การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร

Management of Information Security Technologies in Organization

ผู้ช่วยศาสตราจารย์ ดร.ฉันทนา วิริยเวชกุล

ภาควิชาครุศาสตร์อุตสาหกรรม
คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2551

Management of Information Security Technologies in Organization

Asst.Prof.Dr.Chantana Viriyavejakul

DEPARTMENT OF INDUSTRIAL EDUCATION

FACULTY OF INDUSTRIAL EDUCATION

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2008

งานวิจัยเรื่อง การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร

พ.ศ. 2551

ผู้วิจัย ผู้ช่วยศาสตราจารย์ ดร.ฉันทนา วิริยเวชกุล

ที่ทำงาน อาจารย์ภาควิชาครุศาสตร์อุตสาหกรรม คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10250
โทรศัพท์ 0-2737-3000 ต่อ 6061 โทรสาร 0-2326-4511
อีเมล : kmchanta@kmitl.ac.th

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูลในองค์กร และ 2) เพื่อเสนอแนวทางการจัดการระบบความมั่นคงปลอดภัยของข้อมูลต่อองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

การวิจัยครั้งนี้ใช้วิธีดำเนินการวิจัยเอกสาร (Documentary Research) โดยการวิเคราะห์ทางเอกสาร (Documentary Research) และการศึกษาเชิงคุณภาพ (Documentary Analysis) มุ่งศึกษา วิเคราะห์โดยเอกสารและข้อมูลในรูปแบบบันทึกต่าง ๆ ที่เป็นมาตรฐานเป็นหลัก มุ่งศึกษาวิเคราะห์เอกสาร งานวิจัย ข้อเขียน บทความและข้อมูลเอกสารจากหน่วยงาน องค์กรส่วนราชการทั้งในและต่างประเทศ เพื่อทำความเข้าใจสภาพของการจัดการระบบความปลอดภัยของข้อมูลที่มีต่อองค์กร รวมทั้งผลกระทบที่มีผลต่อการปรับตัวของบุคลากรในคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยนำข้อมูลที่ได้จากแหล่งต่าง ๆ มาวิเคราะห์และสังเคราะห์ผ่านกรอบความรู้ในเชิงสหวิทยาการ (Interdisciplinary) เพื่อให้ได้รูปแบบ และแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรที่มีประสิทธิภาพตามมาตรฐานโลกซึ่งในที่นี้ใช้ระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS

Research Title	Management of Information Security Technologies in Organization
Year	2008
Researcher	Asst.Prof.Dr.Chantana Viriyavejakul
Office	Department of Industrial Education,
	Faculty of Industrial Education.
	King Mongkut's Institute of Technology Ladkrabang
	Chalongkrung Rd., Ladkrabang, Bangkok 10520
	Phone : 0-2737-3000 Ext. 6061 Fax 0-2326-4511
	Email : kmchanta@kmitl.ac.th

ABSTRACT

The objectives of this research are to 1) study new technology in information networks and security in organization and 2) present the accurate and world-standard efficient management guidelines of information security systems to organization.

In this research, documentary research and analyses are used to analyze standard documents and information. The focus is on analyzing documents, researches, articles, and documents from working units, the public organizations, both inside and outside our countries. This is to understand how their conditions of managing information security systems affect their organizations, as well as the adjustment of the personnel in the Faculty of Industrial Education, King Mongkut's Institute of Technology Ladkrabang. The information from various sources are analyzed and synthesized through Interdisciplinary knowledge to find out the formats and guidelines of efficient management of information security technologies in organization according to the world standard. ISO 27001: 2005 Information Security Management System or ISMS is used in this research.

กิตติกรรมประกาศ

รายงานวิจัยเรื่อง การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ครั้งนี้ผู้วิจัยมีความประสงค์เพื่อ ศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูลและเพื่อเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

โอกาสนี้ผู้วิจัยขอขอบพระคุณ รองศาสตราจารย์ พีระวุฒิ สุวรรณจันทร์ คณบดีคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้โอกาสทำงานทางด้านวิชาการและได้รับทุนวิจัยจากงบรายได้คณะปี 2551เป็นจำนวนเงิน 45,000 บาท ในการทำวิจัยอีกด้วย

อนึ่งผู้วิจัยหวังเป็นอย่างยิ่งว่ารายงานการวิจัยฉบับนี้จะเป็นประโยชน์แก่ผู้สนใจไม่มากก็น้อย คุณค่าที่เป็นผลจากการวิจัยนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

ผู้ช่วยศาสตราจารย์ ดร.ฉันทนา วิริยเวชกุล

ผู้วิจัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ข้อมูลหรือเทคโนโลยีสารสนเทศมีความหมายครอบคลุมทั้งระบบสารสนเทศ ระบบคอมพิวเตอร์ เทคโนโลยีการสื่อสารโทรคมนาคม รวมทั้งประเด็นทางจริยธรรมและทางสังคมที่เกี่ยวข้องกับคอมพิวเตอร์ และผลกระทบที่เกิดจากการใช้เทคโนโลยีสารสนเทศในสังคม เทคโนโลยีสารสนเทศเป็นเครื่องมือและเทคนิควิธีการสำหรับการเก็บรวบรวม ประมวลผล เรียกใช้ ส่งผ่านและรับข้อมูล เครื่องมือและอุปกรณ์เหล่านี้ได้แก่ เครื่องคอมพิวเตอร์ ทั้งฮาร์ดแวร์และซอฟต์แวร์ เครื่องใช้สำนักงานและอุปกรณ์โทรคมนาคม สารสนเทศประกอบด้วยคำว่า สาร แปลว่าถ้อยคำใจความ สนเทศ แปลว่า แสดง บอก ชี้แจง ดังนั้น สารสนเทศ จึงมีความหมายว่า ข่าวสาร หรือการชี้แจงข่าวสาร เทคโนโลยีสารสนเทศ เป็นศัพท์บัญญัติจากคำว่า Information Technology ที่ใช้คำย่อว่า IT ซึ่งหมายถึง วิธีการสืบค้นข้อมูลข่าวสารผ่านระบบเครือข่ายคอมพิวเตอร์

การใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์หรือจากอินเทอร์เน็ตอาจเกิดจากการรู้เท่าไม่ถึงการณ์หรือไม่ได้ระมัดระวังอย่างเพียงพอเพราะองค์กรไม่ได้ให้ความสำคัญกับการฝึกอบรมในเรื่องระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรกับบุคลากร ทำให้ผู้ใช้คอมพิวเตอร์ส่วนใหญ่ประสบปัญหาจากการใช้งาน เช่น ไวรัสที่มากับจดหมายอิเล็กทรอนิกส์ จดหมายขยะ การขโมยข้อมูลเพื่อประโยชน์ส่วนตน การติดตั้งไฟล์ผ่านทางเว็บไซต์ ตลอดจนรูปแบบอื่น ซึ่งอาจก่อให้เกิดความเสียหายกับโครงสร้างพื้นฐานทางด้านสารสนเทศขององค์กรได้ ลักษณะดังกล่าวเป็นปัญหาที่เกิดขึ้นกับองค์กรซึ่งอาจส่งผลให้เกิดปัญหาระดับชาติอีกด้วย

ISO 27001 : 2005 Information Security Management System หรือ ISMS เป็นมาตรฐานสากลที่กล่าวถึงมาตรฐานของระบบบริหารจัดการเพื่อความมั่นคงปลอดภัยของข้อมูล โดยจุดประสงค์ของมาตรฐานนี้เพื่อจะทำให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร โดยเริ่มแรกองค์กรต้องทำการวิเคราะห์ความเสี่ยงของระบบ จากภัยคุกคาม และจุดอ่อนต่างๆ ในระบบ จากนั้น จึงวิเคราะห์ และเลือกแนวทางการควบคุม และป้องกันสารสนเทศต่างๆ อย่างเหมาะสมและพอเพียงให้ใช้งานเพื่อควบคุมความเสี่ยงต่าง ๆ ขณะเดียวกัน มาตรฐานนี้ก็ยังกำหนดให้องค์กรจะต้องควบคุมดูแลระบบการรักษาความมั่นคงปลอดภัย และกลไกในการพัฒนาอย่างต่อเนื่องอีกด้วย

ดังนั้นการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลโดยการศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูลของสารสนเทศและการเสนอแนวทางการจัดการระบบของข้อมูลในองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลกอาจเป็นทางเลือกหนึ่งที่สนองต่อปัญหาดังกล่าวข้างต้น

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูล

1.2.2 เพื่อเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

1.3 ขอบเขตของโครงการวิจัย

การวิจัยอาศัยข้อมูลจากเอกสารทางวิชาการ รายงานการวิจัย ข้อเขียน บทความและข้อมูลเอกสารจากหน่วยงาน องค์กรส่วนราชการทั้งในและต่างประเทศ เพื่อทำความเข้าใจสภาพของการจัดการระบบความปลอดภัยของข้อมูลที่มีต่อองค์กร รวมทั้งผลกระทบที่มีผลต่อการปรับตัวของบุคลากรในคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยนำข้อมูลที่ได้จากแหล่งต่าง ๆ มาวิเคราะห์และสังเคราะห์ผ่านกรอบความรู้ในเชิงสหวิทยาการ (Interdisciplinary) เพื่อให้ได้รูปแบบ และแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรที่มีประสิทธิภาพตามมาตรฐานโลกซึ่งในที่นี้ใช้ระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS

1.4 ทฤษฎี สมมุติฐาน หรือกรอบแนวความคิดของโครงการวิจัย

การวิจัยครั้งนี้ผู้วิจัยได้ประยุกต์ใช้แนวความคิดของระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS เพื่อเสนอแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ซึ่งสามารถสรุปตามหลัก PDCA Model ได้ดังนี้

1. Plan

- การกำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง
- การจัดตั้งทีมงานและกำหนดหน้าที่ความรับผิดชอบ

2. Do

- การกำหนดนโยบายความมั่นคงปลอดภัยขององค์กร
- การบริหารจัดการความเสี่ยง ซึ่งประกอบด้วยการประเมินความเสี่ยง การวิเคราะห์และแก้ไข

ความเสี่ยง

- การเลือกใช้มาตรการความมั่นคงปลอดภัยและควบคุมตามมาตรฐาน
- การฝึกอบรมบุคลากรเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุกๆ ระดับ

3. Check

- การตรวจประเมินภายในของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ
- การทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร

4. Act

- การดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยของสารสนเทศตามสิ่งที่ได้ตรวจพบ
- การดำเนินการวิเคราะห์หาสาเหตุของปัญหาที่แท้จริง
- การดำเนินการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 แก้ปัญหาของหน่วยงานที่มีปัญหาการรักษาความปลอดภัยของสารสนเทศ

1.5.2 เป็นองค์ความรู้ในการทำวิจัยครั้งต่อไป

1.5.3 บริการความรู้แก่ประชาชนหรือผู้สนใจ

1.5.4 หน่วยงาน สถาบันการศึกษาและผู้ที่สนใจที่สนใจสามารถนำผลการวิจัยไปใช้ประโยชน์

1.5.5 เผยแพร่ในวารสาร

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การวิจัยครั้งนี้เป็นการจัดการระบบเทคโนโลยีสารสนเทศความมั่นคงปลอดภัยของข้อมูลในองค์กร ผู้วิจัยได้ค้นคว้าสาระสำคัญที่เกี่ยวข้อง ดังต่อไปนี้

2.1 แนวคิดเกี่ยวกับระบบสารสนเทศเพื่อการบริหาร

2.2 ระบบสารสนเทศเพื่อการบริหารของคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

2.3 เทคโนโลยีความมั่นคงปลอดภัยขององค์กร

2.4 เว็บไซต์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กร

2.5 การรักษาความปลอดภัยของระบบเครือข่าย

2.6 ระบบ ISO27001:2005

2.7 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับระบบสารสนเทศเพื่อการบริหาร

2.1.1 **ความหมายของข้อมูลและสารสนเทศ** ข้อมูล คือ ข้อเท็จจริงที่เป็นตัวเลข ข้อความหรือรายละเอียดซึ่งอาจอยู่ในรูปแบบต่าง ๆ เช่น ภาพ เสียง วีดิโอ ข้อมูลคือข้อเท็จจริงของสิ่งที่สนใจ ไม่ว่าจะเป็นคน สัตว์ สิ่งของ หรือเหตุการณ์ต่าง ๆ ดังนั้นการเก็บข้อมูลจึงเป็นการเก็บรวบรวมข้อมูลจึงเป็นการเก็บรวบรวมเกี่ยวกับข้อเท็จจริงของสิ่งที่เราสนใจนั่นเอง ข้อมูลจึงหมายถึงตัวแทนของข้อเท็จจริง หรือความเป็นไปของสิ่งที่เราสนใจอย่างไรก็ดีข้อมูลที่เก็บรวบรวมไว้อาจไม่ให้รายละเอียดทั้งหมด เช่น ข้อมูลของนักเรียนคนหนึ่งที่โรงเรียนได้เก็บรายละเอียดเกี่ยวกับ ชื่อ ที่อยู่ บ้านเลขที่ ชื่อผู้ปกครอง บิดา มารดา เลขที่ใบสำเนาทะเบียนบ้าน ข้อเท็จจริงที่บันทึกไว้นี้ไม่อาจทำให้รู้จักและเข้าใจนักเรียนผู้นี้ได้อย่างถ่องแท้ เพราะมีข้อมูลอย่างอื่นของนักเรียนที่ไม่ได้บันทึกไว้อีกมากเช่น สีผม สีตา ตำหนิ ความสูง น้ำหนัก อาหารที่ชอบ วิชาที่ชอบฯลฯในการดำเนินการใด ๆ จำเป็นต้องเก็บรวบรวมข้อมูลเอาไว้ เช่น เมื่อนักเรียนสมัครเข้าโรงเรียนก็บันทึกประวัติไว้ มีการบันทึกการมาเรียนของนักเรียนทุกวัน บันทึกผลการเรียน ข้อมูลเหล่านี้จึงเป็นข้อเท็จจริงที่เกิดขึ้นและนำมาใช้ประโยชน์ได้ในภายหลัง ในการดำเนินการทางธุรกิจจำเป็นต้องเก็บรวบรวมข้อมูลเอาไว้ใช้งาน เช่น ร้านค้าแห่งหนึ่งเก็บข้อมูล

การขายสินค้าตลอดปีเอาไว้ เขาสามารถนำข้อมูลเหล่านี้มาศึกษาปริมาณการขายต่อเดือน สินค้าใดขายไม่ดี แนวโน้มการขายเป็นอย่างไร สินค้าตัวใดมียอดการขายดีตามเทศกาล หรือมีผลภายนอกเข้ามาเกี่ยวข้อง

สารสนเทศ หมายถึง ข้อมูลที่มีความหมายซึ่งสามารถนำไปใช้ประโยชน์ ดังนั้นสารสนเทศจึงหมายถึงข้อมูลที่ผ่านการประมวลผลด้วยวิธีการที่เหมาะสมและถูกต้องเพื่อให้ได้ผลลัพธ์ตรงตามความต้องการของผู้ใช้อยู่ในรูปแบบที่ใช้งานได้และต้องอยู่ในช่วงเวลาที่ต้องการ เช่น เมื่อต้องการสารสนเทศไปใช้ในการวางแผนการขายสารสนเทศที่ต้องการก็ควรจะเป็นรายงานสรุปยอดการขายแต่ละเดือนในปที่ผ่านมา

ข้อมูล----------> การประมวลผล ----------> สารสนเทศ

สามารถแบ่งแยกประเภทสารสนเทศออกตามสภาพความต้องการที่จัดทำขึ้นได้ดังนี้

1. สารสนเทศที่ทำประจำ เป็นสารสนเทศที่จัดทำขึ้นเป็นประจำ และมีการดำเนินการโดยสม่ำเสมอ เช่นการทำรายงานสรุปจำนวนนักเรียนที่มาโรงเรียนในแต่ละวัน ทำรายงานเกี่ยวกับรายรับรายจ่ายประจำวันของโรงเรียน การทำรายงานเกี่ยวกับผู้มาติดต่อหรือตรวจเยี่ยมโรงเรียนในแต่ละเดือน

2. สารสนเทศที่ต้องทำตามกฎหมาย ตามข้อกำหนดของแต่ละประเทศจะมีการให้ทำรายงานส่งเพ่อการต่าง ๆ เช่นงบดุลของบริษัทที่ต้องทำขึ้น เพ่อยื่นต่อทางราชการและใช้ในการเสียภาษีเป็นต้น

3. สารสนเทศที่ได้รับมอบหมายให้จัดทำขึ้นโดยเฉพาะ ในการดำเนินงานต่าง ๆ บางครั้งจำเป็นต้องทำรายงานข้อมูลมาช่วยสนับสนุนการตัดสินใจ เช่นรัฐบาลต้องการสร้างเขื่อนอเนกประสงค์จำเป็นต้องได้ข้อมูลเพื่อสนับสนุนว่าจะสร้างดีหรือไม่จึงต้องมีการเก็บรวบรวมข้อมูลเพื่อสรุปงานขึ้นเป็นการเฉพาะ แล้วนำสารสนเทศนั้นมาพิจารณาถึงข้อดีข้อเสีย เพื่อช่วยสนับสนุนการตัดสินใจ การดำเนินงานเพื่อให้ได้สารสนเทศเหล่านี้จึงเป็นงานเฉพาะที่จัดทำเป็นครั้งคราวเฉพาะตามโครงการหนึ่งๆ เท่านั้น

ส่วนประกอบของระบบสารสนเทศ ระบบสารสนเทศเป็นงานที่ต้องใช้ส่วนประกอบหลายอย่างในการทำให้เกิดเป็นกลไกในการนำข้อมูลมาใช้ให้เกิดประโยชน์ได้ ส่วนประกอบที่สำคัญของระบบสารสนเทศมี 5 ส่วน คือบุคลากร ขั้นตอนที่ปฏิบัติงาน เครื่องจักรอุปกรณ์ ซอฟต์แวร์ และข้อมูล ทั้งห้าองค์ประกอบมีความเกี่ยวข้องกันเป็นระบบ บุคลากร เป็นส่วนประกอบที่สำคัญ เพราะบุคลากรที่มีความรู้ความสามารถ และเข้าใจวิธีการให้ได้มาซึ่งสารสนเทศ จะเป็นผู้ดำเนินการในการทำงานทั้งหมด บุคลากรจึงต้องมีความรู้ความเข้าใจในการใช้เทคโนโลยีสารสนเทศ บุคลากรภายในองค์การเป็นส่วนประกอบที่จะทำให้เกิดระบบสารสนเทศด้วยกันทุกคน เช่น ร้านขายสินค้าแห่งหนึ่ง บุคลากรที่

ดำเนินการในร้านทุกคน ตั้งแต่ผู้จัดการจนถึงพนักงานขายเป็นส่วนประกอบที่จะทำให้เกิดสารสนเทศ ขั้นตอนการปฏิบัติ เป็นระเบียบวิธีการปฏิบัติงานในการจัดเก็บรักษาข้อมูลให้อยู่ในรูปแบบที่จะทำให้เป็นสารสนเทศได้ เช่น กำหนดให้มีการป้อนข้อมูลทุกวัน ป้อนข้อมูลให้ทันตามกำหนดเวลา มีการแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ กำหนดเวลาในการประมวลผล การทำรายงาน การดำเนินการต่าง ๆ ต้องมีขั้นตอน หากขั้นตอนใดมีปัญหาระบบก็จะมีปัญหาด้วยเพราะทุกขั้นตอนมี

ผลกระทบต่อสารสนเทศ

- เครื่องคอมพิวเตอร์และอุปกรณ์ เป็นเครื่องมือที่ช่วยในการจัดการสารสนเทศคอมพิวเตอร์ช่วยประมวลผล คัดเลือก คำนวณ หรือพิมพ์รายงานตามที่ต้องการ คอมพิวเตอร์เป็นอุปกรณ์ที่ทำงานได้รวดเร็ว มีความแม่นยำในการทำงาน และทำงานได้ต่อเนื่อง คอมพิวเตอร์และอุปกรณ์ต่าง ๆ จึงเป็นองค์ประกอบหนึ่งของระบบ

- ซอฟต์แวร์ คือลำดับขั้นตอนคำสั่งที่สั่งให้เครื่องคอมพิวเตอร์ทำงานตามวัตถุประสงค์ที่วางไว้ ซอฟต์แวร์จึงหมายถึงชุดคำสั่งที่เรียงเป็นลำดับขั้นตอน สั่งให้คอมพิวเตอร์ทำงานตามต้องการ และประมวลผลเพื่อให้ได้สารสนเทศที่ต้องการ

- ข้อมูลเป็นวัตถุดิบที่จะทำให้เกิดสารสนเทศ ข้อมูลที่วัตถุดิบจะต่างกันขึ้นกับสารสนเทศที่ต้องการ เช่นในสถาบันการศึกษามักจะต้องการสารสนเทศที่เกี่ยวข้องกับข้อมูลนักเรียน ข้อมูลผลการเรียน ข้อมูลอาจารย์ ข้อมูลการใช้จ่ายต่าง ๆ ข้อมูลมูลเป็นสิ่งที่สำคัญประการหนึ่งที่มีบทบาทให้เกิดสารสนเทศส่วนประกอบทั้งห้านี้ล้วนมีส่วนที่ทำให้เกิดสารสนเทศได้ หากขาดส่วนประกอบใด หรือส่วนประกอบใดไม่สมบูรณ์ก็อาจทำให้ระบบสารสนเทศไม่สมบูรณ์ เช่น ใช้เครื่องคอมพิวเตอร์ไม่เหมาะสมกับงาน ก็จะทำให้งานล่าช้า ไม่ทันต่อการใช้งาน การดำเนินการระบบสารสนเทศจึงต้องให้ความสำคัญกับส่วนประกอบทั้งห้านี้

ประเภทของข้อมูล ตามที่กล่าวมาแล้วว่า ข้อมูลคือข้อเท็จจริงที่เกี่ยวกับข้องกับสิ่งต่าง ๆ เราแบ่งประเภทของข้อมูลได้เป็นสองประเภท คือ ข้อมูลปฐมภูมิ และ ข้อมูลทุติยภูมิ ข้อมูลปฐมภูมิ หมายถึง ข้อมูลที่ได้จากกากรเก็บรวบรวมหรือบันทึกจากแหล่งข้อมูลโดยตรง ซึ่งอาจจะได้จากการสอบถาม การสัมภาษณ์ การสำรวจ การจดบันทึก ตลอดจนการจัดหามาด้วยเครื่องจักรอัตโนมัติต่าง ๆ ที่ดำเนินการจัดเก็บข้อมูลให้ เช่น เครื่องอ่านรหัสแท่ง เครื่องอ่านแถบแม่เหล็ก ข้อมูลปฐมภูมิจึงเป็นข้อมูลพื้นฐานที่ได้มาจากจุดกำเนิดของข้อมูลนั้น ๆ ข้อมูลทุติยภูมิ หมายถึง ข้อมูลที่มีผู้รวบรวมไว้ให้แล้ว บางครั้งอาจจะมีการประมวลผลเพื่อเป็นสารสนเทศ ผู้ใช้ไม่จำเป็นต้องไปสำรวจเอง ดังตัวอย่างข้อมูลสถิติต่าง ๆ ที่หน่วยงานรัฐบาลทำไว้แล้ว เช่น สถิติจำนวนประชากรแต่ละจังหวด สถิติการส่ง

สินค้าออก สถิติการนำสินค้าเข้า ข้อมูลเหล่านี้มีการตีพิมพ์เผยแพร่เพื่อให้ใช้งานได้หรือนำเอาไปประมวลผลต่อ

