเทศ มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของโปรแกรมสำเร็จรูปโดยไม่ได้รับอนุญาต

7.6.1 การกำจัดการเข้าถึงสารสนเทศ ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมสำเร็จรูปตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง หัวหน้างานสารสนเทศต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหาก ออกมาสำหรับระบบนี้โดยเฉพาะ

7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา ผู้บริหารสารสนเทศ ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน ผู้บริหารสารสนเทศต้องกำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติสำหรับบุคคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์ เพื่อให้แน่ใจว่า ระบบที่พัฒนาหรือสร้างนั้นมีความปลอดภัยเพียงพอสำหรับการใช้งานจริง ป้องกันการสูญเสีย เปลี่ยนแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดในโปรแกรมสำเร็จรูป ป้องกันความลับ การพิสูจน์ทราบตัวตน และความถูกต้องของข้อมูล ทำให้แน่ใจว่าโครงการต่าง ๆ นั้นให้ความสำคัญกับการรักษาความปลอดภัย ดูแลรักษาความปลอดภัยของโปรแกรมสำเร็จรูปและข้อมูล ประกอบด้วย ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยในระบบสารสนเทศ การประมวลผลที่ถูกต้องสารสนเทศในโปรแกรมประยุกต์ มาตรการการเข้ารหัสข้อมูล การรักษาความปลอดระบบไฟล์ การรักษาความปลอดภัยในกระบวนการพัฒนาและดูแลระบบ การบริหารช่องโหว่ทางเทคนิค รายละเอียดดังนี้

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญซึ่งการวิเคราะห์และการระบุข้อกำหนดทางด้านความ

มั่นคงปลอดภัย ผู้พัฒนา และผู้เป็นเจ้าของระบบต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย สำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

8.2 การประมวลผลสารสนเทศในโปรแกรมสำเร็จรูป มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศ โดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

8.2.1 การตรวจสอบข้อมูลนำเข้า ผู้พัฒนาระบบต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้า ของโปรแกรมสำเร็จรูปว่าข้อมูลนั้นมีความถูกต้องและเหมาะสม ก่อนที่จะนำไปประมวลผลต่อไป

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล ผู้พัฒนาระบบต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผล เกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

8.2.3 การตรวจสอบความถูกต้องของข้อความ ผู้พัฒนาระบบต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับโปรแกรมสำเร็จรูป (เพื่อให้สามารถตรวจสอบได้ว่า เป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

8.2.4 การตรวจสอบข้อมูลนำออก ผู้พัฒนาระบบต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากโปรแกรมสำเร็จรูปเพื่อเป็นการทบทวนว่าการประมวลผลสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องเหมาะสม

8.3 มาตรการการเข้ารหัสข้อมูล มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูล โดยใช้วิธีการการเข้ารหัสข้อมูล

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล ผู้บริหารสารสนเทศต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และมีผลบังคับใช้งานภายในองค์กร

8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูล ที่กำหนดเป็นมาตรฐานขององค์กร

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆของระบบที่ให้บริการ

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ หัวหน้างานสารสนเทศต้องจัดให้มีขั้นตอนการปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการ ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ

8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ หัวหน้างานสารสนเทศต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้ เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและกระบวนการสนับสนุน มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

8.5.1 ขั้นตอนการปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ หัวหน้างานสารสนเทศต้องกำหนดขั้นตอนการปฏิบัติอย่างเป็นทางการ สำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.5.2 การตรวจสอบการทำงานของโปรแกรมสำเร็จรูปภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ ผู้ดูแลระบบต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ เพื่อดูว่าโปรแกรมสำเร็จรูปที่ทำงานอยู่บนระบบปฏิบัติการนั้นทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หัวหน้างานสารสนเทศต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หาก

จำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

8.5.4 การป้องกันการรั่วไหลของสารสนเทศ หัวหน้างานสารสนเทศต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป

8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก หัวหน้างานสารสนเทศต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์ และ ซอฟต์แวร์ มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ มาตรการควบคุมช่องโหว่ทางเทคนิค หัวหน้างานสารสนเทศต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่กี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

วัตถุประสงค์ การรายงานเหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัยและการบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัยให้มีความรวดเร็วและมีประสิทธิภาพ

ประกอบด้วย

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย พนักงานหรือผู้ที่องค์กรจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กรต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร พนักงาน หรือผู้ที่องค์กรจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่

ปฏิบัติงานอยู่ภายในองค์กรต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย มีจุดประสงค์เพื่อให้มีวิธีที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ หัวหน้างานสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรและขั้นตอนดังกล่าว ต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ผู้ดูแลระบบต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2.3 การเก็บรวบรวมหลักฐาน หัวหน้างานนิติการและหัวหน้างานสารสนเทศต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือ หลักเกณฑ์ สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้น มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

วัตถุประสงค์ เพื่อป้องกันเหตุการณ์ที่จะขัดขวางการดำเนินธุรกิจจากเหตุการณ์ล้มเหลวขนาดใหญ่หรือภัยธรรมชาติ ประกอบด้วย

10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญ อันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ ผู้บริหารสารสนเทศต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการ

และการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้ จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ หัวหน้างานสารสนเทศต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ ผู้บริหารสารสนเทศต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินการต่างๆ ให้สามารถดำเนินต่อไปได้ ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ ผู้บริหารสารสนเทศต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมด มีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ

10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ ผู้บริหารสารสนเทศต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

11. การปฏิบัติตามข้อกำหนด

วัตถุประสงค์ เพื่อป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่าง ๆ เพื่อทำให้แน่ใจว่า ระบบนั้นไม่ขัดต่อนโยบายการรักษาความปลอดภัยขององค์กรหรือมาตรฐาน เพื่อให้เพิ่มประสิทธิภาพของระบบตรวจสอบ และลดการรบกวนต่อการปฏิบัติงานปกติ ประกอบด้วย

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย หัวหน้างานนิติการต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่าง

องค์กร และบุคคล หรือหน่วยงานภายนอกอื่นๆ) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็น ลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา หัวหน้างานนิติการต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคล หรือ หน่วยงานภายนอกอื่นๆ) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย

11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร หัวหน้างานสารสนเทศต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

11.1.4 การป้องกันข้อมูลส่วนตัว หัวหน้างานนิติการ และหัวหน้างานสารสนเทศต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง

11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ หัวหน้างานสารสนเทศต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กร ผิดวัตถุประสงค์หรือ โดยไม่ได้รับอนุญาต

11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด หัวหน้างานนิติการและหัวหน้างานสารสนเทศต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูล โดยให้ยึดถือตามหรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.1 การปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร ผู้บริหารสารสนเทศต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน

ของผู้ที่อยู่ใต้บังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัย ตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร หัวหน้างานสารสนเทศต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

11.3 การตรวจประเมินระบบสารสนเทศ มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซง หรือ ทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ หัวหน้างานสารสนเทศต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจ ในระหว่างที่ทำการตรวจประเมิน

11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ หัวหน้างานสารสนเทศต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อ ป้องกันการใช้งานผิดวัตถุประสงค์ หรือ การเปิดเผยข้อมูลการตรวจสอบประเมินโดยไม่ได้รับอนุญาต (ThaiCERT, NECTEC, มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550)

สรุปแนวคิดมาตรฐาน ISO/IEC 27001

มาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูล ISO/IEC 27001ข้อกำหนดต่าง ๆ กำหนดขึ้นโดยสถาบันนานาชาติ ISO (The International Organization for Standardization) และ IEC (International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจดำเนินไปอย่างต่อเนื่อง ช่วยป้องกันกระบวนจากภัยคุกคามต่าง ๆ เป็นมาตรฐานเกี่ยวกับการบริหารการรักษาความปลอดภัยข้อมูล เป็นแนวทางในการพัฒนา ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยข้อมูลโดยใช้รูปแบบการบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการพัฒนาระบบการรักษาความปลอดภัย

งานวิจัยที่เกี่ยวข้อง

เพ็ญประภา พิพัฒนาโฆษิต (2550) ได้ศึกษาการสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูลโดยการประยุกต์ใช้ ISO 17799 ของบริษัทให้บริการด้านการจัดซื้อออนไลน์ เพื่อนำเสนอความเสี่ยงในด้านต่างๆ ที่อาจเกิดขึ้น และหาแนวทางการประยุกต์มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 17799 ที่เหมาะสมมาใช้ โดยเป็นการนำเสนอแก่ผู้บริหารองค์กรให้เห็นถึงความเสี่ยงที่อาจเกิดขึ้น ถ้าไม่มีการบริหารหรือการควบคุมความเสี่ยงและภัยคุกคามต่างๆ ก่อน ซึ่งพบว่าความเสี่ยงในเหตุการณ์ต่างๆ สามารถเรียงตามความเสี่ยงและประเภทของความเสี่ยงทั้ง 3 ประเภทคือ สิทธิในการเข้าถึงข้อมูล ความเชื่อถือ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความสามารถในการนำมาใช้ประโยชน์ได้เมื่อต้องการ (Availability) จึงได้เสนอแนวทางการควบคุมเฉพาะความเสี่ยงสูงเนื่องจากความเสี่ยงสูงจัดเป็นภัยคุกคามที่องค์กรต้องให้ความสนใจในการดูแลและจัดหาตัวควบคุมที่เหมาะสมเพื่อลดความเสี่ยงของภัยคุกคามดังกล่าว และจากการนำเสนอแนว เพื่อองค์กรตัวอย่างนำไปปรับใช้ให้เหมาะสมนั้น บางกรณีที่บางข้อเสนอองค์กรได้เริ่มดำเนินการไปบ้างแล้ว แต่ผลจากการประเมินของพนักงานที่มีส่วนเกี่ยวข้องยังจัดให้ความเสี่ยงดังกล่าวเป็นความเสี่ยงสูงอยู่นั้นอาจมีสาเหตุจากพนักงานผู้ตอบแบบสอบถามมีการรับรู้ข้อมูลข่าวสารด้านความปลอดภัยที่แตกต่างกัน และพนักงานผู้ตอบแบบสอบถามไม่เข้าใจความหมายของคำถามอย่างลึกซึ้ง องค์กรเลือกตัวควบคุมความเสี่ยงที่ไม่เหมาะสมหรือขาดการดำเนินงานที่จริงจัง เป็นต้น และจากการทดสอบสมมติฐานเพื่อนำไปประยุกต์ใช้ในการสร้างมาตรฐานการรักษาความปลอดภัยตาม ISO 17799 ให้เหมาะสมในแต่ละกลุ่มตัวอย่างจึงต้องมีการทดสอบสมมติฐานขึ้นมา โดยจากการทดสอบสมมติฐาน แล้วพบว่าตัวแปรอิสระที่นำมาใช้ทดสอบสมมติฐานคือ ช่วงอายุการทำงานของพนักงานที่ตอบแบบสอบถาม และหน่วยงานที่เป็น IT กับหน่วยงานที่เป็น Non-IT เทียบกับตัวแปรตามคือ มาตรฐานความมั่นคงปลอดภัยตาม ISO17799 ทั้ง 11 ข้อ พบว่าตัวแปรอิสระที่นำมามีความคิดเห็นที่แตกต่างในแต่ละข้อของมาตรฐาน ISO17799 ผู้บริหารองค์กรสามารถนำไปใช้สำหรับการให้ความสนใจเป็นรายกลุ่มที่มีความคิดเห็นแตกต่างกันออกไปเช่น ความคิดเห็นด้านการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร ถ้ามองตามช่วงอายุการทำงานพบว่ามีความคิดเห็นแตกต่าง แต่ถ้าการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศองค์กรที่ไม่เท่ากัน ซึ่งอาจเกิดจากประสบการณ์หรือระยะเวลาในการทำงานในองค์กรจึงทำให้การรับรู้ในแต่ละช่วงไม่เท่ากัน ดังนั้นองค์กรควรเพิ่มการประชาสัมพันธ์ด้านนโยบาย และให้ข้อมูลที่แตกต่างกันออกไปตามช่วงอายุการทำงานของพนักงานเช่น พนักงานใหม่หรือพึ่งทำงานได้ไม่นานอาจต้องเพิ่มการดูแลเป็นพิเศษในการให้ข้อมูลข่าวสาร การฝึกอบรม หรือการประชาสัมพันธ์เพิ่มเติม เป็นต้น

นริทธ์ จินดาจามร และคณะ (2550) ได้ศึกษาและจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 โดยมีวัตถุ ประสงค์หลักเพื่อกำหนดแนวปฏิบัติที่เป็นรูปธรรมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้กับองค์กรภาครัฐและเอกชนที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ อ้างอิงตามมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005 ประกอบร่างพระราชกฤษฎีกา มาตรา 25 มาตรา 2 มาตรา 35 แห่งพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งเป็นการนำเอามาตรฐานในการรักษาความปลอดภัยสากลISO/IEC17799:2005 และหลักบริหารความเสี่ยงมาใช้เพื่อเป็นแนวทาง ให้กับกฎหมายธุรกรรมอิเล็กทรอนิกส์ ผลของงานวิจัยได้ระบุข้อปฏิบัติให้กับหน่วยงานต่างๆ ซึ่งข้อปฏิบัติที่จำเป็นต้องปฏิบัติอย่างเข้มข้น และข้อปฏิบัติที่ปฏิบัติตามระดับความเสี่ยงด้านสารสนเทศ พบว่าการที่หน่วยงานภาครัฐและภาคเอกชนสามารถปฏิบัติตามกฎหมายฉบับนี้ โดยนำมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005 มาใช้อ้างอิงได้ จึงจำเป็นต้องมีการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานนั้นๆ ก่อน หลังจากนั้นจึงเข้าสู่แบบจำลองที่ได้จัดทำขึ้นในงานวิจัยฉบับนี้ เพื่อกำหนดแนวปฏิบัติที่เป็นรูปธรรมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์

ผกากรอง บ่ายสว่าง และคณะ (2552) ได้ศึกษาและจัดทำแนวทางในการวางระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก โดยอ้างอิง ISO/IEC 27001 และใช้กรณีศึกษาเป็นธุรกิจร้านกาแฟที่ให้บริการเสริมด้านเครือข่ายไร้สาย โดยมีวิธีการวิจัย คือ การศึกษาถึงสภาพปัจจุบันภายในวิสาหกิจขนาดกลางและขนาดเล็ก ที่มีการใช้เครือข่ายเฉพาะบริเวณแบบไร้สาย และได้จัดทำกรอบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กภายใต้กรอบมาตรฐาน ISO/IEC 27001 ในการวิจัยครั้งนี้มีการเก็บข้อมูลโดยการสัมภาษณ์บริษัทที่เป็นวิสาหกิจขนาดเล็ก การศึกษาเอกสารงานวิจัย ระบบมาตรฐาน ISO/IEC 27001 และในการกำหนดกรอบความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กนั้นได้พิจารณา OSI Model กับ Defense Information System Agency for the Department of Defense (DISA for the DOD) และ United States Department of Homeland Security (DHS) ทั้งนี้ เพื่อให้ได้ระบบที่มีความเสถียรในการใช้งานบนระบบเครือข่าย

ภาคภูมิ ปรีชาพานิช (2550) ได้ทำการวิจัยเรื่องการพัฒนาตัวแบบความมั่นคงปลอดภัยของเว็บเซอร์วิส สำหรับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยงานวิจัยได้ศึกษาและพัฒนาตัวแบบความมั่นคงปลอดภัยของระบบเว็บเซอร์วิส สำหรับหน่วยงานในกระทรวง

เทคโนโลยีสารสนเทศและการสื่อสารและทำการประเมินความมั่นคงปลอดภัยของระบบเว็บเซอร์วิสภายในกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยอิงตัวแบบที่ได้พัฒนาขึ้น

จิตสุนันท์ เพชรก้อน (2549) ทัศนคติเกี่ยวกับการนำมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001:2005) มาใช้ในองค์กร กรณีศึกษาอุตสาหกรรมอิเล็คทรอนิคส์ในประเทศไทย ผลการศึกษาพบว่า ส่วนใหญ่ไม่มีความรู้ว่ามาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ได้ประกาศใช้แล้ว การสนับสนุนของผู้บริหารระดับสูงในการนำเทคโนโลยีใหม่ ๆ มาใช้ในองค์กรเป็นปัจจัยสนับสนุนที่สำคัญที่สุด ส่วนกฎหมายและข้อบังคับเป็นปัจจัยสนับสนุนที่สำคัญน้อยที่สุด ด้านปัญหาอุปสรรค ขาดนโยบายจากผู้บริหารเป็นอุปสรรคที่สำคัญที่สุด การขาดฮาร์ดแวร์และซอฟต์แวร์เป็นปัญหาน้อยที่สุด

ทรงชล มหารมณ์ (2548) การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสำหรับองค์กรขนาดใหญ่และขนาดกลางในเขตกรุงเทพมหานคร การศึกษาถึงภัยคุกคามและปัจจัยที่ก่อให้เกิดความเสี่ยงที่เป็นพฤติกรรมและลักษณะการทำงานของบุคคลในองค์กร ในการรักษาความปลอดภัยข้อมูลสารสนเทศขององค์กรขนาดกลางและขนาดใหญ่ โดยการแยกประเภทของความเสี่ยงตามความปลอดภัยของข้อมูลได้แก่ ความเชื่อถือ ความถูกต้องสมบูรณ์ และความสามารถในการนำมาใช้ประโยชน์ได้เมื่อต้องการ ความเสี่ยงที่เป็นไปได้ว่าเกิดขึ้นกับความปลอดภัยของข้อมูล ซึ่งพบว่าภัยคุกคามที่ก่อให้เกิดความเสี่ยงต่อการรักษาความปลอดภัย ข้อมูลที่มีความเสี่ยงในระดับสูง ซึ่งองค์กรขนาดกลางและใหญ่ควรให้ความสนใจและหาแนวทางการแก้ไขมีอยู่ 8 ภัยคุมคามเรียงลำดับตามความเสี่ยงจากสูงไปต่ำดังนี้

1. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล
2. การรวบรวมข้อมูลสำคัญได้ที่เดียวกันหมด
3. การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้
4. การปกป้องรหัสผ่าน (Password) อย่างไม่เหมาะสม
5. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม
6. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม
7. ระบบการรักษาความปลอดภัยข้อมูลและขั้นตอนการให้สิทธิการใช้งาน ไม่มีการเปลี่ยนแปลงให้ทันสมัย และการออกแบบระบบซับซ้อนเกินไป

สุพล วุฒิเสน (2537) ได้ศึกษาวิจัย เรื่อง พันธกิจของการอุดมศึกษาระดับสูงกว่ามัธยมต่อการพัฒนาประเทศ ช่วงของแผนพัฒนา ระยะที่ 8 -9-10 สรุปผลการศึกษาได้ว่า มหาวิทยาลัยจะต้องเชื่อมโยงวิชาการระดับสากลและท้องถิ่นให้สอดประสานรับกันได้ โดยมี “ระบบปฏิบัติ

หรือ Delivery system" 6 ขั้นตอน และทุกขั้นตอนมีความสัมพันธ์เกี่ยวข้องส่งต่อกันเป็นระบบ เรียกว่า "TRENDS model" มีขั้นตอนดังนี้

ขั้นที่ 1 Transmitting of international knowledge – T คือ การถ่ายทอดความรู้สากลแก่นักศึกษาทุกประเภท อันถือเป็นภารกิจพื้นฐานที่อาจารย์ในสถาบันอุดมศึกษากระทำอยู่แล้ว

ขั้นที่ 2 Research / Recovery of data – R คือ การทำวิจัยและการศึกษาข้อมูลท้องถิ่น ซึ่งเป็นความพยายามเข้าใจท้องถิ่นบนฐานของวิชาการสากล

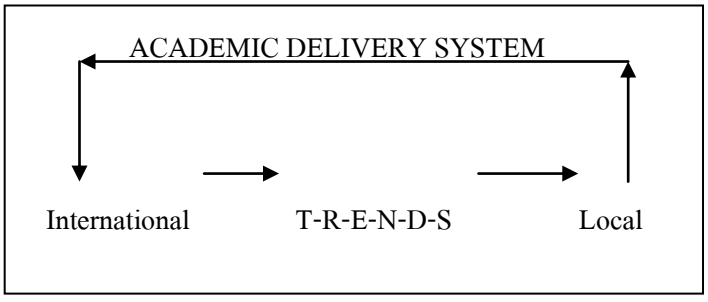
ขั้นที่ 3 Experiment in local situation – E คือ เมื่อได้ข้อมูลหรือความรู้ใหม่จากการสรุปและการวิจัย ต้องมีการทดลอง/ตรวจสอบในท้องถิ่น หรือในสถานการณ์จริงเพื่อให้เกิดความมั่นใจก่อนที่จะนำไปเผยแพร่ต่อไป

ขั้นที่ 4 Newly appropriate knowledge – N คือ การสรุปจาก 3 ขั้นตอนแรกให้เหมาะสมสำหรับการเผยแพร่ในท้องถิ่น สิ่งที่ได้รับจะเป็นความรู้ใหม่ที่เหมาะสมกับท้องถิ่น

ขั้นที่ 5 Distribution of knowledge to development – D คือ ขั้นการเผยแพร่ความรู้ใหม่เพื่อการพัฒนา ซึ่งรวมถึงการเผยแพร่หรือสอนความรู้ใหม่ให้แก่นักศึกษา

ขั้นที่ 6 Service to locality – S คือ ขั้นการนำสิ่งค้นพบสู่การพัฒนาท้องถิ่น โดยปฏิบัติการให้ความรู้ใหม่สนองความต้องการของท้องถิ่น ซึ่งหมายรวมถึงความต้องการของสถาบันอุดมศึกษาในท้องถิ่นด้วย

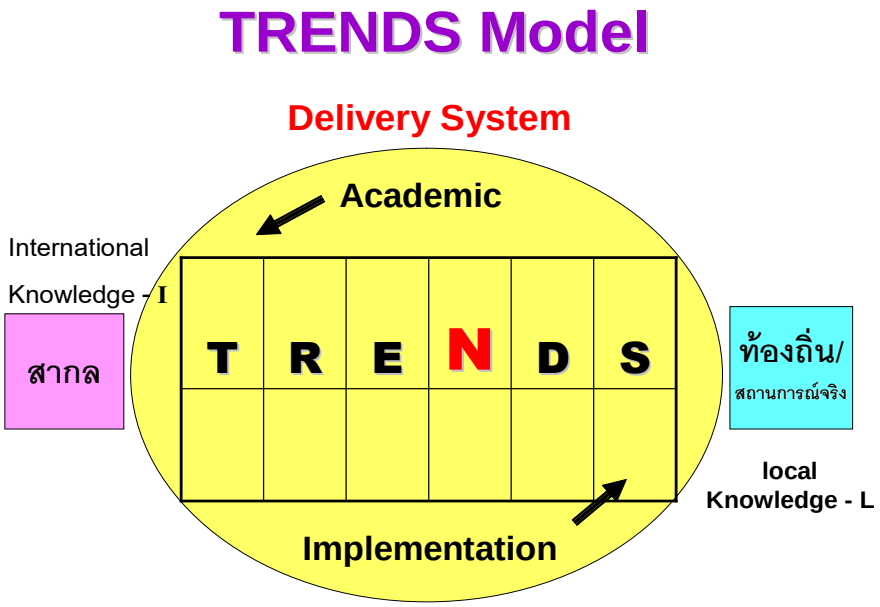
ทั้ง 6 ขั้นตอนมีอาจารย์และนักศึกษา เปรียบเสมือนคนกลางที่ประยุกต์ความรู้สากลให้ไปสู่ท้องถิ่น และเป็นผู้ผลิตองค์ความรู้ใหม่ให้กับสากลผ่านการวิจัยในท้องถิ่นซึ่งเดิมมีรูปแบบดังนี้



ภาพที่ 3 แสดง TRENDS model ในระยะเริ่มต้น

หากปฏิบัติตาม TRENDS model ความรู้ใหม่จากท้องถิ่น (Local knowledge) จะนำไปสู่การพัฒนาความรู้สากล (International knowledge)ในขณะเดียวกันความรู้สากลจะนำไปสู่การพัฒนาความรู้ท้องถิ่นหมุนเวียนเป็นวัฏจักรซึ่งเป็น "ยุทธศาสตร์สถานการณ์" รายงานวิจัยที่

กล่าวมานี้ ยังคงความทันสมัยเพราะ TRENDS model นี้เป็น Dynamic system ซึ่งเป็นรูปแบบที่สามารถมีการเปลี่ยนแปลงได้ตามสภาวะแวดล้อม สามารถยืดหยุ่นและปรับตัวให้เข้ากับสถานการณ์ต่าง ๆได้ และยังเป็น Delivery system คือ สามารถส่งผ่านความรู้สากลสู่ท้องถิ่น ท้องถิ่นสามารถนำไปปรับใช้ ในขณะเดียวกันความรู้ที่เกิดใหม่จากการปรับใช้ในท้องถิ่น สามารถนำความรู้ท้องถิ่นที่ได้นั้นออกสู่สากล วนเวียนได้ไม่รู้จบ



ภาพที่ 4 TRENDS Model

ภาพด้านบนแสดงให้เห็นรูปแบบของ TRENDS Model ในยุคปัจจุบันซึ่งมหาวิทยาลัยราช-ภัฏ บ้านสมเด็จเจ้าพระยา ได้นำไปใช้เป็นหลัก ในการบริหารจัดการศึกษาสามารถอธิบายได้ดังต่อไปนี้

ผลผลิต (Product) ที่ต้องการได้รับ คือ นักศึกษาที่สำเร็จแล้ว ไม่ว่าระดับใด ต้องมีอัตลักษณ์ของมหาวิทยาลัยราชภัฏ บ้านสมเด็จเจ้าพระยา มีความสามารถเฉพาะทาง ตามสาขาที่เรียนมา มีความรู้/ความสามารถพื้นฐานที่เหมือนกัน มีคุณธรรมและจริยธรรมประจำตน ต้องสามารถนำความรู้ความสามารถไปประกอบอาชีพ หรือนำไปปฏิบัติได้ โดยต้องคำนึงถึงการสร้างคุณประโยชน์ต่อสังคมด้วย

กระบวนการบริหารจัดการศึกษา (Processes) ประกอบด้วย

ความรู้สากล International knowledge ที่ได้จากการร่วมจัดการศึกษา การร่วมศึกษา/วิจัย การบูรณการ/เรียนรู้ ระหว่าง มหาวิทยาลัยนานาชาติ เช่น มหาวิทยาลัยในประเทศออสเตรเลีย

ประเทศนิวซีแลนด์ และสาธารณประชาชนลาว ฯลฯ มหาวิทยาลัยต่าง ๆ ในประเทศ สถาบันวิจัยทั้งในประเทศและต่างประเทศ และแหล่งเรียนรู้ต่าง ๆ เชื่อมโยงกับกระบวนการ TRENDS model (Transmitting of international knowledge – T , Research/ Recovery of data – R, Experiment in local situation – E, Newly appropriate knowledge – N และDistribution of knowledge to development – D) โดยใช้การศึกษาผ่านสถาบัน (Academic)

การนำไปปฏิบัติ (Implementation) โดยการผ่านการฝึกอบรมจากการฝึกงาน เหมือนสายอาชีวะที่ต้องผ่านการฝึกอาชีพ (Vocational) โดยเชื่อมโยงไปมาระหว่าง TRENDS model กับสหกิจศึกษา เรียนรู้/ร่วมสอน ร่วมประกอบการ ถ่ายทอดความรู้สู่ท้องถิ่น Local knowledge โดยเป็นผู้ประกอบการ หรือถ่ายทอดให้หน่วยงาน ชุมชน และโรงงาน

ในทางกลับกัน ก็สามารถเริ่มจากความรู้ท้องถิ่น (Local knowledge) ผ่านกระบวนการ TRENDS model ไปสู่ความรู้สากล (International knowledge) ซึ่งอาศัยมหาวิทยาลัย (Academic) คือ อาจารย์และนักศึกษาเป็นตัวกลาง และ การฝึกอาชีพหรือการนำไปปฏิบัติทำให้เกิดเป็น Delivery system และเป็น Dynamic system

สรุป การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา โดยนำความรู้มาตรฐานความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสากล ISO27001 แนวคิดการประเมิน สภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา มาศึกษาเพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อให้มีความเหมาะสมกับสถาบันการศึกษาของประเทศไทย

บทที่ 3

วิธีดำเนินการวิจัย

ในการศึกษาวิจัยเรื่อง การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา มีการดำเนินตามขั้นตอน ดังนี้

1. กลุ่มตัวอย่าง
2. เครื่องมือที่ใช้ในการวิจัย
3. การเก็บรวบรวมข้อมูล
4. สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิจัยครั้งนี้ เป็นการดำเนินการวิจัยที่มีรูปแบบเป็นการวิจัยและพัฒนา (The Research and Development) โดยมีขั้นตอนการวิจัยดังนี้

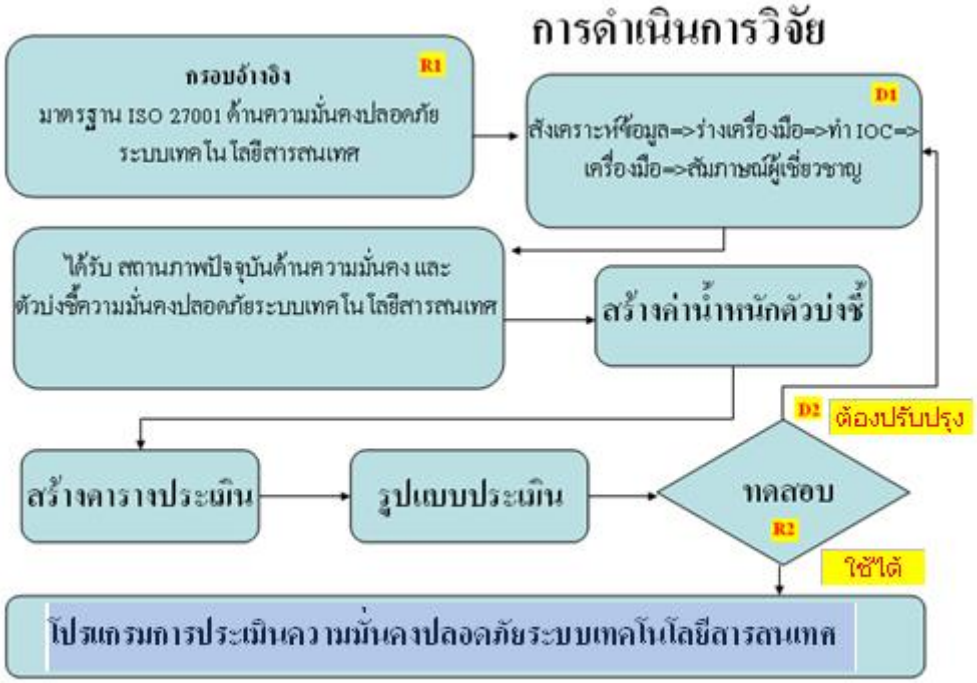
1. ขั้นตอนการวิจัย 1 (R1) ดำเนินการโดยการศึกษาข้อมูลพื้นฐาน สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จากเอกสารและการสัมภาษณ์ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2. ขั้นตอนพัฒนา 1 (D1) ดำเนินการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา โดยการศึกษามาตรฐานความมั่นคงปลอดภัยสากล ISO 27001 นำมาสังเคราะห์ข้อมูล ได้ร่างเครื่องมือวิจัยเป็นแบบสัมภาษณ์ นำแบบสัมภาษณ์เสนอผู้เชี่ยวชาญจำนวน 5 คน ซึ่งเป็นผู้ที่มีความเชี่ยวชาญและรับผิดชอบด้านการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบ ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of Item – Objective Congruence: IOC) โดยกำหนดค่าของความสอดคล้องตั้งแต่ 0.50 ขึ้นไปเป็นเกณฑ์ที่ยอมรับได้ ได้เครื่องมือ นำไปสัมภาษณ์ผู้เชี่ยวชาญด้านบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จำนวน 6 คน ได้ สภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา และได้ตัวบ่งชี้ความมั่นคง

ปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา แล้วสร้างค่าน้ำหนักตัวบ่งชี้ สร้างตารางประเมิน ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา นำไปทดสอบการใช้งาน และเปรียบเทียบกับการประเมินแบบมาตราสากล ทำการปรับปรุงหากได้ผลการประเมินออกมาไม่สอดคล้องกับวิธีประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

3. ขั้นตอนการวิจัย 2 (R2) ดำเนินการทดลอบการใช้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้น โดยการ นำไปทดสอบการใช้งาน และเปรียบเทียบกับการประเมินแบบมาตรฐานสากล

4. ขั้นตอนการพัฒนา 2 (D2) ดำเนินการปรับปรุงรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้น โดยการ ทำการปรับปรุงให้สอดคล้องกับวิธีประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล และพัฒนาโปรแกรมสำเร็จรูปเพื่อประเมินพร้อมคู่มือในการใช้งาน ให้ง่ายและสะดวกรวดเร็วในการใช้ประเมิน ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ผู้วิจัยได้ออกแบบกรอบการวิจัยดังนี้



ภาพที่ 5 กรอบการวิจัย

ภาพด้านบนแสดงถึงกรอบการวิจัย โดยมีการวิจัย R1 การศึกษามาตรฐานความมั่นคงปลอดภัยสากล ISO 27001 การพัฒนา D1 นำมาสังเคราะห์ข้อมูล ได้ร่างเครื่องมือวิจัยเป็นแบบสัมภาษณ์ นำแบบสัมภาษณ์เสนอผู้เชี่ยวชาญที่มีความเชี่ยวชาญด้านการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบ ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of Item – Objective Congruence: IOC) ได้เครื่องมือ นำไปสัมภาษณ์ผู้เชี่ยวชาญด้านบริหารและผู้ดูแลระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้สภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา และได้ตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา สร้างค่าน้ำหนักตัวบ่งชี้ สร้างตารางประเมิน ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา การวิจัย R2 นำไปทดสอบการใช้งาน และเปรียบเทียบกับการประเมินแบบมาตรฐานสากล การพัฒนา D2 ทำการปรับปรุงหากได้ผลการประเมินออกมาไม่สอดคล้องกับวิธีประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล และพัฒนาโปรแกรมสำเร็จรูปเพื่อประเมินพร้อมคู่มือในการใช้งาน ให้ง่ายและสะดวกรวดเร็วในการใช้ประเมิน จึงได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

กลุ่มตัวอย่าง

กลุ่มตัวอย่าง

การวิจัยนี้เป็นการวิจัยและพัฒนา กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ ประกอบด้วยผู้เชี่ยวชาญความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏ เป็นผู้ที่มีประสบการณ์ตรง เป็นผู้ดำรงตำแหน่งในการจัดการด้านความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศในมหาวิทยาลัยราชภัฏในเขตกรุงเทพมหานครจำนวน 3 แห่ง คือ มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มหาวิทยาลัยราชภัฏสวนสุนันทา รวม 6 คน โดยแบ่งเป็น 2 กลุ่ม ประกอบด้วย

1. กลุ่มผู้วางนโยบายบริหารระบบเทคโนโลยีของมหาวิทยาลัยราชภัฏ จำนวน 3 แห่ง รวม 3 คน
2. กลุ่มผู้ดูแลด้านเทคนิคระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จำนวน 3 แห่ง รวม 3 คน

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย คือ แบบสัมภาษณ์

1. ขั้นตอนการพัฒนาเครื่องมือที่ใช้ในการวิจัย (D1)

การพัฒนาแบบสัมภาษณ์

1.1 ศึกษาข้อมูลทุติยภูมิจากเอกสาร โดยใช้วิธีการวิจัยเอกสาร (Document research) ได้แก่ รายละเอียดมาตรฐานการดำเนินงานการรักษาความมั่นคงปลอดภัยสารสนเทศต่างๆ พระราชบัญญัติ และกฎ ระเบียบที่เกี่ยวข้อง งานวิจัยต่าง ๆ ซึ่งประกอบด้วย แนวคิด ทฤษฎีที่เกี่ยวข้องกับสถานการณ์ปัจจุบันในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ บริบทของมหาวิทยาลัยราชภัฏ โดยให้ครอบคลุมเนื้อหาตามวัตถุประสงค์

1.2 พัฒนาแบบสัมภาษณ์มี 2 ชุด

ชุดที่ 1 สำหรับผู้วางนโยบายด้านบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา โดยกำหนดประเด็นในการสัมภาษณ์ โดยใช้คำถามปลายเปิด (Open–ended question) และตั้งคำถามในแบบสัมภาษณ์กึ่งมีโครงพัฒนา (Semi-structure interview) แบ่งออกเป็น 2 ตอน มีรายละเอียดดังนี้

ตอนที่ 1 มีวัตถุประสงค์เพื่อศึกษาสถานภาพ ปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา ผู้วิจัยได้พัฒนาแบบสัมภาษณ์ข้อมูลทั่วไปของผู้เชี่ยวชาญ ได้แก่ เพศ ประสบการณ์ทำงาน สังกัด ตำแหน่ง ความเห็นด้านความสำคัญและการมีของ นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ การจัดการด้านงบประมาณสำหรับความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ การบริหารจัดการด้านนโยบายสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ การบริหารจัดการด้านบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พฤติกรรมผู้ใช้งานเกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ว่ามีสถานภาพปัจจุบันอย่างไร

ตอนที่ 2 เป็นแบบสอบถามเกี่ยวกับความคิดเห็นในประเด็นตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เชิงการวางแผน ปฏิบัติ ติดตามตรวจสอบและประเมินผล โดยใช้แบบสัมภาษณ์แบบมาตราส่วนประมาณค่าของลิเคิร์ท (Rating Scale) โดยแบ่งเป็น 5 ระดับ ดังนี้

5 หมายถึง ระดับความสำคัญมากที่สุด

4 หมายถึง ระดับความสำคัญมาก

3 หมายถึง ระดับความสำคัญปานกลาง

2 หมายถึง ระดับความสำคัญน้อย

1 หมายถึง ระดับความสำคัญน้อยที่สุด

ชุดที่ 2 สำหรับผู้ดูแลด้านเทคนิคความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา โดยกำหนดประเด็นในการสัมภาษณ์ โดยใช้คำถามปลายเปิด (Open–ended

question) และตั้งคำถามในแบบสัมภาษณ์กึ่งมีโครงพัฒนา (Semi-structure interview) แบ่งออกเป็น 2 ตอน มีรายละเอียดดังนี้

ตอนที่ 1 สัมภาษณ์ข้อมูลทั่วไปของผู้เชี่ยวชาญ ได้แก่ เพศ ประสบการณ์ทำงาน สังกัด ลักษณะแบบสัมภาษณ์เป็นแบบตรวจสอบรายการ (Check list) จำนวน 13 ข้อ

ตอนที่ 2 เป็นแบบสอบถามเกี่ยวกับความคิดเห็นในประเด็นตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเชิงเทคนิคและการจัดการ โดยใช้แบบสัมภาษณ์แบบมาตราส่วนประมาณค่าของลิเคิร์ท (Rating Scale) โดยแบ่งเป็น 5 ระดับ ดังนี้

5 หมายถึง ระดับความสำคัญมากที่สุด

4 หมายถึง ระดับความสำคัญมาก

3 หมายถึง ระดับความสำคัญปานกลาง

2 หมายถึง ระดับความสำคัญน้อย

1 หมายถึง ระดับความสำคัญน้อยที่สุด

ผู้วิจัยได้ดำเนินการพัฒนาเครื่องมือที่ใช้ในการวิจัย ตามลำดับขั้นตอน ดังนี้

1. ศึกษาแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องในเรื่องรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการพัฒนาแบบสัมภาษณ์

