ความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

SECURITY IN INFORMATION SYSTEMS OF COLLEGES UNDER THE OFFICE OF VOCATIONAL EDUCATION COMMISSION IN BANGKOK

อรรถสิทธิ์ มีชัย

ATTASIT MEECHAI

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์)

คณะครุศาสตร์อุตสาหกรรม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2552

SECURITY IN INFORMATION SYSTEMS OF COLLEGES UNDER THE OFFICE OF VOCATIONAL EDUCATION COMMISSION IN BANGKOK

ATTASIT MEECHAI

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE IN SCIENCE EDUCATION (COMPUTER)

FACULTY OF INDUSTRIAL EDUCATION

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2009

KMITL – 2009 – ED – M – 214 – 102

คณะครุศาสตร์อุตสาหกรรม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ ความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

Security in Information Systems of Colleges Under the Office of Vocational Education Commission in Bangkok

นักศึกษา นายอรรถสิทธิ์ มีชัย

รหัสประจำตัว 50063929

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา การศึกษาวิทยาศาสตร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.เลิศลักษณ์ กลิ่นหอม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ผศ.ไพฑูรย์ พิมดี

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.รวีวรรณ	ชินะตระกูล	
ผศ.ดร.เลิศลักษณ์	กลิ่นหอม	
ผศ.ไพฑูรย์	พิมดี	
รศ.พีระวุฒิ	สุวรรณจันทร์	
ดร.เชิน	แก้วยศ	

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

วัน / เดือน/ ปี ที่สอบ 20 พฤษภาคม 2552 เวลา 09.00 น. เป็นต้นไป

สถานที่สอบ ณ ห้องสมาคมศิษย์เก่าบัณฑิตศึกษา คณะครุศาสตร์อุตสาหกรรม

คณะครุศาสตร์อุตสาหกรรมรับรองแล้ว

(รองศาสตราจารย์ พีระวุฒิ สุวรรณจันทร์)

คณบดี คณะครุศาสตร์อุตสาหกรรม

วันที่ 27 เดือน พฤษภาคม พ.ศ. 2552

หัวข้อวิทยานิพนธ์	ความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร
นักศึกษา	นายอรรถสิทธิ์ มีชัย
รหัสประจำตัว	50063929
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	การศึกษาวิทยาศาสตร์ (คอมพิวเตอร์)
พ.ศ.	2552
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.เลิศลักษณ์ กลิ่นหอม
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ผู้ช่วยศาสตราจารย์ ไพฑูรย์ พิมดี

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาการจัดการด้านความปลอดภัยในระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยใช้มาตรฐาน ISO17799 : 2005 ซึ่งประกอบไปด้วยหัวข้อที่ต้องการศึกษา 11 หัวข้อใหญ่ ผู้ศึกษาได้กำหนดวิธีการดำเนินการศึกษา ดังนี้ ประชากร เป็นบุคลากรที่เกี่ยวข้องของสถานศึกษาสังกัดสำนักงานคณะ กรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร ทั้ง 21 แห่ง จำนวน 204 คน เครื่องมือที่ใช้ในการวิจัยครั้งนี้คือ แบบสอบถามเกี่ยวกับความปลอดภัยในระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยเทียบจากมาตรฐาน ISO 17799 : 2005 สถิติที่ใช้วิเคราะห์ข้อมูล คือ ความถี่ และ ร้อยละ ผลการวิจัยพบว่า สถานศึกษาสังกัดสำนักงานคณะ กรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง ไม่มีสถานศึกษาแห่งใดในเขตกรุงเทพมหานคร ที่สามารถผ่านมาตรฐานความปลอดภัยในระบบสารสนเทศ ISO17799 : 2005

Thesis Title	Security in Information Systems of Colleges Under the Office of Vocational Education Commission in Bangkok
Student	Mr. Attasit Meechai
Student ID	50063929
Degree	Master of Science
Program	Science Education (Computer)
Year	2009
Thesis Advisor	Assistant Professor Dr. Lertlak Klinhom
Thesis Co-Advisor	Assistant Professor Paitoon Pimdee