อรรณพ เธียรถาวร (2531: 220) ได้ให้ความหมายว่า ข้อมูล หมายถึง ข้อเท็จจริงต่าง ๆ ที่มีอยู่ในธรรมชาติ เป็นกลุ่มสัญลักษณ์แทนปริมาณ หรือการกระทำต่าง ๆ ที่ยังไม่ผ่านการวิเคราะห์ หรือการประมวลผล ข้อมูลอยู่ในรูปของตัวเลข ตัวหนังสือ รูปภาพ แผนภูมิ เป็นต้นสำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา (2546) ได้ให้ความหมายว่าข้อมูลหมายถึงค่าความจริง ซึ่งแสดงถึงความเป็นจริงที่ปรากฏขึ้น เช่น ชื่อพนักงานและจำนวนชั่วโมงการทำงานในหนึ่งสัปดาห์ จำนวนสินค้าที่อยู่ในคลังสินค้า เป็นต้น ข้อมูลมีหลายประเภท เช่น ข้อมูลตัวเลข ข้อมูล ตัวอักษร ข้อมูลรูปภาพ ข้อมูลเสียงและข้อมูลภาพเคลื่อนไหว ซึ่งข้อมูลชนิดต่าง ๆ เหล่านี้ใช้ในการนำเสนอค่าความจริงต่าง ๆ โดยค่าความจริงที่ถูกนำมาจัดการและปรับแต่งเพื่อให้มีความหมายแล้ว จะเปลี่ยนเป็นสารสนเทศ

สถาบันราชภัฏเชียงราย (2546) ได้ให้ความหมายของคำว่า สารสนเทศ หรือ สารนิเทศ เป็นคำศัพท์บัญญัติของคำว่า Information ราชบัณฑิตยสถานกำหนดให้ใช้คำได้ทั้งสองคำในวงการคอมพิวเตอร์ การสื่อสาร และธุรกิจนิยมใช้คำว่า สารสนเทศ ซึ่งมีความหมาย ว่า ข้อมูลข่าวสาร ความรู้ต่าง ๆที่มีการบันทึกทุกอย่างเป็นระบบ ตามหลักวิชาการ เพื่อนำมาเผยแพร่และใช้งานต่าง ๆ ทุกสาขา สำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา (2546) ได้ให้ความหมายของสารสนเทศ ว่าหมายถึงกลุ่มข้อมูลที่ถูกจัดการตามกฎหรือ ถูกกำหนดความสัมพันธ์ให้ เพื่อให้ข้อมูลเหล่านั้นเกิดประโยชน์หรือมีความหมายเพิ่มมากขึ้น ประเภทของสารสนเทศขึ้นอยู่กับความสัมพันธ์ระหว่างข้อมูลที่มีอยู่ และอีกความหมายคือสารสนเทศ หมายถึง ข้อมูลที่ผ่านการเปลี่ยนแปลง หรือจัดกระทำเพื่อผลของการ เพิ่มความรู้ ความเข้าใจของผู้ใช้ ลักษณะของสารสนเทศจะเป็นการรวบรวมข้อมูลหลาย ๆ อย่างที่เกี่ยวข้องกันเพื่อจุดมุ่งหมายอย่างใดอย่างหนึ่งโดยสรุป ข้อมูลคือข้อเท็จจริงหรือตัวเลขที่ยังไม่ได้ผ่านการวิเคราะห์หรือประมวลผล ไม่สามารถนำไปใช้ประกอบการตัดสินใจได้โดยตรง ส่วนสารสนเทศ คือข้อมูลที่ผ่านการวิเคราะห์ประมวลผลแล้ว สามารถนำไปใช้ประกอบการตัดสินใจเพื่อการบริหารได้

2.1.2 **กระบวนการผลิตสารสนเทศ** การผลิตหรือจัดทำสารสนเทศ มีขั้นตอนและวิธีการต่าง ๆ ในการปฏิบัติ 9 วิธี ดังนี้

1. การรวบรวม (capturing) ข้อมูลที่ได้จะต้องมีคุณสมบัติ สำคัญ 2 ประการ คือ ตรงตามความต้องการที่กำหนดไว้ และมีความเชื่อถือได้

2. การตรวจสอบ (verifying) การตรวจสอบข้อมูลเป็นการค้นหา รวบรวมข้อมูลที่ยังมีความผิดพลาดโดยทั่วไป จะกระทำได้ใน 3 ลักษณะ คือ

- การตรวจสอบความเป็นไปได้ หรือความสมเหตุ สมผลของข้อมูล

- การตรวจสอบความสอดคล้องกัน

- การตรวจสอบความสัมพันธ์ของข้อมูล

3. การจำแนก (classifying) เป็นการจัดหมวดหมู่หรือเป็นกลุ่ม ตามคุณสมบัติของข้อมูลในลักษณะที่เหมาะสม

4. การจัดเรียงลำดับ (arranging)

5. การสรุป (summarizing)

6. การคำนวณ (calculating)

7. การจัดเก็บ (storing) เป็นการรักษาข้อมูลที่ได้จากการประมวลผลแล้วไว้ในสื่อต่าง ๆ ที่เหมาะสม เพื่อสามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้

8. การเรียกใช้ (retrieving)

9. การเผยแพร่ (disseminating and reproducing)

วราภรณ์ เทพสัมฤทธิ์พร (2536) ได้เสนอกระบวนการผลิตสารสนเทศ 8 ขั้นตอน ซึ่งได้แก่ การเก็บรวบรวมข้อมูล การจำแนกข้อมูลและกำหนดดัชนีข้อมูล การสรุปข้อมูลให้กระทัดรัด การเก็บรักษาข้อมูล การบริหารข้อมูล การประมวลผลข้อมูล การส่งผ่านข้อมูลและการแสดงผลข้อมูลโดยสรุป กระบวนการผลิตสารสนเทศจะประกอบด้วย การเก็บรวบรวมข้อมูล การประมวลผลข้อมูล การเก็บรักษาข้อมูล การวิเคราะห์ข้อมูล และการนำเสนอข้อมูล ซึ่งจะมีการการตรวจสอบข้อมูลและสารสนเทศตลอดกระบวนการผลิต

2.1.3 **คุณสมบัติของสารสนเทศ**

จีราภรณ์ รักษาแก้ว (2538: 59-61) ได้กล่าวถึงคุณสมบัติของสารสนเทศที่ดี มี 5 ประการคือ ความถูกต้อง ความทันต่อการใช้งาน ความสมบูรณ์ ความกะทัดรัดและตรงกับความต้องการนอกจากนี้ยังกล่าวอีกว่า คุณสมบัติของสารสนเทศแตกต่างไปตามลักษณะงาน ทำให้มีคุณสมบัติแอบแฝง ซึ่งได้แก่ ความละเอียดแม่นยำ คุณสมบัติเชิงปริมาณ ความยอมรับได้ การใช้งานง่ายความไม่ลำเอียง และชัดเจน

สถาบันราชภัฏเชียงราย (2546) กล่าวไว้ว่าสารสนเทศที่ดีต้องมีคุณสมบัติ มีความเที่ยงตรง (accuracy) หมายถึง ปราศจากความเอนเอียง ตรงตามความต้องการของผู้ใช้ (relevancy) หมายถึง มีเนื้อหาตรงกับเรื่องที่ต้องการใช้ของผู้ใช้ และต้องทันต่อเวลา (timeliness) หมายถึงสามารถนำสารสนเทศที่ต้องการไปใช้ได้ทันต่อเหตุการณ์ที่เกิดขึ้น การจัดเตรียมสารสนเทศให้ทันต่อเวลาที่ต้องการใช้ มี 2 ลักษณะ คือ การจัดทำสารสนเทศล่วงหน้าตามกำหนดเวลาที่เหตุการณ์จะเกิดในอนาคต และการจัดทำสารสนเทศอย่างรวดเร็วเพื่อนำไปใช้ในเหตุการณ์ที่กำลังเกิดขึ้นจากคุณสมบัติของสารสนเทศ

ดังกล่าว จึงสรุปได้ว่าคุณสมบัติของข้อมูลและสารสนเทศที่ดีจะต้องมีความถูกต้อง เที่ยงตรง เชื่อถือได้ สมบูรณ์ กะทัดรัด และนำมาใช้ได้อย่างทันต่อการใช้งานและตรงกับความต้องการของผู้ใช้

2.1.4 ความหมายและบทบาทของระบบสารสนเทศ

สำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา (2546) ได้ให้ความหมายของระบบสารสนเทศ (Information System หรือ IS) คือระบบแบบเฉพาะเจาะจงชนิดหนึ่ง ซึ่งอาจกล่าวได้ว่าเป็นกลุ่มของส่วนประกอบพื้นฐานต่าง ๆ ที่ทำงานเกี่ยวข้องกันในการเก็บ (นำเข้า) การจัดการ (ประมวลผล) และการเผยแพร่ (แสดงผล) ข้อมูลและสารสนเทศและสนับสนุนกลไกลของผลสะท้อนกลับ เพื่อให้บรรลุตามวัตถุประสงค์

2.1.5 ส่วนประกอบของระบบสารสนเทศ

ระบบสารสนเทศประกอบด้วย

1. ส่วนที่นำเข้า (input) ได้แก่การรวบรวมและการจัดเตรียมข้อมูลดิบ

2. การประมวลผล (processing) เกี่ยวข้องกับการเปลี่ยนและการแปลงข้อมูลให้อยู่ในรูปของส่วนแสดงผลที่มีประโยชน์

3. ส่วนที่แสดงผล (output) เกี่ยวข้องกับการผลิตสารสนเทศที่มีประโยชน์ มักจะอยู่ในรูปของเอกสาร หรือรายงาน

4. ผลสะท้อนกลับ (feedback) คือส่วนแสดงผลที่ใช้ในการทำให้เกิดการเปลี่ยนแปลงต่อส่วนที่นำเข้าหรือส่วนประมวลผล

สถาบันราชภัฏเชียงราย (2546ข) กล่าวไว้ว่า ส่วนประกอบของระบบสารสนเทศ สามารถแบ่งออกเป็น 6 ส่วน ดังนี้

1. ข้อมูลป้อนเข้า (input) ประกอบด้วยข้อมูลที่เป็นตัวเลข ข้อความ เสียงและภาพ เรียกอีกอย่างว่า ข้อมูลดิบหรือข้อมูลในภาษาอังกฤษ ใช้คำว่า data

2. รูปแบบของการประมวลผล (model) เป็นการกำหนดความสัมพันธ์ของข้อมูลแต่ละรายการเพื่อจัดให้กระทำข้อมูลเหล่านั้นตามที่กำหนดไว้ต่อไป

3. ผลผลิตของระบบ (output) ผลผลิตของระบบสารสนเทศ มีผลต่อส่วนประกอบอื่น ๆ ทั้งหมด หากผลของส่วนนี้ไม่ตรงกับความต้องการของผู้ใช้ย่อมส่งผลให้ส่วนอื่น ๆ ผิดพลาดไปด้วย ผลผลิตระบบนี่จะมีคุณภาพไม่ดีไปกว่าข้อมูลป้อนเข้าและรูปแบบการจัดกระทำของข้อมูล

4. เทคโนโลยี (technology) เป็นส่วนที่ทำหน้าที่เก็บข้อมูล ดำเนินการตามรูปแบบการประมวลผลและทำให้เกิดผลผลิตของระบบออกมาในสื่อที่ต้องการ องค์ประกอบที่สำคัญของเทคโนโลยีมี 3 อย่าง คือ คอมพิวเตอร์ ซอฟท์แวร์ และโทรคมนาคม

5. ฐานข้อมูล (database) เป็นวิธีการที่จะเก็บข้อมูลได้เป็นระบบให้สะดวกต่อการเรียกใช้ สามารถแก้ไขได้ง่าย และให้ผู้ใช้จำนวนมากสามารถป้องกันไม่ให้ผู้มีสิทธิ์ให้เข้าถึงข้อมูลเดียวกันได้

6. การควบคุม (control) เป็นส่วนประกอบที่กำหนดไว้เพื่อให้ระบบสารสนเทศมีความปลอดภัยไม่ถูกทำลายทั้งที่เจตนาและไม่เจตนา

ระบบสารสนเทศ เป็นระบบรวม ทั้งนี้เนื่องจากไม่สามารถเก็บรวบรวมในลักษณะระบบเดียว เนื่องจากขนาดข้อมูลมีขนาดใหญ่และมีความซับซ้อนมาก ทำให้การบริหารข้อมูลทำได้อยาก การนำไปใช้ไม่สะดวก จึงจำเป็นต้องแบ่งระบบสารสนเทศออกเป็นระบบย่อย 4 ส่วนได้แก่ ระบบประมวลผลรายการ (Transaction Processing System :TPS) ระบบจัดการรายงาน(Management Reporting System :MRS) ระบบสนับสนุนการตัดสินใจ (Decision SupportSystem :DSS) และระบบสารสนเทศสำนักงาน (Office Information System :OIS)

2.1.6 รูปแบบการพัฒนาระบบสารสนเทศ

วราภรณ์ เทพสัมฤทธิ์พร(2536) ได้เสนอขั้นตอนการพัฒนาระบบสารสนเทศออกเป็น 5 ขั้นตอน คือ

1. การกำหนดข้อมูลที่จำเป็นต่อการบริหารงานและจุดมุ่งหมายของระบบ โดยต้องได้รับความร่วมมือจากผู้บริหารและผู้ออกแบบให้ข้อมูลที่ถูกต้องต่อกัน

2. เป็นการออกแบบระบบหรือกำหนดองค์กร กำหนดหน้าที่ ผู้รับผิดชอบโครงงาน วิธีดำเนินงาน ระยะเวลา ค่าใช้จ่ายและบุคลากรที่จะปฏิบัติงาน

3. กำหนดรูปแบบของระบบสารสนเทศ เช่น รูปแบบการเก็บข้อมูล รูปแบบการประมวลผล รูปแบบการนำเสนอข้อมูล เป็นต้น ซึ่งขั้นตอนนี้ต้องพิจารณาให้ละเอียดเพื่อพัฒนาในขั้นตอนต่อไป

4. การกำหนดรูปแบบรายละเอียดของระบบสารสนเทศให้ตรงตามความต้องการของผู้บริหารและเหมาะสมกับองค์การของผู้บริหาร หรือเหมาะสมกับสภาพแวดล้อมทั้งในปัจจุบันและอนาคต

5. ขั้นตอนปฏิบัติตามระบบและตรวจสอบผลการปฏิบัติ เพื่อปรับปรุงระบบให้ดียิ่งขึ้น

2.1.7 ความหมายของระบบสารสนเทศเพื่อการบริหาร

สำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา (2546) ได้ให้ความหมายของ

ระบบสารสนเทศเพื่อการบริหารไว้หลายความหมาย ดังต่อไปนี้ระบบสารสนเทศเพื่อการบริหาร (Management Information System : MIS) คือระบบการจัดหาคนหรือข้อมูลที่มีความสัมพันธ์กับข้อมูลเพื่อการดำเนินงานขององค์การ การนำไปใช้งานสามารถแบ่งได้ 4 ระดับดังนี้

1. ระบบสารสนเทศเพื่อการจัดการในการวางแผนนโยบาย กลยุทธ์ และการตัดสินใจของผู้บริหารระดับสูง

2. ระบบสารสนเทศเพื่อการจัดการในส่วนยุทธวิธีในการวางแผนการปฏิบัติและการตัดสินใจของผู้บริหารระดับกลาง

3. ระบบสารสนเทศเพื่อการจัดการในระดับปฏิบัติการและการควบคุมในขั้นตอนนี้ผู้บริหารระดับล่างจะเป็นผู้ใช้สารสนเทศเพื่อช่วยในการปฏิบัติงาน

4. ระบบสารสนเทศที่ได้จากการประมวลผล

ระบบสารสนเทศเพื่อการบริหาร คือระบบที่นำเสนอข้อมูลในรูปแบบที่ผู้บริหารสามารถวิเคราะห์ข้อมูลได้อย่างมีประสิทธิภาพ เรียกว่าระบบ สารสนเทศเพื่อการจัดการ ซึ่งข้อมูลส่วนที่นำเข้าส่วนมาก ได้แก่ข้อมูลจากระบบประมวลผลรายการ ซึ่งถูกนำเข้าไปยังระบบสารสนเทศเพื่อการจัดการขององค์กรเพื่อผลิตรายงานต่าง ๆ ออกมา ทำให้ผู้จัดการตัดสินใจได้อย่างมีประสิทธิผลมากขึ้น จุดประสงค์หลักของระบบสารสนเทศเพื่อการบริหารคือ ช่วยให้องค์กรบรรลุวัตถุประสงค์ได้ โดยช่วยให้ผู้บริหารสามารถเห็นการดำเนินงานที่เกิดขึ้นในองค์กร เพื่อที่จะควบคุม จัดการและวางแผนได้อย่างมีประสิทธิภาพและประสิทธิผลหรือกล่าวได้ว่า ระบบสารสนเทศเพื่อการจัดการช่วยนำเสนอข้อมูลของผู้บริหารเพื่อใช้ในการตัดสินใจได้อย่างมีประสิทธิภาพและช่วยจัดการผลสะท้อนกลับที่เกิดขึ้นในการดำเนินงานรายวันได้

2.1.8 **ส่วนประกอบของระบบสารสนเทศเพื่อการบริหาร**

สำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา (2546) กล่าวว่า ส่วนประกอบของระบบสารสนเทศมี 5 ส่วนหลัก คือ ฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศกระบวนการผลิตและบุคลากร โดยแต่ละส่วนมีความสัมพันธ์กัน ในการนำระบบสารสนเทศเข้ามาใช้เพื่อการจัดการมักจะแบ่งส่วนตามการทำงานหลัก ซึ่งอาจจะเห็นได้จากแผนผังองค์กร ในแต่ละฝ่ายก็จะมีระดับการจัดการต่าง ๆ (กลยุทธ์ ยุทธวิธี และการดำเนินงาน) จึงเรียกการแบ่งการจัดการตามส่วนการทำงานว่าการแบ่งตามแนวตั้ง ส่วนการแบ่งตามระดับการจัดการเรียกว่าการแบ่งตามแนวนอน แต่ละส่วนการทำงานจะมีระบบย่อยที่ทำงานเฉพาะด้านของตนเอง แต่อาจมีการใช้ข้อมูลร่วมกันได้สถาบันราชภัฏเชียงราย (2546) กล่าวว่าระบบสารสนเทศเพื่อการบริหาร หมายถึงกลุ่มของบุคคล, กระบวนการผลิต,ซอฟต์แวร์, ฐานข้อมูล และอุปกรณ์ต่าง ๆ ที่ถูกจัดการเพื่อใช้ในการจัดการสารสนเทศที่เกิดขึ้นเป็นประจำให้แก่

ผู้บริหารหรือผู้ทำการตัดสินใจ จุดประสงค์หลักของระบบสารสนเทศเพื่อการบริหาร อยู่ที่การดำเนินการอย่างมีประสิทธิภาพในด้านการตลาด การผลิตการเงิน และส่วนงานอื่นๆ โดยใช้และจัดเก็บข้อมูลลงในฐานข้อมูล โดยระบบสารสนเทศเพื่อการจัดการเป็นระบบสารสนเทศที่ใช้ในการผลิตรายงานด้านการจัดการ ซึ่งจะใช้ในการสนับสนุนการตัดสินใจในระดับปฏิบัติงาน ระดับยุทธวิธี และระดับกลยุทธ์

2.1.9 บทบาทของระบบสารสนเทศเพื่อการบริหารในองค์กร

ระบบสารสนเทศเพื่อการบริหาร สนับสนุนบทบาทในการจัดการของผู้บริหาร ดังนี้

1. การวางแผน (Plan) หมายถึง การกำหนดเป้าหมาย และกลยุทธ์ในการบริหารองค์กร
2. การจัดการ (Organize) หมายถึง การจัดสรรทรัพยากรที่ต้องการนำมาใช้ในองค์กร
3. การเป็นผู้นำ (Lead) หมายถึง การกระตุ้นพนักงาน เพื่อให้ปฏิบัติการให้บรรลุเป้าหมาย
4. การควบคุม (Control) หมายถึง การควบคุมดูแล เพื่อให้เกิดความก้าวหน้าไปยังเป้าหมายที่วางไว้

สมบุญ พิมพาภรณ์(2538) กล่าวถึงบทบาทของสารสนเทศในการวางแผนและการบริหารการศึกษาว่า สารสนเทศเปรียบเสมือนเส้นเลือดของระบบซึ่งเป็นส่วนสำคัญในการบริหารงานในองค์การ สารสนเทศเป็นทรัพยากรที่มีค่ามากสำหรับการวางแผนควบคุมและการตัดสินใจสำหรับผู้บริหารและนักวางแผน ได้จำแนกระดับสารสนเทศที่ใช้ในองค์การและหน่วยงานต่าง ๆ ตามระดับของการบริหาร หรือระดับของการตัดสินใจ 3 ระดับ คือ

1. ผู้บริหารระดับสูงและนักวางแผน หมายถึง ผู้นำองค์การหรือหน่วยงานหรือผู้มีส่วนร่วมในการวางแผนพัฒนา ผู้บริหารระดับนี้จะใช้สารสนเทศในกระบวนการกำหนดวัตถุประสงค์ขององค์การ การวางแผนระยะยาวเพื่อจัดสรรทรัพยากร การกำหนดนโยบายเพื่อใช้เป็นแนวทางในการจัดหา ตลอดจนการใช้ทรัพยากรต่าง ๆ เหล่านั้น

2. ผู้บริหารระดับกลาง หมายถึง ผู้บริหารที่มีความรับผิดชอบในการจัดการให้เป็นไปตามแผนในช่วงเวลาปีต่อปี และใช้สารสนเทศในการควบคุมการปฏิบัติงานให้มีประสิทธิภาพ

3. ผู้บริหารระดับปฏิบัติการ หมายถึง ผู้ที่มีความรับผิดชอบในด้านการควบคุมการปฏิบัติงานในช่วงเวลาเดือนต่อเดือน และการใช้สารสนเทศเพื่อการปฏิบัติงานให้มีประสิทธิภาพและมีประสิทธิผล

สุพรรณี เมนะเนตร(2543) กล่าวถึงระบบสารสนเทศเพื่อการบริหารว่า เป็นศูนย์กลางที่สำคัญสำหรับการป้อนสารสนเทศแก่ผู้บริหารในระดับต่าง ๆ เพื่อช่วยในการตัดสินใจของผู้บริหาร หรือกล่าวอีกนัยหนึ่งว่า ระบบสารสนเทศเปรียบเสมือนฐานที่สำคัญสำหรับการตัดสินใจของผู้บริหารทุกระดับ และ

ระบบสารสนเทศเพื่อการบริหาร ช่วยเพิ่มคุณภาพด้านการตัดสินใจของผู้บริหารโดยช่วยให้ผู้บริหารมองเห็นปัญหาและโอกาสได้รวดเร็วขึ้น ช่วยให้ผู้บริหารมีเวลาสำหรับการวางแผนได้มากขึ้น ช่วยให้ผู้บริหารใช้เวลาในการพิจารณาปัญหาที่มีความซับซ้อนได้มากขึ้น และยังช่วยให้ผู้บริหารควบคุมการดำเนินการได้ดีขึ้น

ลักษณะของสารสนเทศที่ดี จะต้องสนับสนุนการทำงานของระบบประมวลผลข้อมูลและการจัดเก็บข้อมูลรายวัน ใช้ฐานข้อมูลที่ถูกรวมเข้าด้วยกัน และสนับสนุนการทำงานของฝ่ายต่าง ๆ ในองค์การ ช่วยให้ผู้บริการระดับต้น ระดับกลาง ระดับสูง เรียกใช้ข้อมูลที่เป็นโครงสร้างได้ตามต้องการ มีความยืดหยุ่นสามารถรองรับความต้องการข้อมูลที่เปลี่ยนแปลงไปขององค์กรและต้องมีระบบรักษาความลับของข้อมูลและจำกัดการใช้งานของบุคคลเฉพาะผู้ที่เกี่ยวข้องเท่านั้นโดยสรุป ระบบสารสนเทศเพื่อการบริหาร คือระบบที่นำเสนอข้อมูลในรูปแบบที่ผู้บริหารสามารถวิเคราะห์ข้อมูลได้อย่างมีประสิทธิภาพ โดยจะทำให้ผู้บริหารสามารถเห็นการดำเนินงานที่เกิดขึ้นในองค์กร และสามารถควบคุมจัดการและวางแผนได้อย่างมีประสิทธิภาพ