2. รวบรวมเนื้อหาสาระต่าง ๆ ที่ได้จากการศึกษาค้นคว้าและงานวิจัยที่เกี่ยวข้องเพื่อนิยามศัพท์ตัวแปร กำหนดขอบเขตและการพัฒนาแบบสัมภาษณ์

3. กำหนดกรอบแนวคิดในการพัฒนาแบบสัมภาษณ์เพื่อทราบสถานภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา และเพื่อทราบว่าผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีความเห็นเกี่ยวกับรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา อย่างไร โดยการวิเคราะห์และปรับให้มีความสอดคล้องกับเกณฑ์การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสากล

4. ศึกษาการพัฒนาแบบสัมภาษณ์ แบบสัมภาษณ์แบบมาตราส่วนประมาณค่า ของลิเคิร์ท (Rating Scale) โดยแบ่งเป็น 5 ระดับ ดังนี้

5 หมายถึง ระดับความสำคัญมากที่สุด

4 หมายถึง ระดับความสำคัญมาก

3 หมายถึง ระดับความสำคัญปานกลาง

2 หมายถึง ระดับความสำคัญน้อย

1 หมายถึง ระดับความสำคัญน้อยที่สุด

5. พัฒนาข้อคำถามเพื่อวัดปัจจัยที่เกี่ยวข้องกับการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

6. นำแบบสัมภาษณ์ปรึกษาที่ปรึกษางานวิจัย แล้วนำกลับมาปรับปรุงแก้ไข

7. เพื่อให้แบบสัมภาษณ์ที่พัฒนาขึ้น ได้รับการตรวจสอบแล้วมีความชัดเจนและสอดคล้องกับหัวข้อการวิจัย ผู้วิจัยจึงดำเนินการเพิ่มเติมตามขั้นตอนดังนี้

(1) นำแบบสัมภาษณ์เสนอผู้เชี่ยวชาญ ซึ่งเป็นผู้ที่มีความเชี่ยวชาญและรับผิดชอบด้านนโยบายการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบ ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of Item – Objective Congruence: IOC) โดยกำหนดค่าของความสอดคล้องตั้งแต่ 0.50 ขึ้นไปเป็นเกณฑ์ ที่ยอมรับได้ โดยกำหนดคะแนนของการประเมินดังนี้

+1 หมายถึง แน่ใจว่าข้อคำถามมีความสอดคล้องกับวัตถุประสงค์

0 หมายถึง ไม่แน่ใจว่าข้อคำถามมีความสอดคล้องกับวัตถุประสงค์

- 1 หมายถึง แน่ใจว่าข้อคำถามไม่มีความสอดคล้องกับวัตถุประสงค์

$$\text{สูตร} \quad IOC = \frac{\sum R}{N}$$

IOC แทน ดัชนีความสอดคล้องระหว่างข้อคำถามกับลักษณะที่ต้องการวัด

$\sum R$ แทน ผลรวมของคะแนนผู้เชี่ยวชาญ

N แทน จำนวนผู้เชี่ยวชาญ

ได้ผลค่าความสอดคล้อง มากกว่า 0.5 ทุกข้อ เป็นเกณฑ์ที่ยอมรับได้ (ภาคผนวก แสดงค่าดรรชนีความสอดคล้อง)

(2) นำแบบสัมภาษณ์เสนอที่ปรึกษา และผู้เชี่ยวชาญทั้ง3 คนอีกครั้ง เพื่อตรวจสอบสำนวนภาษา ปรับปรุงการใช้ภาษาให้เหมาะสม เพื่อให้ได้ข้อคำถามที่มีความถูกต้องครอบคลุมครบถ้วน ดังแสดงใน ภาคผนวกตัวอย่างแบบสัมภาษณ์

ผู้วิจัยนำแบบสัมภาษณ์ เดินทางไปสัมภาษณ์และสอบถามผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้านบริหารและรับผิดชอบด้านนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของแต่ละมหาวิทยาลัยราชภัฏ จำนวน 3 แห่ง จำนวน 3 คน และผู้เชี่ยวชาญด้านเทคนิคความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏ 3 แห่ง จำนวน 3 คน

2. ลักษณะเครื่องมือที่ใช้ในการวิจัยเรื่องรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา มีดังต่อไปนี้

ลักษณะของแบบสัมภาษณ์เป็นแบบสัมภาษณ์เชิงลึก (In-depth interview) โดยกำหนดคำถามและรูปแบบสัมภาษณ์ จากการศึกษาขั้นตอนการสัมภาษณ์แบบเชิงลึก ผู้วิจัยดำเนินการตามขั้นตอน ดังต่อไปนี้ 1) มีหนังสือเรียนนัดหมายล่วงหน้า โดยผู้วิจัยดำเนินการสัมภาษณ์ด้วยตนเอง 2) กำหนดขอบเขตและประเด็นคำถามโดยยึดตามวัตถุประสงค์ ตรวจสอบความพร้อมของอุปกรณ์ที่จะใช้ในการสัมภาษณ์ พร้อมทั้งยืนยันวันเวลา สถานที่ ก่อนการสัมภาษณ์ 3) เข้าสู่สถานที่นัดหมาย แนะนำตนเอง เพื่อพัฒนาความสัมพันธ์ที่ดีก่อนเริ่มต้นสัมภาษณ์ 4) ชี้แจงจุดมุ่งหมาย การเก็บรักษาความลับ 5) เริ่มต้นการสัมภาษณ์และเชิงลึกในช่วงเดิมที่ต้องการทราบข้อมูล ในรายละเอียดจากคำถามแรกไปถึงคำถามสุดท้าย โดยจะให้บรรยากาศที่ผ่อนคลาย ให้เป็นไปตามธรรมชาติของการสนทนาเพื่อแลกเปลี่ยนความรู้ความคิดเห็น ในประเด็นที่สัมภาษณ์ 6) ปิดการสนทนา โดยสรุปความเห็นและถามประเด็นที่อยากจะทราบเพิ่มเติม เพื่อให้ผู้ตอบได้แสดง ความคิดเห็นเป็นคำถามด้วยการสัมภาษณ์ 7) การสิ้นสุดการสัมภาษณ์ โดยกล่าวขอบคุณในคุณค่าของข้อมูลที่ได้รับจากการสัมภาษณ์และการเสียสละเวลาอันมีค่าเพื่อผลการศึกษาที่จะเกิดความสมบูรณ์มากที่สุด

3. การพัฒนาต้นแบบรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา มีขั้นตอน ดังต่อไปนี้

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ได้จากการศึกษาเอกสาร ข้อกำหนด พระราชบัญญัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศรวมถึงศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูล ซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยสถาบันนานาชาติ ISO (International Organization for Standardization) และ IEC (International Electro-technical Commission) การประยุกต์ใช้ ISMS ผู้วิจัยได้ศึกษาและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ร่วมพิจารณาถึงตัวบ่งชี้ที่ส่งผลต่อความไม่มั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษาเพื่อช่วยให้กิจกรรมของมหาวิทยาลัยดำเนินไปอย่างต่อเนื่อง ช่วยป้องกันกระบวนจากภัยคุกคามต่าง ๆ โดยอ้างอิงให้สอดคล้องกับมาตรฐานเกี่ยวกับการบริหารการรักษาความปลอดภัยข้อมูล เป็นแนวทางในการพัฒนา ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยข้อมูลโดยใช้รูปแบบการบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการพัฒนาระบบการรักษาความปลอดภัย เป็นพื้นฐานเพื่อที่จะพัฒนาระบบควบคุมให้การบริหารมหาวิทยาลัยราชภัฏบรรลุภารกิจในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และเพื่อให้แน่ใจว่าระบบนั้นควรได้รับการปรับปรุงเมื่อถึงเวลา โดยมีระบบการจัดการความปลอดภัยของข้อมูล 3 ด้าน ประกอบด้วย ความลับ (Confidentiality) เพื่อให้แน่ใจว่าข้อมูลต่าง ๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิเท่านั้น ความถูกต้อง (Integrity) เพื่อปกป้องให้ข้อมูลมีความถูกต้องและความสมบูรณ์ และ

แก้ไขได้เฉพาะผู้มีสิทธิ์เท่านั้น ความพร้อมใช้งาน (Availability) เพื่อแน่ใจว่าผู้ที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้เมื่อมีความต้องการรูปแบบการประเมินนี้ พัฒนาขึ้นให้สอดคล้องกับกระบวนการ การวางแผน การลงมือทำ การปฏิบัติการ การเฝ้าระวัง การทบทวน การดูแลรักษาและการปรับปรุงระบบเทคโนโลยีสารสนเทศ

หลักการของการออกแบบ รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในส่วนโครงพัฒนารูปแบบฯ อ้างอิงรูปแบบ PDCA ซึ่งเป็นหลักการบริหารเดียวกับมาตรฐานสากล

การออกแบบจะพัฒนาขึ้นลำดับกระบวนการ เริ่มจากการ การวางแผนจัดทำ ดำเนินการ (Plan) โดยการเริ่มประเมินตรวจสอบ การมีและการนำไปปฏิบัติ ในด้านการวางแผนประกอบด้วยการกำหนดขอบเขตการจัดทำ กำหนดนโยบาย กำหนดรูปแบบและวิธีการประเมินความเสี่ยง ระบุความเสี่ยง วิเคราะห์และประเมินความเสี่ยง วิเคราะห์และประเมินหนทางในการลดความเสี่ยง กำหนดวัตถุประสงค์และมาตรการในการควบคุมเพื่อลดความเสี่ยง ขออนุมัติผู้บริหารเกี่ยวกับความเสี่ยงที่ไม่มีมาตรการเพื่อควบคุม ขออนุมัติผู้บริหารเกี่ยวกับการทำระบบ จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้

ต่อจากนั้น ตรวจสอบและประเมินในการดำเนินการ (Do) ว่ามหาวิทยาลัยราชภัฏ มีการดำเนินการตามแผนหรือไม่ อย่างไร โดยการกำหนดให้มีและปฏิบัติแผนการกำจัดความเสี่ยง ซึ่งประกอบด้วยแนวทางในการปฏิบัติสำหรับผู้บริหาร ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม ฝึกอบรมและกระตุ้นให้ตระหนักเกี่ยวกับการรักษาความปลอดภัย บริหารการปฏิบัติการ บริหารทรัพยากร กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

ตรวจประเมินว่า มีการจัดตั้งคณะกรรมด้านความมั่นคงปลอดภัย ทำการตรวจเช็ค (Check) ว่ามีการดำเนินการโดยเฝ้าระวังและตรวจสอบ ดำเนินการโดยการเฝ้าระวังและตรวจจับข้อผิดพลาดต่าง ๆ และประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ ตรวจพิจารณาว่าระบบมีประสิทธิภาพเพียงพอหรือไม่ มีการประเมินเป็นประจำว่า ความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ ตรวจสอบภายในระบบ ตรวจสอบและประเมินว่าระบบทำงานตามขอบเขตที่กำหนดหรือไม่ ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดต่าง ๆ ที่ตรวจพบ บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของระบบ

ตรวจสอบประเมินว่า สถาบันการศึกษา มีการรักษาและปรับปรุง (Act) มีการเพิ่มเติมเพื่อปรับปรุงระบบ แก้ไขปัญหาที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นอีก การสื่อสารให้ผู้เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงระบบ ทำให้แน่ใจว่า การปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้หรือไม่

มีการกำหนดเกี่ยวกับการจัดทำเอกสารเพื่อจะชี้ให้เห็นชัดว่านโยบายที่กำหนดนั้นจะนำไปปฏิบัติจริง โดยเอกสารที่ต้องจัดทำ เช่น แถลงการณ์เกี่ยวกับวัตถุประสงค์และนโยบายของระบบของเขตการทำงานของระบบ ข้ออธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง รายงานเกี่ยวกับการประเมินความเสี่ยง การกำหนดแผนเพื่อลดความเสี่ยง การกำหนดแนวทางการปฏิบัติสำหรับองค์กรเพื่อให้สามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ และกำหนดแนวทางในการวัดประสิทธิภาพของมาตรการควบคุมต่าง ๆ การเก็บรักษาเอกสารต่าง ๆ ที่ทำตามมาตรฐานนี้หรือไม่ มีการแถลงการณ์ของการประยุกต์ใช้งานหรือไม่ รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้น มีวัตถุประสงค์เพื่อช่วยให้สถาบันการศึกษา สามารถพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ ทั้งนี้รูปแบบการประเมินนี้สามารถนำมาใช้กับทุก ๆ ประเภทของหน่วยงานอื่น ๆ ของสถาบันการศึกษาที่เกี่ยวข้องกับความมั่นคงปลอดภัย

การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จากการค้นคว้าเอกสาร ที่เกี่ยวข้องกับการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และแนวปฏิบัติในการประเมิน ควรจัดกลุ่มด้านของตัวบ่งชี้และพิจารณาดำเนินการบริหารจัดการเป็นกลุ่ม ๆ ผู้วิจัยจึงนำข้อมูลความคิดเห็นลำดับความสำคัญจากผู้เชี่ยวชาญ 2 กลุ่ม คือ ความคิดเห็นของผู้เชี่ยวชาญด้านบริหารและผู้ดูแลระบบเทคโนโลยีสารสนเทศมาจัดให้อยู่ในหมวดหมู่เดียวกัน จัดลำดับเพื่อให้ทราบลำดับความสำคัญ ตัวบ่งชี้ใดมีลำดับความสำคัญมากสุด ผู้บริหารมหาวิทยาลัย จะได้ทราบว่าต้องจัดลำดับการดำเนินการบริหารจัดการอย่างไร ทำให้การบริหารจัดการความมั่นคงปลอดภัยได้ถูกต้องและมีประสิทธิภาพยิ่งขึ้น ต่อจากนั้นนำข้อมูลมาพิจารณาหาลำดับความสำคัญของตัวบ่งชี้ในแต่ละด้าน โดยการพัฒนาค่าน้ำหนัก

การพัฒนาค่าน้ำหนัก

วัตถุประสงค์ : เพื่อจัดลำดับความสำคัญมีผลต่อผู้บริหารจะได้ทราบว่าตัวบ่งชี้มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศมากที่สุด สามารถลำดับการบริหารจัดการ การใช้ทรัพยากรงบประมาณ เวลาได้อย่างถูกต้องยิ่งขึ้น

วิธีการ 1 กำหนดคะแนน ในช่องความสำคัญ ดังนี้

ค่าความสำคัญมากที่สุด = 5 คะแนน

ค่าความสำคัญมาก = 4 คะแนน

ค่าความสำคัญปานกลาง = 3 คะแนน

ค่าความสำคัญน้อย = 2 คะแนน

ค่าความสำคัญน้อยที่สุด = 1 คะแนน

2. ความเห็นของผู้เชี่ยวชาญ 1 คน ต่อ 1 ตัวบ่งชี้ = 1

3. หาผลรวมของคะแนนแต่ละตัวบ่งชี้ โดยสูตร

คะแนนของแต่ละตัวบ่งชี้

= ผลรวมของ จำนวนความเห็นรวมของผู้เชี่ยวชาญ x คะแนนในช่องความสำคัญ

= (จำนวน*5)+(จำนวน*4)+(จำนวน*3)+(จำนวน*2)+(จำนวน*1)

- *จำนวน=จำนวนความคิดเห็นของผู้เชี่ยวชาญในระดับนั้น*

4. นำผลรวมของแต่ละตัวบ่งชี้ในแต่ละด้านมารวมกัน เป็นคะแนนรวม

5. หาค่าน้ำหนัก ของแต่ละตัวบ่งชี้

มีวิธีการ ดังนี้

1. ปรับฐานคะแนนรวม ให้ เท่ากับ 5 เพื่อให้สอดคล้องการ เกณฑ์การประเมิน

2. นำคะแนนของแต่ละตัวบ่งชี้ x 5/ผลรวมของคะแนนแต่ละตัวบ่งชี้ในแต่ละด้าน

ตัวอย่าง ด้านบ่งชี้ที่ 1 มี 9 ตัวบ่งชี้

ผลรวมของคะแนน ทั้ง 9 ตัวบ่งชี้ = 246 คะแนน

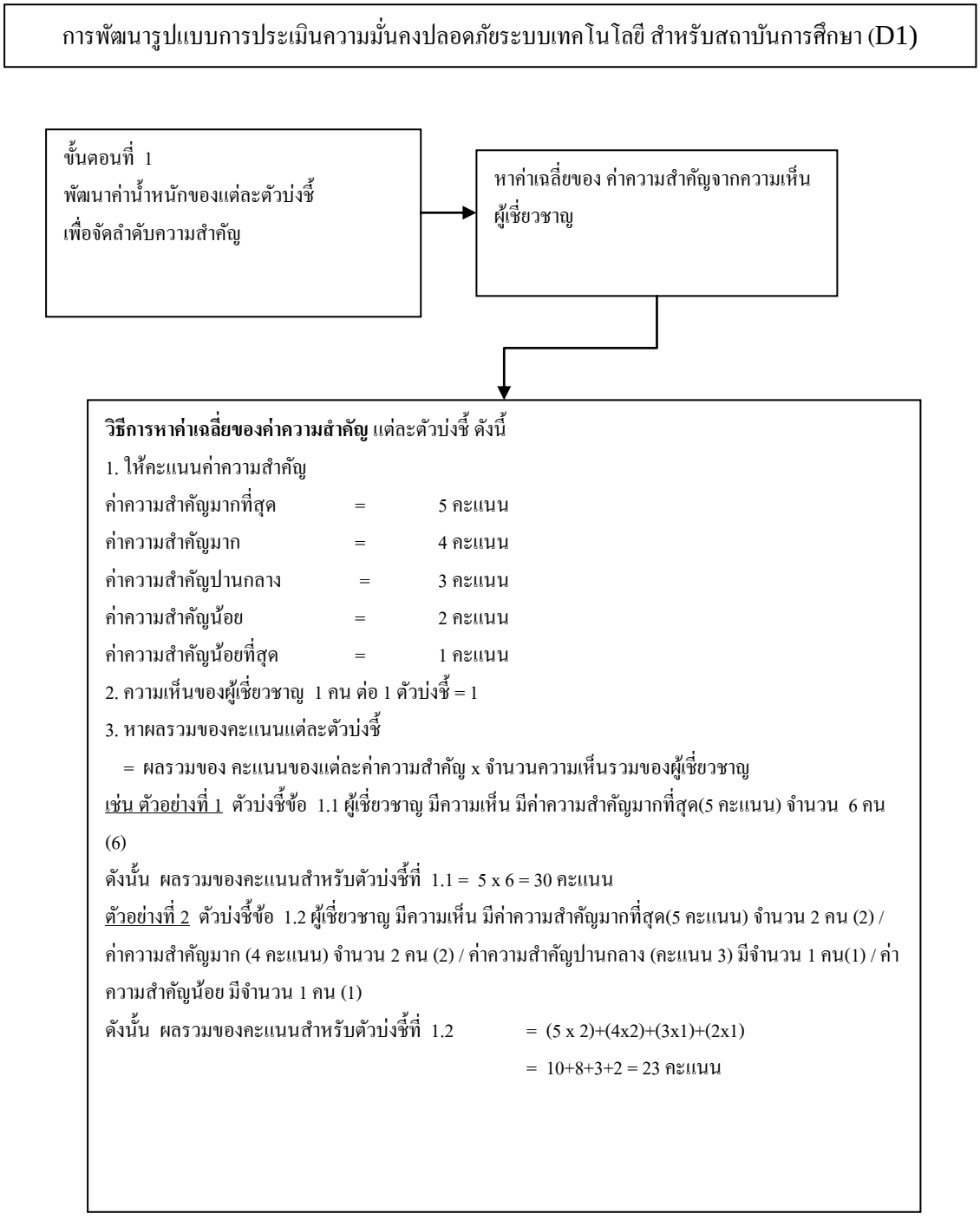
ตัวบ่งชี้ที่ 1.1 มีคะแนน = a คะแนน จะได้ ค่าน้ำหนัก = (a x 5)/ (sum (9))

ตัวบ่งชี้ที่ 1.2 มีคะแนน = b คะแนน จะได้ ค่าน้ำหนัก = (b x 5)/ (sum (9))

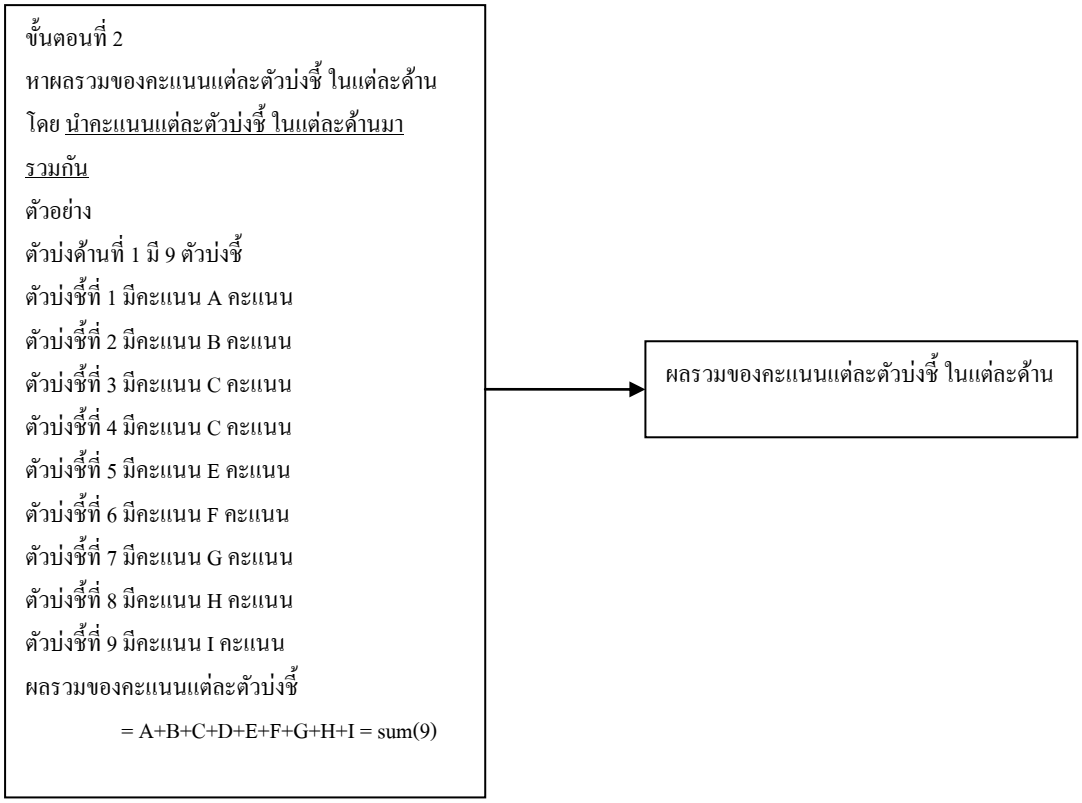
ตัวบ่งชี้ ลำดับต่อ ๆ ไป ใช้การคำนวณด้วยวิธีเดียวกัน

ผลรวมของค่าน้ำหนักรวมในแต่ละด้าน = 5.00

ขั้นตอนสรุปตามภาพและตัวอย่าง



ภาพที่ 6 การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา (D1)



ขั้นตอนที่ 3 หาค่าน้ำหนัก ของแต่ละตัวบ่งชี้

มีวิธีการ ดังนี้

1. ปรับฐานคะแนนรวม ให้ เท่ากับ 5 เพื่อให้สอดคล้องการ เกณฑ์การประเมิน

2. นำคะแนนของแต่ละตัวบ่งชี้ x 5/ผลรวมของคะแนนแต่ละตัวบ่งชี้ในแต่ละด้าน

ตัวอย่าง ด้านบ่งชี้ที่ 1 มี 9 ตัวบ่งชี้

ผลรวมของคะแนน ทั้ง 9 ตัวบ่งชี้ = 246 คะแนน

ตัวบ่งชี้ที่ 1.1 มีคะแนน = a คะแนน จะได้ ค่าน้ำหนัก = (a x 5)/(sum(9))

ตัวบ่งชี้ที่ 1.2 มีคะแนน = b คะแนน **จะได้ ค่าน้ำหนัก = (b x 5)/(sum(9))**

ตัวบ่งชี้ ลำดับต่อ ๆ ไป ใช้**การคำนวณด้วยวิธีเดียวกัน**

ผลรวมของค่าน้ำหนักรวมในแต่ละด้าน = 5.00

ภาพที่ 6 (ต่อ) การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา (D1)

ตารางที่ 1 ตัวอย่าง หาค่าน้ำหนัก สำหรับตัวบ่งชี้ ด้านที่ 1

รายการ	ค่าความสำคัญ					ค่าน้ำหนัก					รวม	ค่าน้ำหนักค่าบ่งชี้ (5 คะแนน)
ตัวบ่งชี้ด้านที่ 1	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1	5	4	3	2	1		
1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร	111111 (6)					6*5=30					30	30*5/246=**0.61**
1.2 การจัดการนโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศได้รับอนุมัติจากคณะกรรมการบริหาร	11111 (5)	1 (1)				5*5=25	1*4=4				25+4=29	29*5/246=**0.59**
1.3 ประกาศใช้และสื่อสารนโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศแก่พนักงานทุกระดับในองค์กรได้ทราบอย่างทั่วถึงและผ่านช่องทางที่หลากหลาย	11111 (5)	1 (1)				5*5=25	1*4=4				25+4=29	29*5/246=**0.59**

ตารางที่ 1 (ต่อ) ตัวอย่าง หาค่าน้ำหนัก สำหรับตัวบ่งชี้ ด้านที่ 1

รายการ	ค่าความสำคัญ					ค่าน้ำหนัก					รวม	ค่าน้ำหนักค่าบ่งชี้ (5 คะแนน)
ตัวบ่งชี้ด้านที่ 1	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1	5	4	3	2	1		
1.4 การประเมินความรู้ความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศในองค์กร	1111 (4)	11 (2)				4*5=20	2*4=8				20+8=28	28*5/246=**0.57**
1.5 นโยบายสื่อสารหรือให้ความรู้เกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศแก่ผู้ใต้บังคับบัญชา	111 (3)	111 (3)				3*5=15	3*4=12				15+12=27	27*5/246=**0.55**
1.6 การให้บุคลากรภายในองค์กรแต่ละหน่วยงานที่ใช้งานมีส่วนร่วมในการจัดทำหรือทบทวนนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ	111 (3)	111 (3)				3*5=15	3*4=12				15+12=27	27*5/246=**0.55**

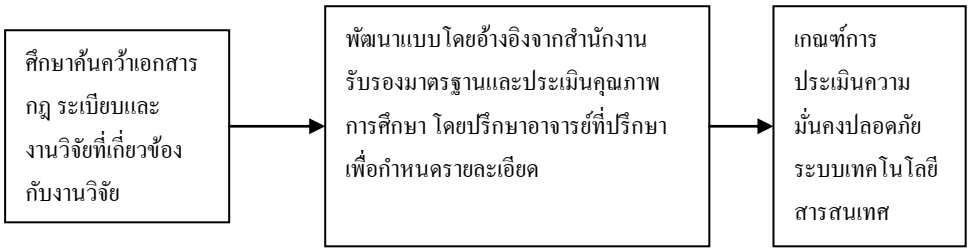
ตารางที่ 1 (ต่อ) ตัวอย่าง หาค่าน้ำหนัก สำหรับตัวบ่งชี้ ด้านที่ 1

รายการ	ค่าความสำคัญ					ค่าน้ำหนัก					รวม	ค่าน้ำหนักค่าบ่งชี้ (5 คะแนน)
ตัวบ่งชี้ด้านที่ 1	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1	5	4	3	2	1		
1.7 ผู้บริหารมีความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างชัดเจน	11 (2)	1111 (4)				2*5=10	4*4=16				10+16=26	26*5/246=**0.53**
1.8 การจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศไว้ในที่ๆ ผู้ใช้งานหรือบุคลากรที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม	11 (2)	111 (4)	1 (1)			2*5=10	3*4=12	1*3=3			10+12+3=25	25*5/246=**0.51**
1.9 การทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันสอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง	11 (2)	111 (4)	1 (1)			2*5=10	3*4=12	1*3=3			10+12+3=25	25*5/246=**0.51**
คะแนนรวม											**246**	**5**

3. พัฒนาตารางประเมิน

เพื่อใช้ในการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถานศึกษา โดยนำคะแนนที่ได้ในตารางการประเมินแต่ละตัวบ่งชี้มาแปรผล ทำให้ทราบสถานะภาพความความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในแต่ละด้าน และแต่ละตัวบ่งชี้ เพื่อใช้เป็นแนวทางในการบริหารจัดการให้มีประสิทธิภาพดีขึ้น

การพัฒนาตารางประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดำเนินการตามขั้นตอน ดังต่อไปนี้



ภาพที่ 7 ขั้นตอนการพัฒนาตารางประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ขั้นตอนที่ 1 ศึกษาค้นคว้าเอกสาร กฎ ระเบียบและ งานวิจัยที่เกี่ยวข้องกับการประเมิน

ขั้นตอนที่ 2 การพัฒนาเกณฑ์ โดยการแปลงความหมายค่าเฉลี่ยนำไปเปรียบเทียบกับเกณฑ์ตามแนวคิดของเบสท์ (Best W. John. 1997,p190) และให้สอดคล้องกับเกณฑ์การประเมินคุณภาพโดยสำนักงานรับรองมาตรฐานและประเมินคุณภาพการศึกษา โดยปรึกษาที่ปรึกษาเพื่อกำหนดรายละเอียด

ขั้นตอนที่ 3 ได้เกณฑ์การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

จากการพัฒนาเกณฑ์การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้รูปแบบ ประกอบไปด้วยช่วงการกระจายค่าน้ำหนักตัวบ่งชี้ เป็นช่วงคะแนน 5 ช่วง ดังนี้

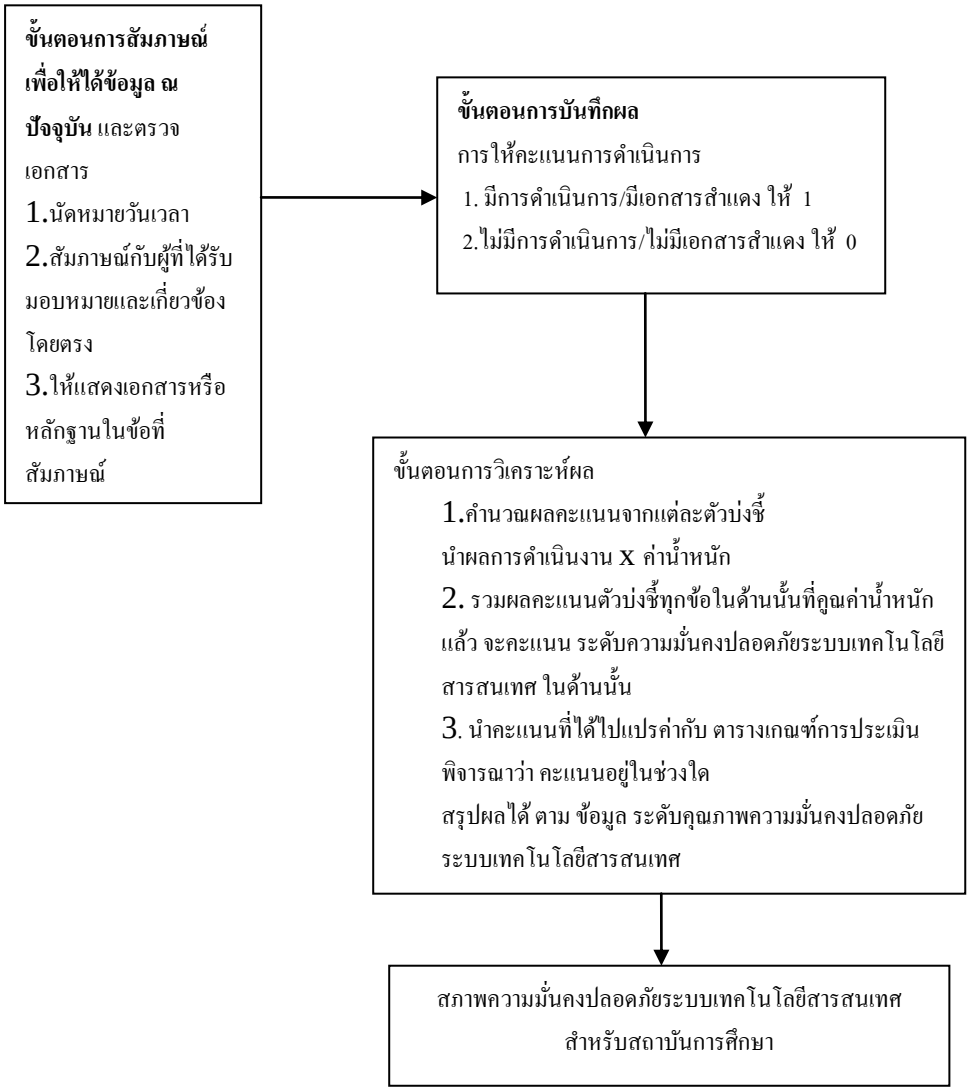
ตารางที่ 2 เกณฑ์การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ช่วงที่	ช่วงคะแนน	ระดับคุณภาพ
1	4.51 – 5.00	ดีมาก
2	3.51- 4.50	ดี
3	2.51 – 3.50	พอใช้
4	1.51 – 2.50	ต้องปรับปรุง
5	0.00 – 1.50	ต้องปรับปรุงเร่งด่วน

จากตารางที่ 2 ช่วงคะแนนแต่ละช่วง สามารถ บ่งชี้ระดับคุณภาพความมั่นคงระบบเทคโนโลยีสารสนเทศในองค์กร เพื่อเป็นข้อมูลให้ ผู้บริหารวางแผนงานนโยบายในการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีเกณฑ์และข้อควรปฏิบัติ ดังต่อไปนี้

1. ช่วงระดับคะแนนประเมิน 4.51-5.00 แสดงถึง
   "ระดับคุณภาพความมั่นคงที่ดีมาก"
   ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ น้อยมาก
   สถานศึกษามีความพร้อมมากในการรักษาความมั่นคงปลอดภัย
2. ช่วงระดับคะแนนประเมิน 3.51-4.50 แสดงถึง
   "ระดับความมั่นคงอยู่ในระดับดี"
   ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ น้อย
   สถานศึกษามีความพร้อมในการรักษาความมั่นคงปลอดภัย
3. ช่วงระดับคะแนนประเมิน 2.51-3.50 แสดงถึง
   "ระดับความมั่นคงอยู่ในระดับพอใช้"
   ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ ปานกลาง
   สถานศึกษามีความพร้อมในการรักษาความมั่นคงปลอดภัยในระดับปานกลาง
   ผู้บริหารควรเพิ่มและปรับปรุงคุณภาพ ตัวบ่งชี้ที่ยังไม่มีประสิทธิภาพ ให้มีประสิทธิภาพยิ่งขึ้น
4. ช่วงระดับคะแนนประเมิน 1.51-2.50 แสดงถึง
   "ระดับความมั่นคงอยู่ในระดับต้องปรับปรุง"
   เป็นระดับความมั่นคงอยู่ในระดับต้องปรับปรุง
   ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ มาก
   ผู้บริหารองค์กรต้องเร่งปรับปรุงคุณภาพตัวบ่งชี้ที่ยังไม่มี หรือ ไม่มีประสิทธิภาพให้มี และมีประสิทธิภาพยิ่งขึ้น
5. ช่วงระดับคะแนนประเมิน 0.00- 1.50 แสดงถึง
   "ระดับความมั่นคงอยู่ในระดับต้องปรับปรุงเร่งด่วน"
   ระดับความมั่นคงอยู่ในระดับ ต่ำมาก
   ต้องเร่งปรับปรุงเร่งด่วน
   ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ มีมากที่สุด
   ผู้บริหารองค์กรต้องเร่งปรับปรุงคุณภาพตัวบ่งชี้ที่ยังไม่มี หรือ ไม่มีประสิทธิภาพให้มี และมีประสิทธิภาพยิ่งขึ้นอย่างเร่งด่วน

4. วิธีการประเมิน การบันทึกผล การแปลผล ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดำเนินขั้นตอนดังนี้



ภาพที่ 8 วิธีและขั้นตอนการประเมิน การบันทึกผล การแปลผล ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

3. นำต้นแบบรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศไปทดสอบการใช้ (R2) กับมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา โดยเปรียบเทียบกับ การประเมินตามมาตรฐานสากล ISO/IEC 27001

4. การปรับแต่งต้นแบบ (D2) โดยการนำความเห็นจากผู้เชี่ยวชาญที่ได้นำไปทดสอบ มาปรับปรุงให้มีประสิทธิภาพมากขึ้น ให้เกิดความถูกต้องและสอดคล้องกับการประเมินแบบสากล เพื่อที่จะนำต้นแบบไปใช้งานจริงและทำการพัฒนาโปรแกรมสำเร็จรูปและคู่มือการใช้งานเพื่อให้ง่ายและสะดวก

การเก็บรวบรวมข้อมูล

ในการเก็บรวบรวมข้อมูลมีขั้นตอนดังนี้

1. ผู้วิจัย ขอความอนุเคราะห์จากผู้เชี่ยวชาญด้านเนื้อหาให้ความคิดเห็นของแบบสอบถาม โดยผู้วิจัยดำเนินการติดต่อและนัดหมาย เพื่อดำเนินการเก็บรวบรวมข้อมูลแบบสอบถามจากผู้เชี่ยวชาญด้านเนื้อหา

2. ผู้วิจัยขอความอนุเคราะห์จากผู้เชี่ยวชาญด้านบริหารสารสนเทศ และผู้ดูแลระบบตอบแบบสอบถาม โดยผู้วิจัยดำเนินการติดต่อและนัดหมาย เพื่อดำเนินการเก็บรวบรวมข้อมูลแบบสอบถามจากผู้เชี่ยวชาญด้านเนื้อหา

ระยะเวลาในการเก็บข้อมูล

ในการวิจัยครั้งนี้ ผู้วิจัยใช้เวลาในการเก็บข้อมูลเป็นเวลา 4 เดือน

การวิเคราะห์ข้อมูล

ในการวิจัยครั้งนี้ ผู้วิจัยได้นำข้อมูลที่เก็บรวบรวมได้ มาวิเคราะห์โดยโปรแกรมสำเร็จตามขั้นตอนดังนี้

1. วิเคราะห์ข้อมูลทั่วไปของผู้เชี่ยวชาญที่ตอบแบบสัมภาษณ์ วิเคราะห์โดยโปรแกรมสำเร็จรูป โดยการแจกแจงความถี่ (Frequency Distribution) และหาค่าร้อยละ (Percentage)

2. วิเคราะห์ข้อมูลความเห็นเกี่ยวกับรูปแบบการประเมินมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา โดยหาค่าเฉลี่ย พัฒนาค่าน้ำหนัก และพัฒนาเกณฑ์ประเมินผลการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูล

การทำวิจัยในครั้งนี้ใช้การวิเคราะห์ข้อมูลทั้งเชิงคุณภาพและเชิงปริมาณ เพื่อที่จะพัฒนารูปแบบการประเมินฯ โดยเป็นข้อมูลในการร่างตัวแบบเพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ แล้วจึง นำข้อมูลที่เก็บรวบรวมมาทำการวิเคราะห์สถิติที่ใช้ในการวิจัย มีดังต่อไปนี้

1. ข้อมูลเชิงคุณภาพ (Qualitative data)

ข้อมูลที่ได้มาจากการค้นคว้าจาก เอกสาร ตำรา รายงานต่าง ๆ รวมถึงข้อมูลจากอินเทอร์เน็ตใช้ในการวิเคราะห์สาร (Content analysis) และการสอบถามเพื่อให้ได้ข้อมูลเบื้องต้นในการวิเคราะห์รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2. ข้อมูลเชิงปริมาณ (Quantitative data)