ABSTRACT

The objective of this research was to study about security management in information systems of colleges under the Office of Vocational Education Commission in Bangkok by applying ISO 17799: 2005 standard which has 11 important articles that needed to be addressed. Researcher has set the study procedure as followed: Population was those who were related with colleges under the Office of Vocational Education Commission in Bangkok totally 21 colleges, at 204 people. Tools used in this research were questionnaires on factors related to security in Information Systems of colleges under the Office of the Vocational education commission in Bangkok by complying with ISO 17799: 2005 standard. Statistical methods used in data analysis were frequencies and percentages calculation. The research results showed that all 21 colleges under the Office of Vocational Education Commission in Bangkok had not passed the ISO 17799: 2005 standards.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำและคำปรึกษาจาก ผู้ช่วยศาสตราจารย์ ดร.เลิศลักษณ์ กลิ่นหอม อาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผู้ช่วยศาสตราจารย์ไพฑูรย์ พิมดี อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ที่ได้ให้คำปรึกษา ช่วยเหลือ ตรวจสอบ แก้ไขข้อบกพร่องของวิทยานิพนธ์ ตลอดจนคำแนะนำต่าง ๆ ที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์ในครั้งนี้ จนสำเร็จได้อย่างสมบูรณ์ ผู้วิจัยรู้สึกซาบซึ้ง และขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณ รศ. ดร.รวีวรรณ ชินะตระกูล รศ.พีระวุฒิ สุวรรณจันทร์ และ ดร.เชน แก้วยศ คณะกรรมการสอบหัวข้อและเค้าโครงวิทยานิพนธ์ที่กรุณาให้คำแนะนำแก้ไขข้อบกพร่อง ทำให้วิทยานิพนธ์ฉบับนี้สมบูรณ์ยิ่งขึ้น

ขอกราบขอบพระคุณ ผศ.ดร.ฉันทนา วิริยเวชกุล อาจารย์สมณธร พุ่มพิมล และคุณรุ่งนิรันดร์ ผดุงพิทักษ์ชน ซึ่งเป็นผู้ทรงคุณวุฒิตรวจสอบความถูกต้องของเครื่องมือแบบสอบถามต่อการทำวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณ บุคลากรที่มีส่วนเกี่ยวข้องในการทำวิทยานิพนธ์ในครั้งนี้ของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง ที่ให้ความอนุเคราะห์ในการทดลองเครื่องมือ และ เก็บรวบรวมข้อมูล สำหรับการทำวิทยานิพนธ์ครั้งนี้

ขอกราบขอบพระคุณบิดา มารดาผู้เป็นที่เคารพรัก ผู้ให้ความรักและความห่วงใย ดูแลเอาใจใส่ ตลอดจนให้โอกาสทางการศึกษาแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

คุณค่า และประโยชน์ใด ๆ ที่เป็นผลจากการทำวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่บิดา มารดา ครู-อาจารย์ และผู้มีพระคุณทุกท่าน ด้วยความเคารพยิ่ง

อรรถสิทธิ์ มีชัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

โลกในปัจจุบันนี้เป็นยุคของข่าวสารข้อมูล โดยเป็นการใช้ข้อมูลเพื่อทำประโยชน์ด้านต่างๆ เช่น การใช้ในด้านการทำธุรกิจหรือในด้านความบันเทิง ซึ่งสามารถกล่าวได้ว่าข้อมูลต่างๆ เป็นสิ่งที่ขาดไม่ได้ในชีวิตประจำวัน ตั้งแต่เช้า มีการอ่านหนังสือพิมพ์เพื่อรับรู้ข่าวสารต่างๆ พอถึงที่ทำงาน ก็มีการดูข้อมูลที่เกี่ยวกับงานที่รับผิดชอบ เช่น แบบงานจากลูกค้า ข้อมูลการเงิน ข้อมูลพนักงาน ข้อมูลบริษัท เป็นต้น และในปัจจุบันนี้ มีการแข่งขันในด้านธุรกิจสูงมาก องค์กรต่างๆ มีการปรับตัวและมีการนำระบบคอมพิวเตอร์มาใช้ในการจัดการเรื่องของข้อมูลอย่างแพร่หลาย ข้อมูลต่างๆ มีการจัดทำขึ้นมากมายเพื่อใช้ในการดำเนินธุรกิจ แม้ข้อมูลต่างๆเหล่านี้จะมีประโยชน์ต่อบริษัทในการดำเนินธุรกิจ แต่หากมองอีกมุมหนึ่งก็เป็นภัยร้ายแรงต่อองค์กรได้เช่นกัน หากข้อมูลต่างๆเหล่านั้นตกไปอยู่ในมือผู้ที่ไม่ประสงค์ดีต่อองค์กร