2.2 ระบบสารสนเทศเพื่อการบริหารของคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

คณะกรรมการด้านการจัดการความรู้ในองค์กร คณะครุศาสตร์อุตสาหกรรม

1. คณบดี
2. รองคณบดีกำกับดูแลงานด้านนโยบายและแผน
3. รองคณบดีกำกับดูแลงานด้านกิจการนักศึกษา
4. ผู้ช่วยคณบดีฝ่ายกิจการพิเศษ
5. หัวหน้าภาควิชาครุศาสตร์สถาปัตยกรรม
6. หัวหน้าภาควิชาครุศาสตร์เกษตร
7. อาจารย์ประจำภาควิชาครุศาสตร์วิศวกรรม

8. อาจารย์ประจำภาควิชาภาษาและสังคม

9. เลขานุการคณะฯ

10. รองคณบดีกำกับดูแลงานด้านวิชาการและพัฒนา

รูปที่ 1 แสดงระบบสารสนเทศบุคลากร คณะครุศาสตร์อุตสาหกรรม

คณะครุศาสตร์ได้แบ่งระบบสารสนเทศบุคลากร ดังนี้

1. สำนักงานคณบดี
2. ภาควิชาภาษาและสังคม
3. ภาควิชาครุศาสตร์อุตสาหกรรม
4. ภาควิชาครุศาสตร์สถาปัตยกรรม
5. ภาควิชาครุศาสตร์เกษตร

รูปที่ 2 ระบบสารสนเทศเพื่อการบริหารงานคณะครุศาสตร์อุตสาหกรรม

การแบ่งส่วนราชการในสำนักงานคณบดี ได้แบ่งส่วนเป็น 5 งานหลักดังนี้

1. งานบริหารและงานธุรการ
2. งานการเจ้าหน้าที่
3. งานพัสดุ
4. งานการเงินและบัญชี
5. งานนโยบายและวางแผน
6. งานบริการการศึกษา
7. งานบริการทางวิชาการและวิจัย

2.3 เทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร

2.3.1 การจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1. นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้องดังนี้

1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

(ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security spolicy)

(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

2.3.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

1. **โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร** (Internal organization)

มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)

(ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญต่อหน้าที่ และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่าง ๆ ภายในองค์เพื่อประสานหรือร่วมมือกันในการสร้างความมั่นคงให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

1.3 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

(ผู้บริหารสานสนเทศ) ต้องกำหนดหน้าที่ ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements) (หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

1.6 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with costomers)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้เข้าถึงได้

1.7 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)

(หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอกเมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.3.3 การบริหารจัดการทรัพย์สินขององค์กร

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)

มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน

1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแล และเอาใจใส่เป็นต้น

2. การจัดหมวดหมู่สารสนเทศ (Information classification)

มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

2.2 การจัดทำป้ายชื่อ และการจัดทำทรัพย์สินสารสนเทศ (Information labeling and handling)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

2.3.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่าง ๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities) (หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงานผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือ หน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร(ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคล หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึงประกอบการคัดเลือกด้วย

1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคคลาการที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

2. **การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน** (During employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsinilities)

(ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security swareness, education, and training)

(หัวหน้างานบุคลากรและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคนปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

2.3 กระบวนการทางวินัยเพื่อการลงโทษ (Disciplinary process)

(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบาย หรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

3. **การสิ้นสุดหรือการเปลี่ยนการจ้างงาน** (Termination or change of employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)

(หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

3.2 การคืนทรัพย์สินขององค์กร (Return of assets)

(หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)

(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

2.3.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

1. **บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย** (Secure areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุมตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

1.2 การควบคุมการเข้า-ออก (Physical entry controls)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)

(หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่น ๆ

1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงาน ในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

(พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อม และอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่าง ๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

2.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling security)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่าง ๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่าง ๆ ที่มีต่ออุปกรณ์เหล่านั้น

2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟแวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟแวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

2.3.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศองค์กร (Communications and operations management)

1. **การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน** (Operational procedures and responsibilities)

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)(ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Seperation of development , test, amd operational facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนาการทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

2. **การบริหารจัดการการให้บริการของหน่วยงานภายนอก** (Third party service delivery management)

มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการและระดับของการให้บริการ

2.2 การตรวจสอบการให้บริการจากหน่วยงานภายนอก (Mornitoring and review of third party services)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่าง ๆ ที่กำหนดให้บันทึกไว้เป็นต้น

2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนแปลงเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

3. **การวางแผนและการตรวจรับทรัพยากรสารสนเทศ** (System planning and acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

4. **การป้องกันโปรแกรมที่ไม่ประสงค์ดี** (Protection against malicious and mobile code)

มีจุดประสงค์เพื่อรักษาซอฟแวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟแวร์ที่ไม่ประสงค์ดี

4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)

(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่น ๆ สามารถทำงานหรือใช้งานได้

5. การสำรองข้อมูล (Back-up)

มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.1 การสำรองข้อมูล (Information back-up)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นที่สนับสนุนการทำงานของเครือข่าย

6.1 มาตรการทางเครือข่าย (Network controls)

(ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย

6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในองค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก

7. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)

มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

7.3 ขั้นตอนการปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system decumentation)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

8. การแลกเปลี่ยนสารสนเทศ (Exchange of information)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟแวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก)โดยผ่านทางช่องทางการสื่อสารทุกชนิด

8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange argeements)

(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟแวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร

8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)

(หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

9. การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

9.2 การทำธุรกรรมออนไลน์ (On-line transactions)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายความเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

10. การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ

10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)

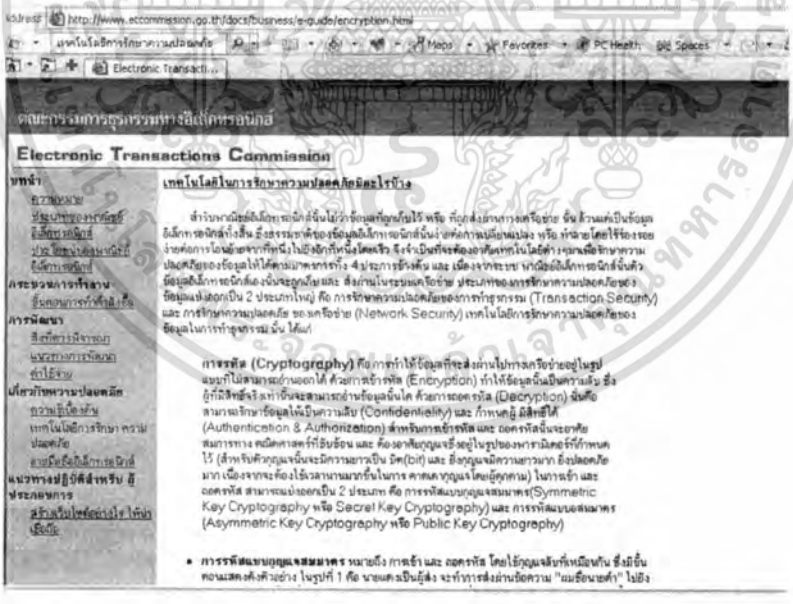
(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

10.5.1 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

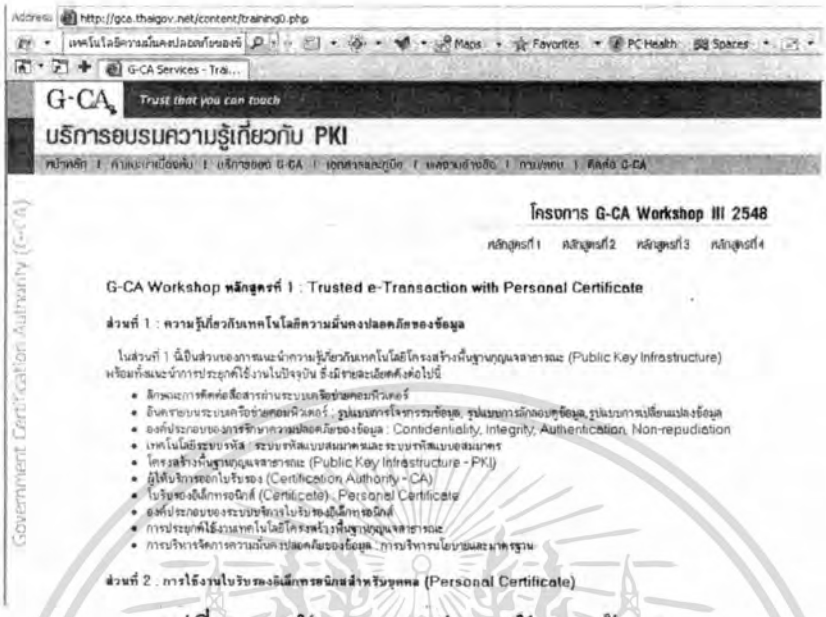
2.4 เว็บไซต์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กร

รูปที่ 3 การป้องกันและรักษาความปลอดภัย http://www.thaiall.com/internet/internet05.htm



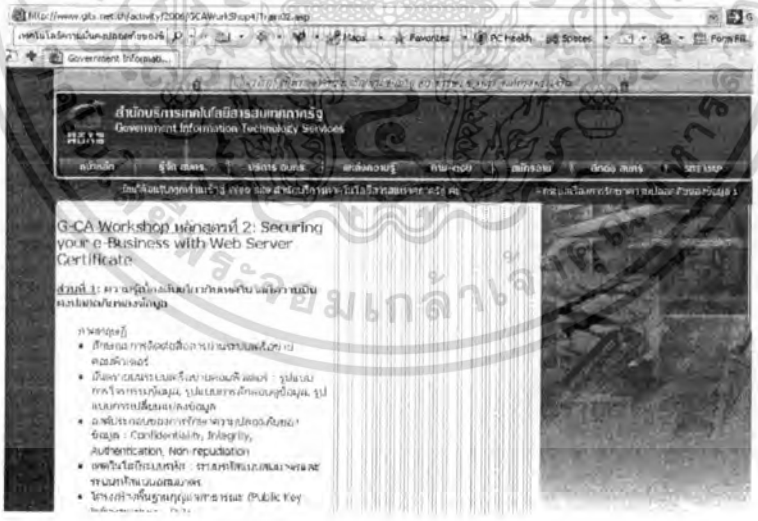
รูปที่ 4 การรักษาความปลอดภัยของข้อมูล

http://www.etcommission.go.th/docs/business/e-guide/encryption.html



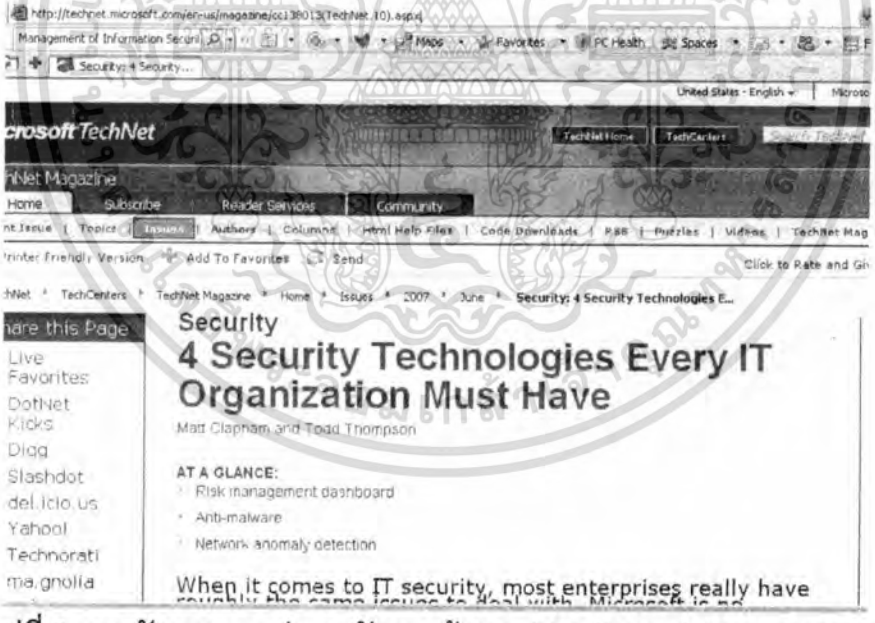
รูปที่ 5 การรักษาความปลอดภัยของข้อมูล

http://www.gits.net.th/activity/2006/GCAWorkShop4/Train02.asp



รูปที่ 6 การรักษาความปลอดภัยของข้อมูล http://202.142.219.4/varticle/18197

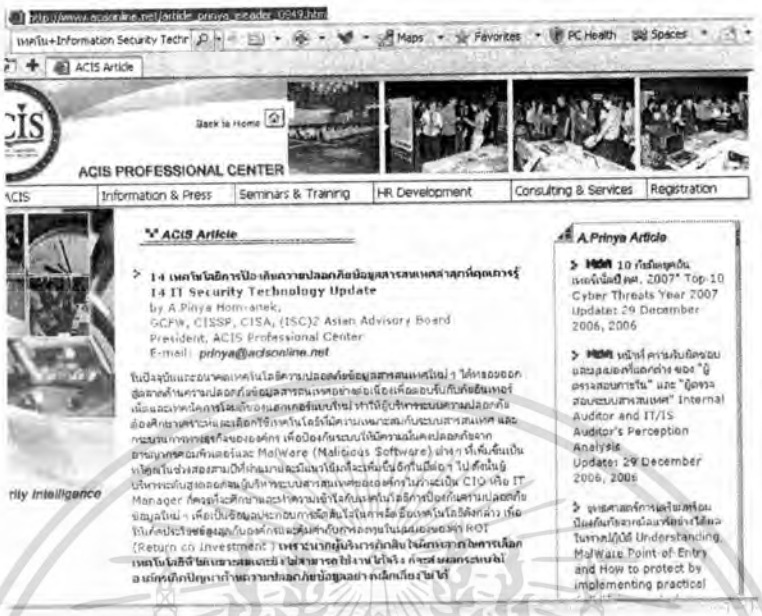
รูปที่ 7 การรักษาความปลอดภัยของข้อมูล http://technet.microsoft.com/en-us/magazine/cc138013(TechNet.10).aspx



รูปที่ 8 การรักษาความปลอดภัยของข้อมูล http://www.istsecure.com/

รูปที่ 9 การรักษาความปลอดภัยของข้อมูล http://www.peterindia.net/ITSecurity.html

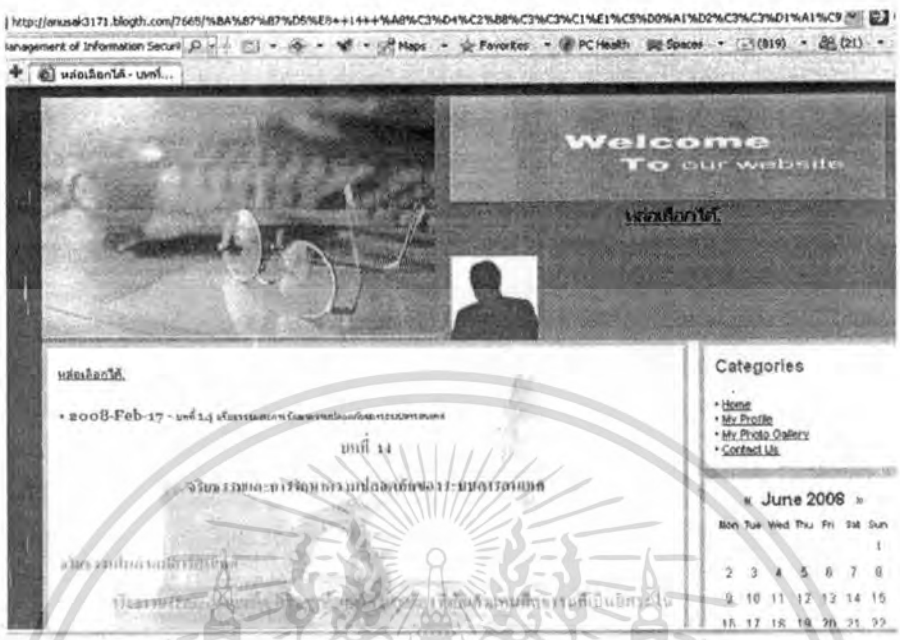
รูปที่ 10 การรักษาความปลอดภัยของข้อมูล จาก
http://www.acisonline.net/article_prinya_eleader_0949.htm



รูปที่ 11 การรักษาความปลอดภัยของข้อมูล http://th.wikipedia.org/w/index.php?

รูปที่ 12 การรักษาความปลอดภัยของข้อมูล

http://elearning.it.kmitl.ac.th/course/search.php?



รูปที่ 13 การรักษาความปลอดภัยของข้อมูล http://anusak3171.blogth.com/

รูปที่ 14 การรักษาความปลอดภัยของข้อมูล

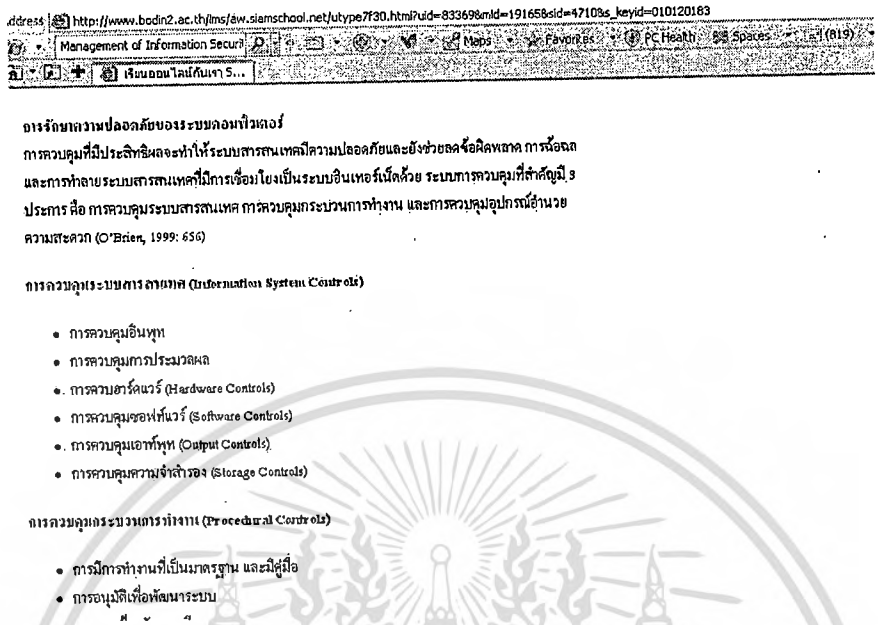
http://www.itharem.com/modules.php?name=News&file=article&sid=217

รูปที่ 15 การรักษาความปลอดภัยของข้อมูล

http://118.175.82.11/manage/PlanDetail.php?Teacher_code=00026&&Plan_code=0001

รูปที่ 16 การรักษาความปลอดภัยของข้อมูล

http://hrm.siamhrm.com/?name=chapter&file=read&max=112



การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การควบคุมที่มีประสิทธิผลจะทำให้ระบบสารสนเทศมีความปลอดภัยและยังช่วยลดข้อผิดพลาด การฉ้อฉล และการทำลายระบบสารสนเทศที่มีการเชื่อมโยงเป็นระบบอินเทอร์เน็ตด้วย ระบบการควบคุมที่สำคัญมี 3 ประการ คือ การควบคุมระบบสารสนเทศ การควบคุมกระบวนการทำงาน และการควบคุมอุปกรณ์อำนวยความสะดวก (O'Brien, 1999: 656)

การควบคุมระบบสารสนเทศ (Information System Controls)

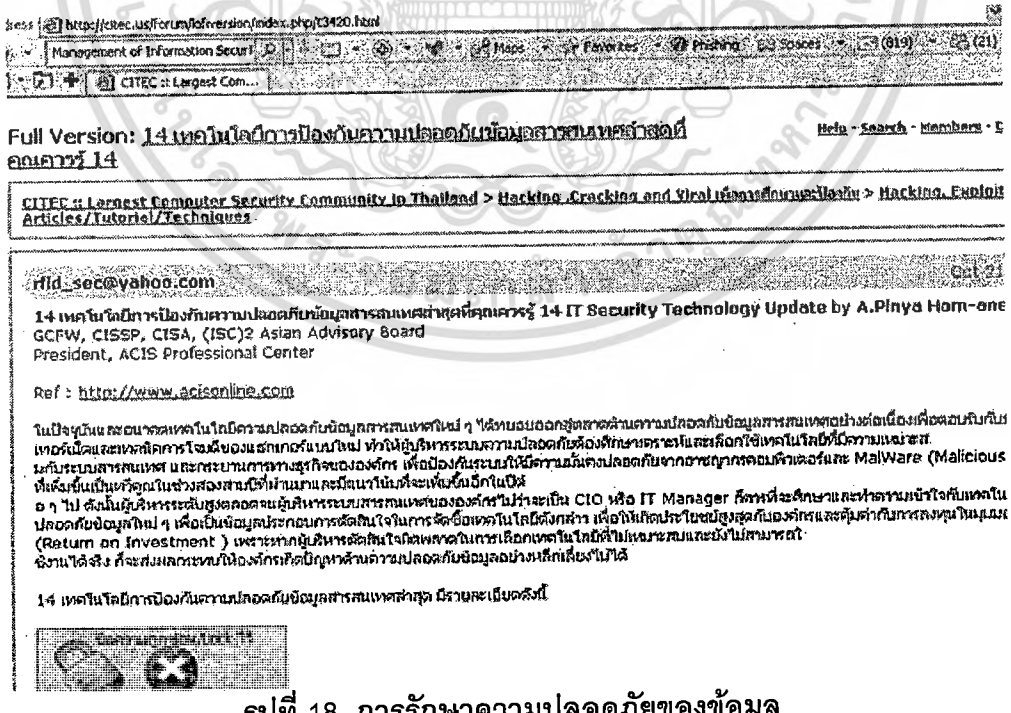
- การควบคุมอินพุท
- การควบคุมการประมวลผล
- การควบฮาร์ดแวร์ (Hardware Controls)
- การควบคุมซอฟท์แวร์ (Software Controls)
- การควบคุมเอาท์พุท (Output Controls)
- การควบคุมความจำสำรอง (Storage Controls)

การควบคุมกระบวนการทำงาน (Procedural Controls)

- การมีการทำงานที่เป็นมาตรฐาน และมีคู่มือ
- การอนุมัติเพื่อพัฒนาระบบ

รูปที่ 17 การรักษาความปลอดภัยของข้อมูล

http://www.bodin2.ac.th/lms/aw.siamschool.net/utype7f30.html?uid=83369&mid=19165&sid=4710&s_keyid=010120183



Full Version: 14 เทคโนโลยีการป้องกันความปลอดภัยข้อมูลสารสนเทศล่าสุดที่คุณควรรู้ 14

CITEC :: Largest Computer Security Community in Thailand > Hacking, Cracking and Viral เพื่อการศึกษาและป้องกัน > Hacking, Exploit Articles/Tutorial/Techniques

rfid_sec@yahoo.com

14 เทคโนโลยีการป้องกันความปลอดภัยข้อมูลสารสนเทศล่าสุดที่คุณควรรู้ 14 IT Security Technology Update by A.Pinya Hom-one
GCFW, CISSP, CISA, (ISC)2 Asian Advisory Board
President, ACIS Professional Center