การวิเคราะห์ข้อมูลเชิงปริมาณในครั้งนี้ ได้ใช้โปรแกรมสำเร็จรูปทางคอมพิวเตอร์ ในการวิเคราะห์ข้อมูล ตามรายละเอียด ดังนี้

2.1 การวิเคราะห์ข้อมูลที่ได้จากการตรวจสอบความตรงของแบบสอบถาม ที่ได้จากผู้เชี่ยวชาญ โดยใช้ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ ที่เรียกว่า Item Objective Congruence index (พิสณุ ฟองศรี, 2552, น.155) จากแบบประเมินความสอดคล้องของผู้เชี่ยวชาญ โดยคะแนนแบ่งออกเป็น 3 ระดับ ดังนี้

แน่ใจว่ามีความสอดคล้อง มีระดับคะแนนเท่ากับ +1

ไม่แน่ใจว่ามีความสอดคล้อง มีระดับคะแนนเท่ากับ 0

แน่ใจว่าไม่มีความสอดคล้อง มีระดับคะแนนเท่ากับ -1

2.2 นำแบบสอบสัมภาษณ์มาวิเคราะห์หาค่าหาค่าเฉลี่ยโดยเกณฑ์ค่าเฉลี่ยคำนวณได้จากการกำหนดคะแนนแต่ละระดับ มีรายละเอียด ดังนี้

ระดับดีมาก	ให้น้ำหนักคะแนนเป็น 5 คะแนน
ระดับมาก	ให้น้ำหนักคะแนนเป็น 4 คะแนน
ระดับปานกลาง	ให้น้ำหนักคะแนนเป็น 3 คะแนน
ระดับน้อย	ให้น้ำหนักคะแนนเป็น 2 คะแนน
ระดับน้อยมาก	ให้น้ำหนักคะแนนเป็น 1 คะแนน

การแปลงความหมายค่าเฉลี่ยนำไปเปรียบกับเกณฑ์ตามแนวคิดของเบสท์ (Best W. John. 1997,p190) โดยถือว่าค่าเฉลี่ยของคะแนนที่ได้จากการตอบแบบสัมภาษณ์อยู่ในช่วงใด แสดงว่าระดับความคิดเห็นของผู้เชี่ยวชาญ อยู่ในระดับนั้น ๆ ดังนี้

4.51-5.00 หมายความว่า ความคิดเห็นด้วยในข้อนั้นระดับดีมาก

3.51-4.50 หมายความว่า ความคิดเห็นด้วยในข้อนั้นระดับมาก

2.51-3.50 หมายความว่า ความคิดเห็นด้วยในข้อนั้นระดับปานกลาง

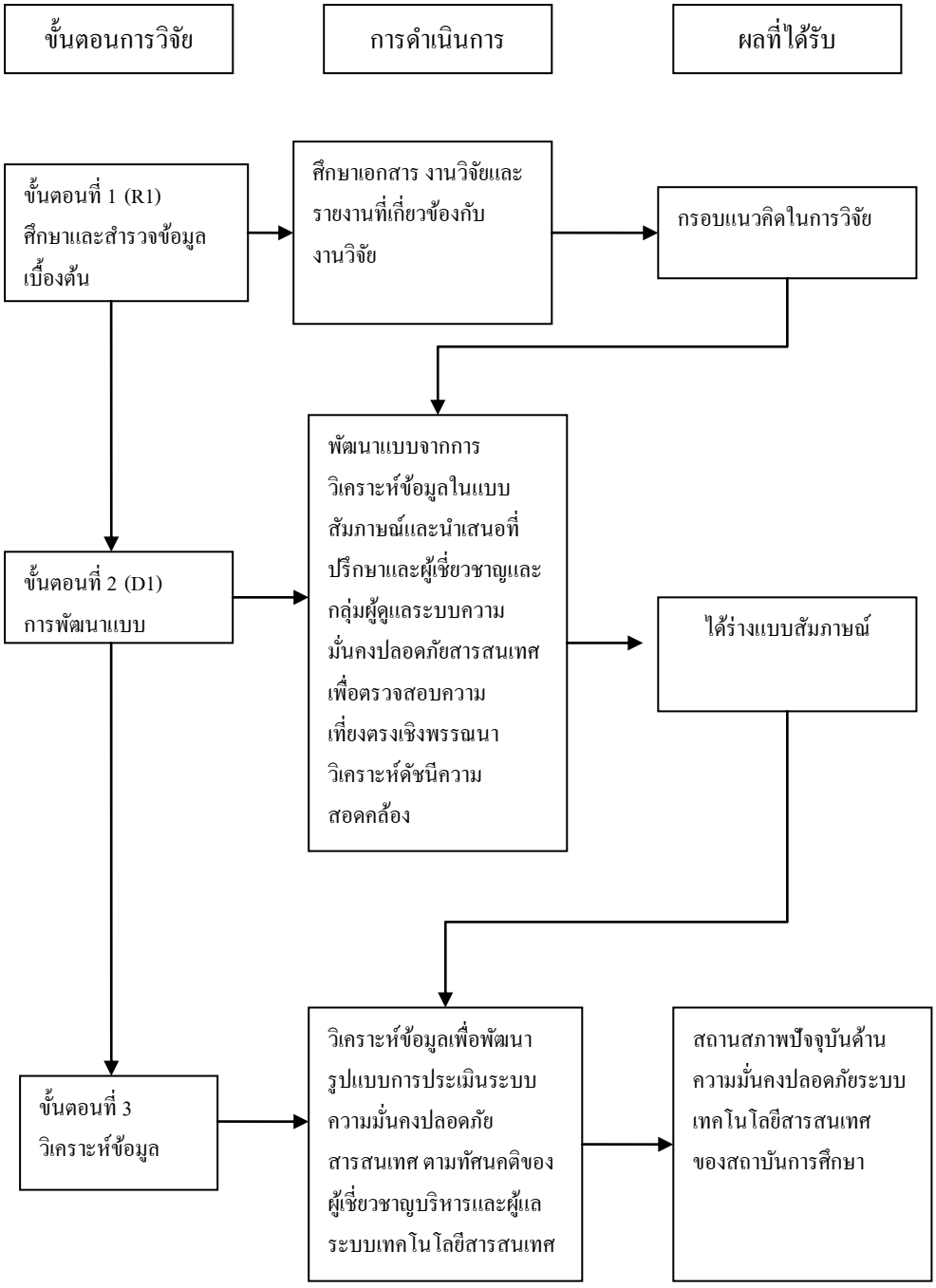
1.51-2.50 หมายความว่า ความคิดเห็นด้วยในข้อนั้นระดับน้อย

0.00-1.50 หมายความว่า ความคิดเห็นด้วยในข้อนั้นระดับน้อยมาก

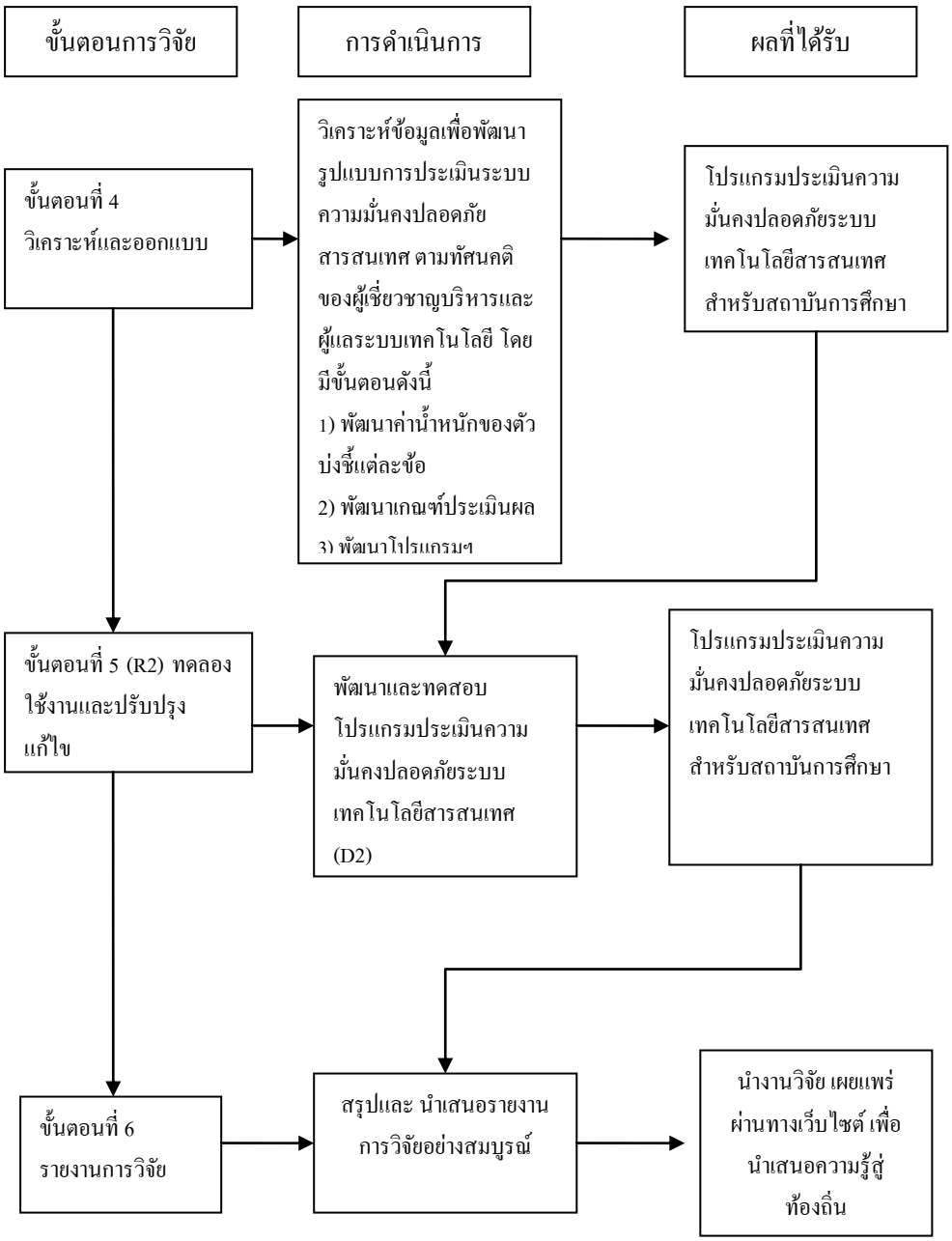
สถิติที่ใช้ในการวิเคราะห์ข้อมูล

ในการวิจัยครั้งนี้ ผู้วิจัยใช้สถิตวิเคราะห์ข้อมูล โดยการใช้สถิติพื้นฐาน ร้อยละ (Percentage)

ขั้นตอนในการทำวิจัย (R1,D2,R2,D2)



ภาพที่ 9 แสดงขั้นตอนในการทำวิจัย (R1,D2,R2,D2)



ภาพที่ 9 (ต่อ) แสดงขั้นตอนการวิจัย (R1,D1,R2,D2)

ขั้นตอนการวิจัย 1 (R1) ศึกษา สำรวจข้อมูลเบื้องต้น ศึกษาเอกสาร งานวิจัย รายงานที่เกี่ยวข้อง ได้กรอบแนวคิดในการวิจัย ทำการพัฒนารูปแบบเพื่อการประเมินความมั่นคง จากการวิเคราะห์ข้อมูล จากแบบสัมภาษณ์และนำเสนออาจารย์ที่ปรึกษาและผู้เชี่ยวชาญและกลุ่มผู้ดูแลระบบความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบความเที่ยงตรงเชิงพรรณนา วิเคราะห์ดัชนีความสอดคล้อง ได้แบบสัมภาษณ์ ทำการวิเคราะห์ข้อมูลเพื่อพัฒนารูปแบบการประเมินระบบความมั่นคงปลอดภัยสารสนเทศ ตามทัศนคติของผู้เชี่ยวชาญบริหารและผู้แลระบบเทคโนโลยีสารสนเทศ ได้สถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา ขั้นตอนการพัฒนา (D1) ทำการวิเคราะห์และออกแบบ วิเคราะห์ข้อมูลเพื่อพัฒนารูปแบบการประเมินระบบความมั่นคงปลอดภัยสารสนเทศ ตามทัศนคติของผู้เชี่ยวชาญบริหารและผู้แลระบบเทคโนโลยี โดยมีขั้นตอน พัฒนาค่าน้ำหนักของตัวบ่งชี้แต่ละข้อ และ พัฒนาเกณฑ์ประเมินผล ได้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา นำไปทดสอบ ทำการปรับปรุงแก้ไข (R2) ได้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

ขั้นตอนการพัฒนาโปรแกรม

นำผลที่ได้ มาพัฒนาเป็นโปรแกรมการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา การพัฒนาโปรแกรมและทดสอบ (D2) วางแผนการพัฒนาโปรแกรม

โดยแบ่งหัวข้อหลักของโปรแกรมออกตามลำดับความสำคัญของการใช้งาน สำรวจข้อมูลพื้นฐานของระบบฮาร์ทแวร์ ซอฟแวร์ บุคลากร งบประมาณ ฯลฯ เพื่อจัดทำฐานข้อมูล การพัฒนาโปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วย ระบบป้อนข้อมูลพื้นฐาน ระบบวิเคราะห์ผล ระบบประเมิน ระบบรายงานผล นำไปทดลองใช้งานโปรแกรม การประเมินผลการศึกษา ผลความพึงพอใจของโปรแกรมจากผู้เกี่ยวข้องด้วยแบบประเมินผลความพึงพอใจของผู้เกี่ยวข้อง ประเมินประสิทธิภาพของโปรแกรมการบริหารจัดการเพื่อการประเมินความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร จากผู้เกี่ยวข้อง ด้วยแบบประเมินประสิทธิภาพการทำงานของโปรแกรม

สรุปและ นำเสนอรายงานการวิจัยอย่างสมบูรณ์ นำงานวิจัย เผยแพร่ ผ่านทางเว็บไซต์ เพื่อนำเสนอความรู้สู่ท้องถิ่น

บทที่ 4

ผลการวิจัย

ผลการวิจัยเรื่อง การพัฒนาโปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา ได้ผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ดังต่อไปนี้

การวิจัยมีวัตถุประสงค์ คือ 1. ศึกษาสถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา 2. พัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา 3. พัฒนาโปรแกรมเพื่อประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา
ได้ผลดังต่อไปนี้

การวิจัยครั้งนี้กำหนดวัตถุประสงค์เพื่อพัฒนาโปรแกรมโปรแกรมเพื่อประเมินความมั่นคงปลอดภัยระบบสารสนเทศสำหรับสถาบันการศึกษา โดยการนำมาตรฐานความมั่นคงปลอดภัย สากล 27001 (ISO 27001) มาสังเคราะห์ข้อมูลเพื่อให้ได้ต้นแบบของวิธีการประเมินที่เหมาะสมสำหรับสถาบันการศึกษาในประเทศไทย

จากการศึกษาบริบท ปัญหาและ สถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา พบว่า

1. ในสถานภาพปัจจุบัน ปัญหาและสถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบันการศึกษา ผู้บริหารสถาบันการศึกษา ให้ความสำคัญด้านมีนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและนโยบายสิ่งแวดล้อม ด้านงบประมาณ ด้านบุคลากร และผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับมากถึงมากที่สุด แต่ปัจจุบันสถาบันการศึกษา ยังไม่มี นโยบายความมั่นคงปลอดภัยตามมาตรฐานสากลและนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร งบประมาณที่ได้รับเพื่อบริหารระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาส่วนใหญ่ไม่เพียงพอ

2. ผลการพัฒนา รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา ได้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

มีตัวบ่งชี้ด้านความมั่นคง 11 ด้าน 105 ตัวบ่งชี้ ประกอบด้วย ด้านที่ 1 มี 9 ตัวบ่งชี้ ด้านที่ 2 มี 5 ตัวบ่งชี้ ด้านที่ 3 มี 4 ตัวบ่งชี้ ด้านที่ 4 มี 9 ตัวบ่งชี้ ด้านที่ 5 มี 10 ตัวบ่งชี้ ด้านที่ 6 มี 19 ตัวบ่งชี้ ด้านที่ 7 มี 29 ตัวบ่งชี้ ด้านที่ 8 มี 7 ตัวบ่งชี้ ด้านที่ 9 มี 5 ตัวบ่งชี้ ด้านที่ 10 มี 3 ตัวบ่งชี้ ด้านที่ 11 มี 5 ตัวบ่งชี้ รวมทั้งสิ้น 11 ด้าน 105 ตัวบ่งชี้ได้แก่ 1) นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ 2) โครงสร้างความมั่นคงปลอดภัยขององค์กร 3) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร 4) นโยบายการบริหารจัดการทรัพย์สิน 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม 6) การบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร 7) การควบคุมการเข้าถึง 8) การจัดหาการพัฒนาและบำรุงระบบสารสนเทศ 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร 11) การปฏิบัติตามข้อกำหนด

ผลการนำรูปแบบประเมินนี้ ไปทำการประเมิน กับสำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา พบว่า

1. นโยบายความมั่นคงปลอดภัย ได้ระดับคะแนน 2.17 สภาพความมั่นคงอยู่ในระดับพอใช้

2. โครงสร้างความมั่นคงปลอดภัยขององค์กร ได้ระดับคะแนน 4.00 สภาพความมั่นคงอยู่ในระดับ ดี

3. การบริหารจัดการทรัพย์สินขององค์กร ได้ระดับคะแนน 3.68 สภาพความมั่นคงอยู่ในระดับ ดี

4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร ได้ระดับคะแนน 4.47 สภาพความมั่นคงอยู่ในระดับ ดี

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ได้ระดับคะแนน 5.0 สภาพความมั่นคงอยู่ในระดับ ดีมาก

6. การบริหารจัดการด้านการสื่อสาร และการดำเนินงานเครือข่ายสารสนเทศขององค์กร ได้ระดับคะแนน 3.73 สภาพความมั่นคงอยู่ในระดับ ดี

7. การควบคุมการเข้าถึง ได้ระดับคะแนน 4.65 สภาพความมั่นคงอยู่ในระดับ ดีมาก

8. การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ ได้ระดับคะแนน 3.80 สภาพความมั่นคงอยู่ในระดับ ดี

9. บริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ได้ระดับคะแนน 3.98 สภาพความมั่นคงอยู่ในระดับ ดี

10. บริหารความต่อเนื่องในการดำเนินงานขององค์กร ได้ระดับคะแนน 0 สภาพความมั่นคงอยู่ในระดับ ต้องปรับปรุงเร่งด่วน***

11. การปฏิบัติตามข้อกำหนดมาตรฐาน ได้ระดับคะแนน 3.97 สภาพความมั่นคงอยู่ในระดับ ดี

เมื่อนำแบบประเมินของสากล ตามแนวมาตรฐาน ISO/IEC27001 ไปทำการประเมิน ผลออกมาสอดคล้องกัน แต่ใช้เวลาในการประเมินมากกว่า และพบว่า ข้อตรวจประเมินมีทั้งหมด 133 ข้อ ความเข้าใจในข้อถามยากกว่า การตรวจเอกสารมีขั้นตอนมากกว่า ต้องเกี่ยวข้องกับบุคลกรหลายฝ่ายหลายระดับ

ผล ผู้ใช้งานรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา เป็นที่พอใจของผู้ใช้ และได้ผลสอดคล้องกับรูปแบบการประเมินความมั่นคงปลอดภัยระบบสารสนเทศแบบสากล

ผลการวิจัยได้รูปแบบรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ได้ทำการเปรียบเทียบกับรูปแบบการประเมินสากล ISO 27001 ดังนี้

ตารางที่ 3 รายการเปรียบเทียบระหว่างรูปแบบการประเมินที่พัฒนาขึ้นกับรูปแบบมาตรฐาน

รายการ	รูปแบบการประเมินที่พัฒนาขึ้น	รูปแบบมาตรฐาน
1 ตัวบ่งชี้	11 ด้าน 105 ตัวบ่งชี้	11 ด้าน 133 ตัวบ่งชี้
2. วิธีการประเมิน	Plan-Do-Check-Act	Plan-Do-Check-Act
3. ความเหมาะสมในการใช้	สถาบันการศึกษา	องค์กรระดับใหญ่
4. แนวคิด	ผู้เชี่ยวชาญของประเทศไทย	ผู้เชี่ยวชาญจากต่างประเทศ
5. ภาษาที่ใช้และการเรียนรู้	ภาษาไทย / จากคู่มือ	ภาษาอังกฤษ / คู่มือ+การอบรม
6. การใช้งาน	ง่าย มีคู่มือ มีโปรแกรมสำเร็จรูป	ยุ่งยาก ซับซ้อน เข้าใจยาก
7. บุคลากร	ผู้ดูแลระบบสารสนเทศ	ผู้เชี่ยวชาญ (Expert)
8. ระยะเวลาในการประเมิน	ภายใน 1 วัน	ภายใน 1 สัปดาห์
9. ค่าใช้จ่าย	สามารถดำเนินการเองได้	1,200,000 บาทขึ้นไป
10. การลำดับความสำคัญ**	มีค่าน้ำหนักตัวบ่งชี้ลำดับความสำคัญของการจัดการ	ไม่มี

3. ผลการพัฒนาการพัฒนาโปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา ได้โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

ประโยชน์ที่ได้รับ

1. ผู้บริหารใช้เป็นเครื่องมือประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษาเพื่อตรวจสอบสภาพปัจจุบันของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

2. ผู้บริหารสามารถได้รับข้อมูลที่เป็นตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่มีระดับความสำคัญ เพื่อลำดับความสำคัญในการบริหารจัดการ

3. สามารถใช้เป็นแนวทางในการวางนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล

4. สร้างภาพลักษณ์ที่ดีให้กับสถาบันการศึกษา เพราะนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศมีความมั่นคง มั่นใจได้ในข้อมูลซึ่งมีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

5. เป็นไปตามข้อกำหนดของกฎหมายประเทศไทยและสากล (รองรับการเปิดเสรีประชาคมอาเซียน)

ข้อเด่นของ โปรแกรมประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

1. ประเมินได้ง่าย ง่ายในการใช้งาน และการเรียนรู้ มีข้อแนะนำ ข้อควรปฏิบัติของผู้เกี่ยวข้องด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทุกฝ่าย ประกอบด้วย ผู้บริหาร ผู้ปฏิบัติการ ผู้ใช้งานทั้งภายในและภายนอก

2. ประหยัดเวลา เข้าใจง่าย

3. ประหยัดค่าใช้จ่าย ดำเนินได้ด้วยตนเอง

4. ประโยชน์ ใช้ได้กับทุกหน่วยงาน

5. ประสิทธิภาพดี สอดคล้องกับการประเมินตามมาตรฐานสากล

ลักษณะการใช้งาน

1. มีเมนูขั้นตอนการนำไปใช้

    ระบบลงทะเบียนผู้ใช้

    ระบบบันทึก ข้อมูล

    ระบบปรับปรุง เพิ่มเติม แก้ไข ข้อมูล

    ระบบประเมินผล

    ระบบรายงานผล

    ระบบการเสนอแนะ แก้ไข ปรับปรุง

    ระบบคู่มือประเมิน

    ระบบคู่มือการใช้โปรแกรม

2. มีเมนูช่วยในการใช้งานแบบง่ายและสะดวก ประกอบด้วย

    คู่มือการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

    แบบฟอร์มสำเร็จรูป ในการ เก็บข้อมูล ตรวจประเมิน

    คู่มือเกณฑ์การประเมิน

    ข้อเสนอแนะ ข้อควรระวัง การป้องกัน การแก้ไข

วิธีการใช้การโปรแกรม

1) เปิด อินเตอร์เน็ตเบราเซอร์
2) เข้าสู่โปรแกรม
3) กรอกข้อมูล สถาบันการศึกษา
4) กดปุ่ม เลือกเมนู เพื่อเริ่มทำแบบประเมิน
5) ทำแบบประเมินทั้ง 11 ข้อเสร็จ ระบบจะประมวบผลและรายงานผลการประเมิน
6) เลือกเมนู ข้อเสนอแนะ เพื่อรับคำแนะนำการปรับปรุงระบบ
7) เลือกเมนูการพิมพ์ สามารถพิมพ์ผลสรุปทั้งหมด

การเข้าสู่โปรแกรมทางอินเตอร์เน็ต

ผู้ใช้งานสามารถเข้าใช้งานโปรแกรมผ่านทางเครือข่ายอินเทอร์เน็ตได้จาก

Website: http://tm.dru.ac.th/assessment/

การทำงานของโปรแกรม

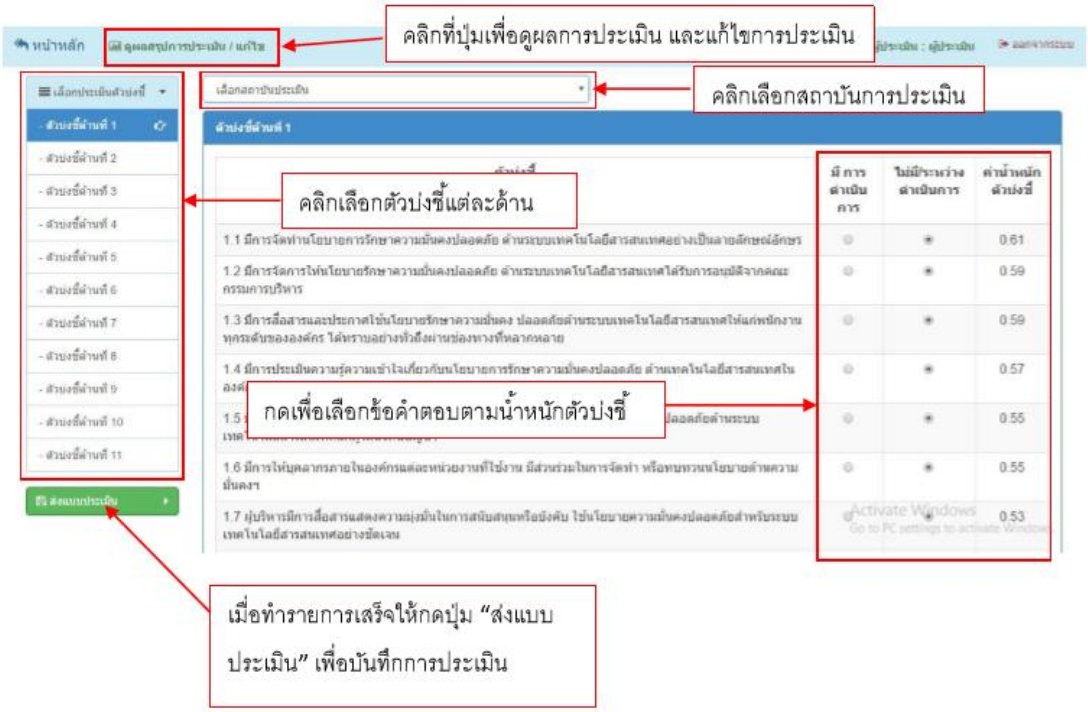
เมื่อเปิดโปรแกรม เข้าสู่เมนูแรก บันทึกสถาบันการศึกษา และหน่วยงานที่ต้องการประเมิน เข้าสู่แบบประเมิน ตามลำดับ ที่ 1 ถึง 11 กดปุ่มประมวลผล จะได้ผลสรุป

ภาพที่ 10 แสดงหน้าจอโปรแกรม

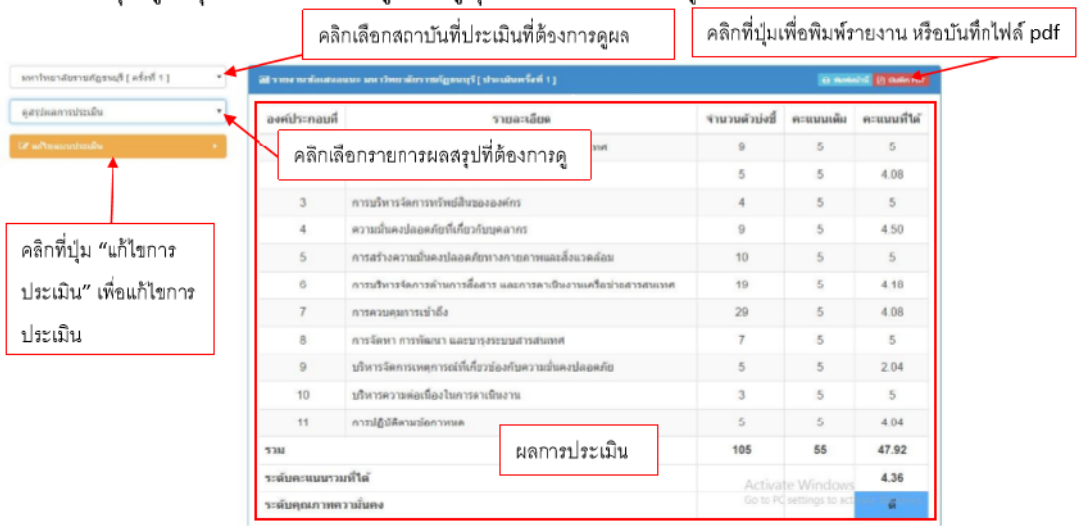
3.แบบประเมิน/ผลสรุป/แก้ไข

1.ประเมินแบบสอบถามทันที

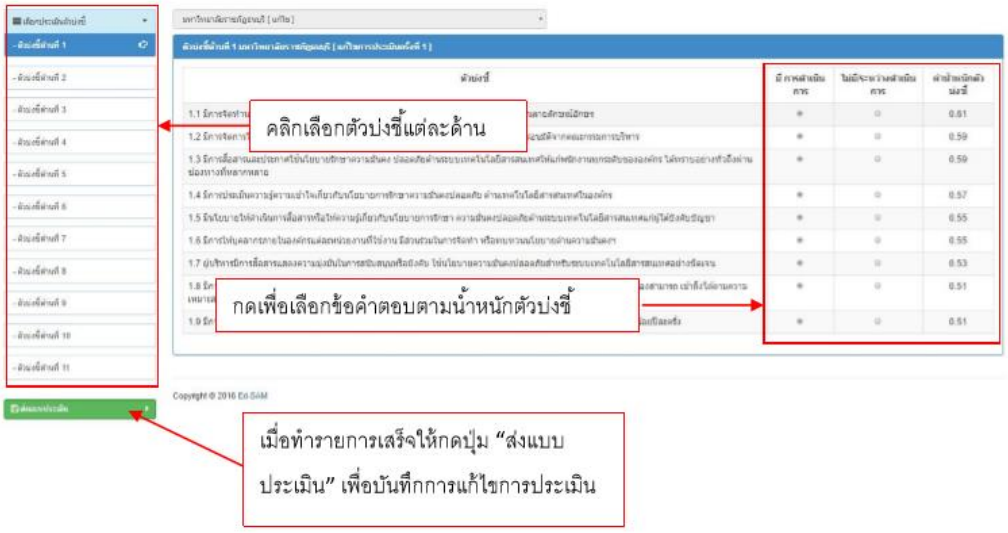
2.ดูผลสรุปการประเมิน / แก้ไขข้อมูล



1.2 **เมื่อคลิกที่ปุ่ม "ดูผลสรุปการประเมิน/แก้ไขข้อมูล " เพื่อดูสรุปผลการประเมิน (ต้องเข้าสู่ระบบก่อนจึงจะทำรายการนี้ได้)**



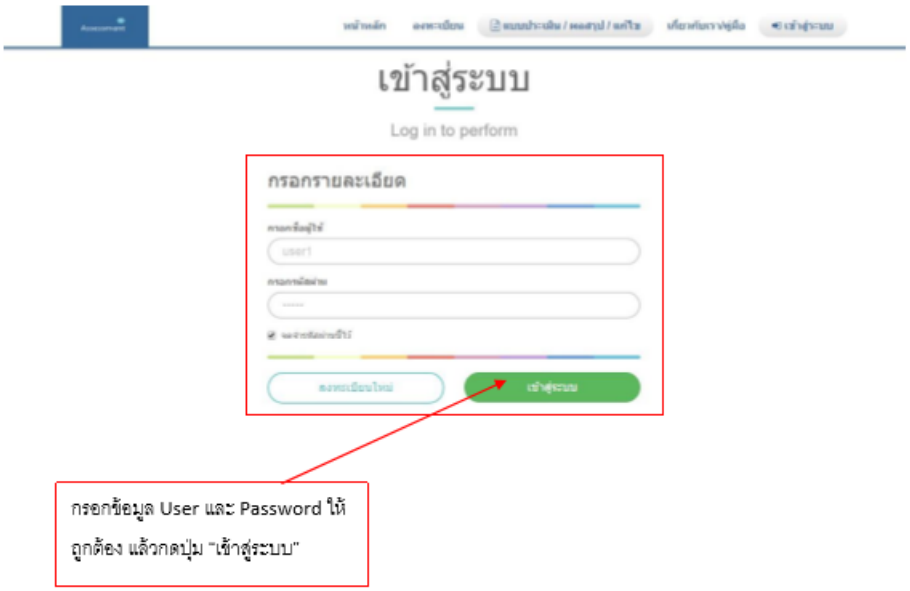
1.2.1 **เมื่อกดปุ่ม "แก้ไขการประเมิน" จะได้หน้าเว็บดังรูป**



4.เกี่ยวกับเรา/คู่มือ

5.เข้าสู่ระบบ

1.เปิดหน้าเว็บไซต์ ไปที่ปุ่ม “เข้าสู่ระบบ” แล้วกรอกข้อมูล User และ Password ให้ครบถ้วนพร้อมตรวจสอบความถูกต้อง แล้วกดปุ่ม “เข้าสู่ระบบ”



การจัดการระบบ

บทที่ 5
สรุปผล อภิปรายผลและข้อเสนอแนะ

การวิจัยเรื่อง การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา กำหนดวัตถุประสงค์การวิจัยไว้ดังนี้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา
2. เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา
3. เพื่อพัฒนาโปรแกรมคอมพิวเตอร์ประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ เป็นการดำเนินการวิจัยที่มีรูปแบบเป็นการวิจัยและพัฒนา มีขั้นตอนการวิจัย ดังนี้

1. ขั้นตอนการวิจัย 1 (R1) ดำเนินการโดยการศึกษาข้อมูลพื้นฐาน สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จากเอกสารและการสัมภาษณ์ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2. ขั้นตอนพัฒนา 1 (D1) ดำเนินการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา โดยการ ศึกษามาตรฐานความมั่นคงปลอดภัยสากล ISO 27001 นำมาสังเคราะห์ข้อมูล ได้ร่างเครื่องมือวิจัยเป็นแบบสัมภาษณ์ นำแบบสัมภาษณ์เสนอผู้เชี่ยวชาญที่มีความเชี่ยวชาญด้านการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบ ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of Item – Objective Congruence: IOC) ได้เครื่องมือ นำไปสัมภาษณ์ผู้เชี่ยวชาญด้านบริหารและผู้ดูแลระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้สภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา และได้ตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา สร้างค่าน้ำหนักตัวบ่งชี้ สร้างตารางประเมิน ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา นำไปทดสอบการใช้งาน และเปรียบเทียบกับ

การประเมินแบบมาตรฐานสากล ทำการปรับปรุงหากได้ผลการประเมินออกมาไม่สอดคล้องกับวิธีประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

3. ขั้นตอนการวิจัย 2 (R2) ดำเนินการทดลองการใช้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้น ณ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ได้ผลการประเมินระดับคุณภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับดี เทียบเท่ากับ การเปรียบเทียบโดยใช้ การประเมินตามแบบมาตรฐานสากล

4. ขั้นตอนการพัฒนา 2 (D2) ดำเนินการปรับปรุงรูปแบบการประเมินการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้น ได้มีการพัฒนาโปรแกรมสำเร็จรูปเพื่อให้มีการใช้งานที่ง่ายและสะดวกขึ้น โปรแกรมจะอธิบายขั้นตอนต่าง ๆ รวมถึงความรู้ทั่วไป ความรู้ในการแก้ไขปัญหาต่าง ๆ กฎระเบียบต่าง ๆ ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทำให้ผู้ใช้งานที่มีความรู้พื้นฐานด้านสารสนเทศ สามารถเข้าใจ และทำการประเมินได้ด้วยตนเอง และทราบผลอย่างรวดเร็ว และทราบวิธีการที่จะต้องปรับปรุงแก้ไขในแต่ละเหตุการณ์ที่เกิดขึ้น จุดเด่นของรูปแบบประเมินนี้ จะแสดงผลลำดับความสำคัญของแต่ละตัวบ่งชี้ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถาบันการศึกษา ทำให้ผู้บริหารสามารถจัดลำดับความสำคัญในการบริหารจัดการได้อย่างเหมาะสม

การดำเนินการวิจัยในครั้งนี้ ผู้วิจัยได้ศึกษาเอกสารงานวิจัย และรายงานที่เกี่ยวข้องกับหลักการทฤษฎี และแนวคิด รูปแบบการประเมินความมั่นคงปลอดภัยระบบสารสนเทศแบบสากล รวมไปถึงการบริหารจัดการคุณภาพของสถาบันการศึกษา โดยออกแบบสัมภาษณ์กึ่งมีโครงสร้าง ปรึกษาผู้เชี่ยวชาญเพื่อตรวจสอบความสอดคล้อง ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of item objective congruence: IOC) ของ 105 ตัวบ่งชี้ ผลปรากฏว่า บ่งชี้ทุกตัวมีค่า IOC อยู่ระหว่าง 0.80-1.00 ซึ่งถือว่าเป็นตัวบ่งชี้ที่ใช้ได้ ผู้วิจัยจึงนำไปพัฒนาปรับปรุงแก้ไขบางส่วนเพื่อให้สำนวนภาษากระชับ เข้าใจได้ง่ายขึ้น และจัดทำเป็นแบบสัมภาษณ์

นำแบบสัมภาษณ์เสนอที่ปรึกษา และผู้เชี่ยวชาญเพื่อตรวจสอบสำนวนภาษา ปรับปรุงการใช้ภาษาให้เหมาะสม เพื่อให้ได้ตัวบ่งชี้ข้อคำถามที่มีความถูกต้องครอบคลุมครบถ้วน ตรงตามนิยามศัพท์เฉพาะ เพื่อไปสัมภาษณ์ผู้เชี่ยวชาญ ผู้ทรงคุณวุฒิด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา 3 แห่งจำนวน 6 คน โดยผู้วิจัยเดินทางไปสัมภาษณ์ด้วยตนเอง

การวิจัยครั้งนี้กลุ่มตัวอย่างคือประชากรโดยแบ่งเป็น 2 กลุ่ม กลุ่มที่ 1 คือ ผู้เชี่ยวชาญด้านนโยบายบริหารระบบเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏ ได้แก่ มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ราชภัฏสวนสุนันทา รวม 3 คน กลุ่มที่ 2 คือ ผู้ดูแลด้าน

เทคนิคระบบเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏรวม 3 แห่ง ได้แก่ มหาวิทยาลัยราชภัฏธนบุรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มหาวิทยาลัยราชภัฏสวนสุนันทา รวม 3 คน ผู้วิจัยขอสรุปผลการวิจัย การอภิปรายผล และการให้ข้อเสนอแนะตามลำดับดังต่อไปนี้

สรุปผลการวิจัย

การวิจัยครั้งนี้สามารถสรุปผลการวิจัยได้ดังนี้

สรุปผลขั้นตอนการวิจัย 1 (R1) ดำเนินการโดยการศึกษาข้อมูลพื้นฐาน สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จากเอกสารและการสัมภาษณ์ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ผลการศึกษาสถานภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาและพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ผลการวิเคราะห์ข้อมูล โดยศึกษาและค้นคว้าเอกสาร รวบรวมแนวคิดหลักการที่เกี่ยวข้องกับการสัมภาษณ์ผู้เชี่ยวชาญด้านบริหารระบบเทคโนโลยีสารสนเทศและผู้ดูแลระบบระบบเทคโนโลยีสารสนเทศ เพื่อทำการพัฒนารูปแบบการประเมินความมั่นคงระบบเทคโนโลยีสารสนเทศ ได้ผลดังนี้

สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา

1. การศึกษาสถานภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา มีรายละเอียดดังนี้

1.1 สถานภาพปัจจุบันด้านนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พบว่า ผู้บริหาร สถาบันการศึกษาทุกแห่งให้ความสำคัญมาก สถาบันการศึกษาส่วนใหญ่ ยังไม่มีการนำนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐานสากลมาใช้ โดยให้เหตุผลว่าไม่มีบุคลากรที่มีความรู้ความชำนาญ งบประมาณมีจำกัด การนำเสนอระบบเข้าใจยาก ระบบบริหารในปัจจุบันยังไม่สนับสนุนการนำนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐานสากลมาใช้

1.2 สถานภาพปัจจุบันด้านงบประมาณสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พบว่า สถาบันการศึกษาสนับสนุนว่า งบประมาณงบประมาณสำหรับความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญมากที่สุด บางสถาบันการศึกษา ได้รับงบประมาณด้านบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงพอ ได้แก่ สถาบันการศึกษาบางแห่งได้รับงบประมาณด้านบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ปานกลาง

1.3 สถานภาพปัจจุบัน ด้านการวางนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร พบว่า ผู้บริหารสถาบันการศึกษาส่วนมาก ให้ความสำคัญมาก ในการวางนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างเป็นลายลักษณ์อักษร

สถานภาพปัจจุบัน พบว่า ไม่มีการวางนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร ในสถาบันการศึกษาส่วนใหญ่

1.4 สถานภาพปัจจุบันของการให้ความสำคัญของผู้บริหารสถาบันการศึกษา ต่อบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับมากที่สุด และสถานภาพความรู้ความเข้าใจเกี่ยวกับกับความมั่นคงปลอดภัยระบบสารสนเทศ ของบุคลากรที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของสถาบันการศึกษา มีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับปานกลาง

1.5 สถานภาพด้านพฤติกรรมผู้ใช้งานที่เกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พบว่า พฤติกรรมผู้ใช้งานเกี่ยวกับความมั่นคงปลอดภัยของระบบ ของสถาบันการศึกษาผู้บริหารให้ความสำคัญ ระดับมาก และพบว่า ผู้ใช้งานที่เกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถาบันการศึกษาบางส่วน มีความรู้ ความเข้าใจ เกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในระดับปานกลาง

สรุปผลขั้นตอนพัฒนา 1 (D1) ดำเนินการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา การศึกษามาตรฐานความมั่นคงปลอดภัยสากล ISO 27001 นำมาสังเคราะห์ข้อมูล ได้ร่างเครื่องมือวิจัยเป็นแบบสัมภาษณ์ นำแบบสัมภาษณ์เสนอผู้เชี่ยวชาญที่มีความเชี่ยวชาญด้านการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบ ความเที่ยงตรงเชิงเนื้อหา (Content validity) วิเคราะห์ดัชนีความสอดคล้อง (Index of Item – Objective Congruence: IOC) ได้เครื่องมือ นำไปสัมภาษณ์ผู้เชี่ยวชาญด้านบริหารและผู้ดูแลระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้สภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา และได้ตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา สร้างค่าน้ำหนักตัวบ่งชี้ สร้างตารางประเมิน ได้รูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา มีผลการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ได้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา มีตัวบ่งชี้ 11 ด้าน ประกอบไปด้วย ด้านที่ 1 มี 9 ตัวบ่งชี้ ด้านที่ 2 มี 5 ตัวบ่งชี้ ด้านที่ 3 มี 4 ตัวบ่งชี้ ด้านที่ 4 มี 9 ตัวบ่งชี้ ด้านที่ 5 มี 10 ตัวบ่งชี้ ด้านที่ 6 มี 19 ตัวบ่งชี้ ด้านที่ 7 มี 29 ตัวบ่งชี้ ด้านที่ 8 มี 7 ตัวบ่งชี้ ด้านที่ 9 มี 5 ตัวบ่งชี้ ด้านที่ 10 มี 3 ตัว

บ่งชี้ ด้านที่ 11 มี 5 ตัวบ่งชี้ รวมทั้งสิ้น 11 ด้าน 105 ตัวบ่งชี้ ได้แก่ 1) นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ 2) โครงสร้างความมั่นคงปลอดภัยขององค์กร 3) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร 4) นโยบายการบริหารจัดการทรัพย์สิน 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม 6) การบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร 7) การควบคุมการเข้าถึง 8) การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร 11) การปฏิบัติตามข้อกำหนด เป็นภารกิจหลักของผู้บริหารต้องให้ความสำคัญในการบริหารจัดการ การกำหนดการลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย การบริหารจัดการทรัพยากรโดยการอบรม การสร้างความตระหนักและการเพิ่มขีดความสามารถเพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย ต้องมีนโยบายตรวจสอบภายในตามรอบระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยมีสถานภาพเพียงใด โดยมีรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เป็นเครื่องมือตรวจสอบ นำทางสู่นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

การบริหารจัดการ ด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร การควบคุมการเข้าถึง การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร การบริหารความต่อเนื่องในการดำเนินงานขององค์กร เป็นภารกิจที่มีปริมาณงานจำนวนมากที่ต้องใช้ความรู้ความสามารถทางเทคนิค ดังนั้นผู้บริหารต้องให้ความสำคัญ ในการพัฒนาความรู้ความสามารถเพื่อเพิ่มศักยภาพให้กับผู้ปฏิบัติงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้น มีแนวคิด แนวดำเนินงาน ความสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสากล ผู้วิจัยได้พัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อเป็นเครื่องมือสำหรับผู้บริหาร เพื่อเป็นแนวทางในการกำหนดนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา สามารถนำผลที่ประเมินเพื่อการวางแผน นโยบาย กลยุทธ์ต่าง ๆ ได้อย่างแม่นยำและมีประสิทธิภาพมากยิ่งขึ้น และเป็นแนวทางในการนำมหาวิทยาลัยเข้าสู่รูปแบบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสากลได้ง่ายขึ้น โดยใช้งบประมาณ

ที่ต่ำกว่าประเมินจากองค์กรภายนอก ซึ่งทางสถาบันการศึกษาต้องใช้งบประมาณจำนวนมาก เพื่อให้ผู้เชี่ยวชาญจากองค์กรภายนอกเข้ามาประเมินความมั่นคงปลอดภัยระบบสารสนเทศ

นอกจากนี้การดำเนินการตามคู่มือการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ผู้บริหารและผู้ปฏิบัติการ สามารถศึกษาและเรียนรู้ได้อย่างง่ายดาย ผู้วิจัยได้พัฒนาเครื่องมือและซอฟต์แวร์สำเร็จรูปมาใช้ ทำให้ง่ายในการเรียนรู้เรื่องความปลอดภัยระบบเทคโนโลยีสารสนเทศ ตัวบ่งชี้ตัวใด ตัวบ่งชี้ด้านใด ควรบริหารจัดการอย่างไร รูปแบบการประเมินนี้จะมีดรรชนีนำเข้าสู่ความรู้และแนวทางป้องกันหรือแนวทางแก้ไขในแต่ละขั้นตอน อย่างง่ายดาย

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เรียกว่า **"Ed-SAM" (Education Security Assessment Model)** เป็นรูปแบบการประเมินความมั่นคงปลอดภัยระบบสารสนเทศด้วยตนเอง สำหรับสถาบันการศึกษา

มีปัจจัยที่เกี่ยวข้องโดยอธิบายรายละเอียดของ โมเดล ดังรูป

การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องเริ่มจากผู้บริหารต้องการการบริหารจัดการ (**M**anagement) ด้านนโยบาย (**P**olicy) ด้านเทคโนโลยี (**T**echnology) ด้านบุคลากร (**H**uman) โดยมีคณะทำงานที่มีเป้าหมายเดียวกัน (**U**nity) มีพันธะสัญญาร่วมกันอย่างมุ่งมั่น (**C**ommitment) ที่จะช่วยเหลือซึ่งกันและกัน (**H**abit) พฤติกรรมผู้ใช้งานของเกี่ยวข้องกับระบบความมั่นคงปลอดภัยขององค์กร (**O**rganization) อย่างเป็นขั้นตอน (**P**rocedure) ในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี (**T**echnology) ให้มีความมั่นคงปลอดภัย ประกอบด้วย ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร และบุคลากร เพื่อรองรับภารกิจของสถาบันการศึกษาในด้าน การเรียนการสอน การบริหารสถานศึกษา การให้บริการชุมชน เพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้งานของ ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ รวมทั้งทรัพย์สินอื่น ๆ ที่มีความสำคัญของสถานศึกษา โดยดำเนินการ นำมาใช้ ตรวจสอบ วัดผล ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารการรักษาความปลอดภัย เพื่อให้สถานศึกษารอดพ้นจากภัยคุกคามต่าง ๆ โดใช้หลัก Plan-Do-Check-Act (PDCA Model) มีแกนหลักในการดำเนินการ 11 ด้าน 105 ตัวบ่งชี้ กระบวนการในการกำหนดนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องใช้การบริหารจัดการจัดการ ด้านเทคโนโลยี การบริหารจัดการทรัพยากรมนุษย์ ผู้บริหารระดับสูงต้องมีการอนุมัติแต่งตั้งคณะทำงานอย่างเป็นลายลักษณ์อักษรและมีการกำหนดภารกิจหน้าที่อย่างชัดเจนเพื่อ

ร่วมกันกำหนด นโยบาย ดำเนินงาน และการติดตามประเมินผล เพื่อให้เกิดความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร บุคลากร เพื่อให้ภารกิจในการเรียนการสอน การบริหารสถานศึกษา และการบริหารชุมชนให้ดำเนินไปอย่างต่อเนื่อง พร้อมใช้งานมี ความถูกต้องสมบูรณ์ และควบคุมการเข้าสู่ชั้นความลับของฐานข้อมูลได้อย่างมีประสิทธิภาพ คณะผู้บริหาร ผู้บริหารระดับสูงต้องตั้งคณะกรรมการจากทุกหน่วยงานที่เกี่ยวข้องเป็นคณะทำงาน ตามแนวทางดำเนินงาน 11 ด้านประกอบด้วย 105 ตัวบ่งชี้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และดำเนินการตามตัวแบบ การจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

“Ed-SAM” (Education Security Assessment Model)”

ความร่วมมือ	
ผู้บริหาร	
ผู้ปฏิบัติการ ผู้ใช้งาน	
Plan Do Check Act	105 ตัวบ่งชี้
11) การปฏิบัติตามข้อกำหนด	5
10) การบริหารความต่อเนื่อง	3
9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง	5
8) การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ	7
7) การควบคุมการเข้าถึง	29
6) การบริหารจัดการด้านการสื่อสาร	19
5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	10
4) นโยบายการบริหารจัดการทรัพย์สิน	9
3) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร	4
2) โครงสร้างความมั่นคงปลอดภัยขององค์กร	5
1) นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ	9
Plan Do Check Act	
ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล การสื่อสาร บุคคลากร	
Commitment Human Unity Management Procedure Habit Organization Technology	

ภาพที่ 11 “Ed-SAM” รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา (Education Security Assessment Model) หรือ Ed-SAM เป็นเครื่องมือประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศด้วยตนเอง โดยต้องมีความร่วมมือกันอย่างมุ่งมั่นและต่อเนื่องของผู้บริหาร ผู้ปฏิบัติการและผู้ใช้ โดยใช้กระบวนการ PDCA วางแผน ดำเนินการ

ตรวจสอบ ปรับปรุง ให้ระบบฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล การสื่อสาร บุคลากร ของมหาวิทยาลัย ดำเนินภารกิจได้อย่างถูกต้องและต่อเนื่อง โดยมี การบริหารจัดการองค์กรและเทคโนโลยี มีข้อตกลง มีพันธะสัญญาของบุคลากรที่เกี่ยวข้อง ร่วมแรงร่วมใจอย่างมุ่งมั่น ดำเนินตามขั้นตอน มีแนวทางการประเมิน 11 ด้าน รวม 105 ตัวบ่งชี้ ลำดับความสำคัญในแต่ละด้านของตัวบ่งชี้ได้ ทราบผล และแนวทางแก้ไข ได้อย่างรวดเร็วและประหยัดงบประมาณ

สรุปขั้นตอนการวิจัย 2 (R2) ดำเนินการทดลองการใช้รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้นโดยทำการทดสอบรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา
ผู้วิจัยได้นำรูปแบบไปทดลองใช้ โดยการนำรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาที่พัฒนาขึ้นนี้ ไปทำการประเมิน กับมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ได้ผลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อยู่ในระดับดี และเปรียบเทียบกับการประเมินด้วย มาตรฐานสากล ISO 27001 ได้ผลออกมา ในระดับ ดี เช่นกัน ซึ่งผลลัพธ์ออกมาสอดคล้องกัน สามารถนำไปใช้งานได้

สรุปขั้นตอนการพัฒนา 2 (D2) ดำเนินการปรับปรุงรูปแบบการประเมินการความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ที่สร้างขึ้น ได้มีการพัฒนาโปรแกรมสำเร็จรูปเพื่อให้มีการใช้งานที่ง่ายและสะดวกขึ้น โปรแกรมจะอธิบายขั้นตอนต่าง ๆ รวมถึงความรู้ทั่วไป ความรู้ในการแก้ไขปัญหาต่าง ๆ กฎระเบียบต่าง ๆ ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทำให้ผู้ใช้งานที่มีความรู้พื้นฐานด้านสารสนเทศ สามารถเข้าใจ และทำการประเมินได้ด้วยตนเอง และทราบผลอย่างรวดเร็ว และทราบวิธีการที่จะต้องปรับปรุงแก้ไขในแต่ละเหตุการณ์ที่เกิดขึ้น จุดเด่นของรูปแบบประเมินนี้ จะแสดงผลลำดับความสำคัญของแต่ละตัวบ่งชี้ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในสถาบันการศึกษา ทำให้ผู้บริหารสามารถจัดลำดับความสำคัญในการบริหารจัดการได้อย่างเหมาะสม

อภิปรายผลการวิจัย

สรุปผลการวิจัยขั้นต้น สามารถนำมาอภิปรายผล เรื่องรูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา สามารถอภิปรายผลเป็น 2 ตอนดังนี้

1. ผลการศึกษาสถานภาพ ปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา

สถานภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้แก่

1. นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2. งบประมาณสำหรับความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ
3. สิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
4. บุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
5. พฤติกรรมผู้ใช้งานที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นปัจจัยที่มีความจำเป็นมากในการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และผลจากการวิจัย พบว่าปัจจัยทั้งหมดนี้ สอดคล้องกับ มาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศแบบสากล ISO/IEC27001 และสอดคล้องกับ งานวิจัยเรื่อง ทัศนคติเกี่ยวกับการนำมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO 27001) มาใช้ในองค์กร กรณีศึกษาอุตสาหกรรมอิเล็คทรอนิคส์ในประเทศไทย ผลการศึกษาพบว่า ส่วนใหญ่ไม่มีความรู้ว่ามาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ได้ประกาศใช้แล้ว การสนับสนุนของผู้บริหารระดับสูงในการนำเทคโนโลยีใหม่ ๆ มาใช้ในองค์กรเป็นปัจจัยสนับสนุนที่สำคัญที่สุด ส่วนกฎหมายและข้อบังคับเป็นปัจจัยสนับสนุนที่สำคัญน้อยที่สุด ด้านปัญหาอุปสรรค ขาดนโยบายจากผู้บริหารเป็นอุปสรรคที่สำคัญที่สุด การขาดฮาร์ดแวร์และซอฟท์แวร์เป็นปัญหาน้อยที่สุด ดังนั้นหากผู้บริหารสามารถนำปัจจัยทั้งหมดนี้ เพื่อเป็นแนวทางในการกำหนดนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษาแล้ว ก็จะสามารถเป็นแนวทางในการสร้างความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาได้มั่นคงยิ่งขึ้น

2. ผลการศึกษาและพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

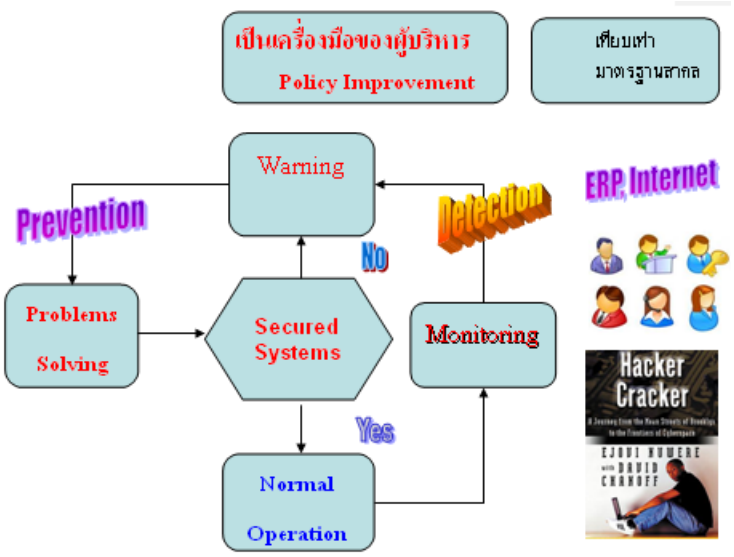
จากศึกษาค้นคว้า อ้างอิงตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สอดคล้องกับ มาตรฐานความมั่นคงปลอดภัยสากล (ภาคผนวก) พระราชบัญญัติความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของประเทศไทย และจากการวิจัยได้พบปัญหาต่าง ๆ รวมถึงการให้ความสำคัญของผู้บริหารในการจัดทำนโยบายความมั่นคงปลอดภัยระบบสารสนเทศในมหาวิทยาลัย และพบว่า

2.1 รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สอดคล้องกับ การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐานความมั่นคงปลอดภัยแบบสากล และพระราชบัญญัติความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของประเทศไทย และมีความสอบคล้องกับงานวิจัยของ เพ็ญประภา พิพัฒนาโฆษิต (2550) ซึ่งได้ศึกษาการสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูลโดยการประยุกต์ใช้ ISO 17799 ของบริษัทให้บริการด้านการจัดซื้อออนไลน์ เพื่อนำเสนอความเสี่ยงในด้านต่างๆ ที่อาจเกิดขึ้น และหาแนวทางการประยุกต์มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO 17799 ที่เหมาะสมมาใช้ โดยเป็นการนำเสนอแก่ผู้บริหารองค์กรให้เห็นถึงความเสี่ยงที่อาจเกิดขึ้น ถ้าไม่มีการบริหารหรือการควบคุมความเสี่ยงและภัยคุกคามต่างๆ ก่อน ซึ่งพบว่าความเสี่ยงในเหตุการณ์ต่างๆ สามารถเรียงตามความเสี่ยงและประเภทของความเสี่ยงทั้ง 3 ประเภทคือ สิทธิในการเข้าถึงข้อมูล ความเชื่อถือ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความสามารถในการนำมาใช้ประโยชน์ได้เมื่อต้องการ (Availability)

มีการนำรูปแบบที่พัฒนาขึ้นไปทดลองใช้ ที่มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา เทียบกับการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐานสากล ผลการทดลองใช้แล้วผู้ใช้ พึงพอใจ และสอดคล้องกับการประเมินโดยมาตรฐานสากล และได้ผลการทดลอง ดังนี้

- มีความง่ายที่จะเรียนรู้
- มีความง่ายในการนำไปใช้
- ได้รับความรู้เพิ่มเติมยิ่งขึ้นในด้านบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
- รวดเร็ว สามารถทราบผลการประเมินได้อย่างรวดเร็ว
- ประหยัด เวลา และงบประมาณ
- ประหยัดค่าใช้จ่าย

สิ่งสำคัญของการต้องมีการประเมินความมั่งปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา เพราะว่า เมื่อมีการตรวจประเมินความมั่นคงระบบเทคโนโลยีสารสนเทศแล้ว ผู้ใช้ที่เป็นผู้ใช้งานปกติหรือผู้ใช้งานที่ไม่ประสงค์กับระบบสารสนเทศ เข้าสู่ระบบ จะมีการตรวจสอบเฝ้าระวัง (Monitor & Detection) หากมีเหตุผิดปกติ ระบบจะมีการแจ้งเตือนให้ทราบและส่งเข้าสู่ระบบป้องกันและแก้ปัญหา (Prevention and Problem Solving) เพื่อให้ระบบมีความมั่นคงปกติ และเข้าสู่การทำงานปกติ แต่หากเกิดเหตุผิดปกติ ระบบจะมีการแจ้งเตือนและป้องกันแก้ปัญหา ดังนั้น ระบบที่มีการตรวจประเมินจะสามารถทำงานได้อย่างต่อเนื่องมีความมั่นคงปลอดภัย



ภาพที่ 12 “Ed-SAM” เป็นเครื่องมือของผู้บริหาร (Policy Improvement)

การรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีความสำคัญยิ่งในการบริหาร เป็นเครื่องมือสำหรับผู้บริหาร เพื่อจัดทำนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Policy Improvement) เป็นการสร้างความมั่นคงและเป็นรากฐานของความมั่นคงทางการศึกษาของประเทศและที่สำคัญที่สุด

รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษาสามารถนำไปปรับใช้กับมหาวิทยาลัยราชภัฏต่าง ๆ มหาวิทยาลัยต่าง ๆ และโรงเรียนหรือสถานศึกษาต่างๆได้จะเป็นประโยชน์ในการสร้างความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและประหยัดงบประมาณได้จำนวนมาก ดังภาพ

ภาพที่ 13 “Ed-SAM” เป็นเครื่องมือเพื่อสร้างรากฐานของความมั่นคงทางการศึกษา

ข้อเสนอแนะ

ข้อเสนอแนะเพื่อปฏิบัติ

1. สถาบันการศึกษา สามารถกำหนดทิศทางนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่ชัดเจน ในการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยมีการสื่อสารและจัดตั้งทีมงานทั้งจากภายในสถาบันการศึกษาและจากภายนอกสถาบันการศึกษา ข้อมูลสารสนเทศ ข่าวสารประชาสัมพันธ์ การกำหนดนโยบายร่วมกัน เพื่อสร้างความเข้าใจอันดี และ การยอมรับของบุคลากรในแต่ละสถาบันการศึกษาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อให้มหาวิทยาลัยมีความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ยิ่งขึ้น

2. การประเมินระบบเทคโนโลยีสารสนเทศ ควรดำเนินการโดยคณะกรรมการอิสระที่ได้รับการแต่งตั้งอย่างเป็นลายลักษณ์อักษรจากผู้บริหารเพื่อเข้ามาตรวจประเมินเพื่อให้เกิดความโปร่งใสในการพิจารณาข้อมูลอ้างอิงเพื่อตรวจสอบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. ผู้สนใจและผู้บริหาร สามารถนำตัวชี้วัดนี้ไปใช้ดำเนินการเป็นการวิจัยและพัฒนาหรือเป็นวิจัยปฏิบัติการ เพื่อพัฒนาตัวบ่งชี้อื่น ๆ ให้คลอบคลุมความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศได้มากขึ้น

2. สถาบันการศึกษาต่าง ๆ สามารถนำแนวทางการพัฒนารูปแบบการประเมินนี้ ไปพัฒนารูปแบบการประเมินด้านอื่น ๆ เพื่อเป็นเครื่องมือบริหารระบบอื่น ๆ ได้มากยิ่งขึ้น

3. ทำการวิจัยต่อเนื่องโดยนำเสนอเป็นรูปแบบ ใยแมงมุม สำหรับตัวบ่งชี้ 11 ด้าน กับกับแต่ละมหาวิทยาลัย เพื่อนำมาปรับปรุงสร้างความมั่นคงปลอดภัยในสถาบันการศึกษาให้กว้างขวางยิ่งขึ้น

4. นำไปปรับใช้ในสถาบันการศึกษา ระดับโรงเรียน ต่าง ๆ

บรรณานุกรม

โครงการจัดทำแผนแม่บท ICT Security แห่งชาติ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, บทที่ 6 แผนปฏิบัติการโครงการเร่งด่วน. ค้นเมื่อวันที่ 19 มกราคม 2555. จาก http://security.mict.go.th/plan/ร่างแผนแม่บท%20ICT%20Security%20แห่งชาติ/pdf_file/บทที่%206.pdf

จตุชัย แพงจันทร์. (2550). **Master in Security**. (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร : อินโฟเพรส.

จิตสุนันท์ เพชรก้อน, (2549). **ทัศนคติเกี่ยวกับการนำมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC 27001:2005) มาใช้ในองค์กรกรณีศึกษาอุตสาหกรรมอิเล็กทรอนิกส์ในประเทศไทย.** บริหารธุรกิจมหาบัณฑิต สาขาบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

ชนม์ชนก วีรวรรณ. (2541). **การใช้เทคโนโลยีสารสนเทศ ในหน่วยงานของรัฐ : จากปัญหาที่มีอยู่การปกครองที่ดี. วารสาร NECTEC**, 5, น.65-77.

ชัยยศ สันติวงศ์ และนิตยา เจริยงประเสริฐ. (2546). **การบริหารระบบสารสนเทศเชิงกลยุทธ์**. กรุงเทพมหานคร : ประชุมช่าง.

ชัชพงศ์ วงษ์สุข และ ปรีชา ปลื้มจิต. **เอกสารประกอบการบรรยาย Competency Assessment.** (ออนไลน์) กรุงเทพมหานคร : สำนักจัดการความรู้ กรมควบคุมโรค กระทรวงสาธารณสุข. จาก www.kmddc.go.th

ทวีป ศิริรัศมี. (2545). **การวางแผนพัฒนาและประเมินโครงการ.** (พิมพ์ครั้งที่ 3). กรุงเทพมหานคร : สำนักงานกองทุนสนับสนุนการวิจัย.

ทรงชล มหารมณ์. (2548). **การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสำหรับองค์กรขนาดกลางและขนาดใหญ่ในเขตกรุงเทพมหานคร.** กรุงเทพมหานคร: วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์.

นริทธ์ จินดาจามร. (2550) **การศึกษาและจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามพระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็คทรอนิคส์ พ.ศ.2544**./นริทธ์ จินดาจามร, ขวัญตา วรรณโภคิน, อรรฆพล คุ้มเศรณี. กรุงเทพมหานคร:มหาวิทยาลัยธรรมศาสตร์.

ปทีป เมธาคุณวุฒิ. (2544). **เทคโนโลยีสารสนเทศเพื่อการบริหารสถาบันอุดมศึกษา**. กรุงเทพมหานคร : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ผกากรอง บ่ายสว่างและคณะ, 2552.**แนวทางในการวางระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก.** วิทยาศาสตร์มหาบัณฑิต สาขาวิชาระบบสารสนเทศคอมพิวเตอร์ มหาวิทยาลัยศรีปทุม.

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสำหรับประเทศไทย. (2550). ค้นเมื่อวันที่ 19 มกราคม 2555. จาก http://www.nectec.or.th/ paper/basic/Book_2.5_FullVersion.pdf

พงศักดิ์ ผกามาศ. (2553). **ระบบไอซีทีและการจัดการยุคใหม่.** กรุงเทพมหานคร : วิตตี้กรุ๊ป.

พนิดา พานิชกุล. (2553). **ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ.** กรุงเทพมหานคร : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

พรพิไล เลิศวิชา. (2541, พ.ค.). **การประเมินผลการใช้อินเตอร์เน็ต.** ไอที ปริทัศน์, *6* (5), 7-9.

พลสัณห์ โพธิ์ศรีทอง. (2547). **มหาวิทยาลัยราชภัฏ: หุ้นส่วนเพื่อการพัฒนาสังคมแห่งอนาคต.** ในเอกสารการประชุมวิชาการ เรื่อง มหาวิทยาลัยราชภัฏ: หุ้นส่วนเพื่อการพัฒนาสังคมแห่งอนาคต 27-28 พฤศจิกายน 2546 โรงแรมรอยัลริเวอร์ กรุงเทพมหานคร.

เพ็ญประภา พิพัฒนาโฆษิต. (2550). **การสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูล โดยการประยุกต์ใช้ ISO 17799 : กรณีศึกษา ของบริษัทให้บริการด้านการจัดซื้อออนไลน์.** กรุงเทพมหานคร : วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์.

พระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ.2547. (2553). ค้นเมื่อวันที่ 10 พฤศจิกายน 2554. จาก http: //www.kodmhai.com/m4/m4-11/New1/N1.html

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (2551). ค้นเมื่อวันที่ 20 พฤศจิกายน 2554. จาก http://www.thaiall.com/article/law.htm.

พิสณุ ฟองศรี. (2552). **การสร้างและพัฒนาเครื่องมือ**. กรุงเทพมหานคร : ด่านสุทธาการพิมพ์.

ภาคภูมิ ปรีชาพานิช, 2550. **“การพัฒนาตัวแบบความมั่นคงปลอดภัยของเว็บเซอร์วิสสำหรับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร”**.บริหารธุรกิจมหาบัณฑิต สาขาวิชาพาณิชย์อิเล็กทรอนิคส์ มหาวิทยาลัยศรีปทุม.

มหาวิทยาลัยราชภัฏจันทรเกษม. (2555). **ประวัติมหาวิทยาลัยราชภัฏจันทรเกษม.** ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.chandra.ac.th

มหาวิทยาลัยราชภัฏธนบุรี. (2555). **ประวัติมหาวิทยาลัยราชภัฏธนบุรี.** ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.dru.ac.th

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา. (2555). **ประวัติมหาวิทยาลัยราชภัฏบ้านสมเด็จ-เจ้าพระยา**. ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.bsru.ac.th

มหาวิทยาลัยราชภัฏพระนคร. (2555). **ประวัติมหาวิทยาลัยราชภัฏพระนคร.** ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.pnru.ac.th

มหาวิทยาลัยราชภัฏสวนดุสิต. (2555). **ประวัติมหาวิทยาลัยราชภัฏสวนดุสิต.** ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.dusit.ac.th

มหาวิทยาลัยราชภัฏสวนสุนันทา. (2555). **ประวัติมหาวิทยาลัยราชภัฏสวนสุนันทา.** ค้นเมื่อวันที่ 20 กันยายน 2555. จาก http://www.ssru.ac.th

มาตรฐานด้านเทคโนโลยีสารสนเทศในประเทศไทย. (2550). ค้นเมื่อวันที่ 19 มกราคม 2550. จาก http://www. paper/basic/Book_2.5_FullVersion.pdf

เยาวดี รางชัยกุล วิบูลย์ศรี. (2544). **การประเมินโครงการ : แนวคิดและปฏิบัติ.** กรุงเทพมหานคร : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

เยาวดี รางชัยกูล. (2542). **การประเมินโครงการแนวคิดและแนวปฏิบัติ**. กรุงเทพมหานคร : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ยุวดี เปรมวิชัย. (2550,มกราคม). **การประเมิน (Assessment):** วารสารโรงเรียนนายเรือ**,** 7(1),31-39.

วรรณวดี ชัยชาญกุล. (2552). **การบริหารจัดการมหาวิทยาลัยราชภัฏในอนาคต.** ปริญญานิพนธ์ดุษฎีบัณฑิต. สาขาการศึกษาเพื่อพัฒนาท้องถิ่น. มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา.

วศิน เพิ่มทรัพย์. (2548). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ.** กรุงเทพมหานคร : โปรวิชั่น.

วีระวัฒน์ ปันนิตามัย. (2540, พฤษภาคม-มิถุนายน). **การประเมินผลการปฏิบัติงาน** : แนวพินิจเชิงระบบ. วารสารข้าราชการ. *42* (3), 16-36.

สมคิด พรมจุ้ย. (2550). **เทคนิคการประเมินโครงการ.** (พิมพ์ครั้งที่ 5). นนทบุรี : จตุพร ดีไซน์.

สมบัติ ธำรงธัญวงศ์. (2546). **การบริหารยุคใหม่ในสถาบันอุดมศึกษา.** ในเอกสารการประชุมวิชาการ เรื่อง มหาวิทยาลัยราชภัฏ: หุ้นส่วนเพื่อการพัฒนาสังคมแห่งอนาคต 27-28 พฤศจิกายน 2546 โรงแรมรอยัลริเวอร์ กรุงเทพมหานคร.

สมหวัง พิธิยานุวัฒน์. (2544). **รวมบทความทางการประเมินโครงการ.** (พิมพ์ครั้งที่ 6). กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย.

สมหวัง พิธิยานุวัฒน์. (2544). **วิธีการประเมิน : ศาสตร์แห่งคุณค่า.** กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย.

สมหวัง พิริยานุวัฒน์. **รวมบทความการประเมินโครงการ.** กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย. 2540.

สามารถ อุฤทธิ์. **การเปรียบเทียบค่าความเชื่อมั่นและความเที่ยงตรงของมาตรวัดเจตคติแบบลิเคอร์ท ที่มีข้อความและรูปแบบคำตอบต่างกัน.** (ออนไลน์) กรุงเทพ ฯ : มหาวิทยาลัยรามคำแหง. เข้าถึงได้จาก www.thaidedresearch.org

สุขุม เฉลยทรัพย์. (2551). **เทคโนโลยีสารสนเทศ.** กรุงเทพมหานคร: มหาวิทยาลัยราชภัฏสวนดุสิต.

สุชาดา นิภานันท์. (2547). **เอกสารสอนรายวิชาระบบสารสนเทศเพื่อการจัดการ.** กรุงเทพมหานคร : คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนดุสิต.

(2532). **การศึกษาและวิจัยท้องถิ่นจากหลักการสู่การปฏิบัติ: กรณีวิทยาลัยครูสุรินทร์.** สุรินทร์ : วิทยาลัยครูสุรินทร์.

สุพล วุฒิเสน. (2537, 22-23 กันยายน). **พันธกิจของการศึกษาระดับสูงกว่ามัธยมต่อการพัฒนาประเทศ ช่วงของแผนพัฒนาระยะที่ 8-9-10.** การจัดการศึกษาระดับอุดมศึกษาไทย. ณ โรงแรมดิเอมเพรส เชียงใหม่.

อลงกรณ์ มีสุทธา. (2551). **การประเมินผล.** (ฉบับปรับปรุง). กรุงเทพมหานคร : สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น).

โอภาส เอี่ยมสิริวงศ์. (2548). **วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ.** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น.

----------. (2549). **การวิเคราะห์และออกแบบระบบ.** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น

----------. (2551). **วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. (ฉบับปรับปรุงเพิ่มเติม). กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น.

ไอทีของภาครัฐ. (2550). กรุงเทพมหานคร : มหาวิทยาลัยธรรมศาสตร์.

ธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550. ค้นเมื่อวันที่ 16 สิงหาคม

อุทุมพร (ทองอุไทย) จามรมาน. **การวัดและประเมินการเรียนการสอนระดับอุดมศึกษา.** กรุงเทพมหานคร: โรงพิมพ์ฟันนี่พับบลิชชิ่ง. 2530.

ThaiCERT, NECTEC, มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550, http://www.thaicert.nectec.or.th/paper/basic/Book_2.5_FullVersion.pdf

Adams, D. A., Todd, P. A., & Nelson, R. R. (1993). A comparative evaluation of the impact of Electronic and voice mail on organizational communication. **Information & Management**, (24), 19-21.

Alkin, M.C. (1969, October). Evaluation theory development. **Evaluation Comment**, *2*, 1, 1-4.

Alter, S. (2002). **Information Systems : The foundation of E-Business**. (4th ed.). Upper Saddle River NJ : Prentice Hall.

Berghout, E., Nijland, M., & Grant, K. (2005, January). Seven ways to get your favored it project accepted politics in IT evaluation. **The Electronic Journal of Information Systems Evaluation**, *8* (1), 31-40.

Boar, B.H. (2001). **The art of Strategic planning for information technology.** (2nd ed). U.S.A. : Wiley Computer Publishing.

Clerehan, R., Kett, G., Gedge, R., & Tuovinen, J.E. (2003, Quarter). Encouraging IT students to get serious about assignment writing : evaluation of a web-based initiative. **Internet and Higher Education,** *6* (4), 327-346.

Deming, W. E. (1986). **Out of the crisis**. Cambridge, Mass.: Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Daniel L. S. & Anthony J. S. (2007). **Evaluation theory, models & application**. Sanfrancisco : Jossey Bass.

Edwards, M.R. and Ewen, A.J. (1996). **360 feedback the powerful new model for employee assessment performance improvement**. New York : AMACOM American Management Association.

Grembergen, W. V. (2001). **Information technology evaluation methods and management** Hershey, Pa. : Idea Group.

Ives, B. & Olson, M. (1984, May). User involvement and MIS success : a review of research. **Management Science**. *30* (5), 586-603.

Kaplan, R. S. and Norton, D. P. (1992, January-February). The balanced scorecard-measures that drive performance. **Harvard Business Review**, 71-79.

Whitman, M. E. & Mattord, H. J. (2005). **Principles of information security**. Boston : Thomson Course Technology.

Stair, R.M. & Reynolds, G.W. (2001). **Principles of information systems**. (5th ed.). Boston : Course Technology.

Stallings, W. (2000). **Data and computer communications**. (6th ed.). Englewood Cliff NJ : Prentice Hall.

Stufflebeam, D.L. & Shinkfield, A.J. (1985). **Systematic evaluation.** Boston : Kluwer Nijhoff.