Ref : http://www.acisonline.com

ในปัจจุบันและอนาคตเทคโนโลยีความปลอดภัยข้อมูลสารสนเทศใหม่ ๆ ได้ทยอยออกสู่ตลาดค้านความปลอดภัยข้อมูลสารสนเทศอย่างต่อเนื่องเพื่อตอบรับกับ เทอร์เน็ตและเทคนิคการโจมตีของแฮกเกอร์แบบใหม่ ทำให้ผู้บริหารระบบความปลอดภัยต้องศึกษาตรวจและติดตั้งใช้เทคโนโลยีที่มีความเหมาะสม กับระบบสารสนเทศ และกระบวนการทางธุรกิจขององค์กร เพื่อป้องกันระบบให้มีความมั่นคงปลอดภัยจากอาชญากรคอมพิวเตอร์และ MalWare (Malicious ที่เติบขึ้นเป็นจำนวนในช่วงสองสามปีที่ผ่านมาและมีแนวโน้มที่จะเพิ่มขึ้นอีกในปีหน้า
๑ ๆ ไป ดังนั้นผู้บริหารระดับสูงตลอดจนผู้บริหารระบบสารสนเทศขององค์กรไม่ว่าจะเป็น CIO หรือ IT Manager ก็ควรที่จะศึกษาและทำความเข้าใจกับเทคโนโล ปลอดภัยข้อมูลใหม่ ๆ เพื่อเป็นข้อมูลประกอบการตัดสินใจในการจัดซื้อเทคโนโลยีดังกล่าว เพื่อให้เกิดประโยชน์สูงสุดกับองค์กรและคุ้มค่ากับการลงทุนในมุมม (Return on Investment) เพราะหากผู้บริหารตัดสินใจผิดพลาดในการเลือกเทคโนโลยีที่ไม่เหมาะสมและยังไม่สามารถใ ช้งานได้จริง ก็จะส่งผลกระทบให้องค์กรเกิดปัญหาด้านความปลอดภัยข้อมูลอย่างหลีกเลี่ยงไม่ได้

14 เทคโนโลยีการป้องกันความปลอดภัยข้อมูลสารสนเทศล่าสุด มีรายละเอียดดังนี้

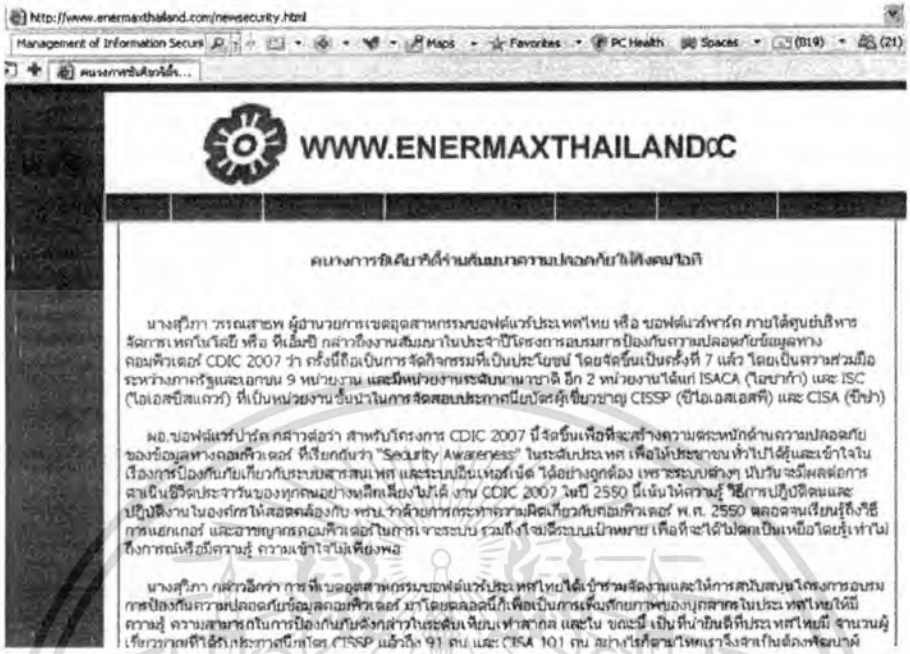
รูปที่ 18 การรักษาความปลอดภัยของข้อมูล

http://citec.us/forum/lofiversion/index.php/t3420.html

รูปที่ 19 การรักษาความปลอดภัยของข้อมูล http://bcoms.net/article/detail.asp?id=91

รูปที่ 20 การรักษาความปลอดภัยของข้อมูล

http://www.islamwit.net/krupim/lesson%20one.html

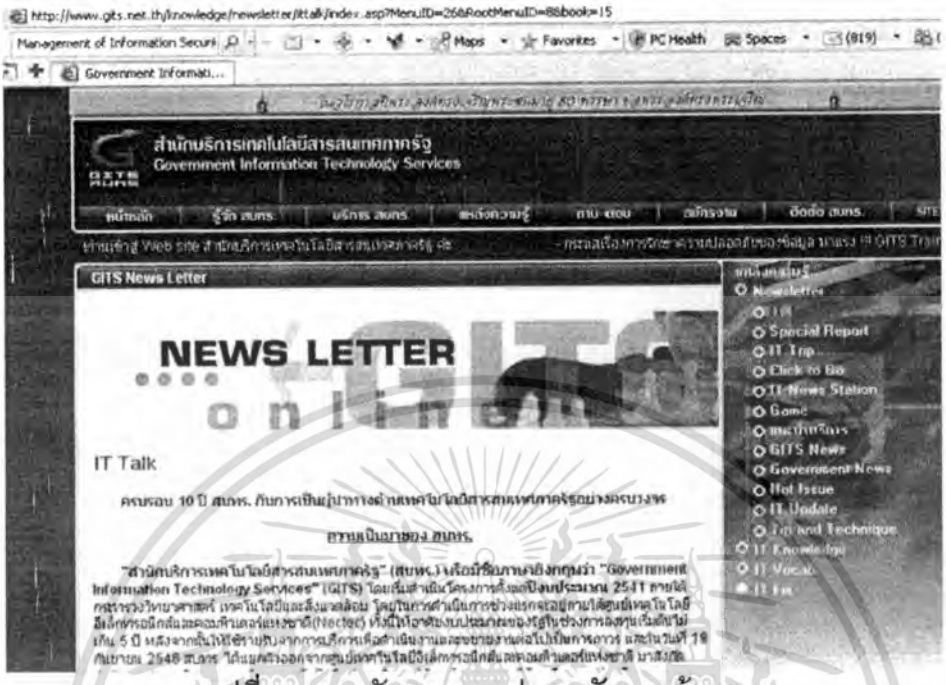


รูปที่ 21 การรักษาความปลอดภัยของข้อมูล

http://www.enermaxthailand.com/newsecurity.html

รูปที่ 22 การรักษาความปลอดภัยของข้อมูล

http://apirukmvp.blogspot.com/2005/02/10.html



รูปที่ 23 การรักษาความปลอดภัยของข้อมูล

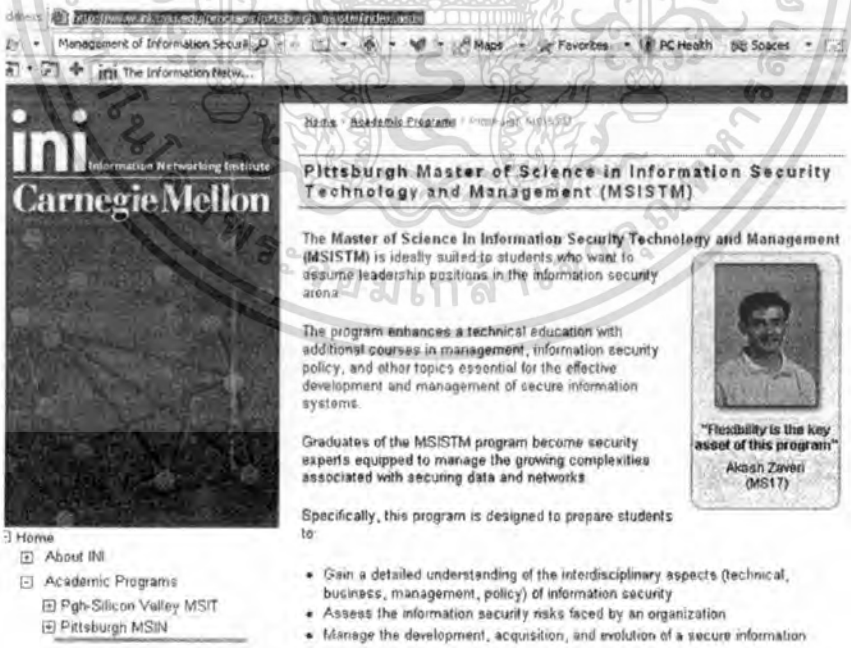
http://www.gits.net.th/knowledge/newsletter/ittalk/index.asp?MenuID=26&RootMenuID=8&book=15

รูปที่ 24 การรักษาความปลอดภัยของข้อมูล

http://www.thaipr.net/nc/printprnews.aspx?newsid=0D769DDA0AE3CC57F5F4D405ED6B0E87

รูปที่ 25 การรักษาความปลอดภัยของข้อมูล

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

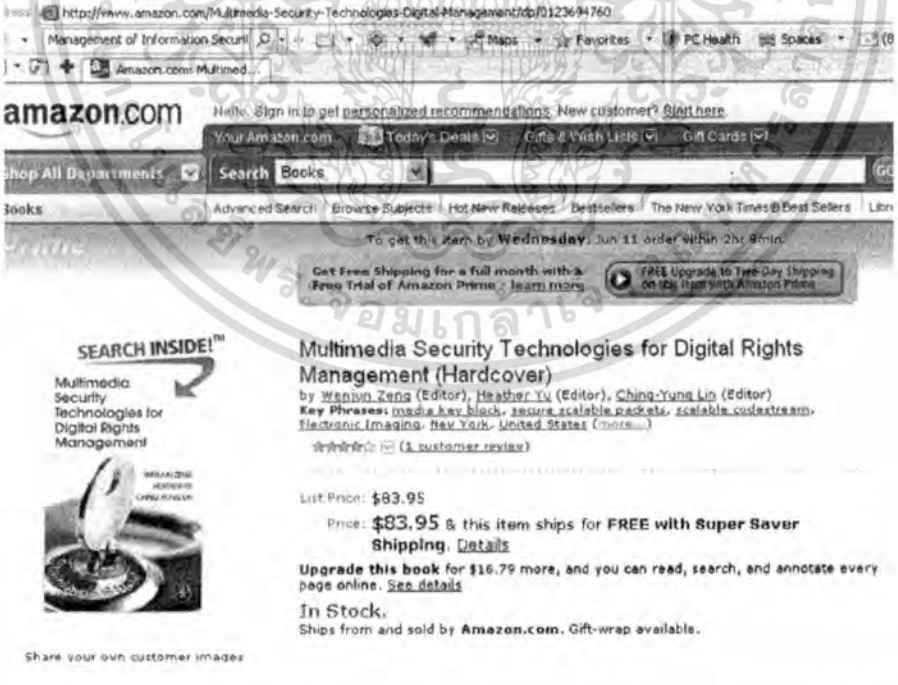


รูปที่ 26 การรักษาความปลอดภัยของข้อมูล

http://www.ini.cmu.edu/programs/pittsburgh_msistm/index.aspx

รูปที่ 27 การรักษาความปลอดภัยของข้อมูล

http://www.securityinfowatch.com/



รูปที่ 28 การรักษาความปลอดภัยของข้อมูล http://www.amazon.com/Multimedia-Security-Technologies-Digital-Management/dp/0123694760

รูปที่ 29 การรักษาความปลอดภัยของข้อมูล http://www.akibia.com/solutions/

รูปที่ 30 การรักษาความปลอดภัยของข้อมูล http://www.techweb.com/wire/security/

2.5 การรักษาความปลอดภัยของระบบเครือข่าย

1 การโจมตีเครือข่าย

เครือข่ายเป็นเทคโนโลยีที่น่าอัศจรรย์ แต่ก็ยังมีความเสี่ยงอยู่มากถ้าไม่มีการควบคุมหรือป้องกันที่ดี การโจมตีหรือการบุกรุกเครือข่าย หมายถึง ความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้การได้ (Deny of Service Attack) และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ได้ตั้งใจของผู้ใช้เองต่อไปนี้เป็นรูปแบบต่าง ๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

1.1 แพ็กเก็ตสนิฟเฟอร์ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นก้อนเล็ก ๆ ที่เรียกว่า "แพ็กเก็ต (Packet)" แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยไม่เข้ารหัส (Encryption) หรือในรูปแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้นข้อมูลอาจจะถูกคัดลอกและโพรเซสโดยแอพพลิเคชันอื่นก็ได้

1.2 ไอพีสปูฟิงไอพีสปูฟิง (IP Spoonfing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแกล้งทำเป็นว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ไอพีแอดเดรสข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบไอพีสปูฟิงเป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปในแพ็กเก็ตที่รับส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์ที่สื่อสารกันในเครือข่าย การที่จะทำอย่างนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติ้งเทเบิ้ลของเราท์เตอรีเพื่อให้ส่งแพ็กเก็ตไปยังเครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือการที่ผู้บุกรุกสามารถแก้ไขให้แอพพลิเคชันส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลิเคชันนั้นผ่านทางอีเมล หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชันได้โดยใช้ข้อมูลดังกล่าว

1.3 การโจมตีรหัสผ่านการโจมตีรหัสผ่าน (Password Attacks) หมายถึงการโจมตีที่ผู้บุกรุกพยายามเดารหัสผ่านของผู้ใช้คนใดคนหนึ่ง ซึ่งวิธีการเดานั้นก็มีหลายวิธี เช่น บรู๊ทฟอร์ซ (Brute-Force) ,โทรจันฮอร์ส (Trojan Horse) , ไอพีสปูฟิง , แพ็กเก็ตสนิฟเฟอร์ เป็นต้น การเดาแบบบรู๊ทฟอร์ซหมายถึง การลองผิดลองถูกรหัสผ่านเรื่อย ๆ จนกว่าจะถูก บ่อยครั้งที่การโจมตีแบบบรู๊ทฟอร์ซใช้การพยายามล็อกอินเข้าใช้รีซอร์สของเครือข่าย โดยถ้าทำสำเร็จผู้บุกรุกก็จะมีสิทธิ์เหมือนกับเจ้าของแอ็คเคาท์นั้น ๆ ถ้าหากแอ็คเคาท์นี้มีสิทธิ์เพียงพอผู้บุกรุกอาจสร้างแอ็คเคาท์ใหม่เพื่อเป็นประตูหลัง (Back Door) และใช้สำหรับการเข้าระบบในอนาคต

1.4 การโจมตีแบบ Man-in-the-Middleการโจมตีแบบ Man-in-the-Middle นั้นผู้โจมตี

ต้องสามารถเข้าถึงแพ็กเก็ตที่ส่งระหว่างเครือข่ายได้ เช่น ผู้โจมตีอาจอยู่ที่ ISP ซึ่งสามารถตรวจจับแพ็กเก็ตที่รับส่งระหว่างเครือข่ายภายในและเครือข่ายอื่น ๆ โดยผ่าน ISP การโจมตีนี้จะใช้ แพ็กเก็ตสนิฟเฟอร์เป็นเครื่องมือเพื่อขโมยข้อมูล หรือใช้เซสชั่นเพื่อแอ็กเซสเครือข่ายภายใน หรือวิเคราะห์การจราจรของเครือข่ายหรือผู้ใช้

1.5 การโจมตีแบบ DOSการโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DOS (Denial-of Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งปกติจะทำโดยการใช้รีซอร์สของเซิร์ฟเวอร์จนหมด หรือถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ (Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่น ๆ ไม่สามารถเข้ามาใช้บริการได้

1.6 โทรจันฮอร์ส เวิร์ม และไวรัสคำว่า "โทรจันฮอร์ส (Trojan Horse)" นี้เป็นคำที่มาจากสงครามโทรจัน ระหว่างทรอย (Troy) และกรีก (Greek) ซึ่งเปรียบถึงม้าโครงไม้ที่ชาวกรีกสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างในแล้วถอนทัพกลับ พอชาวโทรจันออกมาดูเห็นม้าโครงไม้ทิ้งไว้ และคิดว่าเป็นของขวัญที่กรีซทิ้งไว้ให้ จึงนำกลับเข้าเมืองไปด้วย พอตกดึกทหารกรีกที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีกเข้าไปทำลายเมืองทรอย สำหรับในความหมายของคอมพิวเตอร์แล้ว โทรจันฮอร์สหมายถึงดปรแกรมที่ทำลานระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ เช่น เกม สกรีนเวฟเวอร์ เป็นต้น

2 เทคโนโลยีรักษาความปลอดภัยถึงแม้ว่าการปกป้องข้อมูลเป็นสิ่งที่มีลำดับความสำคัญสูงสุด แต่การรักษาเครือข่ายให้ทำงานอย่างถูกต้องก็เป็นปัจจัยที่สำคัญในการปกป้องข้อมูลที่อยู่ในเครือข่ายนั้น ถ้ามีช่องโหว่ของระบบเครือข่ายที่อนุญาตให้โจมตีได้ ความเสียหายที่เกิดขึ้นอาจใช้ทั้งเวลาและความพยายามอย่างมากที่จะทำให้ระบบกลับมาทำงานได้เหมือนเดิม ในหัวข้อต่อไปผู้เขียนจะแนะนำเทคนิคและเทคโนโลยีที่ใช้สำหรับป้องกันและรักษาความปลอดภัยทั้งระบบเครือข่ายเอง และข้อมูลที่จัดเก็บและรับส่งผ่านเครือข่าย

2.1 ไฟร์วอลล์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้เต็มที่ และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ตได้ ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างในได้ รูปที่ 12.3 แสดงการติดตั้งไฟร์วอลล์เพื่อเชื่อมต่อเครือข่ายส่วนบุคคลกับเครือข่ายอินเตอร์เน็ต จากรูปจะเห็นได้ว่าแพ็กเก็ตที่วิ่งระหว่างเครือข่ายภายในและอินเตอรีเน็ตต้องผ่านไฟร์วอลล์เท่านั้น

ประเภทของไฟร์วอลล์ โดยทั่วไปแล้วไฟร์วอลล์แบ่งออกเป็น 2 ประเภท คือ

1. Application Layer Firewall คือ ไฟร์วอลล์ที่ทำงานในระดับแอพพลิเคชันเลเยอร์ (Application Layer Firewall) นั้นบางทีก็เรียกว่า "พร็อกซี่ (Proxy Firewall)" คือ โปรแกรมที่รันบนระบบปฏิบัติการทั่ว ๆ ไป เช่น วินโดวส์เซิร์ฟเวอร์หรือยูนิกซ์หรืออาจจะเป็นฮาร์ดแวร์พร้อมใช้งานแล้วก็ได้ ไฟร์วอลล์จะมีเน็ตเวิร์คการ์ดหลายการ์ด เพื่อสำหรับเชื่อมต่อกับเครือข่ายต่าง ๆ นโยบายการรักษาความปลอดภัยจะเป็นสิ่งที่กำหนดว่าทราฟิกใดสามารถถ่ายโอนระหว่างเครือข่ายใดได้บ้าง ถ้านโยบายไม่ได้ระบุอย่างชัดเจนว่าทราฟิกไหนที่อนุญาตให้ผ่านได้ไฟร์วอลล์ก็จะไม่ส่งผ่านหรือละทิ้งแพ็กเก็ตนั้นทันที นโยบายนั้นจะถูกบังคับใช้โดยพร็อกซี่ในไฟร์วอลล์ระดับแอพพลิเคชันนั้นทุก ๆโปรโตคอลที่อนุญาตให้ผ่านได้จะต้องมีพร็อกซี่สำหรับโปรโตคอลนั้น พร็อกซี่ที่ดีที่สุดนั้นจะเป็นพร็อกซี่ที่ออกแบบมาสำหรับจัดการกับโปรโตคอลนั้นโดยเฉพาะ

2 Packet Filtering Firewallแพ็กเก็ตฟิลเตอร์ริ่งไฟ์วอลล์ (Packet Filtering Firewall) อาจจะเป็นทั้งซอฟต์แวร์หรือฮาร์ดแวร์ที่ทำหน้าที่กรองแพ็กเก็ตที่ผ่านไฟร์วอลล์โดยใช้นโยบายการรักษาความปลอดภัยที่กำหนดไว้ แพ็กเก็ตฟิลเตอร์ริ่งไฟ์วอลล์ นั้นจะอนุญาตให้มีการเชื่อมต่อโดยตรงระหว่างไคลเอนท์และเซิร์ฟเวอร์ ดังนั้นไฟร์วอลล์ประเภทนี้จะทำงานค่อนข้างเร็วกว่าแบบแอพลิเคชันไฟร์วอลล์ เนื่องจากไม่ต้องสร้างคอนเน็กชันใหม่

3. นโยบายการรักษาความปลอดภัยสิ่งที่สำคัญที่สุดสำหรับการใช้ไฟร์วอลล์คือ การกำหนดนโยบายการรักษาความปลอดภัย(Network Security Policy) ถึงแม้ว่าไฟร์วอลล์มีประสิทธิภาพและมีความปลอดภัยมากแค่ไหนก็ตาม แต่ถ้ามีนโยบายการรักาาความปลอดภัยที่หละหลวมไฟร์วอลล์ก็ไม่มีประโยชน์มาก ดังนั้นก่อนที่จะติดตั้งไฟร์วอลล์ควรกำหนดนโยบายการรักษาความปลอดภัยที่สามารถควบคุมหรือป้องกันทราฟิกที่อาจจะมีผลกระทบต่อการใช้งานเครือข่ายให้มากที่สุด เมื่อกำหนดนโยบายได้แล้วขั้นตอนต่อไปคือ นำนโยบานี้ไปบังคับใช้ในไฟร์วอลล์ กฎบังคับใช้นโยบายการรักษาความปลอดภัยในไฟร์วอลล์นั้นจะเรียกว่า "ACL (Access Control List)"

4. ระบบตรวจจับการบุกรุก (Intrusion Detection System)การตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบแจ้งเตือนผู้ดูแลระบบเมื่อมีการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น ถ้าเปรียบกับระบบการรักษาความปลอดภัยของรถ IDS ก็อาจจะเปลี่ยนได้กับระบบกันขโมย ซึ่งระบบนี้จะส่งสัญญาณเมื่อมีการตรวจพบความพยายามที่จะขโมยรถ เช่น การงัดประตู หรือกระจก แต่ระบบนี้ไม่สามารถป้องกันไม่ให้รถถูกขโมยได้ อย่างไรก็ตามโดยธรรมชาติแล้วขโมยจะพยายามหลีกเลี่ยงรถที่ติดตั้งระบบนี้ ระบบเครือข่ายก็เช่นกัน ถ้ามีระบบตรวจจับและแจ้งสัญญาณเตือนการบุก

รุก พวกแฮ็กเกอร์ก็จะหลีกเลี่ยงการบุกรุกเครือข่ายนี้

4.1 ประเภทของ IDS IDS แบ่งออกเป็น 2 ประเภท คือ Host-Based IDS และ Network-Based IDS โดยโฮสต์เบสไอดีเอส นั่นคือ ระบบที่ติดตั้งที่โฮสต์และเฝ้าระวังและตรวจจับความพยายามที่จะบุกรุกโฮสต์นั้น ส่วนเน็ตเว็ค เบสไอดีเอส นั่นคือ ระบบที่ตรวจดูแพ็กเก็ตที่วิ่งอยู่ในเครือข่าย และแจ้งเตือนถ้าพบหลักฐานที่คาดว่าจะเป็นการบุกรุกเครือข่าย

- Host-Based IDSโฮสต์เบสไอดีเอสเป็นซอฟต์แวร์ที่รันบนโฮสต์ โดยปกติแล้ว IDS ประเภทนี้จะวิเคราะห์ล็อก (Log) เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก ในระบบยูนิกซ์นั้นล็อกที่ IDS จะตรวจสอบ เช่น Syslog, Messages, Lastlog และ Wtmp เป็นต้น ส่วนในวินโดวส์นั้น IDS ก็จะตรวจสอบอีเวนต์ล็อกต่าง ๆ เช่น System, Application และ Security เป็นต้น โดยปกติ IDS จะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นในล็อกและเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงก็จะแจ้งทันที ดังนั้นการที่ IDS จะตรวจจับการบุกรุกได้ระบบจะต้องบันทึกเหตุการณ์ต่าง ๆ ที่สำคัญที่เกิดขึ้นกับระบบในล็อกไฟล์ ถ้าไม่เช่นนั้น IDS ก็ไม่มีข้อมูลที่จะใช้วิเคราะห์ว่ามีการบุกรุกหรือไม่