ภาคผนวก

ภาคผนวก ก

รายนามผู้เชี่ยวชาญและผู้ให้สัมภาษณ์

รายนามผู้เชี่ยวชาญตรวจสอบเครื่องมือวิจัย

1. ผู้ช่วยศาสตราจารย์ นายแพทย์ พรณรงค์ โชติวรรณ	คณะแพทย์ศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
2. รองศาสตราจารย์สุรศักดิ์ สงวนพงษ์	ผู้ช่วยอธิการบดี มหาวิทยาลัยเกษตรศาสตร์
3. ผู้ช่วยศาสตราจารย์ ดร.สุรางคนา ธรรมลิขิต	ผู้อำนวยการสำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา
4. ผู้ช่วยศาสตราจารย์ ดร.ฐัศแก้ว ศรีสด	อาจารย์ประจำคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏธนบุรี
5. ผู้ช่วยศาสตราจารย์ ดร.ศิรินุช เทียนรุ่งโรจน์	ผู้อำนวยการสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร
6. อาจารย์เสถียร จันทร์ปลา	ผู้อำนวยการสำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
7. นายอโณทัย อรุณเรือง	นักวิชาการคอมพิวเตอร์ ผู้ดูแลระบบ มหาวิทยาลัยราชภัฏสวนสุนันทา

รายชื่อผู้เชี่ยวชาญด้านบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ผู้ให้สัมภาษณ์

1.	ผู้ช่วยศาสตราจารย์ จันทรัตน์ กิ่งแสง	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยี สารสนเทศ มหาวิทยาลัยราชภัฏจันทรเกษม
2.	อาจารย์พัชนี เดชประเสริฐ	ผู้อำนวยการศูนย์คอมพิวเตอร์ มหาวิทยาลัยราชภัฏธนบุรี
3.	ผู้ช่วยศาสตราจารย์ชลิต วณิชยานันต์	ผู้อำนวยการศูนย์คอมพิวเตอร์ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา
4.	ผู้ช่วยศาสตราจารย์ อารีย์ รังสิโยภาส	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยี สารสนเทศ มหาวิทยาลัยราชภัฏพระนคร
5.	นายวีระพันธ์ ชมพูแดง	รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยี สารสนเทศ มหาวิทยาลัยราชภัฏสวนดุสิต
6.	อาจารย์เสถียร จันทร์ปลา	ผู้อำนวยการศูนย์คอมพิวเตอร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

รายชื่อผู้เชี่ยวชาญดูแลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ผู้ให้สัมภาษณ์

1.	อาจารย์เกียรติพงษ์ ยอดเยี่ยมแกร	มหาวิทยาลัยราชภัฏจันทรเกษม
2.	นายสันติ พิมพ์สว่าง	มหาวิทยาลัยราชภัฏธนบุรี
3.	นายนพฤทธิ์ จันทร์กิ่ง	มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา
4.	นายเอกสิทธิ์ บุรณะชีวิน	มหาวิทยาลัยราชภัฏพระนคร
5.	นายจิรพงษ์ กิจเกียรติ์	มหาวิทยาลัยราชภัฏสวนดุสิต
6.	นายอโณทัย อรุณเรือง	มหาวิทยาลัยราชภัฏสวนสุนันทา

ภาคผนวก ข
ผลการวิเคราะห์เครื่องมือ

ตารางสรุป แสดงค่าดัชนีความสอดคล้องระหว่างข้อคำถามวัตถุประสงค์ (สำหรับผู้บริหารระบบเทคโนโลยีสารสนเทศ)
(Index of item objective Congruence: IOC) โดยผู้เชี่ยวชาญ 5 คน

ประเด็นการสัมภาษณ์/ข้อถาม	ผลการพิจารณาความสอบคล้องของผู้เชี่ยวชาญ จำนวน (N=5)							
	1	2	3	4	5	รวม	IOC	สรุป
1 นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.1 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ								
1.2 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.3 มีการจัดการให้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการบริหาร	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.4 มีการสื่อสารและประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับขององค์กรได้ทราบอย่างทั่วถึงผ่านช่องทางที่หลากหลาย	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.5 ผู้บริหารมีการสื่อสารแสดงความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.6 มีการจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไว้ในที่ที่ผู้ใช้งานหรือบุคลากรที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.7 มีการให้บุคลากรภายในองค์กรแต่ละหน่วยงาน มีส่วนร่วมในการจัดทำนโยบาย	+1	+1	+1	+1	+1	+5	1	ผ่าน
1.8 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันสอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง	+1	+1	+1	+1	+1	+5	1	ผ่าน
2. โครงสร้างความมั่นคงปลอดภัยขององค์กร								
2.1 มีโครงสร้างความมั่นคงปลอดภัยขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
2.2 ผู้บริหารให้ความสำคัญและสนับสนุนในการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน	+1	+1	+1	+1	+1	+5	1	ผ่าน
2.3 มีการจัดการให้มีขั้นตอนในการอนุมัติการใช้งาน การพัฒนาหรือปรับปรุงเปลี่ยนแปลงระบบงานคอมพิวเตอร์	+1	+1	+1	+1	+1	+5	1	ผ่าน
2.4 มีการจัดการให้มีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความเกี่ยวข้องในด้านการรักษาความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศ เช่น เนคเทค สำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ	+1	+1	+1	+1	+1	+5	1	ผ่าน
2.5 มีการตรวจสอบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ จากผู้ตรวจสอบอิสระภายนอก	+1	+1	+1	+1	+1	+5	1	ผ่าน
3 นโยบายบริหารจัดการทรัพย์สิน								
3.1 มีนโยบายบริหารจัดการทรัพย์สิน	+1	+1	+1	+1	+1	+5	1	ผ่าน

	1	2	3	4	5	รวม	IOC	สรุป
4. นโยบายความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร								
4.1 มีนโยบายความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.2 มีการกำหนดให้บุคคลภายในองค์กรหรือหน่วยงานที่องค์กรว่าจ้างจากภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.3 มีกระบวนการทางวินัยเพื่อลงโทษผู้ที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
5. นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม								
5.1 มีนโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	1	2	3	4	5	รวม	IOC	สรุป
6. นโยบายการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร								
6.1 มีนโยบายการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
7. นโยบายการควบคุมการเข้าถึง								
7.1 มีโยบายการควบคุมการเข้าถึง	+1	+1	+1	+1	+1	+5	1	ผ่าน
8. นโยบายการจัดหา การพัฒนาและบำรุงระบบสารสนเทศ								
8.1 มีนโยบายการจัดหา การพัฒนาและบำรุงระบบสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
9. นโยบายการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร								
9. มีนโยบายการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
10. นโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร								
10.1 มีนโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
10.2 มีการประเมินความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศรวมถึงผลกระทบในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ	+1	+1	+1	+1	+1	+5	1	ผ่าน
10.3 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว	+1	+1	+1	+1	+1	+5	1	ผ่าน
10.4 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งานให้เป็นปัจจุบันอยู่เสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน

11. นโยบายการปฏิบัติตามข้อกำหนด								
11.1 มีนโยบายการปฏิบัติตามข้อกำหนด	+1	+1	+1	+1	+1	+5	1	ผ่าน
11.2 มีวิธีปฏิบัติเพื่อให้บุคลากรปฏิบัติตามนโยบายรักษาความมั่นคง	+1	+1	+1	+1	+1	+5	1	ผ่าน

ปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรตามที่กำหนดไว้								
11.3 มีผู้ตรวจสอบภายในและมีผู้ตรวจสอบจากภายนอกเข้ามาตรวจสอบการปฏิบัติงานหรือการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
11.4 มีการกำหนดห้ามละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา	+1	+1	+1	+1	+1	+5	1	ผ่าน
11.5 มีกระบวนการตรวจสอบความปลอดภัยด้านเทคโนโลยีสารสนเทศทั้งจากภายนอกและภายในอย่างสม่ำเสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
11.6 การรวบรวมกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศไว้อย่างครบถ้วน	+1	+1	+1	+1	+1	+5	1	ผ่าน

ตารางสรุป แสดงค่าดัชนีความสอดคล้องระหว่างข้อคำถามวัตถุประสงค์ (สำหรับ ผู้ดูแลระบบเทคโนโลยีสารสนเทศ)
(Index of item objective Congruence: IOC) โดยผู้เชี่ยวชาญ 5 คน

ประเด็นการสัมภาษณ์/ข้อถาม	ผลการพิจารณา ความสอบคล้องของผู้เชี่ยวชาญ จำนวน (N=5)							
	1	2	3	4	5	รวม	IOC	สรุป
1 นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ								
1.1 มีนโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
2. โครงสร้างความมั่นคงปลอดภัยขององค์กร								
2. มีโครงสร้างความมั่นคงปลอดภัยขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
3.การบริหารจัดการทรัพย์สินขององค์กร								
3.1 มีการบริหารจัดการทรัพย์สินขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
3.2 มีการจัดทำและปรับปรุงแก้ไขรายการบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้มีความถูกต้องและเป็นปัจจุบันอยู่เสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
3.3 มีการจัดหมวดหมู่ข้อมูลตามระดับชั้นความลับหรือระดับความสำคัญ	+1	+1	+1	+1	+1	+5	1	ผ่าน
3.4 มีการตรวจสอบรายการบัญชีทรัพย์สินขององค์กรอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง	+1	+1	+1	+1	+1	+5	1	ผ่าน
3.5 มีการจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
4. ด้านความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร								
4.1 มีด้านความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.2 มีการกำหนดหน้าที่ความรับผิดชอบทางด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศให้แก่บุคลากรฝ่ายคอมพิวเตอร์อย่างชัดเจน	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.3 มีการจัดทำขั้นตอนการปฏิบัติงานประจำ ของเจ้าหน้าที่ฝ่ายปฏิบัติการคอมพิวเตอร์ เป็นลายลักษณ์อักษร	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.4 มีการจัดอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.5 มีการยกเลิกสิทธิ์ในการเข้าถึงของพนักงาน เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.6 มีการตรวจสอบ คุณสมบัติ ของผู้สมัคร	+1	+1	+1	+1	+1	+5	1	ผ่าน

4.7 มีการให้พนักงานได้รับการอบรมเพื่อสร้างความตระหนักและเสริมความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
4.8 มีการให้พนักงานคืนทรัพย์สินที่อยู่ในความครอบครอง เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
5. ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม								
5. มีการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.1 มีอุปกรณ์ป้องกันไฟฟ้าขัดข้อง เช่นเครื่องสำรองไฟฟ้า ยูพีเอส เครื่องกำเนิดไฟฟ้าสำรอง	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.2 มีการบำรุงรักษาอุปกรณ์ป้องกันการล้มเหลวและอุปกรณ์สนับสนุนให้สามารถทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.3 มีอุปกรณ์ป้องกันไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน และอยู่ในสภาพพร้อมใช้งาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.4 มีอุปกรณ์เตือนไฟไหม้ เช่นเครื่องตรวจจับควัน ตรวจจับความร้อน	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.5 มีการควบคุมอุณหภูมิและความชื้นภายในศูนย์คอมพิวเตอร์ที่แยกจากแอร์รวม	1	2	3	4	5	รวม	IOC	สรุป
5.6 มีการควบคุมการเข้า ออก บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.7 มีการติดตั้งกล้อง CCTV ไว้ในศูนย์ควบคุมระบบคอมพิวเตอร์อย่างเพียงพอ และอยู่ในสภาพพร้อมใช้งาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
5.8 มีการควบคุมบุคลากรอื่นที่มีความจำเป็นต้องเข้ามาปฏิบัติหน้าที่ในศูนย์คอมพิวเตอร์เป็นการชั่วคราว								
5.9 มีข้อแนะนำให้ความระวังและป้องกันอุปกรณ์จากอุบัติเหตุต่าง ๆ เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชนหรือเสี่ยงต่อการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์	+1	+1	+1	+1	+1	+5	1	ผ่าน
6. ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร								
6.1 มีการสำรองข้อมูลและโปรแกรมเป็นประจำ	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.2 มีการนำสื่อที่ใช้ในการบันทึกข้อมูลสำรองเก็บไว้ในสถานที่ปลอดภัย	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.3 มีการเข้ารหัส ข้อมูลสำคัญที่ส่งผ่านเครือข่าย	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.4 มีการบันทึกกิจกรรมหรือเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ โดยมีการเก็บบันทึกไว้อย่างน้อย 90 วัน	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.5 มีการควบคุมการรับส่งสื่อบันทึกที่จัดเก็บไว้ เช่น การตรวจสอบตัวตนของผู้ที่มารับ-ส่ง มีการระบุผู้รับผิดชอบในการติดต่อ	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.6 มีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.7 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.8 มีแผนฉุกเฉิน เป็นลายลักษณ์อักษรเพื่อรองรับการใช้งานในกรณีระบบล้มเหลว	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.9 มีการทดสอบแผนฉุกเฉิน ว่าสามารถปฏิบัติได้จริง								

6.10 มีระบบป้องกันและตรวจสอบไวรัสที่ครอบคลุมเครือข่ายและลูกข่ายที่สำคัญ	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.11 มีการกำหนดขั้นตอนมาตรฐานในการดำเนินการด้านการสื่อสารและเครือข่ายแต่ละประเภท	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.12 มีการควบคุมไม่ให้ผู้ใช้งานระงับการใช้งาน ระบบป้องกันไวรัสที่ติดตั้งไว้	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.13 มีวิธีการจัดการสื่อบันทึกข้อมูลลับ ที่ไม่ได้ใช้แล้ว	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.14 มีการปรับปรุง Virus Signature ให้เป็นปัจจุบัน	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.15 มีการจัดการให้ระบบปฏิบัติการจริง แยกออกจากระบบที่ใช้ในการพัฒนาหรือทดสอบ	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.16 มีการกำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรการรองรับเพื่อป้องกันปัญหาจากการแลกเปลี่ยนสารสนเทศระหว่างองค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.17 มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.18 มีการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง	+1	+1	+1	+1	+1	+5	1	ผ่าน
6.19 มีการจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานรวมถึงแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ ๆ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7. ด้านการควบคุมการเข้าถึง								
7.1 มีนโยบายควบคุมการเข้าถึงระบบอย่างเป็นลายลักษณ์อักษร มีการกำหนดสิทธิ์การใช้ข้อมูลระบบคอมพิวเตอร์โดยให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.2 มีระบบที่ป้องกันการบุกรุก เช่น firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.3 มีนโยบายควบคุมไม่ให้ข้อมูลมีความสำคัญถูกนำออกภายนอกองค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.4 มีระบบบริหารจัดการรหัสผ่าน สำหรับผู้ใช้ อย่างมีประสิทธิภาพ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.5 มีมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่นกรณีที่ส่งซ่อม ควรลบข้อมูลที่เก็บไว้ในสื่อบันทึกก่อนส่งซ่อม	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.6 มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงและโอนย้ายระบบงาน และทดสอบระบบงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.7 มีการควบคุมและจำกัดการใช้งาน software utility สำหรับระบบงานคอมพิวเตอร์ application system	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.8 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้อง ครบถ้วนและทำงานที่มีประสิทธิภาพ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.9 มีการจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่น เอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบและคู่มือในการใช้งาน เป็นต้น	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.10 มีการควบคุมการแชร์ไฟล์ ข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ส่วนบุคคล กำหนดรหัสผ่าน กำหนดสิทธิ์ให้เฉพาะรายที่จำเป็นเท่านั้น	1	2	3	4	5	รวม	IOC	สรุป

7.11 มีการควบคุมผู้ให้บริการ (IT Outsourcing) ในการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลสารสนเทศขององค์กร	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.12 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.13 มีการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร เมื่อมีการร้องขอให้มีการพัฒนาหรือแก้ไข เปลี่ยนแปลงระบบงานคอมพิวเตอร์	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.14 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.15 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.16 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ในหน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.17 มีนโยบายในการควบคุมการเข้าถึงระบบให้เป็นปัจจุบันอยู่เสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.18 มีการกำหนดและทบทวนสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่การโอนย้ายส่วนงานหรือลาออกอย่างสม่ำเสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.19 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่นสิทธิ์การใช้โปรแกรม และระบบงานคอมพิวเตอร์ Application System สิทธิ์การใช้งานอินเทอร์เน็ต	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.20 มีระบบบังคับอายุของรหัสผ่าน เช่น ตั้งรหัสผ่านให้ยากแก่การคาดเดา บังคับไม่ให้ใช้รหัสผ่านซ้ำของเดิม ระบบล๊อคอัตโนมัติ ในกรณีที่ป้อนรหัสผิดและไม่มีการใช้งานหน้าจอเป็นระยะเวลาหนึ่ง	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.21 มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.22 มีการที่ระบบจะทำการล๊อกหน้าจออัตโนมัติ เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลาหนึ่ง	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.23 มีการบังคับให้ผู้ใช้งาน เปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกหรือเมื่อถูก reset password	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.24 มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่ประกอบไปด้วยขอบเขตของเครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่าง ๆ	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.25 มีการบังคับความยาวขั้นต่ำของรหัสผ่าน	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.26 มีการดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานที่สำคัญเพื่อดูช่องโหว่ต่าง ๆ ของโปรแกรมระบบ system software management	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.27 มีการกำหนดบุคคล ให้สามารถแก้ไขข้อมูลในฐานข้อมูลได้โดยตรงโดยไม่ผ่านระบบงาน system application	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.28 มีการควบคุมการดำเนินการ ในการพัฒนาหรือแก้ไขระบบงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
7.29 มีการแบ่งแยกเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น การแบ่ง	+1	+1	+1	+1	+1	+5	1	ผ่าน

ระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ต กับระบบที่เชื่อมต่ออินทราเน็ต								
8. ด้านการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ								
8.1 มีขั้นตอนหรือวิธีปฏิบัติ และควบคุมในการพัฒนาหรือแก้ไข เปลี่ยนแปลง โอนย้าย และทดสอบระบบงาน	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.2 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้อง ครบถ้วนและทำงานที่มีประสิทธิภาพ	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.3 มีการได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรและจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน เป็นต้น	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.4 มีการวิเคราะห์และประเมินผลกระทบที่เกี่ยวข้องในการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.5 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ในหน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.6 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.7 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล	+1	+1	+1	+1	+1	+5	1	ผ่าน
8.10 การมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ Storage นำเข้า input ประมวลผล process และแสดงผล output ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน	+1	+1	+1	+1	+1	+5	1	ผ่าน
9. ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร								
9.1 มีมาตรการป้องกันและจำกัดสิทธิ์การเข้าถึง การแก้ไข เปลี่ยนแปลง บันทึกต่าง ให้กับบุคคลที่เกี่ยวข้องเท่านั้น	+1	+1	+1	+1	+1	+5	1	ผ่าน
9.2 มีการแจ้งให้ผู้เกี่ยวข้องรับทราบทุกครั้ง โดยผ่านช่องทางที่องค์กรได้จัดเตรียมไว้ ในกรณีที่พบเครื่องติดไวรัสบนคอมพิวเตอร์ที่ใช้งานอยู่	+1	+1	+1	+1	+1	+5	1	ผ่าน
9.3 มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย มีการบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก	+1	+1	+1	+1	+1	+5	1	ผ่าน
9.4 มีช่องทางให้พนักงานรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร เช่นเมื่อพบไวรัสบนเครื่องคอมพิวเตอร์	+1	+1	+1	+1	+1	+5	1	ผ่าน
9.5 มีการฝึกซ้อมรับมือกับ เหตุฉุกเฉินในรูปแบบต่าง ๆ	+1	+1	+1	+1	+1	+5	1	ผ่าน
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร								
10.1 มีการประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศรวมถึงผลกระทบในการดำเนินงานขององค์กรเป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ	+1	+1	+1	+1	+1	+5	1	ผ่าน
10.2 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือ	+1	+1	+1	+1	+1	+5	1	ผ่าน

จัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว								
10.3 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งานให้เป็นปัจจุบันอยู่เสมอ	+1	+1	+1	+1	+1	+5	1	ผ่าน

ภาคผนวก ค
เครื่องมือที่ใช้ในการวิจัย

แบบสัมภาษณ์สำหรับผู้บริหารระบบเทคโนโลยีสารสนเทศ ของสถาบันการศึกษา
เรื่อง การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
ของสถาบันการศึกษา

แบบสัมภาษณ์

เรื่อง การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

ตอนที่ 1 สถานสภาพทั่วไป

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องวาง ❑ ที่ตรงกับคุณสมบัติของท่านหรือความเห็นของท่าน

1. เพศ ❑ ชาย ❑ หญิง

2. ประสบการณ์ทำงาน.....ปี

3. สังกัด.....

1. นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.1 ท่านให้ความสำคัญด้านการมีนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อย่างชัดเจน เป็นลายลักษณ์อักษร เป็นปัจจัยสำคัญ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

1.2 ในสถานศึกษานี้ มีการวางนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามมาตรฐานสากล หรือไม่

....มี ....ไม่มี

1.3 มีการดำเนินการอย่างไร.....

2. งบประมาณสำหรับความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ

2.1 ท่านมีให้ความสำคัญด้าน งบประมาณสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญในการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

2.2 ในสถานศึกษานี้ ได้รับงบประมาณสำหรับความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ เพียงพอเพื่อการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

3. สิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3.1 ท่านให้ความสำคัญด้านการมีนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างเป็นลายลักษณ์อักษร เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

3.2 ในสถานศึกษานี้ มีการวางนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างเป็นลายลักษณ์อักษร หรือไม่

.....มี ....ไม่มี

3.3 มีการดำเนินการอย่างไร.....

4. บุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

4.1 ท่านให้ความสำคัญกับ บุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญในการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

4.2 ในสถานศึกษานี้ บุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีความรู้ ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

5. พฤติกรรมผู้ใช้งานเกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

5.1 ท่านให้ความสำคัญ กับพฤติกรรมผู้ใช้งานเกี่ยวกับความมั่นคงปลอดภัยของระบบเป็นปัจจัยสำคัญในการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

5.2 ในสถานศึกษานี้ ผู้ใช้ มีความรู้ ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพียงใด

.....มากที่สุด ....มาก ....ปานกลาง .....น้อย ....น้อยที่สุด

ตอนที่ 2 คำถามเกี่ยวกับตัวแปรด้านการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่อง (1) ถ้าคำถามสอดคล้องระบบ ลงในช่อง (0) ถ้าไม่แน่ใจว่าคำถามสอดคล้องกับระบบหรือไม่ และลงในช่อง (-1) ถ้าคำถามไม่สอดคล้องกับระบบ

แบบสัมภาษณ์ตอนที่ 2 คือคำถาม เกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

คำชี้แจง: ทำเครื่องหมาย ✓ ลงในช่อง (1) ถ้าคำถามสอดคล้อง ลงในช่อง (0) ถ้าไม่แน่ใจว่าคำถามสอดคล้องหรือไม่ และลงในช่อง (-1) ถ้าคำถามไม่สอดคล้อง

ตัวแปรด้านมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	**ระดับความคิดเห็นความสำคัญ**				
	มากที่สุด	**มาก**	**ปานกลาง**	**น้อย**	**น้อยที่สุด**
1 นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ					
1.1 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ					
1.2 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร					
1.3 มีการจัดการให้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการบริหาร					
1.4 มีการสื่อสารและประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับขององค์กรได้ทราบอย่างทั่วถึงผ่านช่องทางที่หลากหลาย					
1.5 ผู้บริหารมีการสื่อสารแสดงความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศอย่างชัดเจน					
1.6 มีการจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไว้ในที่ที่ผู้ใช้งานหรือบุคลากรที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม					
1.7 มีการให้บุคลากรภายในองค์กรแต่ละหน่วยงาน มีส่วนร่วมในการจัดทำนโยบาย					
1.8 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันสอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง					
2. โครงสร้างความมั่นคงปลอดภัยขององค์กร					

2.1 มีโครงสร้างความมั่นคงปลอดภัยขององค์กร					
2.2 ผู้บริหารให้ความสำคัญและสนับสนุนในการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน					
2.3 มีการจัดการให้มีขั้นตอนในการอนุมัติการใช้งาน การพัฒนาหรือปรับปรุงเปลี่ยนแปลงระบบงานคอมพิวเตอร์					
2.4 มีการจัดการให้มีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความเกี่ยวข้องในด้านการรักษาความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศ เช่น เนคเทค สำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ เป็นต้น ในกรณีที่มีความจำเป็น					
2.5 มีการตรวจสอบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ จากผู้ตรวจสอบอิสระภายนอก					
3 นโยบายบริหารจัดการทรัพย์สิน					
3.1 มีนโยบายบริหารจัดการทรัพย์สิน					
4. นโยบายความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร					
4.1 มีนโยบายความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร					
4.2 มีการกำหนดให้บุคคลภายในองค์กรหรือหน่วยงานที่องค์กรว่าจ้างจากภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร					
4.3 มีกระบวนการทางวินัยเพื่อลงโทษผู้ที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร					
5. นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม					
5.1 มีนโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม					
6. นโยบายการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร					
6.1 มีนโยบายการบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร					
7. นโยบายการควบคุมการเข้าถึง					
7.1 มีโยบายการควบคุมการเข้าถึง					
8. นโยบายการจัดหา การพัฒนาและบำรุงระบบสารสนเทศ					
8.1 มีนโยบายการจัดหา การพัฒนาและบำรุงระบบสารสนเทศ					
9. นโยบายการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร					
9. มีนโยบายการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร					

10. นโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร					
10.1 มีนโยบายการบริหารความต่อเนื่องในการดำเนินงานขององค์กร					
10.2 มีการประเมินความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศ รวมถึงผลกระทบในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ					
10.3 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว					
10.4 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งาน ให้เป็นปัจจุบันอยู่เสมอ					
11. นโยบายการปฏิบัติตามข้อกำหนด					
11.1 มีนโยบายการปฏิบัติตามข้อกำหนด					
11.2 มีวิธีปฏิบัติเพื่อให้บุคลากรปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรตามที่กำหนดไว้					
11.3 มีผู้ตรวจสอบภายในและมีผู้ตรวจสอบจากภายนอกเข้ามาตรวจสอบการปฏิบัติงานหรือการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ					
11.4 มีการกำหนดห้ามละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา					
11.5 มีกระบวนการตรวจสอบความปลอดภัยด้านเทคโนโลยีสารสนเทศทั้งจากภายนอกและภายในอย่างสม่ำเสมอ					
11.6 การรวบรวมกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศไว้อย่างครบถ้วน					

แบบสัมภาษณ์

เรื่อง การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
สำหรับสถาบันการศึกษา

ตอนที่ 1 สถานสภาพทั่วไป

สำหรับผู้เชี่ยวชาญดูแลระบบเทคโนโลยีสารสนเทศ

คำชี้แจง

แบบสัมภาษณ์ชุดนี้เป็นแบบสัมภาษณ์เกี่ยวกับการพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา
โดยมีวัตถุประสงค์เพื่อทราบความคิดเห็นของท่าน แบบสัมภาษณ์ชุดนี้เป็นแบบมาตราส่วนประเมินค่าชนิด 5 ระดับ จึงขอความอนุเคราะห์จากท่านโปรดให้ข้อมูลที่ตรงกับระดับความคิดเห็นของท่านเพื่อที่จะได้นำข้อมูลที่ได้ไปพัฒนารูปแบบต่อไป
แบบสัมภาษณ์แบ่งเป็น 2 ตอน ได้แก่

ตอนที่ 1 แบบสัมภาษณ์สภาพทั่วไปของผู้ตอบแบบสัมภาษณ์

ตอนที่ 2 แบบสัมภาษณ์เกี่ยวกับตัวแปรด้านการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศและการสื่อสาร

โปรดทำเครื่องหมาย √ ลงในแบบสัมภาษณ์ที่ตรงกับข้อความที่เป็นจริงหรือตรงกับระดับความคิดเห็นของท่านมากที่สุด โดยตัวเลขของระดับความคิดเห็นแต่ละด้านมีความหมายดังนี้

5 หมายถึง ระดับความสำคัญของกิจกรรม มีความ สำคัญมากที่สุด
4 หมายถึง ระดับความสำคัญของกิจกรรม มีความ สำคัญมาก
3 หมายถึง ระดับความสำคัญของกิจกรรม มีความ สำคัญปานกลาง
2 หมายถึง ระดับความสำคัญของกิจกรรม มีความ สำคัญน้อย
1 หมายถึง ระดับความสำคัญของกิจกรรม มีความ สำคัญน้อยที่สุด

ตอนที่ 1 สถานสภาพทั่วไป

1. เพศ … ชาย .... หญิง
2. ประสบการณ์ทำงาน.....ปี
3. สังกัด…….
4. ตำแหน่ง……

ตอนที่ 2 คำถามเกี่ยวกับตัวแปรด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตัวบ่งชี้ความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศ	**ระดับความคิดเห็นความสำคัญ**				
	สำคัญมากที่สุด (5)	สำคัญมาก (4)	สำคัญปานกลาง (3)	สำคัญน้อย (2)	สำคัญน้อยที่สุด (1)
1. นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ					
1.1 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร					
1.2 มีการจัดการให้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการบริหาร					
1.3 มีการสื่อสารและประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับขององค์กรได้ทราบอย่างทั่วถึงผ่านช่องทางที่หลากหลาย					
1.4 มีการประเมินความรู้ความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในองค์กร					
1.5 มีนโยบายให้ดำเนินการสื่อสารหรือให้ความรู้เกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศแก่ผู้ใต้บังคับบัญชา					
1.6 มีการให้บุคลากรภายในองค์กรแต่ละหน่วยงานที่ใช้งานมีส่วนร่วมในการจัดทำหรือทบทวนนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ					
1.7 ผู้บริหารมีการสื่อสารแสดงความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศอย่างชัดเจน					
1.8 มีการจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไว้ในที่ที่ผู้ใช้งานหรือบุคลากร					

ที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม					
1.9 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบัน สอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง					
2. โครงสร้างความมั่นคงปลอดภัยขององค์กร					
2.1 ผู้บริหารให้ความสำคัญและสนับสนุนในการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน					
2.2 มีการจัดการให้มีขั้นตอนในการอนุมัติการใช้งาน การพัฒนาหรือปรับปรุงเปลี่ยนแปลงระบบงานคอมพิวเตอร์					
2.3 มีการจัดการให้มีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความเกี่ยวข้องในด้านการรักษาความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศอื่น ๆ ในกรณีที่มีความจำเป็น					
2.4 มีการทบทวนด้านความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบอิสระ					
2.5 มีระเบียบข้อบังคับในเอกสารรับพนักงาน ห้ามมิให้พนักงานที่เข้ามาทำงานในองค์กร เปิดเผยความลับและข้อมูลขององค์กร					
3. ด้านการบริหารจัดการทรัพย์สินขององค์กร					
3.1 มีการจัดทำและปรับปรุงแก้ไขรายการบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้มีความถูกต้องและเป็นปัจจุบันอยู่เสมอ					
3.2 มีการจัดหมวดหมู่ข้อมูลตามระดับชั้นความลับหรือระดับความสำคัญ					
3.3 มีการตรวจสอบรายการบัญชีทรัพย์สินขององค์กรอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง					
3.4 มีการจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ					
4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร					
4.1 มีการกำหนดหน้าที่ความรับผิดชอบทางด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศให้แก่บุคลากรฝ่ายคอมพิวเตอร์อย่างชัดเจน					
4.2 มีการจัดทำขั้นตอนการปฏิบัติงานประจำ ของเจ้าหน้าที่					

ฝ่ายปฏิบัติการคอมพิวเตอร์ เป็นลายลักษณ์อักษร					
4.3 มีการจัดอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ					
4.4 มีการยกเลิกสิทธิ์ในการเข้าถึงของพนักงาน เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน					
4.5 มีการกำหนดให้บุคคลภายในองค์กรหรือหน่วยงานที่องค์กรว่าจ้างจากภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร					
4.6 มีการตรวจสอบ คุณสมบัติ ของผู้สมัคร					
4.7 มีการให้พนักงานได้รับการอบรมเพื่อสร้างความตระหนักและเสริมความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ					
4.8 มีการให้พนักงานคืนทรัพย์สินที่อยู่ในความครอบครองเมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน 4.9 มีกระบวนการทางวินัยเพื่อลงโทษผู้ที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร					
5. ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม					
5.1 มีอุปกรณ์ป้องกันไฟฟ้าขัดข้อง เช่นเครื่องสำรองไฟฟ้า ยูพีเอส เครื่องกำเนิดไฟฟ้าสำรอง					
5.2 มีการบำรุงรักษาอุปกรณ์ป้องกันการล้มเหลวและอุปกรณ์สนับสนุนให้สามารถทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน					
5.3 มีอุปกรณ์ป้องกันไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน และอยู่ในสภาพพร้อมใช้งาน					
5.4 มีอุปกรณ์ดับเพลิง และอยู่ในสภาพพร้อมใช้งาน					
5.5 มีการควบคุมอุณหภูมิและความชื้นภายในศูนย์คอมพิวเตอร์ที่แยกจากเครื่องปรับอากาศรวม					
5.6 มีการควบคุมการเข้า ออก บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย					
5.7 มีการติดตั้งกล้อง CCTV ไว้ในศูนย์ควบคุมระบบคอมพิวเตอร์อย่างเพียงพอ และอยู่ในสภาพพร้อมใช้งาน					

5.8 มีการควบคุมบุคลากรอื่นที่มีความจำเป็นต้องเข้ามาปฏิบัติหน้าที่ในศูนย์คอมพิวเตอร์เป็นการชั่วคราว					
5.9 มีข้อแนะนำให้ความระวังและป้องกันอุปกรณ์จากอุบัติเหตุต่าง ๆ เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชนหรือเสี่ยงต่อการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์					
5.10 มีการควบคุม การเข้าออกบริเวณสำนักงานอย่างมีระบบ เช่นการใช้บัตรรูดก่อนเข้าสำนักงาน					
6. การบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร					
6.1 มีการสำรองข้อมูลและโปรแกรมเป็นประจำ					
6.2 มีการนำสื่อที่ใช้ในการบันทึกข้อมูลสำรองเก็บไว้ในสถานที่ปลอดภัย					
6.3 มีการเข้ารหัส ข้อมูลสำคัญที่ส่งผ่านเครือข่าย					
6.4 มีการบันทึกกิจกรรมหรือเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศโดยมีการเก็บบันทึกไว้อย่างน้อย 90 วัน					
6.5 มีการควบคุมการรับส่งสื่อบันทึกที่จัดเก็บไว้ เช่น การตรวจสอบตัวตนของผู้ที่มารับ-ส่ง มีการระบุผู้รับผิดชอบในการติดต่อ					
6.6 มีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต					
6.7 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ					
6.8 มีแผนฉุกเฉิน เป็นลายลักษณ์อักษรเพื่อรองรับการใช้งานในกรณีระบบล้มเหลว					
6.9 มีการทดสอบแผนฉุกเฉิน ว่าสามารถปฏิบัติได้จริง					
6.10 มีระบบป้องกันและตรวจสอบไวรัสที่ครอบคลุมเครือข่ายและลูกข่ายที่สำคัญ					
6.11 มีการกำหนดขั้นตอนมาตรฐานในการดำเนินการด้านการสื่อสารและเครือข่ายแต่ละประเภท					
6.12 มีการควบคุมไม่ให้ผู้ใช้งานระงับการใช้งาน ระบบป้องกันไวรัสที่ติดตั้งไว้					
6.13 มีวิธีการจัดการสื่อบันทึกข้อมูลลับ ที่ไม่ได้ใช้แล้ว					
6.14 มีการปรับปรุง Virus Signature ให้เป็นปัจจุบัน					

6.15 มีการจัดการให้ระบบปฏิบัติการจริง แยกออกจากระบบที่ใช้ในการพัฒนาหรือทดสอบ					
6.16 มีการกำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรการรองรับเพื่อป้องกันปัญหาจากการแลกเปลี่ยนสารสนเทศระหว่างองค์กร					
6.17 มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงาน					
6.18 มีการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง					
6.19 มีการจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งาน รวมถึงแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับ ไวรัสชนิดใหม่ ๆ					
7. การควบคุมการเข้าถึง					
7.1 มีนโยบายควบคุมการเข้าถึงระบบอย่างเป็นลายลักษณ์อักษร มีการกำหนดสิทธิ์การใช้ข้อมูลระบบคอมพิวเตอร์โดยให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติงาน					
7.2 มีระบบที่ป้องกันการบุกรุก เช่น firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก					
7.3 มีนโยบายควบคุมไม่ให้ข้อมูลมีความสำคัญถูกนำออกภายนอกองค์กร					
7.4 มีระบบบริหารจัดการรหัสผ่าน สำหรับผู้ใช้ อย่างมีประสิทธิภาพ					
7.5 มีมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่นกรณีที่ส่งซ่อม ควรลบข้อมูลที่เก็บไว้ในสื่อบันทึกก่อนส่งซ่อม					
7.6 มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงและโอนย้ายระบบงาน และทดสอบระบบงาน					
7.7 มีการควบคุมและจำกัดการใช้งาน Software Utility สำหรับระบบงานคอมพิวเตอร์ application system					
7.8 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้อง ครบถ้วนและทำงานที่มีประสิทธิภาพ					

7.9 มีการจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน					
7.10 มีการควบคุมการแชร์ไฟล์ ข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ส่วนบุคคล กำหนดรหัสผ่าน กำหนดสิทธิ์ให้เฉพาะรายที่จำเป็นเท่านั้น					
7.11 มีการควบคุมผู้ให้บริการ (IT Outsourcing) ในการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลสารสนเทศขององค์กร					
7.12 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์					
7.13 มีการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรเมื่อมีการร้องขอให้มีการพัฒนาหรือแก้ไข เปลี่ยนแปลงระบบงานคอมพิวเตอร์					
7.14 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร					
7.15 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล					
7.16 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ในหน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน					
7.17 มีนโยบายในการควบคุมการเข้าถึงระบบให้เป็นปัจจุบันอยู่เสมอ					
7.18 มีการกำหนดและทบทวนสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่ การโอนย้ายส่วนงานหรือลาออกอย่างสม่ำเสมอ					
7.19 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่นสิทธิ์การใช้โปรแกรม และระบบงานคอมพิวเตอร์ Application System สิทธิ์การใช้งานอินเทอร์เน็ต					
7.20 มีระบบบังคับอายุของรหัสผ่าน เช่น ตั้งรหัสผ่านให้ยากแก่การคาดเดา บังคับไม่ให้ใช้รหัสผ่านซ้ำของเดิม ระบบล๊อคอัตโนมัติ ในกรณีที่ป้อนรหัสผิดและไม่มีการใช้งานหน้าจอเป็นระยะเวลาหนึ่ง					

7.21 มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง					
7.22 มีการที่ระบบจะทำการล๊อกหน้าจออัตโนมัติ เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลาหนึ่ง					
7.23 มีการบังคับให้ผู้ใช้งาน เปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกหรือเมื่อถูก reset password					
7.24 มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่ประกอบไปด้วยขอบเขตของเครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่าง ๆ					
7.25 มีการบังคับความยาวขั้นต่ำของรหัสผ่าน					
7.26 มีการดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานที่สำคัญเพื่อดูช่องโหว่ต่าง ๆ ของโปรแกรมระบบ system software management					
7.27 มีการกำหนดบุคคล ให้สามารถแก้ไขข้อมูลในฐานข้อมูลได้โดยตรงโดยไม่ผ่านระบบงาน system application					
7.28 มีการควบคุมการดำเนินการ ในการพัฒนาหรือแก้ไขระบบงาน					
7.29 มีการแบ่งแยกเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ต กับระบบที่เชื่อมต่ออินทราเน็ต					
8. การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ					
8.1 มีขั้นตอนหรือวิธีปฏิบัติ และควบคุมในการพัฒนาหรือแก้ไขเปลี่ยนแปลง โอนย้าย และทดสอบระบบงาน					
8.2 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้อง ครบถ้วนและทำงานที่มีประสิทธิภาพ					
8.3 มีการได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรและจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน					
8.4 มีการวิเคราะห์และประเมินผลกระทบที่เกี่ยวข้องในการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์					
8.5 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ใน					

หน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน					
8.6 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร					
8.7 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล					
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร					
9.1 มีมาตรการป้องกันและจำกัดสิทธิ์การเข้าถึง การแก้ไขเปลี่ยนแปลง บันทึกต่าง ให้กับบุคคลที่เกี่ยวข้องเท่านั้น					
9.2 มีการแจ้งให้ผู้เกี่ยวข้องรับทราบทุกครั้ง โดยผ่านช่องทางที่องค์กรได้จัดเตรียมไว้ ในกรณีที่พบเครื่องติดไวรัสบนคอมพิวเตอร์ที่ใช้งานอยู่					
9.3 มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย มีการบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก					
9.4 มีช่องทางให้พนักงานรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร เช่น เมื่อพบไวรัสบนเครื่องคอมพิวเตอร์					
9.5 มีการฝึกซ้อมรับมือกับ เหตุฉุกเฉินในรูปแบบต่าง ๆ					
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร					
10.1 มีการประเมินความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศรวมถึงผลกระทบในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ					
10.2 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว					
10.3 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งาน ให้เป็นปัจจุบันอยู่เสมอ					
11. การปฏิบัติตามข้อกำหนด					
11.1 มีวิธีปฏิบัติเพื่อให้บุคลากรปฏิบัติตามนโยบายรักษา					

ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรตามที่กำหนดไว้					
11.2 มีผู้ตรวจสอบภายในและมีผู้ตรวจสอบอิสระจากภายนอกเข้ามาตรวจสอบการปฏิบัติงานหรือการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ					
11.3 มีการกำกับดูแลและตรวจสอบผู้ใต้บังคับบัญชาให้ปฏิบัติตามนโยบายอย่างถูกต้องอย่างสม่ำเสมอ					
11.4 มีการกำหนดห้ามละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา					
11.5 มีการรวบรวมกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศไว้อย่างครบถ้วน					

ภาคผนวก ง
สำเนาเกียรติบัตรนำเสนอผลงานวิจัยระดับชาติ

Bansomdejchaopraya Rajabhat University

Certificate of Participation

This is to certify that

Jumpot Kanjanakomtorn

participated in the International Conference 2007 on
Innovation for Sustainable Development
19-20 October,2007 at Bansomdejchaopraya Rajabhat University

Supol Wuthisen

(Assoc.Prof.Dr.Supol Wuthisen)

President

ภาคผนวก จ
สำเนาประกาศนียบัตรภาษาไทย/ภาษาอังกฤษ

The 1st International Silpakorn Graduate Study Conference 2011

Creative Education

SILPAKORN UNIVERSITY

The Graduate School, Silpakorn University

presents this honor certificate to

Jumpot KANJANAKOMTORN

for participating

The 1st International Silpakorn Graduate Study Conference 2011 (IGSC)

"Creative Education"

on title

A Security Evaluation Model for Information and Communication Technology of Rajabhat Universities

Given this on May 10th, 2011

(Professor Emeritus Khaisri Sri-aroon)
Chairperson of Silpakorn University Council

(Uthai Dulayakasem, Ph.D.)
President of Silpakorn University

(Assistant Professor Panjai Tantatsanawong, Ph.D.)
Dean of Graduate School, Silpakorn University

TÜV NORD

CERTIFICATE OF SUCCESSFUL COMPLETION

This is to certify that

Jumpot Kanjanakomtorn

Has successfully completed the course

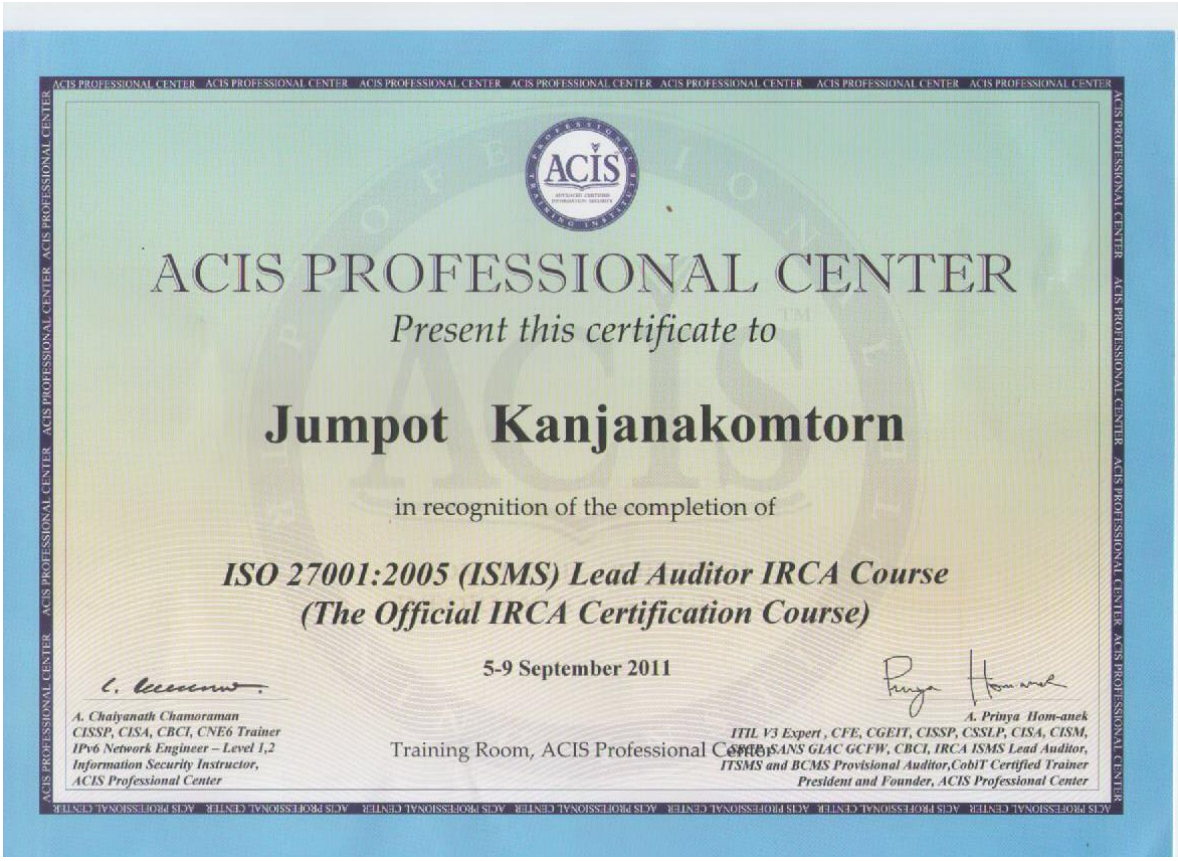
Information Security Management Systems (ISMS) Auditor / Lead Auditor Training Course (In Accordance with ISO 27001:2005)

Venue:	**Thailand**
Dates of Course:	**September 05-09, 2011**
Certificate No.:	**A17242/2011/275**
Signed:	**For TÜV NORD**
	Jack Yeh
Date:	**December 14, 2011**

The certificate is valid for 3 years from the last day of the course for the purpose of IRCA ISMS Auditor Certification Scheme.