- Network-Based IDS เน็ตเวิร์คเบสไอดีเอส คือ ซอฟต์แวร์พิเศษที่รันบนคอมพิวเตอร์เครื่องหนึ่งต่างหาก IDSประเภทนี้จะมีเน็ตเวิร์คที่ทำงานในโหมดที่เรียกว่า "โพรมิสเซียส (Promiscuous Mode)" ซึ่งโหมดนี้เน็ตเวิร์คการ์ดที่รันในโหมดธรรมดานั้นจะรับเอาเฉพาะแพ็กเก็ตที่มีที่อยู่ปลายทางตรงกับเครื่องเท่านั้น เมื่อทุก ๆ แพ็กเก็ตส่งผ่านไปให้แอพพลิเคชัน IDS จะวิเคราะห์ข้อมูลในแพ็กเก็ตเหล่านั้นกับกฎที่ได้ตั้งไว้ก่อนหน้า ถ้าตรงกับกฎก็จะแจ้งเตือนทันที

- การแจ้งเตือนภัย IDSIDS จะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น มีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องคอนฟิกให้กับ IDS สิ่งแรกคือ ซิกเนเจอร์ของการบุกรุก สิ่งที่สองคือเหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือเหตุการณ์ที่คากว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณีต่าง ๆ เหล่านี้อาจเป็นทราฟิกที่ไม่ปกติหรืออาจเป็นบางข้อความในล็อก การคอนฟิกซิกเนเจอร์ให้กับ IDS ของแต่ละองค์กรนั้นอาจจะไม่เหมือนกัน ซึ่งขึ้นอยู่กับว่าองค์กรนั้นจะให้ความสนใจกับการบุกรุกประเภทใด

- การสำรวจเครือข่ายเหตุการณ์ที่เป็นการสำรวจเครือข่ายเป็นการพยายามของผู้บุกรุกที่จะรวบรวมข้อมูลเกี่ยวกับระบบเครือข่ายก่อนที่จะโจมตีจริง ๆ เช่น

IP Scans

Port Scans

Trojan Scans

Vulnerability Scans

File Snooping

- การโจมตีการโจมตีเครือข่ายหรือระบบนั้นควรให้ลำดับความสำคัญสูงสุด เมื่อ IDS รายงานเหตุการณ์นี้ผู้ดูแลระบบต้องตอบสนองกับเหตุการณ์นี้ทันทีเพื่อป้องกันการสูญเสียมากกว่านี้ บางครั้ง IDS อาจแยกแยะระหว่างการโจมตีจริง ๆ กับการสแกนหาจุดอ่อน เนื่องจากเหตุกาณ์ทั้งสองนั้น IDS จะตรวจพบซิกเนเจอร์ของการโจมตีเหมือนกัน ผู้ดูแลระบบอาจต้องวิเคราะห์ข้อมูลเพิ่มเติม การสแกนหาจุดอ่อนนั้น IDS จะรายงานการโจมตีหลาย ๆ รูปแบบในช่วงเวลาสั้น ๆ กับระบบใดระบบหนึ่ง ส่วนการโจมตีจริงนั้นอาจมีการรายงานการโจมตีแค่รูปแบบเดียวกับระบบใดระบบหนึ่ง

- เหตุการณ์ที่น่าสงสัยหรือผิดปกติ

เหตุการณ์อื่น ๆ ที่ผิดปกติและไม่ได้จัดอยู่ในประเภทต่าง ๆ ที่กล่าวมาข้างต้นถือว่าเป็นเหตุการณีที่น่าสงสัยว่าอาจมีการโจมตีเครือข่ายเกิดขึ้น ซึ่งผู้ดูแลระบบต้องวิเคราะห์และสืบหาสาเหตุของเหตุการณ์ที่ว่านี้ต่อ ตัวอย่างเช่น บางโฮสต์อาจส่งแพ็กเก็ตที่มีข้อมูลส่วนหัวผิดไปจากที่กำหนดในมาตรฐานซึ่งเหตุการณ์นี้อาจเกิดขึ้นเนื่องจากการโจมตีแบบใหม่ หรือเน็ตเวิร์คการ์ดเครื่องส่งอาจเสีย

5 . คริพโตกราฟี (Cryptography)โดยทั่วไปแล้วข้อมูลที่รับส่งผ่านเครือข่ายนั้นจะอยู่ในรูปเคลียร์เท็กซ์ (Clear text) ซึ่งข้อมูลนั้อาจถูกอ่านหรือคัดลอกได้ดดยการใช้เทคนิคที่เรียกว่า "สนิฟเฟอริง (Sniffering)" เครื่องมือต่าง ๆ เช่น โปรโตคอลอะนาไลเซอร์

5.1 Symmetric Key Cryptographyการเข้าและถอดรหัสข้อมูลแบบซีเครทคีย์ (Secret Key) เป็นวิธีที่ทั้งการเข้ารหัสและการถอดรหัสจะใช้คีย์ (Key) หรือรหัสลับเดียวกันหรือเรียกอีกอย่างหนึ่งว่า การเข้ารหัวแบบซิมเมทริกซ์ (Symmertric) คีย์ที่ใช้จะมีความยาวคงที่

5.2 Data Encryption Standard (DES)ในปี ค.ศ. 1977 รัฐบาลสหรัฐฯ ได้กำหนดให้ใช้ DES (Data Encryption Standard) ในการเข้ารหัสข้อมูลในชั้นที่มีความลับน้อย ซึ่ง DES ได้ถูกพัฒนาโดย IBM และเป็นอัลกอริธึมที่ใช้อย่างแพร่หลายต่อมา แต่ปัจจุบัน DES ได้กลายเป็นการเข้ารหัสที่ไม่ปลอดภัยแล้ว เนื่องจากการถอดรหัสนั้นทำได้ง่ายและรวดเร็วมาก

5.3 Triple-DESการเข้ารหัสข้อมูลแบบ DES นั้นปัจจุบันถือว่าไม่ปลอดภัยแล้ว เนื่องจากความยาวของคีย์ที่ใช้สั้นเกินไป และด้วยประสิทธิภาพของคอมพิวเตอร์ที่ใช้อยู่ในปัจจุบัน ทำให้การถอดรหัส DES ทำได้ในเวลาอันสั้น

5.4 Public Key Cryptographyปัญหาของการเข้ารหัสข้อมูลแบบเมทริกซ์หรือซีเครทคีย์ คือ ทั้งฝ่ายรับและฝ่ายส่งจะต้องตกลงกันก่อนว่าจะใช้คีย์อะไรในการเข้ารหัสข้อมูล ดังนั้นทั้งสองฝ่ายจะต้องใช้ช่องทางสื่อสารที่คาดว่าจะปลอดภัยเพื่อแลกเปลี่ยนคีย์กัน

5.5 RSA เป็นการเข้ารหัสแบบพับลิกไพรเวทคีย์อีกประเภทหนึ่ง โดยชื่อ RSA มาจากอักษรตัว

แรกของผู้คิดค้นอัลกอริธึมนี้คือ รีเวสท์ (Revest) ชาเมอร์ (Shamir) และแอ็ดเดิลเมน (Adlemen) วิธีนี้สามารถใช้ได้ทั้งกับการเข้ารหัสข้อมูลและลายเซ็นดิจิตอล ข้อมูลที่เข้ารหัสด้วยไพรเวทคีย์จะถูกถอดรหัสได้โดยใช้พับลิกคีย์ที่เป็นคู่กันเท่านั้น เช่น ถ้าอลิสใช้ไพรเวทคีย์ของตัวเองในการเข้ารหัส ใครก็ตามที่มีพับลิกคีย์ของเธอก็สามารถถอดรหัสข้อมูลนั้นได้ แสดงหลักการเข้าและถอดรหัสแบบพับลิกคีย์เอ็นคริพชัน การสื่อสารแบบนี้จะสร้างความเชื่อมั่นในข้อมูลแบบทางเดียว RSA สามารถใช้ประโยชน์ได้หลายด้าน เช่น การเข้ารหัสข้อมูล และการแจกจ่ายซีเครทคีย์ก็ได้

5.6 Diffie-Hellmanวิธีหนึ่งที่ใช้ในการแจกจ่ายซีเครทคีย์คือ การใช้อัลกอริธึมของดิฟฟีเฮลล์แมน (Diffie-Hellman) การทำงานดังแสดงในรูปที่ 12.12 ซึ่งแสดงการสื่อสารระหว่างอลิสและบ๊อบ อลิสและบ๊อบนั้นเป็นตัวละครย่อยนิยมในสังคมการเข้ารหัสข้อมูล

5.7 ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)การเซ็นชื่อในเอกสารทั่วไปเป็นการบ่งบอกว่าผู้เซ็นนั้นเห็นด้วยกับเนื้อหาที่อยู่ในเอกสาร หรือเพื่อเป็นการประกาศรวมเป็นเจ้าของ หรือผู้ที่สร้างเอกสารนั้น ๆ ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เป็นเทคนิคที่ทำให้จุดมุ่งหมายนี้เป็นไปได้ในโลกดิจิตอล

5.8 ใบรับรอง12.5.2.5 อิเล็กทรอนิกส์ Certificate Authority)
การรักษาความปลอดภัยของข้อมูลนั้นไม่ได้ขึ้นอยู่กับอัลกอริธึมและคีย์ที่ใช้เข้ารหัสข้อมูลเท่านั้น แต่ยังขึ้นอยู่กับการสร้าง การแจกจ่าย และการจัดการคีย์ด้วย ถ้าคีย์ถูกขโมยได้ข้อมูลก็จะถูกขโมยได้เช่นกัน ผู้ที่รับผิดชอบในการสร้างคีย์เพื่อแจกจ่ายจะต้องมีระบบการรักษาความปลอดภัยที่รัดกุม ไม่อย่างนั้นระบบที่รับคีย์ไปใช้ก็อาจจะไม่ปลอดภัยไปด้วย

6. คริพโตกราฟีกับการสื่อสารผ่านเครือข่ายทฤษฎีเกี่ยวกับการรักษาความปลอดภัยของข้อมูลแบบต่าง ๆ ไม่ว่าจะเป็นซิมเมทริกซ์คีย์เอ็นคริพชัน, พับลิกคีย์เอ็นคริพชัน, ลายเซ็นอิเล็กทรอนิกส์และใบรับรองอิเล็กทรอนิกส์ ในหัวข้อนี้ผู้เขียนจะขอยกตัวอย่างของการประยุกต์ใช้คริพโตกราฟีกับการสื่อสารผ่านเครือข่ายหรืออินเตอร์เน็ต อย่างที่ทราบกันดีแล้วว่าการสื่อสารบนเครือข่ายนั้นแบ่งออกเป็นโปรโตคอลหลาย ๆ เลเยอร์

6.1 PGP (Pretty Good Privacy) เป็นการประยุกต์ใช้คริพโตกราฟีกับการสื่อสารด้วยอีเมลซึ่งถูกออกแบบโดย ฟิวส์ ซิมเมอร์แมนน์ (Phil Zimmermann) ในปี ค.ศ. 1991 และปัจจุบันได้กลายเป็นมาตรฐานที่ใช้สำหรับการรับส่งอีเมลอย่างปลอดภัย PGPใช้ทั้งซิมเมทริกซ์คีย์เอ็นคริพชันและพับลิกคีย์เอ็นคริพชันเพื่อให้บริการทั้งการปกปิด (Secrecy), การพิสูจน์ตัวตน (Authentication) และความคงสภาพ (Integrity) ของข้อความที่รับส่งกัน รูปข้างล่างแสดงการเข้ารหัสข้อมูลอีเมลแบบ PGP ก่อนที่จะส่งข้อความ

6.2 SSL การรับส่งข้อมูลระหว่างเว็บเซิร์ฟเวอร์และไคลเอ็นท์นั้นถือว่าไม่ปลอดภัย เนื่องจากข้อมูลที่รับส่งนั้นอยู่ในรูปแบบของเคลียร์เท็กซ์ในช่วงหลัง ๆ ของการใช้อินเตอร์เน็ตนั้นมีการประยุกต์ใช้อินเตอร์เน็ตเพื่อจุดประสงค์ทางด้านธุรกิจหรือที่เรียกว่า "อีคอมเมิร์ซ" ส่วนใหญ่การติดต่อสื่อสารที่เกี่ยวกับธุรกิจนั้นผู้รับและผู้ส่งจำเป็นที่จะต้องปกปิดข้อมูล

6.3 VPN เครือข่ายส่วนบุคคลเสมือน หรือ (Virtual Private Network) หมายถึง ระบบเครือข่ายส่วนบุคคลที่สร้างโดยการใช้แชร์ลิงค์ ซึ่งลิงค์ที่ว่านี้จะเป็นเครือข่ายอินเตอร์เน็ตหรือเป็นลิงค์ที่ถือว่าไม่มีความปลอดภัยของข้อมูล VPN แบ่งออกเป็น 3 ประเภท ขึ้นอยู่กับลักษณะการใช้งาน

- PPTP (Point-to-Point Tunneling Protocol) เป็นโปรโตคอลแรกที่ใช้สร้างระบบ VPN โปรโตคอลนี้เป็นที่นิยมกับระบบไดอัลอัพ (Dial-Up) สาเหตุก็เนื่องจากไมโครซอฟต์ได้ให้การสนับสนุนในการพัฒนาและทำให้เป็นส่วนหนึ่งของวินโดวส์ NT 4.0 และได้ติดตั้งในไคลเอนท์วินโดวส์ 95 ต่อมาได้รวมเข้าไปในวินโดวส์ 98 และเวอร์ชันหลัง ๆ อย่างไรก็ตาม PPTP ยังไม่ถูกรับรองว่าเป็นมาตรฐานโดยองค์กรมาตรฐาน เช่น IETF (Internet Engineering Task Force) เนื่องจากถูกออกแบบสำหรับเฉพาะวินโดวส์เท่านั้น

- L2F (Layer 2 Forwarding) เป็นโปรดตคอลที่พัฒนาในช่วงแรก ๆ ที่มีการพัฒนา VPN เหมือนกันกับ PPTP โปรโตคอล L2F ถูกออกแบบมาใช้กับการสร้างการเชื่อมต่อปลอดภัยระหว่างผู้ใช้กับเครือข่ายขององค์กร ข้อแตกต่างระหว่าง PPTP และ L2F ก็คือ การสร้างท่อ (Tunneling) ของ L2F นั้นไม่ได้ขึ้นอยู่กับโปรโตคอล IP ดังนั้นโปรโตคอลนี้จึงสามารถทำงานร่วมกับโปรดตคอลอื่น ๆ ได้โดยตรง

- L2TP (Layer 2 Tunneling Protocol) ออกแบบโดย IETF (Internet Engineering Task Force) เพื่อใช้แทนโปรโตคอล PPTP และ L2F และได้กำหนดให้เป็นมาตรฐานที่รับรองโดย IETF โปรโตคอล L2TP พัฒนาเพื่อขจัดจ้อบกพร่องของ L2F และ PPTP ซึ่งทั้งสองโปรโตคอลนี้จะอาศัยดปรดตคอล PPP ในการสร้างการเชื่อมต่อ แต่ L2TP จะใช้วิธีการสร้างการเชื่อมต่อแบบใหม่ ซึ่งพัฒนาต่อจาก L2F นอกจากนี้ L2TP ยังได้กำหนดประเภทของแพ็กเก็ตที่ส่งมาด้วย

- IPSec IPSec (IP Security) เป็นโปรโตคอลที่ให้บริการการรักษาความปลอดภัยข้อมูลในระดับเน็ตเวิร์คเลเยอร์ ดดยปรโตคอลนี้ได้ถูกออกแบบสำหรับการเข้ารหัสข้อมูลแพ็กเก็ตของดปรโตคอล IP โปรโตคอลนี้จะรับรองความลับของข้อมูล (Confidentality), ความคงสภาพของข้อมูล (Integrity) และการพิสูจน์ตัวตนของฝ่ายส่ง (Authentication)

2.6 ระบบ ISO27001:2005

กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

ข้อ 1 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1.1 ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการทางธุรกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้องแนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ตามแสดงใน รูปภาพที่ 1

รูปที่ 31 แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act

1.2 กำหนดและบริหารจัดการ ระบบบริหารจัดการความมั่นคงปลอดภัย

1.2.1 กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

องค์กรจะต้องปฏิบัติดังนี้

a) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาถึงลักษณะ

ของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย

b) กำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี

b.1 กรอบในการดำเนินการ ทิศทางและหลักการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ

b.2 ข้อกำหนดทางธุรกิจ ข้อกำหนดในสัญญาต่าง ๆ ระเบียบปฏิบัติ ข้อบังคับ รวมทั้งกฎหมายของประเทศ

b.3 การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ในระดับองค์กร

b.4 เกณฑ์ในการประเมินความเสี่ยง (ดูข้อ 1.2.1 c)

b.5 การได้รับอนุมัติจากผู้บริหาร

c) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร

c.1 ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยขององค์กร

c.2 กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้

d) ระบบความเสี่ยง

d.1 ระบุทรัพย์สินที่อยู่ในขอบเขตของระบบบริหารจัดการความปลอดภัยรวมทั้งผู้เป็นเจ้าของทรัพย์สินเหล่านั้น

d.2 ระบุภัยคุกคามที่มีต่อทรัพย์สินเหล่านั้น

d.3 ระบุจุดอ่อนที่ภัยคุกคามอาจจะใช้ให้เป็นประโยชน์

d.4 ระบุผลกระทบที่ก่อให้เกิดความสูญเสียทางด้านความลับความสมบูรณ์ความพร้อมใช้ของทรัพย์สินเหล่านั้น

e) วิเคราะห์และประเมินความเสี่ยง

e.1 ประเมินผลกระทบที่มีต่อธุรกิจซึ่งอาจเป็นผลจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย โดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

e.2 กำหนดความน่าจะเป็นของความเสี่ยงอันเกิดจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย

e.3 กำหนดระดับความเสี่ยง

e.4 กำหนดว่าความเสี่ยงเหล่านั้น สามารถยอมรับได้หรือไม่ โดยใช้เกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้ในข้อ 1.2.1) c.2)

e) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ อาจรวมถึง

f.1 ใช้มาตรการที่เหมาะสม

f.2 ยอมรับความเสี่ยงเหล่านั้น โดยมีเงื่อนไขว่า ความเสี่ยงเหล่านั้นจะต้องอยู่ภายในเกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้ในข้อ 1.2.1) c.2)

f.3 หลีกเลี่ยงความเสี่ยงเหล่านั้น

f.4 โอนย้ายความเสี่ยงเหล่านั้นไปสู่ผู้อื่น เช่น บริษัทประกันภัย เป็นต้น

g) เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยเพื่อจัดการกับความเสี่ยงวัตถุประสงค์และมาตรการดังกล่าวสามารถเลือกมาจากมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ในตอนท้ายของมาตรฐานฉบับนี้

h) ขอการอนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

i) ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

j) จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรการตามที่แสดงไว้ในส่วนของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ เอกสารดังกล่าวควรมีองค์ประกอบดังนี้

j.1 วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัย ตามที่ได้เลือกไว้ในข้อ 1.2.1) g) รวมทั้งเหตุผลการใช้งาน

j.2 วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยที่ได้ใช้งานอยู่ในปัจจุบัน

j.3 วัตถุประสงค์และมาตรการความมั่นคงปลอดภัยที่ไม่มีการใช้งานรวมทั้งเหตุผลที่ไม่มีการใช้งาน

1.2.2 ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติ ดังนี้ (Do)

a) จัดทำแผนการจัดการความเสี่ยงซึ่งกล่าวถึงการดำเนินการเชิงบริหารจัดการทรัพยากรที่จำเป็น หน้าที่ความรับผิดชอบ และลำดับการดำเนินการเพื่อบริหารจัดการความเสี่ยงที่พบ

b) ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงเพื่อบรรลุในวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

c) ลงมือปฏิบัติตามมาตรการที่ได้เลือกไว้ในข้อ 1.1.2) g) เพื่อบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยของมาตรการดังกล่าว

d) กำหนดวิธีการในการวัดความสัมฤทธิผลของมาตรการที่เลือกมาใช้งาน การวัดดังกล่าวจะต้องสามารถสร้างผลลัพธ์ที่สามารถเปรียบเทียบได้ รวมทั้งสามารถสร้างผลลัพธ์เดิมขึ้นมาอีกครั้งหนึ่งได้

e) จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก

f) บริหารการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

g) บริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

h) จัดทำและลงมือปฏิบัติตามขั้นตอนและมาตรการอื่น ๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

1.2.3 เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Check)

a) ลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวน เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสามารถ

a.1 ตรวจจับข้อผิดพลาดจากการประมวลผล

a.2 ระบุการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องกับความ มั่นคงปลอดภัย

a.3 ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่คาดหมายไว้ หรือไม่

a.4 ตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยโดยอาศัยตัวบ่งชี้ต่าง ๆ เพื่อช่วยในการตรวจจับเหตุการณ์ต่าง ๆที่ไม่คาดคิด

a.5 ตรวจสอบได้ว่าการดำเนินการเพื่อแก้ไขการละเมิดทางด้านความมั่นคงปลอดภัยมีความสัมฤทธิผลหรือไม่

b) ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสม่ำเสมอ โดยนำสิ่งต่าง ๆ ต่อไปนี้มาพิจารณาร่วมด้วย ได้แก่ ผลการตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือหน่วยงานที่เกี่ยวข้อง เป็นต้น

c) วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

d) ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ โดยพิจารณาการเปลี่ยนแปลงของสิ่งต่อไปนี้ประกอบด้วย

d.1 องค์กร

d.2 เทคโนโลยี

d.3 วัตถุประสงค์และกระบวนการทางธุรกิจ

d.4 ภัยคุกคามที่ระบุไว้ก่อนหน้านี้ กับสภาพการเปลี่ยนแปลงปัจจุบัน

d.5 ความสัมฤทธิผลของมาตรการที่ได้ลงมือปฏิบัติไปแล้ว

d.6 เหตุการณ์ภายนอก ได้แก่ การเปลี่ยนแปลงที่มีต่อกฎระเบียบ กฎหมาย ข้อกำหนดในสัญญาที่ทำไว้ หรือข้อกำหนดอื่น ๆ และการเปลี่ยนแปลงทางสังคม เป็นต้น

e) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยภายในองค์กรตามรอบระยะเวลาที่ได้กำหนดไว้

f) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหารอย่างสม่ำเสมอ

g) ปรับปรุงแผนทางด้านความมั่นคงปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย

h) บันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

1.2.4 บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Act)

a) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้

b) ใช้มาตรการเชิงแก้ไขและป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่น ๆ มาช่วยในการปรับปรุงให้ดีขึ้น

c) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

d) ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

ข้อ 3 การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย

องค์กรควรดำเนินการตรวจสอบภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัถตุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัย

a) สอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องหรือไม่

b) สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือไม่

c) ได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิผลหรือไม่

d) เป็นไปตามที่คาดหมายไว้หรือไม่

องค์กรต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่าง ๆ ที่จะได้รับการตรวจสอบ รวมทั้งผลการตรวจสอบจากครั้งต่าง ๆที่ผ่านมา องค์กรจะต้องกำหนดเกณฑ์ในการตรวจสอบ ขอบเขต ความถี่ และวิธีการที่ใช้ในการตรวจสอบ การคัดเลือกผู้ตรวจสอบ และการดำเนินการตรวจสอบจะต้องคำนึงถึงหลักฐานตามความเป็นจริง และความเที่ยงธรรมของผู้ตรวจสอบ รวมทั้งผู้ ตรวจสอบจะต้องไม่ตรวจสอบงานของตนเอง องค์กรจะต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่าง ๆ ในการวางแผนและ ดำเนินการตรวจสอบ และบำรุงรักษาบันทึกข้อมูลที่เกี่ยวข้องกับการตรวจสอบนั้น อย่าง เป็นลายลักษณ์อักษร ผู้บริหารที่รับผิดชอบในส่วนที่ได้รับการตรวจสอบจะต้องควบคุมให้การ

ดำเนินการแก้ไขเพื่อกำจัดความไม่สอดคล้องและสาเหตุที่เกี่ยวข้องได้รับการดำเนินการโดย ปราศจากความล่าช้าที่เกินควร รวมทั้งจะต้องควบคุมให้มีกิจกรรมการติดตามเพื่อ ตรวจสอบการดำเนินการที่ได้ดำเนินการไปแล้ว และมีการจัดทำรายงานผลการตรวจสอบนั้น .

2.7 งานวิจัยที่เกี่ยวข้อง

วัสกา ดวงอ่อนนาม (2546) ทำการศึกษาเรื่องการใช้เทคโนโลยีสารสนเทศในวิทยาลัยเกษตรและเทคโนโลยีสังกัดกรมอาชีวศึกษา ประชากรที่ใช้ในการศึกษาคือผู้บริหาร หัวหน้างาน และครูผู้สอนวิชาเกษตรกรรม ในวิทยาลัยเกษตรและเทคโนโลยี สังกัดกรมอาชีวศึกษาทั่วประเทศ โดยตัวแปรอิสระที่ใช้ตัวหนึ่งคือ ประสบการณ์การทำงาน โดยแบ่งเป็นประสบการณ์มาก (ทำงานมากกว่า 5 ปี) และประสบการณ์การทำงานน้อย (ทำงาน 1-5 ปี) ตั้งสมมติฐานว่าผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปริมาณการใช้เทคโนโลยีสารสนเทศต่างกัน ผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีความสามารถในการใช้เทคโนโลยีสารสนเทศต่างกัน และผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปัญหาในการใช้เทคโนโลยีสารสนเทศต่างกัน ผลการวิจัยสรุปว่า ผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปริมาณการใช้เทคโนโลยีสารสนเทศและความสามารถในการใช้เทคโนโลยีสารสนเทศต่างกัน แต่ผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปัญหาในการใช้เทคโนโลยีสารสนเทศไม่แตกต่างกัน

ธนา จินดาวัฒนะ (2534) ได้ศึกษาเรื่องการจัดระบบสารสนเทศ เพื่อการวางแผนในโรงเรียนมัธยมศึกษาขนาดใหญ่ สังกัดกรมสามัญศึกษา เขตการศึกษา 5 มีวัตถุประสงค์เพื่อศึกษาสภาพปัจจุบันปัญหาและความต้องการในการจัดระบบสารสนเทศเพื่อการวางแผนในโรงเรียนมัธยมศึกษาขนาดใหญ่ สังกัดกรมสามัญศึกษา เขตการศึกษา 5 และเสนอแนวทางในการจัดระบบสารสนเทศเพื่อการวางแผนในโรงเรียน ประชากรที่ศึกษามีจำนวน 352 คน ประกอบด้วยผู้บริหารโรงเรียน 150 คน ผู้จัดระบบสารสนเทศ 202 คน ผลการวิจัยพบว่า ในการจัดระบบสารสนเทศนั้น ผู้บริหารโรงเรียนมีความเห็นว่าข้อมูลที่จัดเก็บอยู่ในระดับมาก คือข้อมูลครูอาจารย์ ข้อมูลนักเรียน ข้อมูลการเรียนการสอน สารสนเทศมีความถูกต้องตรงกับความต้องการ ทันต่อเหตุการณ์และเพียงพอต่อการใช้ในระดับมาก มีการใช้เครื่องคอมพิวเตอร์ในการจัดระบบสารสนเทศน้อย สำหรับในเรื่องการตัดสินใจในการวางแผนและการบริหารงาน ผู้บริหารโรงเรียนใช้ข้อมูลและสารสนเทศมากกว่าการใช้ประสบการณ์และสามัญสำนึก

วราภรณ์ เทพสัมฤทธิ์พร (2536) ได้ทำการศึกษาเรื่องระบบสารสนเทศเพื่อการบริหารของมหาวิทยาลัยเกษตรศาสตร์ กลุ่มตัวอย่างที่ใช้วิจัยคือผู้ปฏิบัติงานและผู้บริหารของมหาวิทยาลัย จำนวน 152 คน ผลการวิจัยพบว่า การดำเนินงานของระบบสารสนเทศอยู่ในระดับที่เป็นการพัฒนา ปัญหาที่พบมากได้แก่การขาดแคลนบุคลากรความรู้ความสามารถเกี่ยวกับระบบสารสนเทศเพื่อการบริหาร ผู้บริหารเห็นว่าคุณสมบัติของมีความเชื่อถือได้ ซึ่งวัตถุประสงค์ส่วนใหญ่ของการใช้ข้อมูลเพื่อประกอบการตัดสินใจแนวทางการจัดระบบสารสนเทศควรกำหนดนโยบายการจัดระบบ การใช้ และการพัฒนาระบบสารสนเทศให้ชัดเจนและต่อเนื่อง ควรมีหน่วยงานกลางเพื่อทำหน้าที่รวบรวมข้อมูลเพื่อการบริหาร

วิจิตร อุ่นสากล (2537) ทำการวิจัยเรื่องการศึกษาระบบสารสนเทศในโรงเรียนมัธยมศึกษา สังกัดกรมสามัญศึกษา เขตการศึกษา 9 เพื่อการศึกษาการจัดปัญหาและความต้องการในการจัดระบบสารสน เทศในโรงเรียนมัธยมศึกษาขนาดใหญ่ สังกัดกรมสามัญศึกษา เขตการศึกษา 9 กลุ่มตัวอย่างที่ใช้ในการศึกษาประกอบด้วยผู้บริหารโรงเรียนจำนวน 170 คน ผู้จัดระบบสารสนเทศ จำนวน 201 คน ซึ่งพบว่า

1. ในการจัดระบบสารสนเทศมีคณะกรรมการจัดระบบสารสนเทศในโรงเรียนทำหน้าที่รับผิดชอบในการจัดระบบสารสนเทศ มีการจัดสรรงบประมาณ วัสดุ อุปกรณ์ ให้มีความเพียงพอ มีห้องปฏิบัติงานในการจัดระบบสารสนเทศ ผู้ทำหน้าที่จัดระบบสารสนเทศมีความรู้ความสามารถด้านคอมพิวเตอร์ ด้านสถิติ และมีคุณลักษณะในการจัดระบบสารสนเทศอยู่ในระดับมาก

2. ในการเก็บรวบรวมข้อมูลใช้แบบสำรวจของทางโรงเรียน โดยขอความร่วมมือจากผู้เกี่ยวข้องเก็บรวบรวมข้อมูลให้ใช้เครื่องคอมพิวเตอร์และเครื่องคิดเลขในการประมวลผลข้อมูลค่าสถิติที่ใช้คือ ค่าร้อยละและค่าเฉลี่ย เก็บรักษาข้อมูลและสารสนเทศด้วยเครื่องคอมพิวเตอร์ การนำเสนอข้อมูลและสารสนเทศมีลักษณะเป็นเอกสารในรูปของความเรียงแสดงตารางตัวเลข ค่าสถิติการให้บริการข้อมูลและสารสนเทศจะเป็นการให้ยืมเอกสาร ข้อมูลและสารสนเทศมีคุณสมบัติด้านความถูกต้อง ตรงตามความต้องการ ทันเหตุการณ์และมีความเพียงพอและเหมาะสมในระดับมาก

3. ผู้บริหารโรงเรียนนำข้อมูลและสารสนเทศไปใช้ในการปฏิบัติงานด้านต่าง ๆ ในระดับมาก

4. ปัญหาในการจัดระบบสารสนเทศ พบว่า ผู้บริหารโรงเรียนมีความเห็นเกี่ยวกับปัญหาในการจัดระบบสารสนเทศอยู่ในระดับน้อย ส่วนผู้จัดระบบสารสนเทศเห็นว่าเป็นปัญหาอยู่ในระดับมาก รายการที่เห็นว่าเป็นปัญหามาก คือ ความรับผิดชอบเกี่ยวกับภาระงานอื่นของผู้ปฏิบัติหน้าที่รับผิดชอบในการจัดระบบสารสนเทศ

5. ความต้องการในการจัดระบบสารสนเทศ พบว่าผู้บริหารโรงเรียนและผู้จัดระบบสารสนเทศมีความเห็นสอดคล้องกัน เกี่ยวกับความต้องการในการจัดระบบสารสนเทศอยู่ในระดับมาก ทุกรายการที่มีความต้องการมาก คือ ให้มีการจัดฝึกอบรมบุคลากรที่รับผิดชอบการจัดระบบสารสนเทศให้มีความรู้ความเข้าใจในหน้าที่

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยเรื่อง การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ผู้วิจัยได้ดำเนินการ โดยมีรายละเอียดดังนี้

3.1 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูล
2. เพื่อเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กร ในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

3.2 วิธีดำเนินการวิจัยเชิงคุณภาพ

3.2.1 เครื่องมือเก็บรวบรวมข้อมูล

ผู้วิจัยเก็บข้อมูลด้วยตนเองเป็นหลัก และอาศัยเครื่องมือที่ช่วยในการเก็บรวบรวมข้อมูลบางอย่าง ได้แก่ เว็บไซต์และเอกสารข้อมูลต่าง ๆ

3.2.2 การเก็บรวบรวมข้อมูล

1) การเข้าสู่สนามเพื่อเก็บรวบรวมข้อมูล

ผู้วิจัยได้ชี้แจงกับหน่วยงานเกี่ยวกับวัตถุประสงค์การวิจัย ขั้นตอน และวิธีการเก็บรวบรวมข้อมูล รวมทั้งได้ศึกษาเอกสารต่าง ๆ ที่เกี่ยวข้อง

2) วิธีการเก็บรวบรวมข้อมูลและการตรวจสอบข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการโดย 4 วิธีการคือ การศึกษาเอกสาร การสังเกต การสัมภาษณ์แบบไม่เป็นทางการ

การตรวจสอบเพื่อหาความน่าเชื่อถือได้ของข้อมูล และตรวจสอบความครบถ้วนและคุณภาพของข้อมูล โดยการตรวจสอบข้อมูลแบบสามเส้า(Triangulation) ตามวิธีการตรวจสอบเชิงคุณภาพ (สุภางค์ จันทวานิช, 2542: 34) ดำเนินการใน 2 วิธีการ คือ 1) ตรวจสอบแบบสามเส้าด้านข้อมูล(Data Triangulation) คือ การตรวจสอบข้อมูลจากแหล่งเวลา แหล่งสถานที่ และแหล่งบุคคลที่แตกต่าง 2) การตรวจสอบแบบสามเส้าด้านวิธีการรวบรวม

ข้อมูล(Methodological Triangulation) คือ การใช้วิธีการต่าง ๆ เก็บรวบรวมข้อมูลโดยการสังเกต การสัมภาษณ์

3) การวิเคราะห์ข้อมูล

ผู้วิจัยได้ดำเนินการตามขั้นตอนการวิเคราะห์โดยมีการตรวจสอบและตีความข้อมูลตลอดเวลาขณะที่ปฏิบัติการภาคสนาม มีการจัดทำบันทึกภาคสนามไว้อย่างละเอียดและเป็นระบบ พร้อมทั้งได้มีการทำดัชนี(Index) ตามกรอบแนวคิดการวิจัยที่ได้กำหนดไว้อย่างกว้างเพื่อตอบปัญหาการวิจัย สำหรับวิธีวิเคราะห์ข้อมูลที่ได้จากเอกสารผู้วิจัยใช้การวิเคราะห์เนื้อหา (Content Analysis) ข้อมูลที่ได้จากการสังเกต การสัมภาษณ์ และการสนทนากลุ่ม ใช้วิธีการจำแนกประเภทข้อมูล (Typological Analysis) และการเปรียบเทียบข้อมูล(Comparison)

3.2.3 **การสังเคราะห์ผลการศึกษา**

การสังเคราะห์ผลการศึกษาเป็นการนำข้อค้นพบจากการศึกษาทั้ง 2 ส่วนมาสังเคราะห์เพื่อให้ได้ข้อสรุปที่เป็นข้อความรู้ตามวัตถุประสงค์การวิจัย โดยนำข้อสรุปต่าง ๆ มาเชื่อมโยงจนเป็นโครงสร้างของข้อสรุปที่สามารถตอบคำถามการวิจัยได้ โดยกำหนดเกณฑ์การพิจารณาการยอมรับข้อค้นพบทั้ง 2 ส่วนให้เป็นผลการสังเคราะห์ ดังนี้

1. ข้อค้นพบจากการศึกษาทั้ง 2 ส่วน ที่ตรงกันหรือมีความเชื่อมโยงสามารถอธิบายในเชิงสาเหตุต่อกันได้

2. ข้อค้นพบจากการศึกษาเชิงปริมาณที่ระบุว่าเป็นปัจจัยในระดับมากแม้ข้อค้นพบเชิงคุณภาพไม่ได้ระบุไว้

3. ข้อค้นพบจากการศึกษาเชิงคุณภาพที่มีข้อมูลหลักฐานปรากฏชัดเจน แม้ข้อค้นพบเชิงปริมาณไม่ได้ระบุไว้

3.2.4 **การนำเสนอรายงานการวิจัย**การนำเสนอผลการวิจัย แบ่งเป็น 5 บท คือ

บทที่ 1 บทนำ

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง

บทที่ 3 วิธีดำเนินการวิจัย

บทที่ 4 ผลการวิเคราะห์ข้อมูล

บทที่ 5 สรุป อภิปรายผลและข้อเสนอแนะ

3.3 วิธีดำเนินการวิจัยเอกสาร (Documentary Research)

การวิเคราะห์ทางเอกสาร (Documentary Research) และการศึกษาเชิงคุณภาพ (Documentary Analysis) มุ่งศึกษา วิเคราะห์โดยเอกสารและข้อมูลในรูปแบบบันทึกต่าง ๆ ที่เป็นมาตรฐานเป็นหลัก มุ่งศึกษาวิเคราะห์เอกสาร งานวิจัย ข้อเขียน บทความและข้อมูลเอกสารจากหน่วยงาน องค์กรสวนราชการทั้งในและต่างประเทศ เพื่อทำความเข้าใจสภาพของการจัดการระบบความปลอดภัยของข้อมูลที่มีต่อองค์กร รวมทั้งผลกระทบที่มีผลต่อการปรับตัวของบุคลากรในคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยนำข้อมูลที่ได้จากแหล่งต่าง ๆ มาวิเคราะห์และสังเคราะห์ผ่านกรอบความรู้ในเชิงสหวิทยาการ (Interdisciplinary) เพื่อให้ได้รูปแบบ และแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรที่มีประสิทธิภาพตามมาตรฐานโลกซึ่งในที่นี้ใช้ระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS

1. **การศึกษาเพื่อกำหนดกรอบแนวคิดในการวิจัย** การวิจัยครั้งนี้ผู้วิจัยได้ประยุกต์ใช้แนวความคิดของระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS เพื่อเสนอแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ซึ่งสามารถสรุปตามหลัก PDCA Model ได้ดังนี้

1. Plan
   - การกำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง
   - การจัดตั้งทีมงานและกำหนดหน้าที่ความรับผิดชอบ
2. Do
   - การกำหนดนโยบายความมั่นคงปลอดภัยขององค์กร
   -การบริหารจัดการความเสี่ยง ซึ่งประกอบด้วยการประเมินความเสี่ยง การวิเคราะห์และแก้ไขความเสี่ยง
   - การเลือกใช้มาตรการความมั่นคงปลอดภัยและควบคุมตามมาตรฐาน
   - การฝึกอบรมบุคลากรเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุกๆ ระดับ
3. Check
   - การตรวจประเมินภายในของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ

- การทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร

4. Act

- การดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยของสารสนเทศตามสิ่งที่ได้ตรวจพบ
- การดำเนินการวิเคราะห์หาสาเหตุของปัญหาที่แท้จริง
- การดำเนินการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก

บทที่ 4
ผลการวิเคราะห์ข้อมูล

การวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดของข้อมูล และเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กร โดย ประยุกต์ใช้แนวความคิดของระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS เพื่อเสนอแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร โดยสรุปตามหลัก PDCA Model ได้ดังนี้

1. **ศึกษาระบบสารสนเทศในการกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) ของคณะครุศาสตร์อุตสาหกรรม โดยศึกษาจาก**

- ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาถึงลักษณะของเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย
- ศึกษานโยบายในการรักษาความมั่นคงปลอดภัย โดยพิจารณาถึงโครงสร้างการบริหารงาน
- กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร
- ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยของคณะครุศาสตร์อุตสาหกรรม
- กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้

2. **ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัย องค์กรควรปฏิบัติ ดังนี้ (Do) โดยกำหนดแนวทางการจัดการ เทคโนโลยีความมั่นคงปลอดภัยของข้อมูล ของคณะครุศาสตร์อุตสาหกรรม**

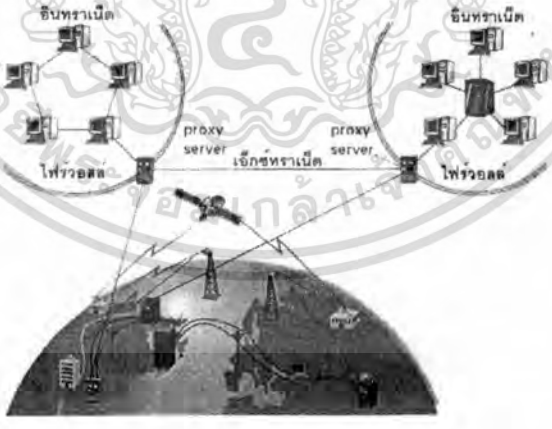
1. การจัดสรรทรัพยากรของคณะครุศาสตร์อุตสาหกรรม

1.1 Hardware

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีสมรรถนะ ความสามารถสูง เพื่อใช้บริการในแต่ละหน่วยงาน ในคณะครุศาสตร์อุตสาหกรรม
- เครื่องสำรองไฟ เพื่อให้ระบบสามารถใช้ไฟฟ้าได้อย่างต่อเนื่อง วางแผนสำหรับการกู้ระบบคืน เมื่อมีเหตุการณ์เลวร้ายเกิดขึ้น

1.2 software

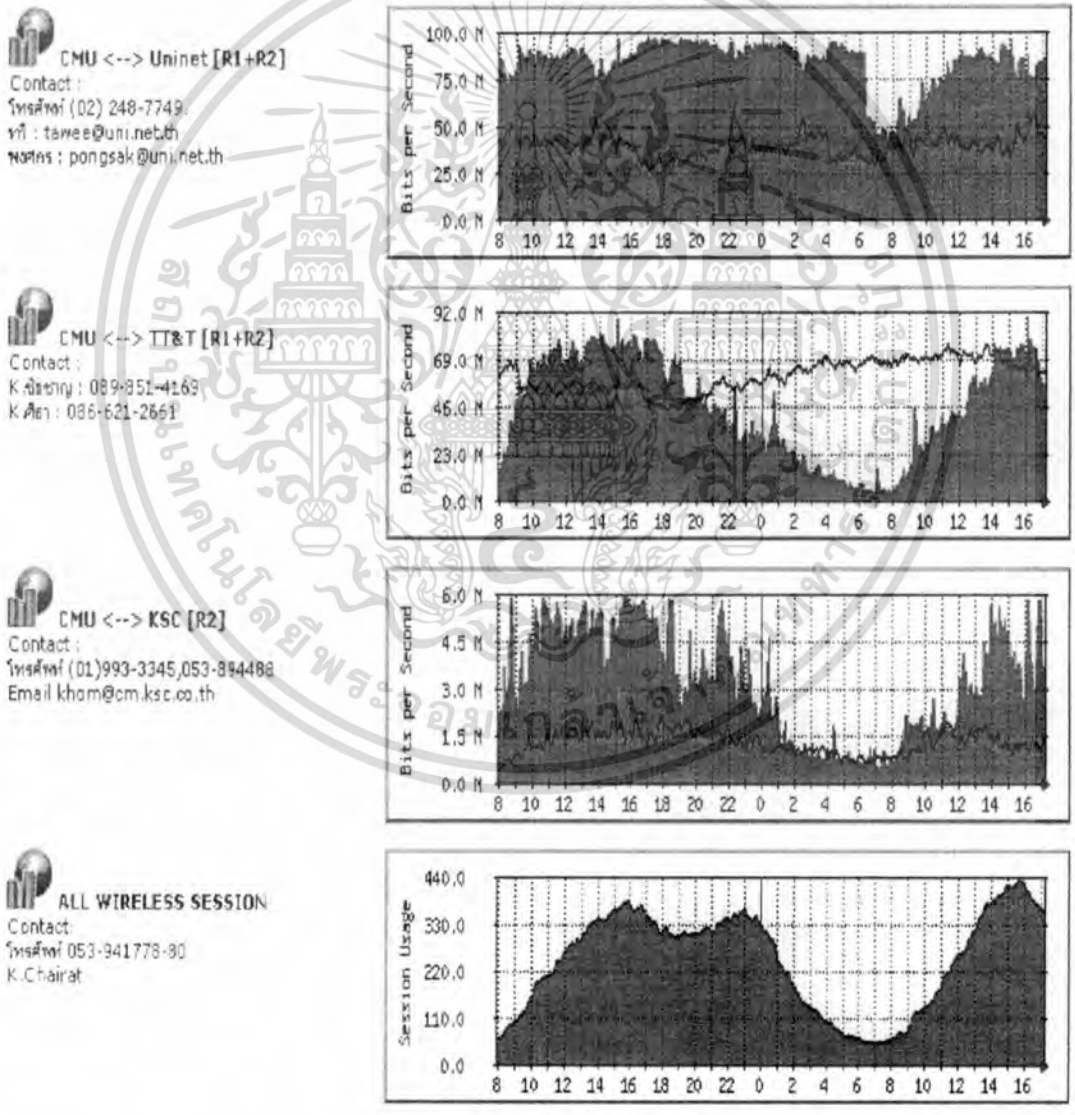
- การป้องกันระบบเครือข่าย โดยใช้ Firewall ซึ่งเป็นเทคโนโลยีที่ทำการป้องกันผู้บุกรุกเข้า-ออกระบบ และกำหนดโซนการให้บริการ การเข้าถึงข้อมูล ที่เหมาะสม กำหนดขอบเขต และโซนการทำงานที่เหมาะสม กำหนดบริการ และการเข้าถึงระบบสำหรับผู้ที่ได้รับอนุญาตเท่านั้น



-ใช้ระบบปฏิบัติการทีมความเสถียรและมีประสิทธิภาพสูง นอกจากจะฟรีแล้ว Debian ยังมีระบบการลงซอฟต์แวร์ที่เรียกว่า apt-get ของ Debian นั้น ได้รับการยอมรับ เพราะอาสาสมัครผู้ดูแลแพ็คเกจ apt ของ Debian นั้น มีจำนวนเป็นหลักพัน และช่วยกันหาโปรแกรมเวอร์ชั่นใหม่ๆ มาเพิ่มให้ Debian ตลอดเวลา นอกจากนี้ชุมชนนักพัฒนา Debian ได้รับการยอมรับว่า เป็นชุมชนโอเพ่นซอร์สที่แข็งแกร่งมากแห่งหนึ่ง ปัญหาที่พบใน Debian จะถูกแก้ไขไปอย่างรวดเร็ว

- ติดตั้งเว็บเซอร์เวอร์ (Web server) บริการเว็บไซต์แต่ละหน่วยงาน โดยใช้ Apache webserver, Squid proxy, PHP and MySQL เพื่อบริการฐานข้อมูล