IRCA CERTIFIED TRAINING COURSE
IRCA No. 17242

TÜV Asia Pacific Ltd.
A Company of the TÜV NORD Group



ACIS PROFESSIONAL CENTER

ACIS PROFESSIONAL CENTER

Present this certificate to

Jumpot Kanjanakomtorn

in recognition of the completion of

ISO 27001:2005 (ISMS) Lead Auditor IRCA Course
(The Official IRCA Certification Course)

5-9 September 2011

A. Chaiyanath Chamoraman
CISSP, CISA, CBCI, CNE6 Trainer
IPv6 Network Engineer – Level 1,2
Information Security Instructor,
ACIS Professional Center

Training Room, ACIS Professional Center

A. Prinya Hom-anek
ITIL V3 Expert , CFE, CGEIT, CISSP, CSSLP, CISA, CISM, GSEC, SANS GIAC GCFW, CBCI, IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor,CobiT Certified Trainer
President and Founder, ACIS Professional Center

ภาคผนวก ฉ
คู่มือการประเมิน

คู่มือ โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เรียกว่า **“Ed-SAM” (Education Security Assessment Model)** เป็นรูปแบบประเมินความมั่นคงปลอดภัยระบบสารสนเทศด้วยตนเอง สำหรับสถาบันการศึกษา

บทนำ ปัจจัยที่เกี่ยวข้องโดยอธิบายรายละเอียดของ โมเดล ดังรูป

ความร่วมมือ	
ผู้บริหาร	
ผู้ปฏิบัติการ ผู้ใช้งาน	
Plan Do Check Act	105 ตัวบ่งชี้
11) การปฏิบัติตามข้อกำหนด	5
10) การบริหารความต่อเนื่อง	3
9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง	5
8) การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ	7
7) การควบคุมการเข้าถึง	29
6) การบริหารจัดการด้านการสื่อสาร	19
5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	10
4) นโยบายการบริหารจัดการทรัพย์สิน	9
3) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร	4
2) โครงสร้างความมั่นคงปลอดภัยขององค์กร	5
1) นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ	9
Plan Do Check Act	
ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล การสื่อสาร บุคคลากร	
Commitment Human Unity Management Procedure Habit Organization Technology	

ขอบเขตสำหรับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องเริ่มจากผู้บริหารต้องการการบริหารจัดการ (**M**anagement) ด้านนโยบาย (**P**olicy) ด้านเทคโนโลยี (**T**echnology) ด้านบุคลากร (**H**uman) โดยมีคณะทำงานที่มีเป้าหมายเดียวกัน (**U**nity) มีพันธะสัญญาร่วมกันอย่างมุ่งมั่น (**C**ommitment) ที่จะช่วยเหลือซึ่งกันและกัน (**H**abit) พฤติกรรมผู้ใช้งานของเกี่ยวข้องกับระบบความมั่นคงปลอดภัยขององค์กร (**O**rganization) อย่างเป็นขั้นตอน (**P**rocedure) ในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี (**T**echnology) ให้มีความมั่นคงปลอดภัย ประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร และบุคลากร เพื่อรองรับภารกิจของมหาวิทยาลัยราชภัฏในด้าน การเรียนการสอน การบริหารสถานศึกษา การให้บริการชุมชน เพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้งานของ ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ รวมทั้งทรัพย์สินอื่น ๆ ที่มีความสำคัญของสถานศึกษา โดยดำเนินการ นำมาใช้ ตรวจสอบ วัดผล ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารการรักษาความปลอดภัย เพื่อให้สถานศึกษารอดพ้นจากภัยคุกคามต่าง ๆ โดใช้หลัก Plan-Do-Check-Act (PDCA Model) มีแกนหลักในการดำเนินการ 11 ด้าน 105 ตัวบ่งชี้ กระบวนการในการกำหนดนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องใช้การบริหารจัดการจัดการด้านเทคโนโลยี การบริหารจัดการทรัพยากรมนุษย์ ผู้บริหารระดับสูงต้องมีการอนุมัติแต่งตั้งคณะทำงานอย่างเป็นลายลักษณ์อักษรและมีการกำหนดภารกิจหน้าที่อย่างชัดเจนเพื่อร่วมกันกำหนด นโยบาย ดำเนินงาน และการติดตามประเมินผล เพื่อให้เกิดความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร บุคลากร เพื่อให้ภารกิจในการเรียนการสอน การบริหารสถานศึกษา และการบริหารชุมชุนให้ดำเนินไปอย่างต่อเนื่องพร้อมใช้งานมี ความถูกต้องสมบูรณ์ และควบคุมการเข้าสู่ชั้นความลับของฐานข้อมูลได้อย่างมีประสิทธิภาพ คณะผู้บริหาร ผู้บริหารระดับสูงต้องตั้งคณะกรรมการจากทุกหน่วยงานที่เกี่ยวข้องเป็นคณะทำงาน ตามแนวทางดำเนินงาน 11 ด้านประกอบด้วย 105 ตัวบ่งชี้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และดำเนินการตามโมเดล การจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

รูปแบบการประเมิน “Ed-SAM”

(Education Security Assessment Model)”

คุณลักษณะ เป็นเครื่องมือทางการบริหาร สำหรับตรวจประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หลักการของการออกแบบโครงสร้างจะใช้อ้างอิงรูปแบบ PDCA ซึ่งเป็นหลักการบริหารเดียวกับมาตรฐานสากลอื่น ที่นิยมใช้กันทั่วโลก ตามกระบวน PDCA เริ่มจาก การวางแผน การลงมือทำ การปฏิบัติการ การเฝ้าระวัง การทบทวน การดูแลรักษา และการปรับปรุงระบบเทคโนโลยีสารสนเทศ

ขั้นตอนการปฏิบัติ PDCA เพื่อการนำรูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ **Ed-SAM Model** จะดำเนินการตรวจประเมิน ดังนี้

การวางแผนงาน (Plan) ตรวจประเมินการวางแผนจัดทำ ดำเนินการ โดยการ กำหนดขอบเขตการจัดทำ กำหนดนโยบาย กำหนดรูปแบบและวิธีการประเมินความเสี่ยง ระบุความเสี่ยง วิเคราะห์และประเมินความเสี่ยง วิเคราะห์และประเมินหนทางในการลดความเสี่ยง กำหนดวัตถุประสงค์และมาตรการในการควบคุมเพื่อลดความเสี่ยง ขออนุมัติผู้บริหารเกี่ยวกับความเสี่ยงที่ไม่มีมาตรการเพื่อควบคุม ขออนุมัติผู้บริหารเกี่ยวกับการทำระบบ จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้

การปฏิบัติการตามแผน (Do) ตรวจประเมินดำเนินการตามแผน กำหนดแผน กำจัดความเสี่ยง ซึ่งประกอบด้วยแนวทางในการปฏิบัติสำหรับผู้บริหาร ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม ฝึกอบรมและกระตุ้นให้ตระหนักเกี่ยวกับการรักษาความปลอดภัย บริหารการปฏิบัติการ บริหารทรัพยากร กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

การเฝ้าระวังและตรวจสอบ (Check) ตรวจประเมิน การเฝ้าระวังและตรวจสอบ การเฝ้าระวังและตรวจจับข้อผิดพลาดต่าง ๆ แผนประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ ตรวจพิจารณาระบบมีประสิทธิภาพเพียงพอหรือไม่ ประเมินเป็นประจำว่า ความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ ตรวจสอบภายในระบบ ตรวจสอบและประเมินว่าระบบทำงานตามขอบเขตที่กำหนดหรือไม่ ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดต่าง ๆ ที่ตรวจพบ บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของระบบ

การรักษาและปรับปรุง (Act) ตรวจประเมินการรักษาและปรับปรุง การเพิ่มเติมเพื่อปรับปรุงระบบ แก้ไขปัญหาที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นอีก สื่อสารให้ผู้เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงระบบ ทำให้แน่ใจว่า การปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

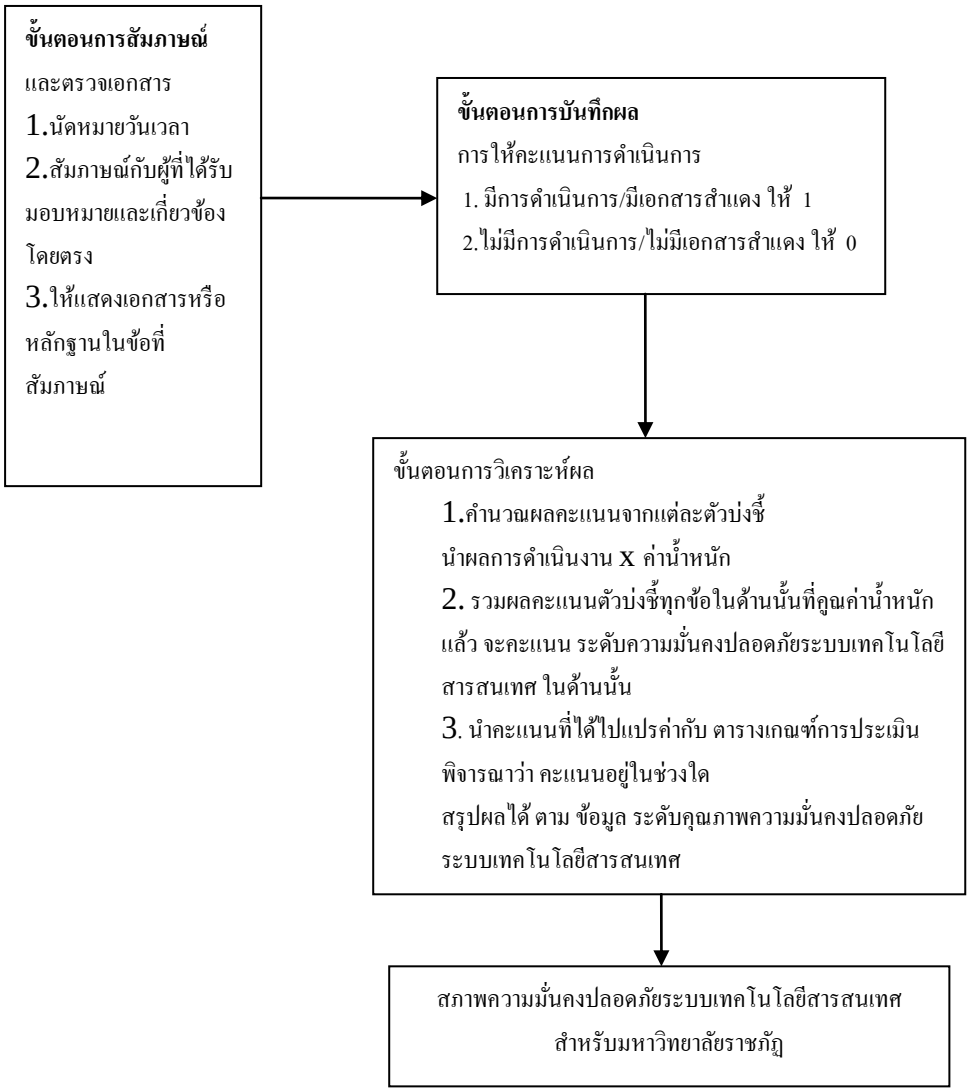
ตรวจสอบการมีการกำหนดเกี่ยวกับการจัดทำเอกสารเพื่อจะชี้ให้เห็นชัดว่านโยบายที่กำหนดนั้นจะนำไปปฏิบัติจริง โดยเอกสารที่ต้องจัดทำประกอบด้วย

1. แถลงการณ์เกี่ยวกับวัตถุประสงค์และนโยบายของระบบ
2. ของเขตการทำงานของระบบ
3. ข้ออธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง
4. รายงานเกี่ยวกับการประเมินความเสี่ยง
5. กำหนดแผนเพื่อลดความเสี่ยง
6. กำหนดแนวทางการปฏิบัติสำหรับองค์กรเพื่อให้สามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ และกำหนดแนวทางในการวัดประสิทธิภาพของมาตรการควบคุมต่าง ๆ
7. การเก็บรักษาเอกสารต่าง ๆ ที่ทำตามมาตรฐานนี้
8. แถลงการณ์ของการประยุกต์ใช้งาน

โดยพัฒนาปรับปรุงเพื่อความเหมาะสมของตัวบ่งชี้ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษามี 11 ด้าน และ 105 ตัวบ่งชี้ ประกอบด้วย

1. นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2. โครงสร้างความมั่นคงปลอดภัยขององค์กร
3. การบริหารจัดการทรัพย์สินขององค์กร
4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
6. การบริหารจัดการด้านการสื่อสาร และการดำเนินงานเครือข่ายสารสนเทศ
7. การควบคุมการเข้าถึง
8. การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ
9. บริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
10. บริหารความต่อเนื่องในการดำเนินงาน
11. การปฏิบัติตามข้อกำหนด

แผนภาพวิธีการประเมิน การบันทึกผล การแปลผล ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดำเนินขั้นตอนดังนี้



ขั้นตอนการสัมภาษณ์และตรวจเอกสาร

1. นัดหมายวันเวลา
2. สัมภาษณ์กับผู้ที่ได้รับมอบหมายและเกี่ยวข้องโดยตรง
3. ให้แสดงเอกสารหรือหลักฐานในข้อที่สัมภาษณ์ (รายละเอียด ในภาคผนวก)

ขั้นตอนการบันทึกผล

การให้คะแนนการดำเนินการ

1. มีการดำเนินการ/มีเอกสารสำแดง ให้ 1
2. ไม่มีการดำเนินการ/ไม่มีเอกสารสำแดง ให้ 0

ขั้นตอนการวิเคราะห์ผล

1. คำนวณผลคะแนนจากแต่ละตัวบ่งชี้
   นำผลการดำเนินงาน x ค่าน้ำหนัก
2. รวมผลคะแนนตัวบ่งชี้ทุกข้อในด้านนั้นที่คูณค่าน้ำหนักแล้ว จะได้คะแนน ระดับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในด้านนั้น
3. นำคะแนนที่ได้ไปแปลค่ากับ ตารางเกณฑ์การประเมิน พิจารณาว่า คะแนนอยู่ในช่วงใด สรุปผลได้ ตาม ข้อมูล ระดับคุณภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตารางประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ประกอบด้วยตัวบ่งชี้ 11 ด้าน 105 ตัวบ่งชี้

1. นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ ประกอบด้วย 9 ตัวบ่งชี้

วัตถุประสงค์ : เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบที่เกี่ยวข้อง

จำนวนตัวบ่งชี้ **:** 9 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 1.1 = 0.61 / 1.2 = 0.59 / 1.3 = 0.59 / 1.4 = 0.57 / 1.5 = 0.55 / 1.6 = 0.55 / 1.7 = 0.53 / 1.8 = 0.51 / 1.9 = 0.51

เอกสารหรือข้อมูลประกอบ :

1. นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ
2. ใบประเมินความรู้ของบุคลากร
3. แผนการติดตามนโยบายความมันคงปลอดภัย

ตาราง แสดงจำนวนตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน และเอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 1	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้ (รวม 5 คะแนน)	คะแนน	เอกสารหรือข้อมูลประกอบ
1.1 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร		0.61		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.2 มีการจัดการให้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการบริหาร		0.59		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.3 มีการสื่อสารและประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับขององค์กรได้ทราบอย่างทั่วถึงผ่านช่องทางที่หลากหลาย		0.59		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตัวบ่งชี้ ด้านที่ 1	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
1.4 มีการประเมินความรู้ความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในองค์กร		0.57		ใบประเมินความรู้ของบุคลากร
1.5 มีนโยบายให้ดำเนินการสื่อสารหรือให้ความรู้เกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศแก่ผู้ใต้บังคับบัญชา		0.55		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.6 มีการให้บุคลากรภายในองค์กรแต่ละหน่วยงานที่ใช้งาน มีส่วนร่วมในการจัดทำหรือทบทวนนโยบายด้านความมั่นคงฯ		0.55		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.7 ผู้บริหารมีการสื่อสารแสดงความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศอย่างชัดเจน		0.53		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.8 มีการจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไว้ในที่ที่ผู้ใช้งานหรือบุคลากรที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม		0.51		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.9 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันสอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง		0.51		รายงานการประชุมและนโยบายความมั่นคงปลอดภัย

2. โครงสร้างความมั่นคงปลอดภัยขององค์กร

วัตถุประสงค์ : เพื่อบริหารและจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 2.1 = 1.04 / 2.2 = 1 / 2.3 = 1 / 2.4 = 1.04 / 2.5 = 0.93

เอกสารหรือข้อมูลประกอบ :

1. นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2. ระเบียบบริหารการเปลี่ยนแปลง
3. ระเบียบการติดตามและประเมินผล
4. ระเบียบบริหารบุคลากร

ตาราง ตัวบ่งชี้ / ค่าน้ำหนัก / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 2	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
2.1 ผู้บริหารให้ความสำคัญและสนับสนุนในการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน		1.04		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2.2 มีการจัดการให้มีขั้นตอนในการอนุมัติการใช้งาน การพัฒนาหรือปรับปรุงเปลี่ยนแปลงระบบงานคอมพิวเตอร์		1.00		ระเบียบบริหารการเปลี่ยนแปลง
2.3 มีการจัดการให้มีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความเกี่ยวข้องในด้านการรักษาความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศอื่น ๆ ในกรณีที่มีความจำเป็น		1.00		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนัก / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 2	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
2.4 มีการทบทวนด้านความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบอิสระ		1.04		ระเบียบการติดตามและประเมินผล
2.5 มีระเบียบข้อบังคับในเอกสารรับพนักงาน ห้ามมิให้พนักงานที่เข้ามาทำงานในองค์กร เปิดเผยความลับและข้อมูลขององค์กร		0.93		ระเบียบบริหารบุคลากร

3. การบริหารจัดการทรัพย์สินขององค์กร

วัตถุประสงค์ : เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

จำนวน ตัวบ่งชี้ : 4 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 3.1 = 1.32 / 3.2 = 1.32 / 3.3 = 1.27 / 3.4 = 1.08

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารพัสดุภัณฑ์
2. ระเบียบบริหารจัดการฐานข้อมูล

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 3	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
3.1 มีการจัดทำและปรับปรุงแก้ไขรายการบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้มีความถูกต้องและเป็นปัจจุบันอยู่เสมอ		1.32		ระเบียบบริหารพัสดุภัณฑ์
3.2 มีการจัดหมวดหมู่ข้อมูลตามระดับชั้นความลับหรือระดับความสำคัญ		1.32		ระเบียบบริหารจัดการฐานข้อมูล
3.3 มีการตรวจสอบรายการบัญชีทรัพย์สินขององค์กรอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง		1.27		ระเบียบบริหารพัสดุภัณฑ์
3.4 มีการจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ		1.08		ระเบียบบริหารพัสดุภัณฑ์

4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์ : เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกงและการใช้อุปกรณ์ผิดวัตถุประสงค์

จำนวน ตัวบ่งชี้ : 9 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 4.1 = 0.61 / 4.2 = 0.59 / 4.3 = 0.59 / 4.4 = 0.59 / 4.5 = 0.57 / 4.6 = 0.53 / 4.7 = 0.53 / 4.8 = 0.51 / 4.9 = 0.49

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารบุคลากร

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 4	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
4.1 มีการกำหนดหน้าที่ความรับผิดชอบทางด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศให้แก่บุคลากรฝ่ายคอมพิวเตอร์อย่างชัดเจน		0.61		ระเบียบบริหารบุคลากร
4.2 มีการจัดทำขั้นตอนการปฏิบัติงานประจำ ของเจ้าหน้าที่ฝ่ายปฏิบัติการคอมพิวเตอร์ เป็นลายลักษณ์อักษร		0.59		ระเบียบบริหารบุคลากร
4.3 มีการจัดอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ		0.59		ระเบียบบริหารบุคลากร

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 4	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
4.4 มีการยกเลิกสิทธิ์ในการเข้าถึงของพนักงาน เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน		0.59		ระเบียบบริหารบุคลากร
4.5 มีการกำหนดให้บุคคลภายในองค์กรหรือหน่วยงานที่องค์กรว่าจ้างจากภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร		0.57		ระเบียบบริหารบุคลากร
4.6 มีการตรวจสอบ คุณสมบัติของผู้สมัคร		0.53		ระเบียบบริหารบุคลากร
4.7 มีการให้พนักงานได้รับการอบรมเพื่อสร้างความตระหนักและเสริมความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ		0.53		ระเบียบบริหารบุคลากร
4.8 มีการให้พนักงานคืนทรัพย์สินที่อยู่ในความครอบครอง เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน		0.51		ระเบียบบริหารบุคลากร
4.9 มีกระบวนการทางวินัยเพื่อลงโทษผู้ที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร		0.49		ระเบียบบริหารบุคลากร

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์ : เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนการเข้าถึงหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร และป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

จำนวน ตัวบ่งชี้ : 10 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 5.1 = 0.54 / 5.2 =0.54 / 5.3 = 0.52 / 5.4 = 0.52 / 5.5 = 0.50 / 5.6 = 0.50 / 5.7 = 0.50 / 5.8 = 0.48 / 5.9 = 0.46 / 5.10 = 0.45

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการเทคโนโลยี
2. ระเบียบบริหารจัดการสิ่งแวดล้อม
3. ระเบียบบริหารบุคลากร

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 5	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
5.1 มีอุปกรณ์ป้องกันไฟฟ้าขัดข้อง เช่นเครื่องสำรองไฟฟ้า ยูพีเอส เครื่องกำเนิดไฟฟ้าสำรอง		0.54		ระเบียบบริหารจัดการเทคโนโลยี
5.2 มีการบำรุงรักษาอุปกรณ์ป้องกันการล้มเหลวและอุปกรณ์สนับสนุนให้สามารถทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน		0.54		ระเบียบบริหารจัดการเทคโนโลยี
5.3 มีอุปกรณ์ป้องกันไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน และอยู่ในสภาพพร้อมใช้งาน		0.52		ระเบียบบริหารจัดการเทคโนโลยี

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 5	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
5.4 มีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน ตรวจจับความร้อน		0.52		ระเบียบบริหารจัดการเทคโนโลยี
5.5 มีการควบคุมอุณหภูมิและความชื้นภายในศูนย์คอมพิวเตอร์ที่แยกจากเครื่องปรับอากาศรวม		0.50		ระเบียบบริหารจัดการเทคโนโลยี
5.6 มีการควบคุมการเข้า ออกบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย		0.50		ระเบียบบริหารจัดการสิ่งแวดล้อม
5.7 มีการติดตั้งกล้อง CCTV ไว้ในศูนย์ควบคุมระบบคอมพิวเตอร์อย่างเพียงพอ และอยู่ในสภาพพร้อมใช้งาน		0.50		ระเบียบบริหารจัดการเทคโนโลยี
5.8 มีการควบคุมบุคลากรอื่นที่มีความจำเป็นต้องเข้ามาปฏิบัติหน้าที่ในศูนย์คอมพิวเตอร์เป็นการชั่วคราว		0.48		ระเบียบบริหารบุคลากร
5.9 มีข้อแนะนำให้ความระวังและป้องกันอุปกรณ์จากอุบัติเหตุต่าง ๆ เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชนหรือเสี่ยงต่อการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์		0.46		ระเบียบบริหารจัดการสิ่งแวดล้อม
5.10 มีการควบคุม การเข้าออกบริเวณสำนักงานอย่างมีระบบ เช่นการใช้การ์ดรูดก่อนเข้าสำนักงาน		0.45		ระเบียบบริหารจัดการสิ่งแวดล้อม

6. การบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร

วัตถุประสงค์ : เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย และรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก ลดความเสี่ยงจากความล้มเหลวของระบบ รักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี รักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาตและการติดขัดหรือหยุดชะงักทางธุรกิจ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก สร้างความมั่นคงปลอดภัยสำหรับพาณิชย์อิเล็คทรอนิคส์และการใช้งาน ตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

จำนวน ตัวบ่งชี้ : 19 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 6.1 = 0.32 / 6.2 = 0.32 / 6.3 = 0.32 / 6.4 = 0.32 / 6.5 = 0.31 / 6.6 = 0.30 / 6.7 = 0.30 / 6.8 = 0.30 / 6.9 = 0.30 / 6.10 = 0.30 / 6.11 = 0.30 / 6.12 = 0.29 / 6.13 = 0.29 / 6.14 = 0.24 / 6.15 = 0.18 / 6.16 = 0.16 / 6.17 = 0.16 / 6.18 = 0.16 / 6.19 = 0.16

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการฐานข้อมูล
2. ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
3. ระเบียบบริหารบุคลากร
4. ระเบียบบริหารจัดการเทคโนโลยี
5. ระเบียบบริหารการเปลี่ยนแปลง

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 6	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
6.1 มีการสำรองข้อมูลและโปรแกรมเป็นประจำ		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.2 มีการนำสื่อที่ใช้ในการบันทึกข้อมูลสำรองเก็บไว้ในสถานที่ปลอดภัย		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.3 มีการเข้ารหัส ข้อมูลสำคัญที่ส่งผ่านเครือข่าย		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.4 มีการบันทึกกิจกรรมหรือเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศโดยมีการเก็บบันทึกไว้อย่างน้อย 90 วัน		0.28		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.5 มีการควบคุมการรับส่งสื่อบันทึกที่จัดเก็บไว้ เช่น การตรวจสอบข้อตนของผู้ที่มารับ-ส่ง มีการระบุผู้รับผิดชอบในการติดต่อ		0.27		ระเบียบบริหารจัดการฐานข้อมูล
6.6 มีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.7 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ		0.26		ระเบียบบริหารบุคลากร
6.8 มีแผนฉุกเฉิน เป็นลายลักษณ์อักษรเพื่อรองรับการใช้งานในกรณีระบบล้มเหลว		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.9 มีการทดสอบแผนฉุกเฉิน ว่าสามารถปฏิบัติได้จริง		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 6	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
6.10 มีระบบป้องกันและตรวจสอบไวรัสที่ครอบคลุมเครือข่ายและลูกข่ายที่สำคัญ		0.26		ระเบียบบริหารจัดการเทคโนโลยี
6.11 มีการกำหนดขั้นตอนมาตรฐานในการดำเนินการด้านการสื่อสารและเครือข่ายแต่ละประเภท		0.26		ระเบียบบริหารจัดการเทคโนโลยี
6.12 มีการควบคุมไม่ให้ผู้ใช้งานระงับการใช้งาน ระบบป้องกันไวรัสที่ติดตั้งไว้		0.25		ระเบียบบริหารจัดการเทคโนโลยี
6.13 มีวิธีการจัดการสื่อบันทึกข้อมูลลับ ที่ไม่ได้ใช้แล้ว		0.25		ระเบียบบริหารจัดการฐานข้อมูล
6.14 มีการปรับปรุง Virus Signature ให้เป็นปัจจุบัน		0.25		ระเบียบบริหารจัดการเทคโนโลยี
6.15 มีการจัดการให้ระบบปฏิบัติการจริงแยกออกจากระบบที่ใช้ในการพัฒนาหรือทดสอบ		0.25		ระเบียบบริหารการเปลี่ยนแปลง
6.16 มีการกำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรการรองรับเพื่อป้องกันปัญหาจากการแลกเปลี่ยนสารสนเทศระหว่างองค์กร		0.25		ระเบียบบริหารจัดการฐานข้อมูล
6.17 มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงาน		0.25		ระเบียบบริหารจัดการการเปลี่ยนแปลง
6.18 มีการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง		0.24		ระเบียบบริหารจัดการเทคโนโลยี
6.19 มีการจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานรวมถึงแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ ๆ		0.24		ระเบียบบริหารจัดการเทคโนโลยี

7. การควบคุมการเข้าถึง

วัตถุประสงค์ : เพื่อควบคุมการเข้าถึงสารสนเทศ ควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ไปดำเนินการเปิดเผยหรือขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต **จำนวน ตัวบ่งชี้ :** 29 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 7.1 = 0.19 / 7.2 = 0.19 / 7.3 = 0.19 / 7.4 = 0.19 / 7.5 = 0.19 / 7.6 = 0.19 / 7.7 = 0.19 / 7.8 = 0.18 / 7.9 = 0.18 / 7.10 = 0.18 / 7.11 = 0.17 / 7.12 = 0.17 / 7.13 = 0.17 / 7.14 = 0.17 / 7.15 = 0.17 / 7.16 = 0.17 / 7.17 = 0.17 / 7.18 = 0.17 / 7.19 = 0.17 / 7.20 = 0.17 / 7.21 = 0.17 / 7.22 = 0.17 / 7.23 = 0.17 / 7.24 = 0.16 / 7.25 = 0.16 / 7.26 = 0.15 / 7.27 = 0.15 / 7.28 = 0.15 / 7.29 = 0.15

เอกสารหรือข้อมูลประกอบ : 1.ระเบียบบริหารการเปลี่ยนแปลง 2.ระเบียบการบริหารจัดการฐานข้อมูล 3.ระเบียบบริหารจัดการเทคโนโลยี

ตารางที่ 46 ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.1 มีนโยบายควบคุมการเข้าถึงระบบอย่างเป็นลายลักษณ์อักษร มีการกำหนดสิทธิ์การใช้ข้อมูลระบบคอมพิวเตอร์โดยให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติงาน		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.2 มีระบบที่ป้องกันการบุกรุก เช่น firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก		0.19		ระเบียบบริหารจัดการเทคโนโลยี
7.3 มีนโยบายควบคุมไม่ให้ข้อมูลมีความสำคัญถูกนำออกภายนอกองค์กร		0.19		ระเบียบบริหารจัดการฐานข้อมูล

ตารางที่ 46 (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.4 มีระบบบริหารจัดการรหัสผ่าน สำหรับผู้ใช้ อย่างมีประสิทธิภาพ		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.5 มีมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น กรณีที่ส่งซ่อม ควรลบข้อมูลที่เก็บไว้ในสื่อบันทึกก่อนส่งซ่อม		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.6 มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงและโอนย้ายระบบงาน และทดสอบระบบงาน		0.19		ระเบียบบริหารการเปลี่ยนแปลง
7.7 มีการควบคุมการดำเนินการในการพัฒนาหรือแก้ไขระบบงาน		0.19		ระเบียบบริหารจัดการเทคโนโลยี
7.8 มีการควบคุมและจำกัดการใช้งาน software utility สำหรับระบบงานคอมพิวเตอร์ application system		0.18		ระเบียบบริหารจัดการเทคโนโลยี
7.9 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้องครบถ้วนและทำงานที่มีประสิทธิภาพ		0.18		ระเบียบบริหารการเปลี่ยนแปลง

ตารางที่ 46 (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.10 มีการจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน		0.18		ระเบียบบริหารการเปลี่ยนแปลง
7.11 มีการควบคุมการแชร์ไฟล์ ข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ส่วนบุคคล กำหนดรหัสผ่าน กำหนดสิทธิ์ให้เฉพาะรายที่จำเป็นเท่านั้น		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.12 มีการควบคุมผู้ให้บริการ (IT Outsourcing) ในการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลสารสนเทศขององค์กร		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.13 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.14 มีการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร เมื่อมีการร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์		0.17		ระเบียบบริหารการเปลี่ยนแปลง

ตารางที่ 46 (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.15 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร		0.17		ระเบียบบริหารการเปลี่ยนแปลง
7.16 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.17 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บในหน่วยจัดเก็บ การนำเข้า การประมวลผล และการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.18 มีนโยบายในการควบคุมการเข้าถึงระบบให้เป็นปัจจุบันอยู่เสมอ		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.19 มีการกำหนดและทบทวนสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่ การโอนย้ายส่วนงานหรือลาออกอย่างสม่ำเสมอ		0.17		ระเบียบการบริหารจัดการฐานข้อมูล

ตารางที่ 46 (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.20 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่นสิทธิ์การใช้โปรแกรม และระบบงานคอมพิวเตอร์ Application System สิทธิ์การใช้งานอินเตอร์เน็ต		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.21 มีระบบบังคับอายุของรหัสผ่าน เช่น ตั้งรหัสผ่านให้ยากแก่การคาดเดา บังคับไม่ให้ใช้รหัสผ่านซ้ำของเดิม ระบบป้องกันอัตโนมัติ ในกรณีที่ป้อนรหัสผิดและไม่มีการใช้งานหน้าจอเป็นระยะเวลาหนึ่ง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.22 มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.23 มีการที่ระบบจะทำการป้องกันหน้าจออัตโนมัติ เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลาหนึ่ง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.24 มีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกหรือเมื่อถูก reset password		0.16		ระเบียบการบริหารจัดการฐานข้อมูล

ตารางที่ 46 (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.25 มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่ประกอบไปด้วยขอบเขตของเครือข่ายภายในเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ		0.16		ระเบียบบริหารจัดการเทคโนโลยี
7.26 มีการบังคับความยาวขั้นต่ำของรหัสผ่าน		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.27 มีการดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานที่สำคัญเพื่อดูช่องโหว่ต่าง ๆ ของโปรแกรมระบบ System software management		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.28 มีการกำหนดบุคคล ให้สามารถแก้ไขข้อมูลในฐานข้อมูลได้โดยตรงโดยไม่ผ่านระบบงาน system application		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.29 มีการแบ่งแยกเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเตอร์เน็ตกับระบบที่เชื่อมต่ออินทราเน็ต		0.15		ระเบียบบริหารจัดการเทคโนโลยี

8. การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ

วัตถุประสงค์ : เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัย ป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับไฟล์ต่าง ๆ ของระบบที่ให้บริการ รักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ เพื่อลดความเสี่ยงจากการถูกโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

จำนวน ตัวบ่งชี้ : 7 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 8.1 = 0.87 / 8.2 = 0.84 / 8.3 = 0.84 / 8.4 = 0.81 / 8.5 = 0.75 / 8.6 = 0.45 / 8.7 = 0.45

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารการเปลี่ยนแปลง
2. ระเบียบบริหารจัดการฐานข้อมูล

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.1 มีขั้นตอนหรือวิธีปฏิบัติและควบคุมในการพัฒนาหรือแก้ไขเปลี่ยนแปลง โอนย้าย และทดสอบระบบงาน		0.78		ระเบียบบริหารการเปลี่ยนแปลง
8.2 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้องครบถ้วนและทำงานที่มีประสิทธิภาพ		0.75		ระเบียบบริหารการเปลี่ยนแปลง