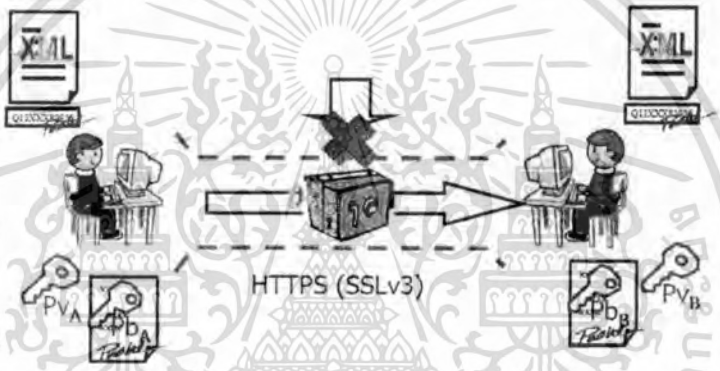
- ติดตั้ง ซอฟท์แวร์ที่ใช้ในการตรวจสอบเครือข่ายสามารถตรวจสอบการใช้งาน Network Traffic โดยแยก Port เป็นอิสระต่อกันได้ทันที



- การติดตั้ง Anti Spam โดยใช้โปรแกรม SpamAssassin เพื่อเป็นกรองเมล์ขยะ หรือเมล์ที่ไม่พึงประสงค์

- การติดตั้งระบบ Anti-Virus เพื่อทำการป้องกัน และกำจัดไวรัสที่มีการอัพเดตข้อมูลอย่างสม่ำเสมอ

- การติดตั้งระบบ SSL เนื่องจากมีประสิทธิภาพในการรักษาความปลอดภัยขั้นสูง หน้าที่ของ SSL คือ สลับที่ข้อมูลและแปลงเป็นรหัสตัวเลขทั้งหมด ยิ่งความละเอียดในการเข้ารหัสมีมากเท่าไร ความปลอดภัยก็ยิ่งสูงขึ้นเท่านั้น ระดับความละเอียดของการเข้ารหัสมีหน่วยเป็น บิท โดยเว็บไซท์แต่ละหน่วยงาน ได้ใช้การเข้ารหัสระดับ 128 บิท



1.3 ทรัพยากรบุคคล

- ผู้บริหาร ทำหน้าที่บริหารนโยบายหน่วยงาน สรุปผลดำเนินการของหน่วย ดูผลสรุปในด้านต่างๆ

- ผู้ดูแลระบบ (Administrator) มีอำนาจสูงสุดของระบบในการควบคุม เข้าถึงทรัพยากร / ข้อมูลทั้งหมดของระบบ แต่ละหน่วยงานควรมีอย่างน้อย 1 คน

- ผู้ใช้งาน จะต้องมีความรู้ ความสามารถในการใช้งานได้อย่างถูกต้อง

2. การบริหารจัดการด้านความปลอดภัย

2.1 การจู่โจมโดยการหลอกลวง

☐ ใช้จุดอ่อนของคน เพื่อหลอกให้ทำให้

หลอกว่าเป็นเจ้าหน้าที่เพื่อขอข้อมูล

ขอให้เปิดประตูให้

ส่งอีเมล์หลอกให้ทำบางอย่างให้

☐ แอบดูรหัสผ่าน ที่วางอยู่บนโต๊ะทำงาน

ตัวอย่างวิธีการ

☐ Dumpster Diving แอบหาข้อมูลจากเศษกระดาษหรือขยะ

☐ Shoulder surfing แอบมองหน้าจอ

☐ Phishing ส่งอีเมล์จากสถาบันการเงิน แล้วถามข้อมูลส่วนบุคคล

☐ Piggybacking แอบเดินตามหลังพนักงานเพื่อผ่านเข้าประตู

วิธีการป้องกัน

☐ การฝึกอบรมเจ้าหน้าที่ให้ระมัดระวัง

☐ สอบถามข้อมูลมากขึ้นเพื่อตรวจสอบ

☐ เตรียมข้อมูลไว้เพื่อสอบถาม

☐ สอบถามเหตุผล

☐ จัดวางเอกสารให้ปลอดภัย

☐ จัดวางสื่อเก็บข้อมูลให้ปลอดภัย

ความปลอดภัยทางกายภาพ

☐ การล็อคประตู

☐ เจ้าหน้าที่รักษาความปลอดภัย (สุนัข)

☐ อุปกรณ์ดับเพลิง

☐ การติดตั้งทีวีวงจรปิด

☐ การติดตั้งรั้วกั้นพื้นที่

☐ การติดตั้งอุปกรณ์ป้องกันการเข้าประตู

☐ การติดตั้งอุปกรณ์ส่องสว่างอย่างเพียงพอ

2.2 การกำหนดสิทธิในการใช้งาน

- เตือนให้ผู้ใช้ปกป้องรหัสผ่าน เปลี่ยนรหัสผ่านให้บ่อย ๆ และยากต่อการเดา ทำการ Log off ออกจากระบบงานเมื่อเลิกใช้

การตั้งรหัสผ่านที่ดี (Good Passwords)

เป็นเรื่องสำคัญที่องค์กรควรจะต้องมีนโยบาย ในการส่งเสริมให้พนักงานของตนตั้งรหัสผ่าน (Password) ที่ยากแก่การแกะรหัส ข้อแนะนำในการตั้งรหัสผ่านที่ดี เช่น

- มีความยาวอย่างน้อย 6 ตัวอักษร
- มีการเปลี่ยนแปลงตัวอักษรในบางแห่ง ซึ่งไม่ควรเป็นตัวแรก เช่นจะใช้คำว่า Superman อาจเปลี่ยนเป็น Supemman เป็นต้น

- ควรมีตัวเลข (0-9) อย่างน้อย 1 ตัว และไม่ควรเป็นตัวสุดท้าย
- ถ้าเป็นไปได้ ควรใส่อักขระพิเศษที่ไม่ใช่ ตัวอักษรและตัวเลข ทั่วไป เช่น #, @ เป็นต้น

- Log on ด้วยAccount Admin. ใช้เฉพาะเมื่อจำเป็น และไม่ Log on ด้วยAccount Admin. จาก Work Station ในสภาวะแวดล้อมที่ไม่คุ้นเคย

- แสดงข่าวสารให้ผู้ใช้ทราบว่า Log on เวลาครั้งล่าสุด

2.3 ระเบียบปฏิบัติเกี่ยวกับ Account ของผู้ใช้และกลุ่มผู้ใช้

- ผู้ใช้ที่อยู่ในกลุ่ม Admin. จำเป็นต้องมี 2 Accounts (1 Account = มีสิทธิพิเศษในการจัดการระบบ, 1 Account = มีสิทธิจำกัดเพื่อใช้ในกิจกรรมปกติ)

- เปลี่ยนชื่อAccount Admin. ให้ยากต่อการเดา

- ทางเลือกเสริม Implement การLog on ด้วย Account Admin ในลักษณะ False – Safe (มีบุคคลมากกว่า 1คน จำรหัสผ่านแต่ละช่วงของรหัสผ่านทั้งหมด เมื่อต้อง Log on ด้วย Account Admin. ก็ให้ทุกคนดังกล่าวมาระบุรหัสผ่านในส่วนที่ตนจำ แล้วนำมาประกอบกัน ให้รหัสผ่านนั้นสมบูรณ์)

- กำหนดจำนวนสูงสุดที่อนุญาตให้ผู้ใช้ระบุรหัสผิดได้ (เกินนี้ให้ Log out)

- Disable หรือลบ Account พนักงานที่ลาออก

- กำหนดสิทธิให้ผู้ใช้แต่ละคนให้น้อยที่สุดไว้ก่อน

- Disable Account Guest หากต้องการใช้ต้องทบทวนอย่างระมัดระวัง

- ไม่ควรมี Account ที่ไม่จำเป็นในระบบ

- Set up บทบาทที่ชัดเจนในการดูแลระบบของกลุ่มแต่ละหน่วยงาน

2.4 **การกำหนดสิทธิในการเข้าถึงข้อมูล**

- กำหนดขอบเขตของกลุ่มบุคคลต่อแหล่งข้อมูลที่เหมาะสมกับบทบาทและหน้าที่ ก็ต้องมา กำหนดหน้าที่เฉพาะหรือสิทธิพิเศษในการกระทำต่อข้อมูลนั้น ๆ ยกตัวอย่างเช่น user ที่ login เข้ามา อาจได้รับสิทธิ์ในการเข้าถึงได้เพียงเฉพาะที่เกี่ยวข้อง และสามารถทำได้เพียงแค่การอ่านข้อมูล แต่ไม่มีสิทธิ์แก้ไข ในขณะที่ admin มีสิทธิ์ที่จะเข้าถึงได้ทุกไฟล์ และกระทำกับข้อมูลได้ทุกอย่าง

- การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ ไม่รู้วิธีการและคีย์ในการเข้าและถอดรหัส

- การควบคุมการเข้าถึง (Access Control) เพื่อพิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบ เป็นการปกป้องความลับของข้อมูลที่จัดเก็บไว้ในระบบ

2.5 **การเข้าถึงข้อมูลแต่ละหน่วยงาน**

1. งานบริหารงานและธุรการ

- โปรแกรมธุรการสารบรรณอิเล็กทรอนิกส์ (e-office) เพื่อลดการใช้กระดาษลง ใช้สำหรับวางแผนงานและระบบปฏิบัติการเพื่อการติดตามประเมินผล รับ-เข้าหนังสือภายใน ภายนอก หนังสือราชการ ประวัติการฝึกอบรม

- งานอาคาร สถานที่และยานพาหนะ

2. งานการเจ้าหน้าที่

- งานการเจ้าหน้าที่

3. งานพัสดุ

- งานพัสดุ ระบบฐานข้อมูลการจัดเก็บอุปกรณ์ หรือรายการพัสดุที่มีอยู่แต่ละหน่วยงาน

4. งานการเงินและบัญชี

- งานการเงินและบัญชี ผู้ใช้ควรมีความแม่นยำในการใช้งาน ควรมีการสำรองข้อมูลทุกวัน เนื่องจากเป็นข้อมูลที่สำคัญ ในกรณีที่มีปัญหา สามารถกู้คืนข้อมูลได้ทันที

5. งานนโยบายและแผน

- งานนโยบายและแผน

6. งานบริการการศึกษา

- หน่วยประสานงานทะเบียน เป็นการเก็บข้อมูลระบบสารสนเทศสำหรับผู้บริหารระบบสารสนเทศสำหรับนักศึกษาปริญญาโท-เอก ระบบสารสนเทศสำหรับนักศึกษาปริญญาตรี และระบบสารสนเทศสำหรับบุคคลทั่วไป

- หน่วยโสตทัศนูปกรณ์ การยืม-คืนอุปกรณ์ต่าง ๆ

- หน่วยห้องสมุดและสารสนเทศ สืบค้นหนังสือในห้องสมุด ตรวจสอบการยืมคืน การยืมต่อด้วยตัวเอง

- หน่วยกิจการนักศึกษา ศูนย์สารสนเทศนักศึกษา กิจกรรมชุมนุมต่างๆ ในแต่ละหน่วยงาน

7. งานบริการทางวิชาการและวิจัย

- หน่วยสารสนเทศ
- หน่วยตำราและเอกสารการพิมพ์
- หน่วยประกันคุณภาพ
- หน่วยประชาสัมพันธ์

แต่ละหน่วยงาน จะมีการใช้งานที่แตกต่างกัน ขึ้นอยู่กับลักษณะงานนั้น แต่ละหน่วยงานสามารถแก้ไขข้อมูลของตนเองเท่านั้น ไม่สามารถแก้ไขหน่วยงานอื่นได้

2.6 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- การควบคุมช่องทางหรือพอร์ทที่ใช้ในการเข้าระบบเพื่อการตรวจวินิจฉัยและการปรับแต่งระบบควรได้รับการควบคุมโดยมีการใช้คีย์ล็อคและกระบวนการที่ดีสนับสนุนการควบคุม
- การสร้างความเชื่อมั่นได้ว่า ช่องทางหรือพอร์ทที่ใช้ในการตรวจวินิจฉัยและปรับแต่งนั้นสามารถเข้าถึงได้เฉพาะกรณีที่อยู่ภายใต้การควบคุมดูแลจากผู้จัดการ กับเจ้าหน้าที่สนับสนุนเท่านั้น
- พอร์ท เซอร์วิสที่ติดตั้งอยู่ในคอมพิวเตอร์หรือเครือข่ายซึ่งไม่มีความจำเป็นต้องใช้เพื่อภารกิจควรปิดหรือกำจัดออก

2.7 การเข้าถึงระบบอย่างมั่นคงปลอดภัย

- ไม่แสดงเลขที่ระบบหรือเลขที่โปรแกรมจนกว่ากระบวนการล็อกอินจะเสร็จสิ้นสมบูรณ์
- แสดงข้อความเตือนว่าคอมพิวเตอร์ควรถูกใช้งานโดยผู้ใช้ที่ได้รับอนุญาตเท่านั้น
- ไม่ควรแสดง help ระหว่างการกระบวนการล็อกอินซึ่งอาจเป็นการช่วยให้ผู้ที่ไม่ได้รับอนุญาตค้นหาช่องทางเข้าได้
- ตรวจสอบความถูกต้องของข้อมูลที่อินพุทเฉพาะเมื่อการอินพุทเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาดระบบไม่ควรแสดงว่าข้อมูลที่อินพุทส่วนไหนไม่ถูกต้อง
- จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้เกิน 3 ครั้ง เป็นต้น และควรพิจารณาเพิ่มเติมประเด็นต่อไปนี้

> บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ

> หลังจากใส่ข้อมูลล๊อกอินผิดพลาดบังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้พยายามครั้งต่อไป

> ตัดการเชื่อมโยงเครือข่าย

> ส่งข้อความเตือนไปยังหน้าจอของระบบถ้าความพยายามในการล๊อกอินหลายครั้งเกิดจำนวนครั้งมากที่สุดที่ยอมรับได้

> กำหนดรหัสผ่านให้เหมาะสมกับความยาวของรหัสผ่านและมูลค่าของระบบที่จะต้องได้รับการป้องกัน

- จำกัดจำนวนครั้งสูงสุดและจำนวนครั้งที่ต่ำสุดสำหรับกระบวนการล๊อกอินถ้าเกินกว่านั้นระบบควรหยุดการให้ล๊อกอิน

- แสดงข้อมูลต่อไปนี้หลังจากที่ล๊อกอินสำเร็จแล้ว

> วันที่และเวลาของการเข้าล๊อกอินครั้งที่แล้ว

> รายละเอียดของการพยายามล๊อกอินที่ไม่สำเร็จ ตั้งแต่การล๊อกอินครั้งที่แล้ว

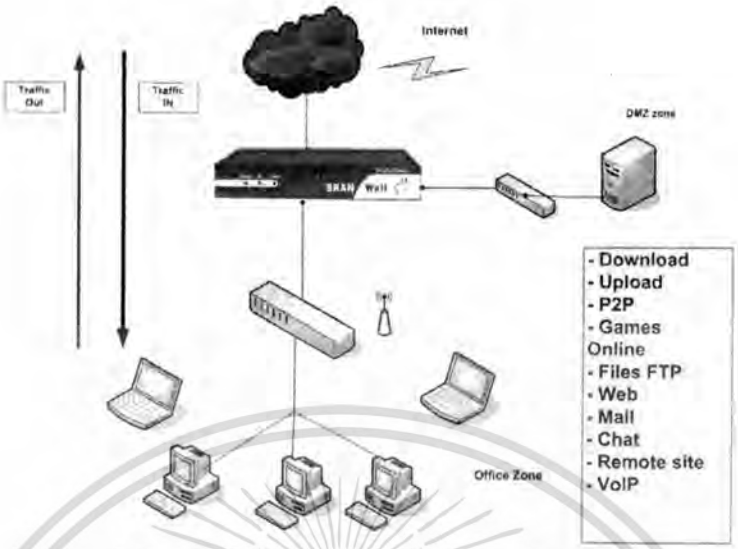
- ไม่แสดงรหัสผ่านที่ได้อินพุทหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

- ไม่ส่งรหัสผ่านผ่านเครือข่ายโดยไม่เข้ารหัสเพื่อรักษาความลับก่อน

2.8 การตรวจสอบความปลอดภัยของระบบ

- Monitoring ตรวจจับการบุกรุก พฤติกรรม Hacker และการเข้าถึงทรัพยากรโดยไม่ได้รับอนุญาตสามารถทำได้โดยการตรวจสอบจากล็อกไฟล์ที่สร้างขึ้นจากโปรแกรม syslog daemon ที่ถูกติดตั้งใน linux ซึ่งจะทำการเก็บล็อกไฟล์ไว้ ภายในล็อกไฟล์ดังกล่าวจะเก็บข้อมูลสถานะการทำงานของเครื่องตั้งแต่เริ่มบูตเครื่อง

- Reporting การรายงานผลความปลอดภัยต่าง ๆ ที่มีในแต่ละวัน เพื่อเป็นการวิเคราะห์ข้อผิดพลาดของระบบงานในแต่ละหน่วยงานที่รับผิดชอบ



2.9 **นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย**

- ข้อมูลที่สำคัญมาก เช่น ข้อมูลในกระดาษ ข้อมูลในสื่อหน่วยความจำสำรอง ควรได้รับการปกป้อง (เช่นในตู้เซฟ หรือในชั้นหรือในตู้และอื่น ๆ) เมื่อไม่จำเป็นต้องใช้และเมื่อมีการยกเลิกหรือพ้นจากตำแหน่ง

- เมื่อไม่มีการใช้งาน คอมพิวเตอร์ควรได้รับการล๊อกเอ้า หรือได้รับการป้องกันจากการใช้หน้าจอและคีย์บอร์ด หรือการป้องกันโดยใช้รหัสผ่าน อุปกรณ์โทเค่น หรือการตรวจสอบและยืนยันตัวตนแบบอื่น

- จุดรับเข้าและส่งออกจดหมาย และเครื่องโทรสารที่ไม่ได้ใช้งานควรได้รับการป้องกัน

- เครื่องถ่ายเอกสารและอุปกรณ์ผลิตซ้ำแบบอื่น (เช่น เครื่องสแกนเนอร์ กล้องดิจิตอล) ควรได้รับการปกป้องจากการใช้งานที่ไม่ได้รับอนุญาต

- เอกสารที่มีข้อมูลสำคัญควรนำออกจากเครื่องพิมพ์ทันที

2.10 Session time-out (**การหมดเวลาการใช้งานระบบสารสนเทศ**)

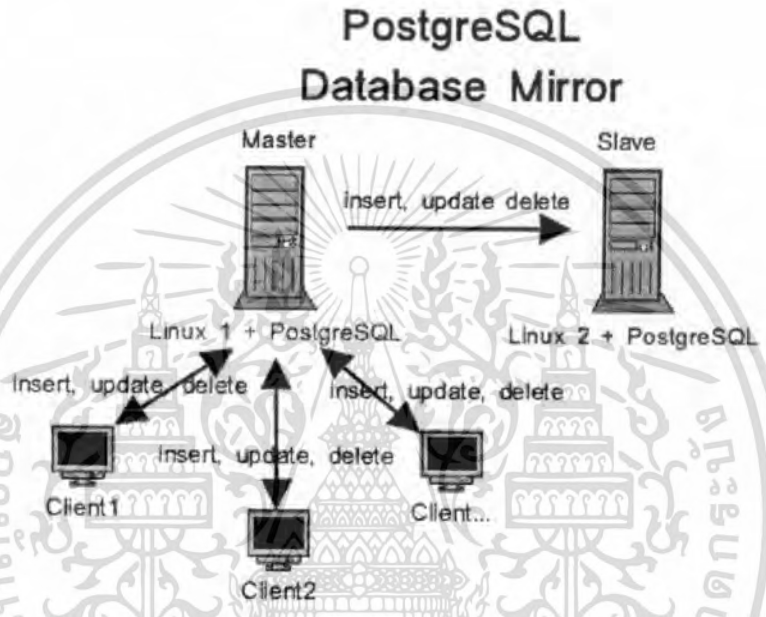
- ควรมีกลไกในการเคลียเซสชั่นเมื่อไม่ได้มีการใช้งานมาเป็นระยะเวลาที่กำหนด (time-out)

- time-out ควรกำหนดให้เหมาะสมกับความเสี่ยงนั้น ประเภทข้อมูลที่เกี่ยวข้อง และระบบซอฟต์แวร์นั้น

- อาจใช้รูปแบบเพียงเคลียและล๊อกหน้าจอโดยไม่ต้องยกเลิกเซสชั่นก็ได้

3. การบำรุงรักษา

3.1 การสำรองข้อมูลแบบ Mirror เป็นการสำรองข้อมูลจากฮาร์ดิสก์ไปสู่อีกฮาร์ดิสก์หนึ่งโดยอัตโนมัติ
เช่น การสำรองข้อมูลจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง



3.2 การสำรองข้อมูลด้วย rsync เป็นถูกออกแบบมาให้ทำงานได้บนระบบปฏิบัติการ Unix เป็นหลัก ด้วยวิธีการสำรองข้อมูลในรูปแบบของการทำ Synchronizes files และ directory โดยทำการ sync ข้อมูลจากที่หนึ่ง ไปยังอีกที่หนึ่ง โดยในระหว่างการโอนถ่ายข้อมูลนั้น สามารถที่จะทำการย่อขนาดของข้อมูล

- กำหนดการสำรองข้อมูลทุกวัน ระบบฐานข้อมูลเป็นประจำทุกวัน และทำการ Roll Back ย้อนหลังได้ 30 วัน เช่น ข้อมูลทะเบียนประวัติ

- กำหนดการสำรองข้อมูลทุกสัปดาห์ ระบบ Backup เว็บไซต์เป็นประจำทุกสัปดาห์ และทำการ Roll Back ย้อนหลังได้ 3 สัปดาห์ เช่น ข้อมูลเว็บไซต์แต่ละหน่วยงาน

```
#!/bin/sh

export PATH=/usr/local/bin:/usr/bin:/bin

LIST="rootfs usr data data2"

for d in $LIST; do
        mount /backup/$d
        rsync -ax --exclude fstab --delete /$d/ /backup/$d/
        umount /backup/$d
done

DAY=`date "+%A"`

rsync -a --delete /usr/local/apache /data2/backups/$DAY
rsync -a --delete /data/solid /data2/backups/$DAY
```

3.3 การกู้คืนข้อมูล (Restore) เป็นการนำข้อมูลที่สำรองเอาไว้ มาแทนที่ข้อมูลที่เสียหายไป ทำให้ข้อมูลในระบบงานสามารถทำงานได้ตามปกติ ซึ่งอาจจะเป็นข้อมูลส่วนใดส่วนหนึ่งหรือข้อมูลทั้งหมดก็ได้

3.4 การสร้างความตะหนักในการใช้ข้อมูลสารสนเทศในองค์กร (Information Security Awareness Training) การให้ความรู้ ระเบียบข้อปฏิบัติในการใช้สารสนเทศที่ถูกต้อง และมีประสิทธิภาพ มีความปลอดภัยในการใช้งาน

- อบรมระดับผู้บริหาร
- อบรมระดับกลุ่มผู้ใช้งานทั่วไป
- อบรมสำหรับกลุ่มผู้ดูแลระบบเครือข่าย

3. เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยของคณะครุศาสตร์อุตสาหกรรมควรปฏิบัติดังนี้ (Check)

1. ลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวน เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสามารถ
   - ตรวจจับข้อผิดพลาดจากการประมวลผล

- ระบุการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องกับความ มั่นคงปลอดภัย

- ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคง ปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่ คาดหมายไว้ หรือไม่

2. ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคง ปลอดภัยสม่ำเสมอ โดยนำสิ่งต่าง ๆ ต่อไปนี้มาพิจารณาร่วมด้วย ได้แก่ ผล การตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือ หน่วยงานที่เกี่ยวข้อง เป็นต้น