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.3 มีการได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรและจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน		0.75		ระเบียบบริหารการเปลี่ยนแปลง
8.4 มีการวิเคราะห์และประเมินผลกระทบที่เกี่ยวข้องในการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์		0.72		ระเบียบบริหารการเปลี่ยนแปลง
8.5 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ในหน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลสัมพันธ์กัน		0.72		ระเบียบบริหารจัดการฐานข้อมูล

ตาราง (ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.6 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร		0.72		ระเบียบบริหารการเปลี่ยนแปลง
8.7 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล		0.72		ระเบียบการบริหารจัดการฐานข้อมูล

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

วัตถุประสงค์ : เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม ให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย สำหรับสารสนเทศขององค์กร

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 9.1 = 11.02 / 9.2 = 1.02 / 9.3 = 0.99 / 9.4 = 0.99 / 9.5 = 0.99

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการฐานข้อมูล
2. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
3. ระเบียบบริหารจัดการเทคโนโลยี

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 9	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
9.1 มีมาตรการป้องกันและจำกัดสิทธิ์การเข้าถึง การแก้ไข เปลี่ยนแปลง บันทึกต่าง ให้กับบุคคลที่เกี่ยวข้องเท่านั้น		1.02		ระเบียบบริหารจัดการฐานข้อมูล
9.2 มีการแจ้งให้ผู้เกี่ยวข้องรับทราบทุกครั้ง โดยผ่านช่องทางที่องค์กรได้จัดเตรียมไว้ ในกรณีที่พบเครื่องติดไวรัสบนคอมพิวเตอร์ที่ใช้งานอยู่		1.02		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง(ต่อ) ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 9	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
9.3 มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย มีการบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก		0.99		ระเบียบบริหารจัดการเทคโนโลยี
9.4 มีช่องทางให้พนักงานรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร เช่นเมื่อพบไวรัสบนเครื่องคอมพิวเตอร์		0.99		ระเบียบบริหารจัดการเทคโนโลยี
9.5 มีการฝึกซ้อมรับมือกับเหตุฉุกเฉินในรูปแบบต่าง ๆ		0.99		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

วัตถุประสงค์ : เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

จำนวน ตัวบ่งชี้ : 3 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 10.1 =1.79 / 10.2 = 1.73 / 10.3 = 1.49

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 10	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
10.1 มีการประเมินความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศรวมถึงผลกระทบในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ		1.79		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
10.2 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว		1.73		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
10.3 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งาน ให้เป็นปัจจุบันอยู่เสมอ		1.49		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

11. การปฏิบัติตามข้อกำหนด

วัตถุประสงค์ : เพื่อหลีกเลี่ยงการละเมินข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ ให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร ให้การตรวจประเมินสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 11.1 = 1.07 / 11.2 = 1.03 / 11.3 = 0.99 / 11.4 = 0.95 / 11.5 = 0.95

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 11	การดำเนินการมี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
11.1 มีวิธีปฏิบัติเพื่อให้บุคลากรปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรตามที่กำหนดไว้		1.07		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.2 มีผู้ตรวจสอบภายในและมีผู้ตรวจสอบอิสระจากภายนอกเข้ามาตรวจสอบการปฏิบัติงานหรือการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ		1.03		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.3 มีการกำกับดูแลและตรวจสอบผู้ใต้บังคับบัญชาให้ปฏิบัติตามนโยบายอย่างถูกต้องอย่างสม่ำเสมอ		0.99		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.4 มีการกำหนดห้ามละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา		0.95		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตัวบ่งชี้ ด้านที่ 11	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
11.5 มีการรวบรวมกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศไว้อย่างครบถ้วน		0.95		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

โปรแกรมสำเร็จรูป
เพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
สำหรับสถาบันการศึกษา

1. มีเมนู ภาพรวมของ Ed-SAM สามารถ กดเข้าสู่ตารางประเมินได้อัตโนมัติ

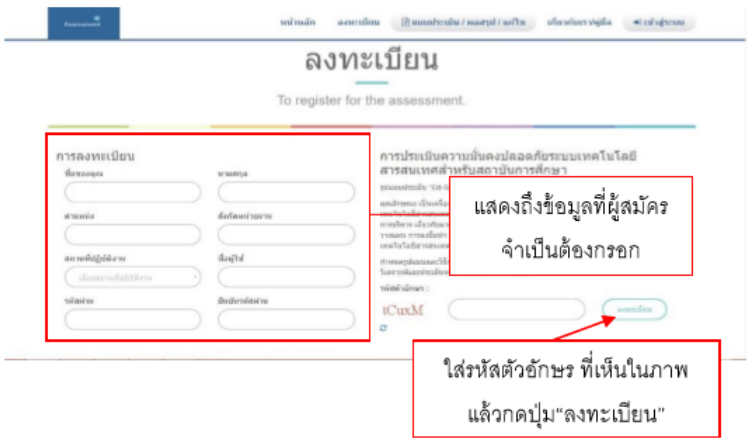
1.รูปแบบหน้าหลัก

1.หน้าหลัก
2.ลงทะเบียน
3.แบบประเมิน/ผลสรุป/แก้ไข
4.เกี่ยวกับเรา/คู่มือ
5.เข้าสู่ระบบ

2.การลงทะเบียน

1. กรอกข้อมูลผู้สมัครโดยควรกรอกข้อมูลตามจริง เพื่อสะดวกในการติดต่อสื่อสาร

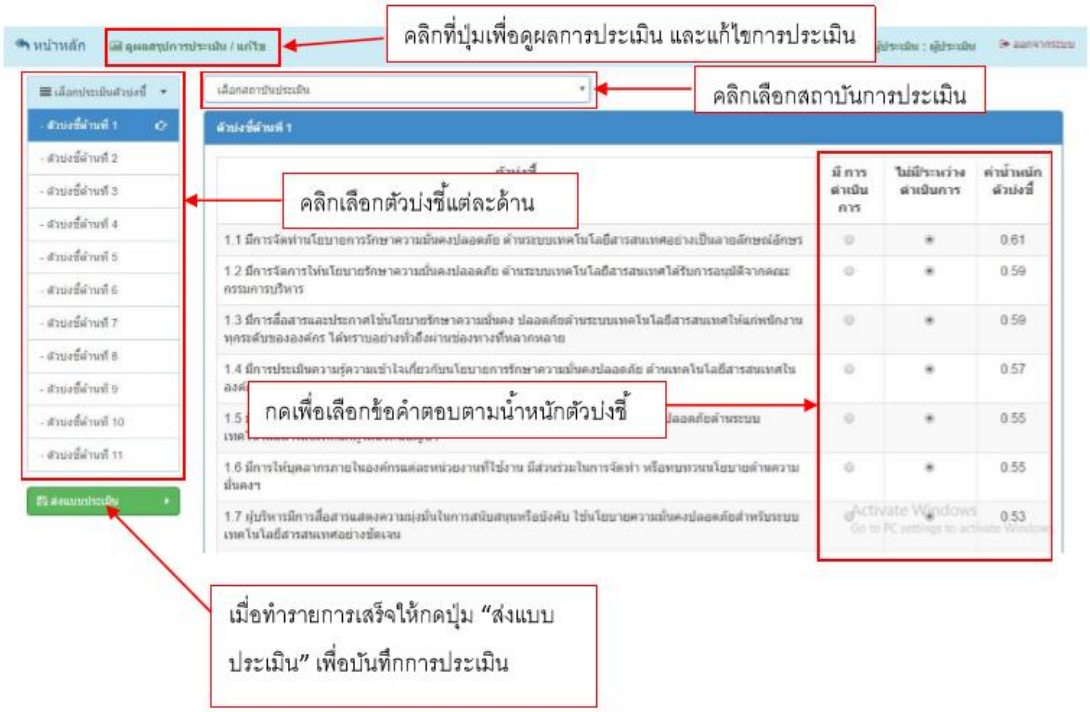
2. ใส่รหัสตัวอักษร ที่เห็นในภาพ แล้วกดปุ่ม“ลงทะเบียน”



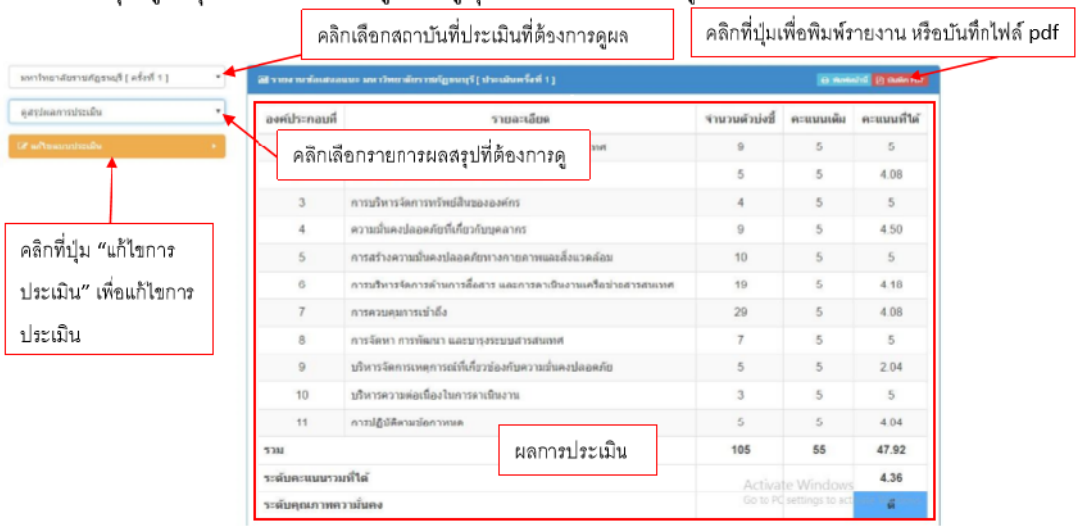
3.แบบประเมิน/ผลสรุป/แก้ไข

1.ประเมินแบบสอบถามทันที

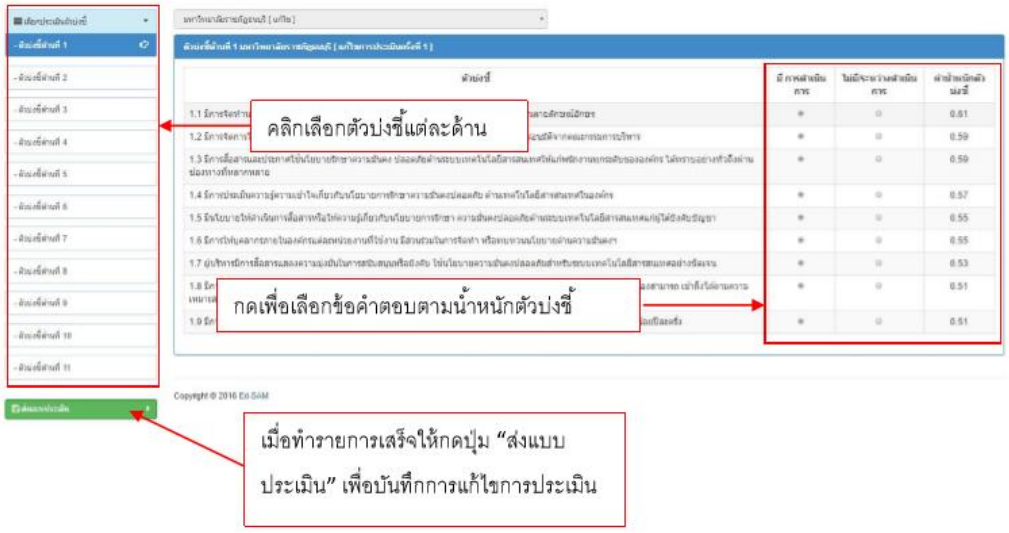
2.ดูผลสรุปการประเมิน / แก้ไขข้อมูล



1.2 **เมื่อคลิกที่ปุ่ม "ดูผลสรุปการประเมิน/แก้ไขข้อมูล " เพื่อดูสรุปผลการประเมิน (ต้องเข้าสู่ระบบก่อนจึงจะทำรายการนี้ได้)**



1.2.1 **เมื่อกดปุ่ม "แก้ไขการประเมิน" จะได้หน้าเว็บดังรูป**

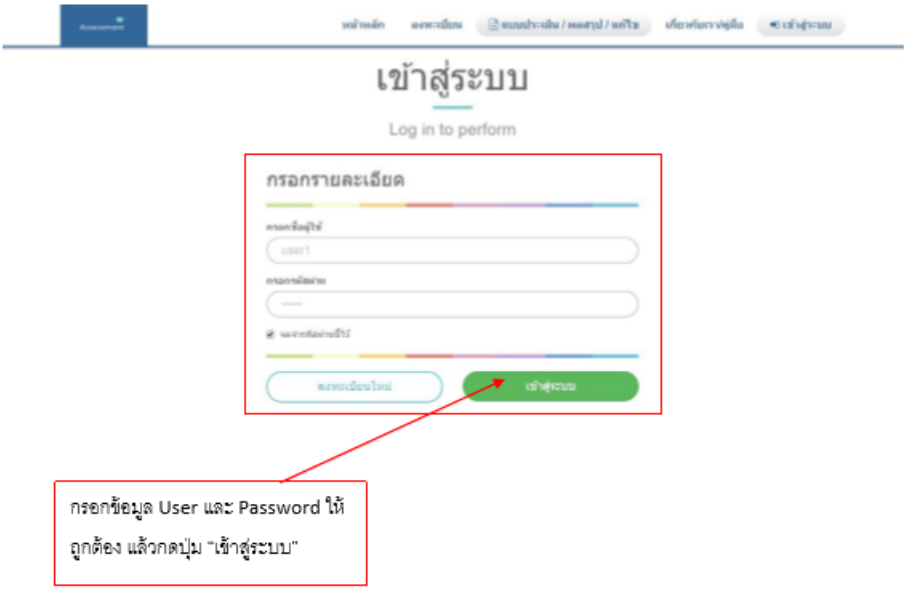


4.เกี่ยวกับเรา/คู่มือ

การจัดการระบบ

5.เข้าสู่ระบบ

1.เปิดหน้าเว็บไซต์ ไปที่ปุ่ม “เข้าสู่ระบบ” แล้วกรอกข้อมูล User และ Password ให้ครบถ้วนพร้อมตรวจสอบความถูกต้องแล้วกดปุ่ม “เข้าสู่ระบบ”



การจัดการระบบ

ประวัติผู้วิจัย

ชื่อ – สกุล	ดร จุมพฏ กาญจนกำธร
(ภาษาอังกฤษ)	MR.JUMPOT KANJANAKOMTORN
วัน เดือน ปี เกิด	25 มีนาคม พ.ศ. 2505
ที่อยู่	40 บางแวก 26 แยก 9 แขวงบางแวก เขตภาษีเจริญ กรุงเทพมหานคร 10160
สถานที่ทำงาน	บริษัทเจเอ็มเคเนทเวิร์ค จำกัด

ประวัติการศึกษา

พ.ศ. 2527	สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตร์บัณฑิต (วท.บ.) วิชาเอกฟิสิกส์ จากมหาวิทยาลัยศรีนครินทรวิโรฒ บางแสน
พ.ศ. 2539	สำเร็จการศึกษาระดับปริญญาโท บริหารธุรกิจ สาขาการบริหารธุรกิจระหว่างประเทศ มหาวิทยาลัยสยาม
พ.ศ. 2555	สำเร็จการศึกษาระดับปริญญาเอก สาขาการจัดการเทคโนโลยี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

ประวัติการทำงาน

พ.ศ. 2549 - ปัจจุบัน	อาจารย์พิเศษ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ด้านบริหารธุรกิจ คอมพิวเตอร์ พัฒนาทรัพยากรมนุษย์
พ.ศ. 2554 - ปัจจุบัน	กรรมการผู้จัดการบริษัทเจเอ็มเคเนทเวิร์ค จำกัด วางระบบคอมพิวเตอร์ ฮาร์ดแวร์ เครือข่าย ซอฟท์แวร์ ISO 27001:2005 (ISMS) Lead Auditor IRCA Certification

เอกสารหมายเลข 5

แบบสรุปปิดโครงการวิจัย

สัญญาเลขที่ *RDG*5840015 **ชื่อโครงการ** *"การพัฒนาโปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา"*

หัวหน้าโครงการ *ดร จุมพฏ กาญจนกำธร* **หน่วยงาน** *บริษัทเจเอ็มเคเนทเวิร์ค จำกัด*

โทรศัพท์ 0827823346 024105601 **โทรสาร** 024105601 Email: jumpotkan@hotmail.com

สถานะผลงาน **ปกปิด** **/ ไม่ปกปิด**

ความสำคัญ/ความเป็นมา

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญอย่างยิ่ง ในการบริหารจัดการและการเรียนรู้ในสถาบันการศึกษา ปัจจุบันได้มีการนำเทคโนโลยีสารสนเทศมาใช้มากขึ้นในด้าน การบริหาร การเรียนการสอนและให้บริหารชุมชนซึ่งระบบสารสนเทศที่ดีจะต้องมีกระบวนการทำงานอย่างต่อเนื่อง มีบุคลกรที่มีความรู้ความสามารถ ฮาร์ดแวร์และซอฟท์แวร์ต้องมีประสิทธิภาพและทำงานได้อย่างต่อเนื่อง ข้อมูลต้องมีความมั่นคงปลอดภัย โดยต้องมีสภาพพร้อมใช้งาน มีความถูกต้องแม่นยำ มีความเป็นส่วนตัวและควบคุมความลับได้อย่างมีประสิทธิภาพ แต่ในขณะที่หน่วยงานต่าง ๆ ได้มีการจัดหาและลงทุนด้วยงบประมาณจำนวนมากกับระบบสารสนเทศที่มีอยู่จำกัด

ปัจจุบันภัยคุกคามต่าง ๆ ต่อระบบเทคโนโลยีสารสนเทศมีมากขึ้น ดังนั้นหากไม่ให้ความสำคัญในการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแล้ว ย่อมก่อให้เกิดความเสียหายอย่างมากต่อผู้บริหาร อาจารย์ เจ้าหน้าที่ นักศึกษา ผู้รับบริการและผู้ให้บริการ

สิ่งสำคัญที่สุดในการบริหารในปัจจุบันคือระบบเทคโนโลยีสารสนเทศ สร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศในสถาบันการศึกษาได้มากเท่าใด ประสิทธิภาพในการบริหารงานก็จะสูงเท่านั้น ปัจจัยที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ นโยบายความมั่นคง งบประมาณด้านความมั่นคง สิ่งแวดล้อมที่เกี่ยวข้องกับความมั่นคง บุคลากรและพฤติกรรมผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังนั้นการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา ผู้บริหาร มีความจำเป็น

ต้องนำระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศมาใช้ มี 2 ทางเลือก

ทางเลือกที่ 1 คือ การนำระบบสากล (ISO 27001) ต้องใช้งบประมาณสูงมาก (มากกว่า 1 ล้านบาท) บุคลากรทางด้าน IT Security มีน้อย การสื่อสารเอกสารและผู้รับดำเนินงานส่วนใหญ่ใช้ภาษาอังกฤษ ในสถานการณ์ปัจจุบันสถาบันการศึกษาส่วนใหญ่ มีงบประมาณจำกัด ไม่สามารถนำระบบมาตรฐานสากล (ISO 27001) มาใช้ได้

ทางเลือกที่ 2 คือ การพัฒนาขึ้นมาใช้เอง โดยอ้างอิงระบบสากลและปรับใช้สำหรับมหาวิทยาลัย ใช้การสื่อสารภาษาไทย สามารถดำเนินการตรวจประเมินได้เอง ประหยัดงบประมาณ จึงจำเป็นต้องทำการวิจัยเพื่อพัฒนาโปรแกรมประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษานี้

ปัญหาต่างๆ เหล่านี้เกิดขึ้นจากผู้บริหารไม่มีข้อมูลสภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา ไม่ทราบว่าการบริหารระบบเทคโนโลยีสารสนเทศมีเรื่องใดที่ต้องดำเนินการ รวมถึงไม่ทราบสภาพความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในปัจจุบันมีอะไรและเป็นอย่างไร ทำให้การตัดสินใจในการบริหารด้านที่เกี่ยวข้อง ขาดข้อมูลที่เพียงพอ ส่งผลต่อคุณภาพของสถาบันการศึกษา ตามมาตรา 48 แห่งพระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2545 ระบุว่า "ให้หน่วยงานต้นสังกัดและสถาบันการศึกษาจัดให้มีระบบการประกันคุณภาพภายในสถาบันการศึกษาและให้ถือว่าการประกันคุณภาพภายในเป็นส่วนหนึ่งของกระบวนการบริหารการศึกษาที่ต้องดำเนินการอย่างต่อเนื่อง"

ถ้าผู้บริหารสถาบันการศึกษามีเครื่องมือที่ใช้สำหรับการตรวจสอบและประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศย่อมทำให้ผู้บริหารได้ทราบแนวทางการวางนโยบายและสถานภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และสามารถนำผลจากรูปแบบการประเมินความมั่นคงปลอดภัยนี้ไปวางนโยบายแผนพัฒนาระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยและประสิทธิภาพในการบริหารสถาบันการศึกษาดียิ่งขึ้น สามารถพัฒนาภาพลักษณ์ที่ดีของสถาบันการศึกษาให้สอดคล้องกับ พระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2545 และรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้เป็นอย่างดี

การได้มาซึ่งระบบการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
สำหรับสถาบันการศึกษา มี 2 ทางเลือก

ผู้วิจัยมีแนวคิดว่า ทางเลือกที่ 2 คือ พัฒนาขึ้นมาใช้เอง โดยอ้างอิงระบบสากลและปรับใช้สำหรับสถาบันการศึกษาของประเทศไทย ทำให้สามารถสื่อสารเป็นภาษาไทย ประหยัดงบประมาณ และสะดวกและง่ายในการใช้ จะเป็นประโยชน์อย่างยิ่งกับสถาบันการศึกษาของประเทศไทย

ดังนั้นการวิจัยครั้งนี้จึงมีวัตถุประสงค์เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

วัตถุประสงค์ของโครงการ

1) *เพื่อศึกษาสถานสภาพปัจจุบันด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันการศึกษา*

2) *เพื่อพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา*

3) *เพื่อพัฒนาโปรแกรมเพื่อประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ*

ผลการวิจัย

1. *ผู้บริหารสถาบันการศึกษา ให้ความสำคัญด้านมีนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและนโยบายสิ่งแวดล้อม ด้านงบประมาณ ด้านบุคลากร และผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในระดับมากถึงมากที่สุด แต่ปัจจุบันสถาบันการศึกษาส่วนใหญ่ ยังไม่มี นโยบายความมั่นคงปลอดภัยตามมาตรฐานสากล และนโยบายด้านสิ่งแวดล้อมสำหรับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร อีกทั้งงบประมาณที่ได้รับเพื่อบริหารระบบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับมหาวิทยาลัยบางแห่งยังไม่เพียงพอ มีสถาบันการศึกษา ระดับความรู้ความเข้าใจของบุคลากรและผู้ใช้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับปานกลาง*

2. *รูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เรียกว่า “Education Security Assessment Model” หรือ Ed-SAM เป็นเครื่องมือบริหารเพื่อสร้างนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีตัวบ่งชี้ด้านความมั่นคง 11 ด้าน 105 ตัวบ่งชี้ สามารถนำไปใช้งานและเรียนรู้ง่าย ประหยัดเวลาและค่าใช้จ่าย สามารถดำเนินการได้ด้วยตนเอง มีประสิทธิภาพดีสอดคล้องกับรูปแบบการประเมินตามมาตรฐานสากล*

3. *โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา*
https://www.facebook.com/Ed-SAM-1824475104495803/?fref=ts

คำสืบค้น (Keywords) *โปรแกรมเพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา*

การนำผลงานวิจัยไปใช้ประโยชน์

ด้านนโยบาย

โดย ผู้บริหารสถาบันการศึกษา

มีการนำไปใช้ประโยชน์ในการตรวจสอบและประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศภายในสถาบันการศึกษาได้ด้วยบุคลากรภายในเอง เพื่อนำข้อมูลที่ได้มาวางแผนการบริหารจัดการและงบประมาณ

ด้านสาธารณะ

โดย ศูนย์คอมพิวเตอร์มหาวิทยาลัยราชภัฏธนบุรี

มีการนำไปใช้เพื่อให้มีความรู้ความเข้าใจ เกิดความตระหนัก รู้เท่าทันการเปลี่ยนแปลง ซึ่งนำไปสู่การเปลี่ยนวิธีคิด พฤติกรรม เพื่อเพิ่มคุณภาพชีวิตของประชาชน สร้างสังคมคุณภาพและส่งเสริมคุณภาพสิ่งแวดล้อม

ด้านชุมชนและพื้นที่

โดยสโมสรโรตารีพระปกเกล้าธนบุรี

มีการนำไปใช้โดยการนำกระบวนการ วิธีการ องค์ความรู้ การเปลี่ยนแปลง การเสริมพลัง อันเป็นผลกระทบที่เกิดจากการวิจัยและพัฒนาชุมชน ท้องถิ่น พื้นที่ ไปใช้เพื่อเกิดประโยชน์การขยายผลต่อชุมชน

ด้านพาณิชย์

โดยบริษัทเจเอ็มเคเนทเวิร์ค จำกัด

มีการนำไปใช้เพื่อสร้างความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของสถานประกอบการนั้น ๆ

ด้านวิชาการ

โดยสำนักคอมพิวเตอร์มหาวิทยาลัยราชภัฏธนบุรี

มีการนำไปใช้โดยการนำองค์ความรู้จากผลงานวิจัยเพื่อตีพิมพ์ในรูปแบบต่าง ๆ เช่น ผลงานตีพิมพ์ในวารสารระดับนานาชาติ ระดับชาติ หนังสือ ตำรา บทเรียน เพื่อเป็นประโยชน์ทางวิชาการ การเรียนรู้ การเรียน

การเผยแพร่/ประชาสัมพันธ์

1 **เว็บไซต์** http://tm.dru.ac.th/assessment/

https://www.facebook.com/Ed-SAM-1824475104495803/?fref=ts

คู่มือ โปรแกรมการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

การพัฒนารูปแบบการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา เรียกว่า **"Ed-SAM" (Education Security Assessment Model)** เป็นรูปแบบประเมินความมั่นคงปลอดภัยระบบสารสนเทศด้วยตนเอง สำหรับสถาบันการศึกษา

ปัจจัยที่เกี่ยวข้องโดยอธิบายรายละเอียดของ โมเดล ดังรูป

ความร่วมมือ	
ผู้บริหาร	
ผู้ปฏิบัติการ ผู้ใช้งาน	
Plan Do Check Act	105 ตัวบ่งชี้
11) การปฏิบัติตามข้อกำหนด	5
10) การบริหารความต่อเนื่อง	3
9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง	5
8) การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ	7
7) การควบคุมการเข้าถึง	29
6) การบริหารจัดการด้านการสื่อสาร	19
5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	10
4) นโยบายการบริหารจัดการทรัพย์สิน	9
3) ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร	4
2) โครงสร้างความมั่นคงปลอดภัยขององค์กร	5
1) นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ	9
Plan Do Check Act	
ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล การสื่อสาร บุคคลากร	
Commitment Human Unity Management Procedure Habit Organization Technology	

ขอบเขตสำหรับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

การบริหารจัดการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องเริ่มจากผู้บริหารต้องการการบริหารจัดการ (**M**anagement) ด้านนโยบาย (**P**olicy) ด้านเทคโนโลยี (**T**echnology) ด้านบุคลากร (**H**uman) โดยมีคณะทำงานที่มีเป้าหมายเดียวกัน (**U**nity) มีพันธะสัญญาร่วมกันอย่างมุ่งมั่น (**C**ommitment) ที่จะช่วยเหลือซึ่งกันและกัน (**H**abit) พฤติกรรมผู้ใช้งานของเกี่ยวข้องกับระบบความมั่นคง

ปลอดภัยขององค์กร (**O**rganization) อย่างเป็นขั้นตอน (**P**rocedure) ในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี (**T**echnology) ให้มีความมั่นคงปลอดภัย ประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร และบุคลากร เพื่อรองรับภารกิจของมหาวิทยาลัยราชภัฏในด้าน การเรียนการสอน การบริหารสถานศึกษา การให้บริการชุมชน เพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้งานของ ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ รวมทั้งทรัพย์สินอื่น ๆ ที่มีความสำคัญของสถานศึกษา โดยดำเนินการ นำมาใช้ ตรวจสอบ วัดผล ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารการรักษาความปลอดภัย เพื่อให้สถานศึกษารอดพ้นจากภัยคุกคามต่าง ๆ โดใช้หลัก Plan-Do-Check-Act (PDCA Model) มีแกนหลักในการดำเนินการ 11 ด้าน 105 ตัวบ่งชี้ กระบวนการในการกำหนดนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ต้องใช้การบริหารจัดการจัดการ ด้านเทคโนโลยี การบริหารจัดการทรัพยากรมนุษย์ ผู้บริหารระดับสูงต้องมีการอนุมัติแต่งตั้งคณะทำงานอย่างเป็นลายลักษณ์อักษรและมีการกำหนดภารกิจหน้าที่อย่างชัดเจนเพื่อร่วมกันกำหนด นโยบาย ดำเนินงาน และการติดตามประเมินผล เพื่อให้เกิดความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล กระบวนการ การสื่อสาร บุคลากร เพื่อให้ภารกิจในการเรียนการสอน การบริหารสถานศึกษา และการบริหารชุมชุนให้ดำเนินไปอย่างต่อเนื่องพร้อมใช้งานมี ความถูกต้องสมบูรณ์ และควบคุมการเข้าสู่ชั้นความลับของฐานข้อมูลได้อย่างมีประสิทธิภาพ คณะผู้บริหาร ผู้บริหารระดับสูงต้องตั้งคณะกรรมการจากทุกหน่วยงานที่เกี่ยวข้องเป็นคณะทำงาน ตามแนวทางดำเนินงาน 11 ด้านประกอบด้วย 105 ตัวบ่งชี้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และดำเนินการตามโมเดล การจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

รูปแบบ โปรแกรมการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา “**Ed-SAM”**

(Education Security Assessment Model)”

คุณลักษณะ เป็นเครื่องมือทางการบริหาร สำหรับตรวจประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หลักการของการออกแบบโครงสร้างจะใช้อ้างอิงรูปแบบ PDCA ซึ่งเป็นหลักการบริหารเดียวกับมาตรฐานสากลอื่น ที่นิยมใช้กันทั่วโลก ตามกระบวน PDCA เริ่มจาก การวางแผน การลงมือทำ การปฏิบัติการ การเฝ้าระวัง การทบทวน การดูแลรักษา และการปรับปรุงระบบเทคโนโลยีสารสนเทศ

ขั้นตอนการปฏิบัติ PDCA เพื่อการนำรูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ **Ed-SAM Model** จะดำเนินการตรวจประเมิน ดังนี้

การวางแผนงาน (Plan) ตรวจประเมินการวางแผนจัดทำ ดำเนินการ โดยการ กำหนดขอบเขตการจัดทำ กำหนดนโยบาย กำหนดรูปแบบและวิธีการประเมินความเสี่ยง ระบุความเสี่ยง วิเคราะห์และประเมินความเสี่ยง วิเคราะห์และประเมินหนทางในการลดความเสี่ยง กำหนดวัตถุประสงค์และมาตรการในการควบคุมเพื่อลดความเสี่ยง ขออนุมัติผู้บริหารเกี่ยวกับความเสี่ยงที่ไม่มีมาตรการเพื่อควบคุม ขออนุมัติผู้บริหารเกี่ยวกับการทำระบบ จัดทำเอกสารสรุปแนวทางในการประยุกต์ใช้

การปฏิบัติการตามแผน (Do) ตรวจประเมินดำเนินการตามแผน กำหนดแผน กำจัดความเสี่ยง ซึ่งประกอบด้วยแนวทางในการปฏิบัติสำหรับผู้บริหาร ทรัพยากรที่ใช้ ความรับผิดชอบ และลำดับความสำคัญของความเสี่ยง ปฏิบัติตามแผนลดความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ ดำเนินการตามมาตรการควบคุมที่เลือก เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ กำหนดเกณฑ์สำหรับวัดประสิทธิภาพของมาตรการควบคุม ฝึกอบรมและกระตุ้นให้ตระหนักเกี่ยวกับการรักษาความปลอดภัย บริหารการปฏิบัติการ บริหารทรัพยากร กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับ และตอบโต้เมื่อเกิดเหตุการณ์เกี่ยวกับความปลอดภัย

การเฝ้าระวังและตรวจสอบ (Check) ตรวจประเมิน การเฝ้าระวังและตรวจสอบ การเฝ้าระวังและตรวจจับข้อผิดพลาดต่าง ๆ แผนประเมินประสิทธิภาพการปฏิบัติตามมาตรการต่าง ๆ ตรวจพิจารณาระบบมีประสิทธิภาพเพียงพอหรือไม่ ประเมินเป็นประจำว่า ความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่ ตรวจสอบภายในระบบ ตรวจสอบและประเมินว่าระบบทำงานตามขอบเขตที่กำหนดหรือไม่ ปรับปรุงแผนรักษาความปลอดภัยเพื่อป้องกันข้อผิดพลาดต่าง ๆ ที่ตรวจพบ บันทึกการปฏิบัติและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพการทำงานของระบบ

การรักษาและปรับปรุง (Act) ตรวจประเมินการรักษาและปรับปรุง การเพิ่มเติมเพื่อปรับปรุงระบบ แก้ไขปัญหาที่เกิดขึ้นและป้องกันไม่ให้เกิดขึ้นอีก สื่อสารให้ผู้เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงระบบ ทำให้แน่ใจว่า การปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

ตรวจสอบการมีการกำหนดเกี่ยวกับการจัดทำเอกสารเพื่อจะชี้ให้เห็นชัดว่านโยบายที่กำหนดนั้นจะนำไปปฏิบัติจริง โดยเอกสารที่ต้องจัดทำประกอบด้วย

1. แถลงการณ์เกี่ยวกับวัตถุประสงค์และนโยบายของระบบ
2. ของเขตการทำงานของระบบ
3. ข้ออธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง
4. รายงานเกี่ยวกับการประเมินความเสี่ยง
5. กำหนดแผนเพื่อลดความเสี่ยง
6. กำหนดแนวทางการปฏิบัติสำหรับองค์กรเพื่อให้สามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ และกำหนดแนวทางในการวัดประสิทธิภาพของมาตรการควบคุมต่าง ๆ

7. การเก็บรักษาเอกสารต่าง ๆ ที่ทำตามมาตรฐานนี้

8. แถลงการณ์ของการประยุกต์ใช้งาน

โดยพัฒนาปรับปรุงเพื่อความเหมาะสมของตัวบ่งชี้ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษามี 11 ด้าน และ 105 ตัวบ่งชี้ ประกอบด้วย

1. นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

2. โครงสร้างความมั่นคงปลอดภัยขององค์กร

3. การบริหารจัดการทรัพย์สินขององค์กร

4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

6. การบริหารจัดการด้านการสื่อสาร และการดำเนินงานเครือข่ายสารสนเทศ

7. การควบคุมการเข้าถึง

8. การจัดหา การพัฒนา และบำรุงระบบสารสนเทศ

9. บริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

10. บริหารความต่อเนื่องในการดำเนินงาน

11. การปฏิบัติตามข้อกำหนด

ประโยชน์ ที่ได้จากรูปแบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา หรือ Education Security Assessment Model (Ed-SAM)

1. สามารถใช้เป็นเครื่องมือในการตรวจสอบสภาพปัจจุบันของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในสถาบันการศึกษาต่างๆ

2. ผู้บริหารสามารถได้รับข้อมูลที่เป็นตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่มีระดับความสำคัญ เพื่อลำดับความสำคัญในการบริหารจัดการ

3. สามารถใช้เป็นแนวทางในการวางนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล

4. สร้างภาพลักษณ์ที่ดีให้กับสถาบันการศึกษา เพราะนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศมีความมั่นคง มั่นใจได้ในข้อมูลซึ่งมีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

5. เป็นไปตามข้อกำหนดของกฎหมายประเทศไทยและสากล (รองรับการเปิดเสรีประชาคมอาเซียน)

จุดเด่นของ “Ed-SAM” มี 5 ป ดังนี้

1. **ประเมิน**ได้ง่าย ง่ายในการใช้งาน และการเรียนรู้ มีข้อแนะนำ ข้อควรปฏิบัติของผู้เกี่ยวข้องด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทุกฝ่าย ประกอบด้วย ผู้บริหาร ผู้ปฏิบัติการ ผู้ใช้งานทั้งภายในและภายนอก

2. **ประหยัดเวลา** เข้าใจง่าย

3. **ประหยัดค่าใช้จ่าย** ดำเนินได้ด้วยตนเอง

4. **ประโยชน์** ใช้ได้กับทุกหน่วยงาน

5. **ประสิทธิภาพ** มีตัวถ่วงน้ำหนักในแต่ละตัวบ่งชี้ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศทำให้ทราบลำดับความสำคัญ ทำให้ง่ายในการวางนโยบายต่าง ๆ ผู้บริหารสามารถรู้ จัดสรรทรัพยากรได้อย่างมีประสิทธิภาพยิ่งขึ้น

ลักษณะการใช้งาน“Ed-SAM”

1. มีการบอกขั้นตอนการนำไปใช้

ขั้นตอนการเก็บข้อมูล

ขั้นตอนการวิเคราะห์

ขั้นตอนการประเมินผล

ขั้นตอนเสนอแนะ แก้ไข ปรับปรุงด้านการบริหารจัดการ บุคลากรและเทคโนโลยี

2. มีสื่อในการใช้งาน เป็นเอกสาร ประกอบด้วย กระบวนการ Plan-Do-Check-Act

มีคู่มือการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

มีแบบฟอร์มสำเร็จรูป ในการ เก็บข้อมูล ตรวจประเมิน

มีคู่มือเกณฑ์การประเมิน

มีข้อเสนอแนะ ข้อควรระวัง การป้องกัน การแก้ไข

มี ซอฟต์แวร์สำเร็จรูป สามารถนำไปใช้และทราบผลการประเมิน พร้อมแนวทางในการปรับปรุงแก้ไข อย่างอัตโนมัติและรวดเร็ว

มี Website Help Desk Service ให้บริการตลอด 24 ชั่วโมง ทุกหนทุกแห่ง

วิธีการใช้แบบประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

ขั้นตอนเก็บข้อมูล

1 สัมภาษณ์ และตรวจหลักฐาน ในแต่ละข้อ

ทำการบันทึก การปฏิบัติการหรือการมีการดำเนินการแต่ละข้อ และขอตรวจหลักฐาน เป็นเอกสาร หรือรายงานการปฏิบัติงาน กฎ ระเบียบ ข้อบังคับ ต่าง ๆ ที่เกี่ยวข้องในประเด็นที่กำลังประเมิน

2 การให้คะแนน หลักเกณฑ์ในการให้คะแนนในแต่ละกิจกรรม มีดังนี้

กรณีที่ 1 มีการดำเนินการ ให้คะแนน 1 คะแนน

กรณีที่ 2 ไม่มีการดำเนินการ ให้คะแนน 0 คะแนน

กรณีที่ 3 อยู่ระหว่างดำเนินการ ให้คะแนน 0 คะแนน

(เพราะผลความมั่นคงปลอดภัยมีผลเช่นเดียวกับไม่มีการดำเนินการ)