3.วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

4. **บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยของคณะครุศาสตร์อุตสาหกรรมควรปฏิบัติดังนี้** (Act)

1. ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้

2. ใช้มาตรการเชิงแก้ไขและป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่น ๆ มาช่วยในการปรับปรุงให้ดีขึ้น

3. แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ผู้วิจัยได้ดำเนินการ โดยมีรายละเอียดดังนี้

5.1 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูล
2. เพื่อเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

5.2 วิธีดำเนินการวิจัยเชิงคุณภาพ

5.2.1 เครื่องมือเก็บรวบรวมข้อมูล

ผู้วิจัยเก็บข้อมูลด้วยตนเองเป็นหลัก และอาศัยเครื่องมือที่ช่วยในการเก็บรวบรวมข้อมูลบางอย่าง ได้แก่ ข้อมูลจากเว็บไซต์และเอกสารต่าง ๆ ที่เกี่ยวข้อง

5.2.2 การเก็บรวบรวมข้อมูล

1) การเข้าสู่สนามเพื่อเก็บรวบรวมข้อมูล

ผู้วิจัยได้ชี้แจงกับหน่วยงานเกี่ยวกับวัตถุประสงค์การวิจัย ขั้นตอน และวิธีการเก็บรวบรวมข้อมูล รวมทั้งได้ศึกษาเอกสารต่าง ๆ ที่เกี่ยวข้อง

2) วิธีการเก็บรวบรวมข้อมูลและการตรวจสอบข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการโดย 4 วิธีการคือ การศึกษาเอกสาร การสังเกต การสัมภาษณ์แบบไม่เป็นทางการ

การตรวจสอบเพื่อหาความน่าเชื่อถือได้ของข้อมูล และตรวจสอบความครบถ้วนและคุณภาพของข้อมูล โดยการตรวจสอบข้อมูลแบบสามเส้า(Triangulation) ตามวิธีการตรวจสอบเชิงคุณภาพ (สุภางค์ จันทวานิช, 2542: 34) ดำเนินการใน 2 วิธีการ คือ 1) ตรวจสอบแบบสามเส้าด้านข้อมูล(Data Triangulation) คือ การตรวจสอบข้อมูลจากแหล่งเวลา แหล่งสถานที่ และแหล่งบุคคลที่แตกต่าง 2) การตรวจสอบแบบสามเส้าด้านวิธีการรวบรวมข้อมูล(Methodological Triangulation) คือ การใช้วิธีการต่าง ๆ เก็บรวบรวมข้อมูลโดยการสังเกต การสัมภาษณ์ 3) การวิเคราะห์ข้อมูล

ผู้วิจัยได้ดำเนินการตามขั้นตอนการวิเคราะห์โดยมีการตรวจสอบและตีความข้อมูลตลอดเวลาขณะที่ปฏิบัติการภาคสนาม มีการจัดทำบันทึกภาคสนามไว้อย่างละเอียดและเป็นระบบ พร้อมทั้งได้มีการทำดัชนี(Index) ตามกรอบแนวคิดการวิจัยที่ได้กำหนดไว้อย่างกว้างเพื่อตอบปัญหาการวิจัย สำหรับวิธีวิเคราะห์ข้อมูลที่ได้จากเอกสารผู้วิจัยใช้การวิเคราะห์เนื้อหา(Content Analysis) ข้อมูลที่ได้จากการสังเกต การสัมภาษณ์ และการสนทนากลุ่ม ใช้วิธีการจำแนกประเภทข้อมูล (Typological Analysis) และการเปรียบเทียบข้อมูล (Comparison)

5.2.3 **การสังเคราะห์ผลการศึกษา**

การสังเคราะห์ผลการศึกษาเป็นการนำข้อค้นพบจากการศึกษาทั้ง 2 ส่วนมาสังเคราะห์เพื่อให้ได้ข้อสรุปที่เป็นข้อความรู้ตามวัตถุประสงค์การวิจัย โดยนำข้อสรุปต่าง ๆ มาเชื่อมโยงจนเป็นโครงสร้างของข้อสรุปที่สามารถตอบคำถามการวิจัยได้ โดยกำหนดเกณฑ์การพิจารณาการยอมรับข้อค้นพบทั้ง 2 ส่วนให้เป็นผลการสังเคราะห์ ดังนี้

1. ข้อค้นพบจากการศึกษาทั้ง 2 ส่วน ที่ตรงกันหรือมีความเชื่อมโยงสามารถอธิบายในเชิงสาเหตุต่อกันได้

2. ข้อค้นพบจากการศึกษาเชิงปริมาณที่ระบุว่าเป็นปัจจัยในระดับมากแม้ข้อค้นพบเชิงคุณภาพไม่ได้ระบุไว้

3. ข้อค้นพบจากการศึกษาเชิงคุณภาพที่มีข้อมูลหลักฐานปรากฏชัดเจน แม้ข้อค้นพบเชิงปริมาณไม่ได้ระบุไว้

5.2.4 **การนำเสนอรายงานการวิจัย**การนำเสนอผลการวิจัย แบ่งเป็น 5 บท คือ

บทที่ 1 บทนำ

บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง

บทที่ 3 วิธีดำเนินการวิจัย

บทที่ 4 ผลการวิเคราะห์ข้อมูล

บทที่ 5 สรุป อภิปรายผลและข้อเสนอแนะ

5.3 วิธีดำเนินการวิจัยเอกสาร

การวิเคราะห์ทางเอกสาร (Documentary Research) และการศึกษาเชิงคุณภาพ (Documentary Analysis) มุ่งศึกษา วิเคราะห์โดยเอกสารและข้อมูลในรูปแบบบันทึกต่าง ๆ ที่เป็นมาตรฐานเป็นหลัก มุ่งศึกษาวิเคราะห์เอกสาร งานวิจัย ข้อเขียน บทความและข้อมูลเอกสารจากหน่วยงาน องค์กรส่วนราชการทั้งในและต่างประเทศ เพื่อทำความเข้าใจสภาพของการจัดการระบบความปลอดภัยของข้อมูลที่มีต่อองค์กร รวมทั้งผลกระทบที่มีผลต่อการปรับตัวของบุคลากร

ในคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยนำข้อมูลที่ได้จากแหล่งต่าง ๆ มาวิเคราะห์และสังเคราะห์ผ่านกรอบความรู้ในเชิงสหวิทยาการ (Interdisciplinary) เพื่อให้ได้รูปแบบ และแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรที่มีประสิทธิภาพตามมาตรฐานโลกซึ่งในที่นี้ใช้ระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS

1. การศึกษาเพื่อกำหนดกรอบแนวคิดในการวิจัย การวิจัยครั้งนี้ผู้วิจัยได้ประยุกต์ใช้แนวความคิดของระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS เพื่อเสนอแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ซึ่งสามารถสรุปตามหลัก PDCA Model ได้ดังนี้

1. Plan
   - การกำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง
   - การจัดตั้งทีมงานและกำหนดหน้าที่ความรับผิดชอบ
2. Do
   - การกำหนดนโยบายความมั่นคงปลอดภัยขององค์กร
   -การบริหารจัดการความเสี่ยง ซึ่งประกอบด้วยการประเมินความเสี่ยง การวิเคราะห์และแก้ไขความเสี่ยง
   - การเลือกใช้มาตรการความมั่นคงปลอดภัยและควบคุมตามมาตรฐาน
   - การฝึกอบรมบุคลากรเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุกๆ ระดับ
3. Check
   - การตรวจประเมินภายในของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ
   - การทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร
4. Act
   - การดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยของสารสนเทศตามสิ่งที่ได้ตรวจพบ
   - การดำเนินการวิเคราะห์หาสาเหตุของปัญหาที่แท้จริง
   - การดำเนินการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก

5.4 สรุปผลการวิจัย

การวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดของข้อมูล และเสนอแนวทางการจัดการระบบความความมั่นคงปลอดภัยของข้อมูลต่อองค์กร โดย ประยุกต์ใช้แนวความคิดของระบบ ISO 27001 : 2005 Information Security Management System หรือ ISMS เพื่อเสนอแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร โดยสรุปตามหลัก PDCA Model ได้ดังนี้

1. **ศึกษาระบบสารสนเทศในการกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) ของคณะครุศาสตร์อุตสาหกรรม โดยศึกษาจาก**

- ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาถึงลักษณะของเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล

- ศึกษานโยบายในการรักษาความมั่นคงปลอดภัย โดยพิจารณาถึงโครงสร้างการบริหารงาน

- กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร

- ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยของข้อมูลของคณะครุศาสตร์อุตสาหกรรม

- กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้

2. **ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติ ดังนี้ (Do) โดยกำหนดแนวทางการจัดการ เทคโนโลยีความมั่นคงปลอดภัยของข้อมูล ของคณะครุศาสตร์อุตสาหกรรม**

1. การจัดสรรทรัพยากรของคณะครุศาสตร์อุตสาหกรรม

1.1 Hardware

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีสมรรถนะ ความสามารถสูง เพื่อใช้บริการในแต่ละหน่วยงาน ในคณะครุศาสตร์อุตสาหกรรม

- เครื่องสำรองไฟ เพื่อให้ระบบสามารถใช้ไฟฟ้าได้อย่างต่อเนื่อง วางแผนสำหรับการกู้ระบบคืน เมื่อมีเหตุการณ์เลวร้ายเกิดขึ้น

1.2 software

- การป้องกันระบบเครือข่าย โดยใช้ Firewall ซึ่งเป็นเทคโนโลยีที่ทำการป้องกันผู้บุกรุกเข้า-ออกระบบ และกำหนดโซนการให้บริการ การเข้าถึงข้อมูล ที่เหมาะสม กำหนดขอบเขต และโซนการทำงานที่เหมาะสม กำหนดบริการ และการเข้าถึงระบบสำหรับผู้ที่ได้รับอนุญาตเท่านั้น

2. การบริหารจัดการด้านความปลอดภัย

2.1 การจู่โจมโดยการหลอกลวง

2.2 การกำหนดสิทธิในการใช้งาน

2.3 ระเบียบปฏิบัติเกี่ยวกับ Account ของผู้ใช้และกลุ่มผู้ใช้

2.4 การกำหนดสิทธิในการเข้าถึงข้อมูล

2.5 การเข้าถึงข้อมูลแต่ละหน่วยงาน

2.6 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

2.7 การเข้าถึงระบบอย่างมั่นคงปลอดภัยของข้อมูล

2.8 การตรวจสอบความปลอดภัยของระบบ

2.9 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

2.10 Session time-out (การหมดเวลาการใช้งานระบบสารสนเทศ)

3. การบำรุงรักษา

3.1 การสำรองข้อมูลแบบ Mirror เป็นการสำรองข้อมูลจากฮาร์ดดิสก์ไปสู่อีกฮาร์ดดิสก์หนึ่งโดยอัตโนมัติ เช่น การสำรองข้อมูลจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง

3.2 การสำรองข้อมูลด้วย sync เป็นถูกออกแบบมาให้ทำงานได้บนระบบปฏิบัติการ Unix เป็นหลัก ด้วยวิธีการสำรองข้อมูลในรูปแบบของการทำ Synchronizes files และ directory โดยทำการ sync ข้อมูลจากที่หนึ่ง ไปยังอีกที่หนึ่ง โดยในระหว่างการโอนถ่ายข้อมูลนั้น สามารถที่จะทำการย่อขนาดของข้อมูล

3.3 การกู้คืนข้อมูล (Restore) เป็นการนำข้อมูลที่สำรองเอาไว้ มาแทนที่ข้อมูลที่เสียหายไป ทำให้ข้อมูลในระบบงานสามารถทำงานได้ตามปกติ ซึ่งอาจจะเป็นข้อมูลส่วนใดส่วนหนึ่งหรือข้อมูลทั้งหมดก็ได้

3. เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล คณะครุศาสตร์อุตสาหกรรมควรปฏิบัติดังนี้ (Check)

1. ลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวน เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสามารถ
   - ตรวจจับข้อผิดพลาดจากการประมวลผล
   - ระบุการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

- ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่ คาดหมายไว้ หรือไม่

2. ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสม่ำเสมอ โดยนำสิ่งต่าง ๆ ต่อไปนี้มาพิจารณาร่วมด้วย ได้แก่ ผล การตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือ หน่วยงานที่เกี่ยวข้อง เป็นต้น

3.วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

4. บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยของคณะครุศาสตร์อุตสาหกรรมควร ปฏิบัติ ดังนี้ (Act)

1. ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้

2. ใช้มาตรการเชิงแก้ไขและป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่น ๆ มาช่วยในการปรับปรุงให้ดีขึ้น

3. แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

5.5 อภิปรายผล

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาเทคโนโลยีใหม่ทางด้านระบบเครือข่ายและความมั่นคงปลอดภัยของข้อมูลในองค์กร และ 2) เพื่อเสนอแนวทางการจัดการระบบความมั่นคงปลอดภัยของข้อมูลต่อองค์กรในแนวทางที่ถูกต้องและมีประสิทธิภาพตามมาตรฐานโลก

การวิจัยครั้งนี้ใช้วิธีดำเนินการวิจัยเอกสาร (Documentary Research) โดยการวิเคราะห์ทางเอกสาร (Documentary Research) และการศึกษาเชิงคุณภาพ (Documentary Analysis) มุ่งศึกษา วิเคราะห์โดยเอกสารและข้อมูลในรูปแบบบันทึกต่าง ๆ ที่เป็นมาตรฐานเป็นหลัก มุ่งศึกษาวิเคราะห์เอกสาร งานวิจัย ข้อเขียน บทความและข้อมูลเอกสารจากหน่วยงาน องค์กรส่วนราชการทั้งในและต่างประเทศ เพื่อทำความเข้าใจสภาพของการจัดการระบบความปลอดภัยของข้อมูลที่มีต่อองค์กรรวมทั้งผลกระทบที่มีผลต่อการปรับตัวของบุคลากรในคณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยนำข้อมูลที่ได้จากแหล่งต่าง ๆ มาวิเคราะห์และสังเคราะห์ผ่านกรอบความรู้ในเชิงสหวิทยาการ (Interdisciplinary) เพื่อให้ได้รูปแบบและแนวทางการจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กรที่มีประสิทธิภาพตามมาตรฐานโลกซึ่งในที่นี้ใช้ระบบ ISO 27001 : 2005 Information Security Management

System หรือ ISMS นอกจากนี้คณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังยังมีระบบสารสนเทศที่มีประสิทธิภาพมากโดยเฉพาะระบบสารสนเทศเพื่อการบริหาร โดยเฉพาะสารสนเทศที่เป็นตัวบ่งชี้การปฏิบัติงาน(Performance indicators) ซึ่งผู้บริหารสามารถใช้ในการตัดสินใจ วางนโยบายและบริหารงานเพื่อพัฒนาองค์กรได้เป็นอย่างดี ตัวบ่งชี้นี้อาจหมายถึง สิ่งที่แสดงออกเป็นตัวเลขที่ใช้วัดแง่มุมต่าง ๆ เชิงนามธรรมให้เป็นตัวแปรเชิงรูปธรรมที่สามารถวัดได้โดยอาศัยระบบสารสนเทศที่เป็นเอกภาพ เพื่อประกอบการตัดสินใจของผู้บริหาร ตัวบ่งชี้ต่าง ๆ ในที่นี้อาจหมายถึง ข้อเท็จจริงต่าง ๆ ปัญหา สภาวะหรืออุปสรรคในการดำเนินงานของช่วงเวลาใดเวลาหนึ่งซึ่งเป็นข้อมูลสำหรับการวางกลยุทธ์ การกำหนดนโยบาย การบริหารงาน การติดตามและประเมินผลการทำงาน รวมทั้งการประกันคุณภาพ ซึ่งตัวบ่งชี้ของคณะอาจไม่มีความละเอียดมากนัก อาจไม่จำเป็นต้องถูกต้องแม่นยำ แต่ข้อมูลที่จำเป็นของคณะเป็นข้อมูลที่เป็นภาพรวมซึ่งมาจากหลาย ๆ ด้าน ซึ่งมีเกณฑ์หรือมาตรฐานที่กำหนดเอาไว้ชัดเจน ผู้วิจัยตั้งข้อสังเกตการทำงานของผู้บริหารของคณะครุศาสตร์อุตสาหกรรมพบว่า มีระบบการทำงานที่มีประสิทธิภาพโดยพบว่า กลุ่มผู้บริหารมีการตัดสินใจจากสารสนเทศที่ถูกต้องและแม่นยำซึ่งหลักการทำงานนี้สอดคล้องกับงานวิจัยของวัสกา ดวงอ่อนนาม (2546) ที่ทำการศึกษาเรื่องการใช้เทคโนโลยีสารสนเทศในวิทยาลัยเกษตรและเทคโนโลยีผลการวิจัยพบว่า ผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปริมาณการใช้เทคโนโลยีสารสนเทศต่างกัน ผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีความสามารถในการใช้เทคโนโลยีสารสนเทศต่างกันและผู้บริหารที่มีประสบการณ์ทำงานต่างกันจะมีปัญหาในการใช้เทคโนโลยีสารสนเทศต่างกัน โดยผู้บริหารของคณะครุศาสตร์อุตสาหกรรมมีประสบการณ์การทำงานไม่ต่างกัน นอกจากนี้ยังสอดคล้องกับงานวิจัยของ ธนา จินดาวัฒนะ (2534) ที่พบว่า ข้อมูลครูอาจารย์ ข้อมูลนักเรียน ข้อมูลการเรียนการสอนสารสนเทศที่มีความถูกต้องตรงกับความต้องการ ทันต่อเหตุการณ์นั้นมีความสำคัญต่อการตัดสินใจในการวางแผนและบริหารงานของผู้บริหารมากกว่าการใช้ประสบการณ์และสามัญสำนึก

5.6 ข้อเสนอแนะทั่วไป

1. ด้านการวางแผน ควรมีการกำหนดขอบเขตให้ชัดเจน และจัดตั้งทีมรับผิดชอบ ศึกษาโครงสร้างในคณะอื่นๆ ด้วยเพื่อจะได้เป็นแนวทางในการวางแผน

2. ด้านการลงมือปฏิบัติ ควรศึกษาการกำหนดนโยบายความมั่นคงปลอดภัยของคณะอื่นๆ ด้วยเพื่อจะได้ประกอบการประเมินความเสี่ยง การวิเคราะห์และแก้ไข ความเสี่ยง โดยเลือกใช้การเลือกใช้มาตรการความมั่นคงปลอดภัยและควบคุมตามมาตรฐาน ได้อย่างชัดเจน และทำการฝึกอบรมบุคลากรเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุกระดับ

3. ด้านการตรวจสอบ ควรมีตรวจประเมินภายในของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ของคณะอย่างสม่ำเสมอ และการทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร เป็นประจำ

4. ด้านการประเมินผล ควรดำเนินการวิเคราะห์หาสาเหตุของปัญหาที่แท้จริงและแก้ปัญหาที่เกิดขึ้น รวมทั้งทำการสรุปอย่างเป็นระยะ

5.7 ข้อเสนอแนะในการวิจัยครั้งต่อไป

1. ควรมีการศึกษาวิเคราะห์ปัจจัยที่เกี่ยวกับระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร ที่เป็นอุปสรรคต่อการพัฒนาองค์กรต่าง ๆ

2. ควรมีการสร้างสื่อการให้ความรู้ เรื่อง การจัดการระบบเทคโนโลยีความมั่นคงปลอดภัยของข้อมูลในองค์กร อย่างแพร่หลายเพื่อให้ นักเรียน นักศึกษา ได้เห็นความสำคัญต่อระบบความมั่นคงปลอดภัยของข้อมูลต่อการพัฒนาประเทศชาติ

บรรณานุกรม

"โครงการผลิตเอกสารชุดวิชาและสื่อประกอบการเรียนการสอน". **เทคโนโลยีสารสนเทศ.** (online)Available: http://www.uni.net.th/~08_2543/chap07.html, 16 กรกฎาคม 2546.

โครงการจัดทำโฮมเพจวิชาเทคโนโลยีสารสนเทศ(online)Available:http://www.learning .ricr.ac.th/ it4life/lesson4/lesson4.html , 16 กรกฎาคม 2546.

โครงการจัดทำโฮมเพจรายวิชาเทคโนโลยีสารสนเทศ (online)Available: http://www. rikc.ac.th/thanhomepage/data%20base.doc, 16 กรกฎาคม 2546.

จีราพร รักษาแก้ว. 2538. "สารสนเทศ". น.53-81. **เอกสารการสอนชุดวิชาระบบสารสนเทศเพื่อการจัดการ หน่วยที่** 1- 8. (พิมพ์ครั้งที่ 2). กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมาธิราช.

ฉวีวรรณ กินาวงศ์. 2533. **การศึกษาเด็ก**. กรุงเทพมหานคร: สำนักพิมพ์โอเดียนสโตร์.

ธนา จินดาวัฒนะ. 2534. **การจัดการระบบสารสนเทศเพื่อการวางแผนในโรงเรียนมัธยมศึกษาขนาดใหญ่ สังกัดกรัมสามัญศึกษา เขตการศึกษา 5**. วิทยานิพนธ์ปริญญาโท,มหาวิทยาลัยขอนแก่น.

ระบบสารสนเทศเพื่อการบริหารงาน (online) Available: http://www.kmitl.ac.th/~kpwichai/

วราภรณ์ เทพสัมฤทธิ์พร. 2536. **การศึกษาระบบสารสนเทศเพื่อการบริหารของ** มหาวิทยาลัยเกษตรศาสตร์. วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยเกษตรศาสตร์.

วิจิตร อุ่นสากล. 2537. **การศึกษาระบบสารสนเทศในโรงเรียนมัธยมศึกษาขนาดใหญ่สังกัดกรมสามัญศึกษา เขตการศึกษา 9**. วิทยานิพนธ์ปริญญาโท มหาวิทยาลัยขอนแก่น.

วัสกา ดวงอ่อนนาม. 2546. **การใช้เทคโนโลยีสารสนเทศในวิทยาลัยเกษตรกรรมและเทคโนโลยีสังกัดกรมอาชีวศึกษา**.วิทยานิพนธ์ปริญญาโท มหาวิทยาลัยเกษตรศาสตร์.

สถาบันราชภัฏเชียงราย. 2546. **โครงการจัดทำโฮมเพจรายวิชาเทคโนโลยีสารสนเทศ** (online) Available: http://www.learning.ricr.ac.th/it4life /lesson1/lesson1.html , 16 กรกฎาคม 2546.

สุชา จันทน์เอม. 2520. **จิตวิทยาสังคม**. กรุงเทพมหานคร:โรงพิมพ์แพร่พิทยา.

สุพรรณี เมนะเนตร. 2543. **การจัดระบบสาสนเทศในการบริหารในโรงเรียนสังกัด**

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีคอมพิวเตอร์แห่งชาติ. 2538.

รายงานการศึกษาเรื่อง แนวทางการพัฒนาบุคลากรด้านเทคโนโลยีคอมพิวเตอร์ของประเทศไทย. กรุงเทพมหานคร : บริษัท 21 เซ็นจูรี่ จำกัด.สำนักบริหารเทคโนโลยีและสารสนเทศเพื่อพัฒนาการศึกษา ทบวงมหาวิทยาลัย.

สุภางค์ จันทวานิช. 2537. **วิธีการวิจัยเชิงคุณภาพ.** พิมพ์ครั้งที่ 5. กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย.

สมบุญ พิมพาภรณ์. 2538. **การจัดระบบสารสนเทศของสำนักงานสามัญการศึกษาจังหวัด กรมสามัญศึกษา.** วิทยานิพนธ์ปริญญาโท, มหาวิทยาลัยเกษตรศาสตร์.

อรรณพ เธียรถาวร. 2531. **การปฏิวัติสารสนเทศใหม่**. ภาควิชาการสื่อสารมวลชน คณะนิเทศศาสตร์

Nectec 2550. มาตรฐานการรักษาความปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์.