3. การจัดลำดับความสำคัญของตัวบ่งชี้ โดยใช้ค่าถ่วงน้ำหนัก

ในแต่ละด้านของตัวบ่งชี้ จะประกอบด้วย ข้อของตัวบ่งชี้ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในด้านนั้น

ตัวบ่งชี้แต่ละข้อ จะมีค่าน้ำหนักคะแนน เพื่อใช้ในการจัดลำดับความสำคัญ

การบริหารจัดการพิจารณาเป็นแต่ละด้าน คะแนนรวมแต่ละด้านเท่ากัน และมีคะแนนเต็มเท่ากับ 5 คะแนน

ให้คะแนน ในแต่ละข้อ โดย นำคะแนนที่ได้จากการดำเนินงาน (0 = ไม่มีการดำเนินการหรืออยู่ระหว่างดำเนินการ, 1 = มีการดำเนินการ) คูณ คะแนนน้ำหนัก

นำคะแนนที่ได้ในแต่ละข้อ ในด้านนั้น ๆ มารวมกัน (แต่ละด้าน มีคะแนนเต็ม = 5 คะแนน) จะได้ ผลรวมของคะแนน เพื่อที่จะนำไปประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในด้านนั้น

ขั้นตอนการวิเคราะห์

การวิเคราะห์ เพื่อประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในด้านนั้น โดยการนำผลรวมของคะแนนที่ได้ในแต่ละด้าน ไปเปรียบเทียบกับ ตารางเกณฑ์ประเมิน

เกณฑ์การประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ช่วงที่	ช่วงคะแนน	ระดับคุณภาพ
1	4.51-5.00	ดีมาก
2	3.51-4.50	ดี
3	2.51-3.50	พอใช้
4	1.51-2.50	ต้องปรับปรุง
5	0.00-1.50	ต้องปรับปรุงเร่งด่วน

ช่วงคะแนนแต่ละช่วง สามารถ บ่งชี้ระดับคุณภาพความมั่นคงระบบเทคโนโลยีสารสนเทศในองค์กร ผู้บริหารสามารถนำข้อมูลนี้ไปใช้ในการวางนโยบายและแผนในการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีเกณฑ์และข้อควรปฏิบัติในการบริการจัดการ ดังต่อไปนี้

1. ช่วงระดับคะแนนประเมิน 4.51-5.00 เป็นระดับคุณภาพความมั่นคงที่ดีมากโอกาสในการเกิดเหตุการณ์ต่าง ๆ น้อยมาก องค์กรมีความพร้อมมากในการรักษาความมั่นคงปลอดภัย

2. ช่วงระดับคะแนนประเมิน 3.51-4.50 เป็นระดับความมั่นคงอยู่ในระดับดี ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ น้อย องค์กรมีความพร้อมในการรักษาความมั่นคงปลอดภัย

3. ช่วงระดับคะแนนประเมิน 2.51-3.50 เป็นระดับความมั่นคงอยู่ในระดับพอใช้ ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ ปานกลาง องค์กรมีความพร้อมในการรักษาความมั่นคงปลอดภัยในระดับปานกลาง ผู้บริหารควรเพิ่มและปรับปรุงคุณภาพ ตัวบ่งชี้ที่ยังไม่มีประสิทธิภาพ ให้ มีประสิทธิภาพยิ่งขึ้น

4. ช่วงระดับคะแนนประเมิน 1.51-2.50 เป็นระดับความมั่นคงอยู่ในระดับต้องปรับปรุง ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ มาก ผู้บริหารองค์กรต้องเร่งปรับปรุงคุณภาพตัวบ่งชี้ที่ยังไม่มี หรือ ไม่มีประสิทธิภาพ ให้มี และมีประสิทธิภาพยิ่งขึ้น

5. ช่วงระดับคะแนนประเมิน 0.00- 1.50 เป็นระดับความมั่นคงอยู่ในระดับ ต่ำมาก ต้องเร่งปรับปรุงเร่งด่วน ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ มีมากที่สุด ผู้บริหารองค์กรต้องเร่งปรับปรุงคุณภาพตัวบ่งชี้ที่ยังไม่มี หรือ ไม่มีประสิทธิภาพ ให้มี และมีประสิทธิภาพยิ่งขึ้นอย่างเร่งด่วน

การแปลค่า

ผลจากการประเมิน จะได้รับคะแนนที่ปรับน้ำหนักแล้ว

เรียงลำดับคะแนนจาก มาก ไปหา น้อย จะได้ ตัวบ่งชี้ที่มีความสำคัญมาก เรียงลำดับลงมาตามความสำคัญ

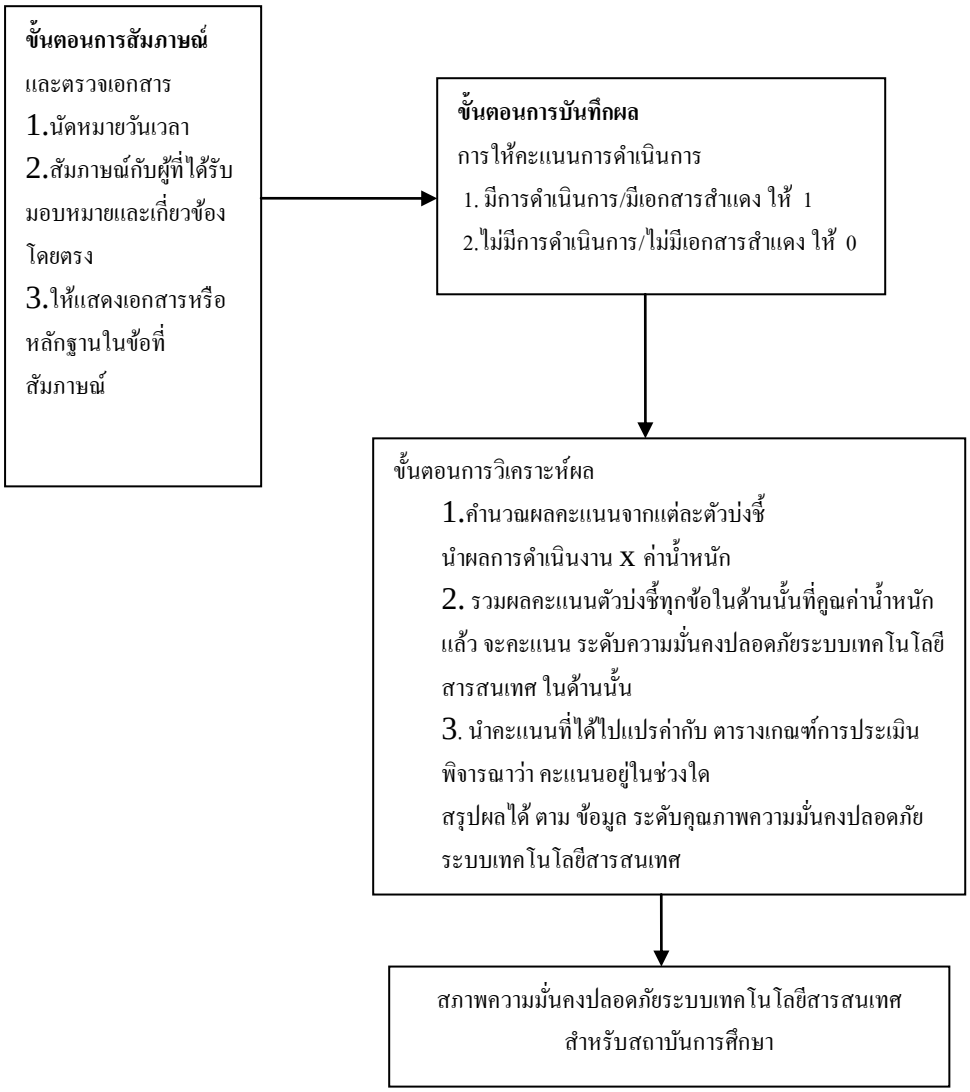
การบริหารจัดการ

พิจารณา ตัวบ่งชี้ที่สำคัญมากเป็นลำดับแรก และรองลงมา ในการกำหนดนโยบาย ต่าง ๆ

การปรับปรุง

จะมีข้อมูลเสนอแนะ ในตารางข้อมูลเสนอแนะเพื่อดำเนินการวางแผน ปรับปรุงแก้ไขตามลำดับ

แผนภาพวิธีการประเมิน การบันทึกผล การแปลผล ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดำเนินขั้นตอนดังนี้



ขั้นตอนการสัมภาษณ์และตรวจเอกสาร

1. นัดหมายวันเวลา
2. สัมภาษณ์กับผู้ที่ได้รับมอบหมายและเกี่ยวข้องโดยตรง
3. ให้แสดงเอกสารหรือหลักฐานในข้อที่สัมภาษณ์

ขั้นตอนการบันทึกผล

การให้คะแนนการดำเนินการ

1. มีการดำเนินการ/มีเอกสารสำแดง ให้ 1
2. ไม่มีการดำเนินการ/ไม่มีเอกสารสำแดง ให้ 0

ขั้นตอนการวิเคราะห์ผล

1. คำนวณผลคะแนนจากแต่ละตัวบ่งชี้
   นำผลการดำเนินงาน x ค่าน้ำหนัก
2. รวมผลคะแนนตัวบ่งชี้ทุกข้อในด้านนั้นที่คูณค่าน้ำหนักแล้ว จะได้คะแนน ระดับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ในด้านนั้น
3. นำคะแนนที่ได้ไปแปลค่ากับ ตารางเกณฑ์การประเมิน พิจารณาว่า คะแนนอยู่ในช่วงใด สรุปผลได้ ตาม ข้อมูล ระดับคุณภาพความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตารางประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ประกอบด้วยตัวบ่งชี้ 11 ด้าน 105 ตัวบ่งชี้

1. นโยบายความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ ประกอบด้วย 9 ตัวบ่งชี้

วัตถุประสงค์ : เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบที่เกี่ยวข้อง

จำนวนตัวบ่งชี้ **:** 9 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 1.1 = 0.61 / 1.2 = 0.59 / 1.3 = 0.59 /

1.4 = 0.57 / 1.5 = 0.55 / 1.6 = 0.55 / 1.7 = 0.53 / 1.8 = 0.51 / 1.9 = 0.51

เอกสารหรือข้อมูลประกอบ :

1. นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ
2. ใบประเมินความรู้ของบุคลากร
3. แผนการติดตามนโยบายความมันคงปลอดภัย

ตาราง แสดงจำนวนตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน และเอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 1	การดำเนินการมี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้ (รวม 5 คะแนน)	คะแนน	เอกสารหรือข้อมูลประกอบ
1.1 มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร		0.61		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.2 มีการจัดการให้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศควรได้รับการอนุมัติจากคณะกรรมการบริหาร		0.59		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.3 มีการสื่อสารและประกาศใช้นโยบายรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับขององค์กรได้ทราบอย่างทั่วถึงผ่านช่องทางที่หลากหลาย		0.59		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตัวบ่งชี้ ด้านที่ 1	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
1.4 มีการประเมินความรู้ความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในองค์กร		0.57		ใบประเมินความรู้ของบุคลากร
1.5 มีนโยบายให้ดำเนินการสื่อสารหรือให้ความรู้เกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศแก่ผู้ใต้บังคับบัญชา		0.55		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.6 มีการให้บุคลากรภายในองค์กรแต่ละหน่วยงานที่ใช้งาน มีส่วนร่วมในการจัดทำหรือทบทวนนโยบายด้านความมั่นคงฯ		0.55		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.7 ผู้บริหารมีการสื่อสารแสดงความมุ่งมั่นในการสนับสนุนหรือบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศอย่างชัดเจน		0.53		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.8 มีการจัดเก็บนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไว้ในที่ที่ผู้ใช้งานหรือบุคลากรที่เกี่ยวข้องสามารถเข้าถึงได้ตามความเหมาะสม		0.51		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.9 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันสอดคล้องกับการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง		0.51		รายงานการประชุมและนโยบายความมั่นคงปลอดภัย

2. โครงสร้างความมั่นคงปลอดภัยขององค์กร

วัตถุประสงค์ : เพื่อบริหารและจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 2.1 = 1.04 / 2.2 = 1 / 2.3 = 1 /

2.4 = 1.04 / 2.5 = 0.93

เอกสารหรือข้อมูลประกอบ :

1. นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2. ระเบียบบริหารการเปลี่ยนแปลง
3. ระเบียบการติดตามและประเมินผล
4. ระเบียบบริหารบุคลากร

ตาราง ตัวบ่งชี้ / ค่าน้ำหนัก / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 2	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
2.1 ผู้บริหารให้ความสำคัญและสนับสนุนในการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน		1.04		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
2.2 มีการจัดการให้มีขั้นตอนในการอนุมัติการใช้งาน การพัฒนาหรือปรับปรุงเปลี่ยนแปลงระบบงานคอมพิวเตอร์		1.00		ระเบียบบริหารการเปลี่ยนแปลง
2.3 มีการจัดการให้มีรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มที่มีความเกี่ยวข้องในด้านการรักษาความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศอื่น ๆ ในกรณีที่มีความจำเป็น		1.00		นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ตัวบ่งชี้ ด้านที่ 2	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
2.4 มีการทบทวนด้านความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบอิสระ		1.04		ระเบียบการติดตามและประเมินผล
2.5 มีระเบียบข้อบังคับในเอกสารรับพนักงาน ห้ามมิให้พนักงานที่เข้ามาทำงานในองค์กร เปิดเผยความลับและข้อมูลขององค์กร		0.93		ระเบียบบริหารบุคลากร

3. การบริหารจัดการทรัพย์สินขององค์กร

วัตถุประสงค์ : เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

จำนวน ตัวบ่งชี้ : 4 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 3.1 = 1.32 / 3.2 = 1.32 / 3.3 = 1.27 / 3.4 = 1.08

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารพัสดุภัณฑ์
2. ระเบียบบริหารจัดการฐานข้อมูล

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 3	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
3.1 มีการจัดทำและปรับปรุงแก้ไขรายการบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้มีความถูกต้องและเป็นปัจจุบันอยู่เสมอ		1.32		ระเบียบบริหารพัสดุภัณฑ์
3.2 มีการจัดหมวดหมู่ข้อมูลตามระดับชั้นความลับหรือระดับความสำคัญ		1.32		ระเบียบบริหารจัดการฐานข้อมูล
3.3 มีการตรวจสอบรายการบัญชี		1.27		ระเบียบบริหาร

ทรัพย์สินขององค์กรอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง				พัสดุภัณฑ์
3.4 มีการจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ		1.08		ระเบียบบริหารพัสดุภัณฑ์

4. ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์ : เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกงและการใช้อุปกรณ์ผิดวัตถุประสงค์

จำนวน ตัวบ่งชี้ : 9 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 4.1 = 0.61 / 4.2 = 0.59 / 4.3 = 0.59 / 4.4 = 0.59 / 4.5 = 0.57 / 4.6 = 0.53 / 4.7 = 0.53 / 4.8 = 0.51 / 4.9 = 0.49

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารบุคลากร

ตัวบ่งชี้ ด้านที่ 4	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
4.1 มีการกำหนดหน้าที่ความรับผิดชอบทางด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศให้แก่บุคลากรฝ่ายคอมพิวเตอร์อย่างชัดเจน		0.61		ระเบียบบริหารบุคลากร
4.2 มีการจัดทำขั้นตอนการปฏิบัติงานประจำ ของเจ้าหน้าที่ฝ่ายปฏิบัติการคอมพิวเตอร์ เป็นลายลักษณ์อักษร		0.59		ระเบียบบริหารบุคลากร
4.3 มีการจัดอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ		0.59		ระเบียบบริหารบุคลากร

ตัวบ่งชี้ ด้านที่ 4	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
4.4 มีการยกเลิกสิทธิ์ในการเข้าถึงของพนักงาน เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน		0.59		ระเบียบบริหารบุคลากร
4.5 มีการกำหนดให้บุคคลภายในองค์กรหรือหน่วยงานที่องค์กรว่าจ้างจากภายนอกปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร		0.57		ระเบียบบริหารบุคลากร
4.6 มีการตรวจสอบ คุณสมบัติของผู้สมัคร		0.53		ระเบียบบริหารบุคลากร
4.7 มีการให้พนักงานได้รับการอบรมเพื่อสร้างความตระหนักและเสริมความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ		0.53		ระเบียบบริหารบุคลากร
4.8 มีการให้พนักงานคืนทรัพย์สินที่อยู่ในความครอบครอง เมื่อพนักงานมีการเปลี่ยนแปลงลักษณะงาน		0.51		ระเบียบบริหารบุคลากร
4.9 มีกระบวนการทางวินัยเพื่อลงโทษผู้ที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กร		0.49		ระเบียบบริหารบุคลากร

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์ : เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหายและการก่อกวนการเข้าถึงหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร และป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

จำนวน ตัวบ่งชี้ : 10 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 5.1 = 0.54 / 5.2 =0.54 / 5.3 = 0.52 / 5.4 = 0.52 / 5.5 = 0.50 / 5.6 = 0.50 / 5.7 = 0.50 / 5.8 = 0.48 / 5.9 = 0.46 / 5.10 = 0.45

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการเทคโนโลยี
2. ระเบียบบริหารจัดการสิ่งแวดล้อม
3. ระเบียบบริหารบุคลากร

ตัวบ่งชี้ ด้านที่ 5	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
5.1 มีอุปกรณ์ป้องกันไฟฟ้าขัดข้อง เช่นเครื่องสำรองไฟฟ้า ยูพีเอส เครื่องกำเนิดไฟฟ้าสำรอง		0.54		ระเบียบบริหารจัดการเทคโนโลยี
5.2 มีการบำรุงรักษาอุปกรณ์ป้องกันการล้มเหลวและอุปกรณ์สนับสนุนให้สามารถทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน		0.54		ระเบียบบริหารจัดการเทคโนโลยี
5.3 มีอุปกรณ์ป้องกันไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน และอยู่ในสภาพพร้อมใช้งาน		0.52		ระเบียบบริหารจัดการเทคโนโลยี

ตัวบ่งชี้ ด้านที่ 5	การดำเนินการมี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
5.4 มีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน ตรวจจับความร้อน		0.52		ระเบียบบริหารจัดการเทคโนโลยี
5.5 มีการควบคุมอุณหภูมิและความชื้นภายในศูนย์คอมพิวเตอร์ที่แยกจากเครื่องปรับอากาศรวม		0.50		ระเบียบบริหารจัดการเทคโนโลยี
5.6 มีการควบคุมการเข้า ออกบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย		0.50		ระเบียบบริหารจัดการสิ่งแวดล้อม
5.7 มีการติดตั้งกล้อง CCTV ไว้ในศูนย์ควบคุมระบบคอมพิวเตอร์อย่างเพียงพอ และอยู่ในสภาพพร้อมใช้งาน		0.50		ระเบียบบริหารจัดการเทคโนโลยี
5.8 มีการควบคุมบุคลากรอื่นที่มีความจำเป็นต้องเข้ามาปฏิบัติหน้าที่ในศูนย์คอมพิวเตอร์เป็นการชั่วคราว		0.48		ระเบียบบริหารบุคลากร
5.9 มีข้อแนะนำให้ความระวังและป้องกันอุปกรณ์จากอุบัติเหตุ ต่าง ๆ เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชนหรือเสี่ยงต่อการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์		0.46		ระเบียบบริหารจัดการสิ่งแวดล้อม
5.10 มีการควบคุม การเข้าออกบริเวณสำนักงานอย่างมีระบบ เช่น การใช้การ์ดรูดก่อนเข้าสำนักงาน		0.45		ระเบียบบริหารจัดการสิ่งแวดล้อม

6. การบริหารจัดการด้านการสื่อสารและการดำเนินการของเครือข่ายสารสนเทศขององค์กร

วัตถุประสงค์ : เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย และรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก ลดความเสี่ยงจากความล้มเหลวของระบบ รักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี รักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาตและการติดขัดหรือหยุดชะงักทางธุรกิจ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก สร้างความมั่นคงปลอดภัยสำหรับพาณิชย์อิเล็คทรอนิคส์และการใช้งาน ตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

จำนวน ตัวบ่งชี้ : 19 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 6.1 = 0.32 / 6.2 = 0.32 / 6.3 = 0.32 / 6.4 = 0.32 / 6.5 = 0.31 / 6.6 = 0.30 / 6.7 = 0.30 / 6.8 = 0.30 / 6.9 = 0.30 / 6.10 = 0.30 / 6.11 = 0.30 / 6.12 = 0.29 / 6.13 = 0.29 / 6.14 = 0.24 / 6.15 = 0.18 / 6.16 = 0.16 / 6.17 = 0.16 / 6.18 = 0.16 / 6.19 = 0.16

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการฐานข้อมูล
2. ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
3. ระเบียบบริหารบุคลากร
4. ระเบียบบริหารจัดการเทคโนโลยี
5. ระเบียบบริหารการเปลี่ยนแปลง

ตัวบ่งชี้ ด้านที่ 6	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
6.1 มีการสำรองข้อมูลและโปรแกรมเป็นประจำ		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.2 มีการนำสื่อที่ใช้ในการบันทึกข้อมูลสำรองเก็บไว้ในสถานที่ปลอดภัย		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.3 มีการเข้ารหัส ข้อมูลสำคัญที่ส่งผ่านเครือข่าย		0.28		ระเบียบบริหารจัดการฐานข้อมูล
6.4 มีการบันทึกกิจกรรมหรือเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศโดยมีการเก็บบันทึกไว้อย่างน้อย 90 วัน		0.28		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.5 มีการควบคุมการรับส่งสื่อบันทึกที่จัดเก็บไว้ เช่น การตรวจสอบข้อตนของผู้ที่มารับ-ส่ง มีการระบุผู้รับผิดชอบในการติดต่อ		0.27		ระเบียบบริหารจัดการฐานข้อมูล
6.6 มีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.7 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ		0.26		ระเบียบบริหารบุคลากร
6.8 มีแผนฉุกเฉิน เป็นลายลักษณ์อักษรเพื่อรองรับการใช้งานในกรณีระบบล้มเหลว		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย
6.9 มีการทดสอบแผนฉุกเฉิน ว่าสามารถปฏิบัติได้จริง		0.26		ระบบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตัวบ่งชี้ ด้านที่ 6	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
6.10 มีระบบป้องกันและตรวจสอบไวรัสที่ครอบคลุมเครือข่ายและลูกข่ายที่สำคัญ		0.26		ระเบียบบริหารจัดการเทคโนโลยี
6.11 มีการกำหนดขั้นตอนมาตรฐานในการดำเนินการด้านการสื่อสารและเครือข่ายแต่ละประเภท		0.26		ระเบียบบริหารจัดการเทคโนโลยี
6.12 มีการควบคุมไม่ให้ผู้ใช้งานระงับการใช้งาน ระบบป้องกันไวรัสที่ติดตั้งไว้		0.25		ระเบียบบริหารจัดการเทคโนโลยี
6.13 มีวิธีการจัดการสื่อบันทึกข้อมูลลับ ที่ไม่ได้ใช้แล้ว		0.25		ระเบียบบริหารจัดการฐานข้อมูล
6.14 มีการปรับปรุง Virus Signature ให้เป็นปัจจุบัน		0.25		ระเบียบบริหารจัดการเทคโนโลยี
6.15 มีการจัดการให้ระบบปฏิบัติการจริงแยกออกจากระบบที่ใช้ในการพัฒนาหรือทดสอบ		0.25		ระเบียบบริหารการเปลี่ยนแปลง
6.16 มีการกำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรการรองรับเพื่อป้องกันปัญหาจากการแลกเปลี่ยนสารสนเทศระหว่างองค์กร		0.25		ระเบียบบริหารจัดการฐานข้อมูล
6.17 มีการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงาน		0.25		ระเบียบบริหารจัดการการเปลี่ยนแปลง
6.18 มีการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง		0.24		ระเบียบบริหารจัดการเทคโนโลยี
6.19 มีการจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานรวมถึงแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ ๆ		0.24		ระเบียบบริหารจัดการเทคโนโลยี

7. การควบคุมการเข้าถึง

วัตถุประสงค์ : เพื่อควบคุมการเข้าถึงสารสนเทศ ควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ไปดำเนินการเปิดเผยหรือขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

จำนวน ตัวบ่งชี้ : 29 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 7.1 = 0.19 / 7.2 = 0.19 / 7.3 = 0.19 / 7.4 = 0.19 / 7.5 = 0.19 / 7.6 = 0.19 / 7.7 = 0.19 / 7.8 = 0.18 / 7.9 = 0.18 / 7.10 = 0.18 / 7.11 = 0.17 / 7.12 = 0.17 / 7.13 = 0.17 / 7.14 = 0.17 / 7.15 = 0.17 / 7.16 = 0.17 / 7.17 = 0.17 / 7.18 = 0.17 / 7.19 = 0.17 / 7.20 = 0.17 / 7.21 = 0.17 / 7.22 = 0.17 / 7.23 = 0.17 / 7.24 = 0.16 / 7.25 = 0.16 / 7.26 = 0.15 / 7.27 = 0.15 / 7.28 = 0.15 / 7.29 = 0.15

เอกสารหรือข้อมูลประกอบ : 1.ระเบียบบริหารการเปลี่ยนแปลง 2.ระเบียบการบริหารจัดการฐานข้อมูล 3.ระเบียบบริหารจัดการเทคโนโลยี

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.1 มีนโยบายควบคุมการเข้าถึงระบบอย่างเป็นลายลักษณ์อักษร มีการกำหนดสิทธิ์การใช้ข้อมูลระบบคอมพิวเตอร์โดยให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติงาน		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.2 มีระบบที่ป้องกันการบุกรุก เช่น firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก		0.19		ระเบียบบริหารจัดการเทคโนโลยี
7.3 มีนโยบายควบคุมไม่ให้ข้อมูลมีความสำคัญถูกนำออกภายนอกองค์กร		0.19		ระเบียบบริหารจัดการฐานข้อมูล

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.4 มีระบบบริหารจัดการรหัสผ่าน สำหรับผู้ใช้ อย่างมีประสิทธิภาพ		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.5 มีมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น กรณีที่ส่งซ่อม ควรลบข้อมูลที่เก็บไว้ในสื่อบันทึกก่อนส่งซ่อม		0.19		ระเบียบบริหารจัดการฐานข้อมูล
7.6 มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงและโอนย้ายระบบงาน และทดสอบระบบงาน		0.19		ระเบียบบริหารการเปลี่ยนแปลง
7.7 มีการควบคุมการดำเนินการในการพัฒนาหรือแก้ไขระบบงาน		0.19		ระเบียบบริหารจัดการเทคโนโลยี
7.8 มีการควบคุมและจำกัดการใช้งาน software utility สำหรับระบบงานคอมพิวเตอร์ application system		0.18		ระเบียบบริหารจัดการเทคโนโลยี
7.9 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้องครบถ้วนและทำงานที่มีประสิทธิภาพ		0.18		ระเบียบบริหารการเปลี่ยนแปลง

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.10 มีการจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน		0.18		ระเบียบบริหารการเปลี่ยนแปลง
7.11 มีการควบคุมการแชร์ไฟล์ ข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ส่วนบุคคล กำหนดรหัสผ่าน กำหนดสิทธิ์ให้เฉพาะรายที่จำเป็นเท่านั้น		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.12 มีการควบคุมผู้ให้บริการ (IT Outsourcing) ในการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลสารสนเทศขององค์กร		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.13 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.14 มีการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร เมื่อมีการร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์		0.17		ระเบียบบริหารการเปลี่ยนแปลง

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.15 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงานด้านระบบรักษาความปลอดภัยและระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร		0.17		ระเบียบบริหารการเปลี่ยนแปลง
7.16 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.17 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บในหน่วยจัดเก็บ การนำเข้า การประมวลผล และการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.18 มีนโยบายในการควบคุมการเข้าถึงระบบให้เป็นปัจจุบันอยู่เสมอ		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.19 มีการกำหนดและทบทวนสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่ การโอนย้ายส่วนงานหรือลาออกอย่างสม่ำเสมอ		0.17		ระเบียบการบริหารจัดการฐานข้อมูล

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.20 มีการกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ เช่นสิทธิ์การใช้โปรแกรม และระบบงานคอมพิวเตอร์ Application System สิทธิ์การใช้งานอินเตอร์เน็ต		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.21 มีระบบบังคับอายุของรหัสผ่าน เช่น ตั้งรหัสผ่านให้ยากแก่การคาดเดา บังคับไม่ให้ใช้รหัสผ่านซ้ำของเดิม ระบบป้องกันอัตโนมัติ ในกรณีที่ป้อนรหัสผิดและไม่มีการใช้งานหน้าจอเป็นระยะเวลาหนึ่ง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.22 มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.23 มีการที่ระบบจะทำการป้องกันหน้าจออัตโนมัติ เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลาหนึ่ง		0.17		ระเบียบการบริหารจัดการฐานข้อมูล
7.24 มีการบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่เข้าระบบครั้งแรกหรือเมื่อถูก reset password		0.16		ระเบียบการบริหารจัดการฐานข้อมูล

ตัวบ่งชี้ ด้านที่ 7	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
7.25 มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่ประกอบไปด้วยขอบเขตของเครือข่ายภายในเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ		0.16		ระเบียบบริหารจัดการเทคโนโลยี
7.26 มีการบังคับความยาวขั้นต่ำของรหัสผ่าน		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.27 มีการดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานที่สำคัญเพื่อดูช่องโหว่ต่าง ๆ ของโปรแกรมระบบ System software management		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.28 มีการกำหนดบุคคล ให้สามารถแก้ไขข้อมูลในฐานข้อมูลได้โดยตรงโดยไม่ผ่านระบบงาน system application		0.15		ระเบียบการบริหารจัดการฐานข้อมูล
7.29 มีการแบ่งแยกเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเตอร์เน็ตกับระบบที่เชื่อมต่ออินทราเน็ต		0.15		ระเบียบบริหารจัดการเทคโนโลยี

8. การจัดหา การพัฒนาและบำรุงระบบสารสนเทศ

วัตถุประสงค์ : เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัย ป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับไฟล์ต่าง ๆ ของระบบที่ให้บริการ รักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ เพื่อลดความเสี่ยงจากการถูกโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

จำนวน ตัวบ่งชี้ : 7 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 8.1 = 0.87 / 8.2 = 0.84 / 8.3 = 0.84 / 8.4 = 0.81 / 8.5 = 0.75 / 8.6 = 0.45 / 8.7 = 0.45

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารการเปลี่ยนแปลง
2. ระเบียบบริหารจัดการฐานข้อมูล

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.1 มีขั้นตอนหรือวิธีปฏิบัติและควบคุมในการพัฒนาหรือแก้ไขเปลี่ยนแปลง โอนย้าย และทดสอบระบบงาน		0.78		ระเบียบบริหารการเปลี่ยนแปลง
8.2 มีการทดสอบโปรแกรมที่พัฒนาหรือแก้ไขเพื่อให้มั่นใจได้ว่าระบบงานนั้นมีการประมวลผลที่ถูกต้อง ครบถ้วน และทำงานที่มีประสิทธิภาพ		0.75		ระเบียบบริหารการเปลี่ยนแปลง

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.3 มีการได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรและจัดทำเอกสารประกอบการแก้ไขระบบงานในแต่ละขั้นตอน เช่นเอกสารร้องขอจากผู้ใช้งาน เอกสารในการทดสอบ เอกสารตรวจรับระบบ และคู่มือในการใช้งาน		0.75		ระเบียบบริหารการเปลี่ยนแปลง
8.4 มีการวิเคราะห์และประเมินผลกระทบที่เกี่ยวข้องในการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์		0.72		ระเบียบบริหารการเปลี่ยนแปลง
8.5 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ ในหน่วยจัดเก็บ การนำเข้า การประมวลผล แบะการแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลสัมพันธ์กัน		0.72		ระเบียบบริหารจัดการฐานข้อมูล

ตัวบ่งชี้ ด้านที่ 8	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
8.6 มีการประเมินผลกระทบของการพัฒนาหรือแก้ไขระบบงานสารสนเทศ ทั้งก่อนทำ และหลังทำระบบ ในด้านการปฏิบัติงาน ด้านระบบรักษาความปลอดภัย และระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร		0.72		ระเบียบบริหารการเปลี่ยนแปลง
8.7 มีการจัดทำนโยบายควบคุมและบังคับใช้งานการเข้ารหัสข้อมูล		0.72		ระเบียบการบริหารจัดการฐานข้อมูล

9. **การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร**

วัตถุประสงค์ : เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม ให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย สำหรับสารสนเทศขององค์กร

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 9.1 = 11.02 / 9.2 = 1.02 / 9.3 = 0.99 / 9.4 = 0.99 / 9.5 = 0.99

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารจัดการฐานข้อมูล
2. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
3. ระเบียบบริหารจัดการเทคโนโลยี

ตัวบ่งชี้ ด้านที่ 9	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
9.1 มีมาตรการป้องกันและจำกัดสิทธิ์การเข้าถึง การแก้ไข เปลี่ยนแปลง บันทึกต่าง ให้กับบุคคลที่เกี่ยวข้องเท่านั้น		1.02		ระเบียบบริหารจัดการฐานข้อมูล
9.2 มีการแจ้งให้ผู้เกี่ยวข้องรับทราบทุกครั้ง โดยผ่านช่องทางที่องค์กรได้จัดเตรียมไว้ ในกรณีที่พบเครื่องติดไวรัสบนคอมพิวเตอร์ที่ใช้งานอยู่		1.02		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตัวบ่งชี้ ด้านที่ 9	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
9.3 มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย มีการบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก		0.99		ระเบียบบริหารจัดการเทคโนโลยี
9.4 มีช่องทางให้พนักงานรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร เช่นเมื่อพบไวรัสบนเครื่องคอมพิวเตอร์		0.99		ระเบียบบริหารจัดการเทคโนโลยี
9.5 มีการฝึกซ้อมรับมือกับเหตุฉุกเฉินในรูปแบบต่าง ๆ		0.99		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

วัตถุประสงค์ : เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

จำนวน ตัวบ่งชี้ : 3 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 10.1 =1.79 / 10.2 = 1.73 / 10.3 = 1.49

เอกสารหรือข้อมูลประกอบ :

1. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 10	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
10.1 มีการประเมินความเสี่ยงทางด้านระบบเทคโนโลยีสารสนเทศรวมถึงผลกระทบในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ		1.79		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
10.2 มีการกำหนดแผนหรือกลยุทธ์เพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว		1.73		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
10.3 มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับการใช้งาน ให้เป็นปัจจุบันอยู่เสมอ		1.49		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

11. การปฏิบัติตามข้อกำหนด

วัตถุประสงค์ : เพื่อหลีกเลี่ยงการละเมินข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ ให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร ให้การตรวจประเมินสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

จำนวน ตัวบ่งชี้ : 5 ตัวบ่งชี้

ค่าน้ำหนักตัวบ่งชี้แต่ละข้อ เรียงลำดับดังนี้ : 11.1 = 1.07 / 11.2 = 1.03 / 11.3 = 0.99 / 11.4 = 0.95 / 11.5 = 0.95

เอกสารหรือข้อมูลประกอบ : 1. ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

ตาราง ตัวบ่งชี้ / ค่าน้ำหนักตัวบ่งชี้ / คะแนน / เอกสารหรือข้อมูลประกอบ

ตัวบ่งชี้ ด้านที่ 11	การดำเนินการ มี (1) ไม่มี/ระหว่างดำเนินการ(0)	ค่าน้ำหนักตัวบ่งชี้	คะแนน	เอกสารหรือข้อมูลประกอบ
11.1 มีวิธีปฏิบัติเพื่อให้บุคลากรปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรตามที่กำหนดไว้		1.07		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.2 มีผู้ตรวจสอบภายในและมีผู้ตรวจสอบอิสระจากภายนอกเข้ามาตรวจสอบการปฏิบัติงานหรือการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ		1.03		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.3 มีการกำกับดูแลและตรวจสอบผู้ใต้บังคับบัญชาให้ปฏิบัติตามนโยบายอย่างถูกต้องอย่างสม่ำเสมอ		0.99		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.4 มีการกำหนดห้ามละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา		0.95		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย
11.5 มีการรวบรวมกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศไว้อย่างครบถ้วน		0.95		ระเบียบบริหารความต่อเนื่องความมั่นคงปลอดภัย

วิธีการใช้โปรแกรม
เพื่อการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
สำหรับสถาบันการศึกษา

ประโยชน์ที่ได้รับ

1. ผู้บริหารใช้เป็นเครื่องมือประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษาเพื่อตรวจสอบสภาพปัจจุบันของความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับสถาบันการศึกษา

2. ผู้บริหารสามารถได้รับข้อมูลที่เป็นตัวบ่งชี้ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่มีระดับความสำคัญ เพื่อลำดับความสำคัญในการบริหารจัดการ

3. สามารถใช้เป็นแนวทางในการวางนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบสากล

4. สร้างภาพลักษณ์ที่ดีให้กับสถาบันการศึกษา เพราะนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศมีความมั่นคง มั่นใจได้ในข้อมูลซึ่งมีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

5. เป็นไปตามข้อกำหนดของกฎหมายประเทศไทยและสากล (รองรับการเปิดเสรีประชาคมอาเซียน)

ข้อเด่นของ โปรแกรมประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับสถาบันการศึกษา

1. ประเมินได้ง่าย ง่ายในการใช้งาน และการเรียนรู้ มีข้อแนะนำ ข้อควรปฏิบัติของผู้เกี่ยวข้องด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทุกฝ่าย ประกอบด้วย ผู้บริหาร ผู้ปฏิบัติการ ผู้ใช้งานทั้งภายในและภายนอก

2. ประหยัดเวลา เข้าใจง่าย

3. ประหยัดค่าใช้จ่าย ดำเนินได้ด้วยตนเอง

4. ประโยชน์ ใช้ได้กับทุกหน่วยงาน

5. ประสิทธิภาพดี สอดคล้องกับการประเมินตามมาตรฐานสากล

ลักษณะการใช้งาน

1. มีเมนูขั้นตอนการนำไปใช้

ระบบลงทะเบียนผู้ใช้

ระบบบันทึก ข้อมูล

ระบบปรับปรุง เพิ่มเติม แก้ไข ข้อมูล

ระบบประเมินผล

ระบบรายงานผล

ระบบการเสนอแนะ แก้ไข ปรับปรุง

ระบบคู่มือประเมิน

ระบบคู่มือการใช้โปรแกรม

2. มีเมนูช่วยในการใช้งานแบบง่ายและสะดวก ประกอบด้วย

คู่มือการประเมินความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

แบบฟอร์มสำเร็จรูป ในการ เก็บข้อมูล ตรวจประเมิน

คู่มือเกณฑ์การประเมิน

ข้อเสนอแนะ ข้อควรระวัง การป้องกัน การแก้ไข

วิธีการใช้การโปรแกรม

1) เปิด อินเตอร์เน็ตเบราเซอร์
2) เข้าสู่โปรแกรม
3) กรอกข้อมูล สถาบันการศึกษา
4) กดปุ่ม เลือกเมนู เพื่อเริ่มทำแบบประเมิน
5) ทำแบบประเมินทั้ง 11 ข้อเสร็จ ระบบจะประมวบผลและรายงานผลการประเมิน
6) เลือกเมนู ข้อเสนอแนะ เพื่อรับคำแนะนำการปรับปรุงระบบ
7) เลือกเมนูการพิมพ์ สามารถพิมพ์ผลสรุปทั้งหมด

การเข้าสู่โปรแกรมทางอินเตอร์เน็ต

ผู้ใช้งานสามารถเข้าใช้งานโปรแกรมผ่านทางเครือข่ายอินเทอร์เน็ตได้จาก

Website: http://tm.dru.ac.th/assessment/