หนังสือพิมพ์โลกวันนี้ ปีที่ 10 ฉบับที่ 2415 (2551) [Online] ทุกวันนี้ต้องยอมรับว่าระบบสารสนเทศในสถานศึกษาเกือบทุกแห่งสามารถเป็นแหล่งที่เสี่ยงต่อภัยคุกคามในหลารูปแบบ ภัยคุกคามดังกล่าวมีผลต่อความรู้สึกถึงความปลอดภัยในชีวิตและทรัพย์สินของเจ้าของสถานศึกษาและผู้ที่เข้ามาศึกษาหาความรู้โดยตรง กล่าวคือ อาจก่อให้เกิดความรู้สึกที่ดีและความรู้สึกแย่ต่อสถาบันนั้นๆได้ในทันทีที่สำคัญยิ่งภัยคุกคามอยู่ในรูปแบบที่ซับซ้อนของเทคโนโลยีสารสนเทศที่ใช้ในสถานศึกษาก็จะมีความสุ่มเสี่ยงต่อภาพลักษณ์และความเสียหายต่อสถานศึกษาโดยตรง

ยอดเยี่ยม เหล่านนท์ชัย (2551) [Online] สำนักปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ลงวันที่ 8 กุมภาพันธ์ 2550 จึงได้จัดทำโครงการจัดทำแผนแม่บท ICT Security แห่งชาติขึ้นโดยมีหลักการและเหตุผลดังนี้

หน่วยงานภาครัฐมีการพัฒนาและใช้งานระบบสารสนเทศในการบริหารราชการแผ่นดินและการบริการประชาชนมากขึ้น เมื่อมีการจัดเก็บและบริหารข้อมูลในรูปแบบอิเล็กทรอนิกส์ ซึ่งให้บริการประชาชน ดังนั้นความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลจึงยิ่งทวีความสำคัญมากขึ้น จำเป็นต้องมีมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขอบเขตกว้างและครอบคลุมหลายมิติ เช่น มิติด้านกายภาพ มิติทางด้านการเชื่อมโยงเครือข่าย มิติด้านการควบคุมการเข้าถึง มิติทางด้านขั้นตอนวิธีปฏิบัติ มิติทางด้านความต่อเนื่องของการใช้งานระบบ เป็นต้น

ปัจจุบันกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อยู่ระหว่างดำเนินการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย (Information Security) ขั้นพื้นฐานของระบบสารสนเทศของหน่วยงานภาครัฐตลอดจนดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานภาครัฐเพื่อให้หน่วยงานของรัฐใช้เป็นแนวทางในการดำเนินการจัดทำนโยบายดังกล่าวในทิศทางเดียวกัน

อย่างไรก็ตามการนำเอาแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในหน่วยงานภาครัฐที่กำหนดขึ้นนั้น ไปใช้ในทางปฏิบัติจำเป็นต้องอาศัยความรู้อย่างเพียงพอ จึงจำเป็นต้องสร้างความเข้าใจและความเข้มแข็งให้แก่บุคลากรของหน่วยงานภาครัฐในเรื่องดังกล่าวอย่างจริงจัง เพื่อให้สอดคล้องตามเจตนารมณ์ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

เพื่อให้บุคลากรภาครัฐสามารถดำเนินการวางแผนพัฒนาเจ้าหน้าที่ของหน่วยงานภาครัฐมีความเข้าใจและมีศักยภาพในการพัฒนาความมั่นคงปลอดภัยด้านระบบสารสนเทศของตน จึงจำเป็นต้องสร้างความเข้าใจและเพิ่มศักยภาพให้กับบุคลากรภาครัฐเป็นสำคัญ

วัตถุประสงค์เพื่อ มุ่งเน้นให้มีความรู้ความเข้าใจเกี่ยวกับความรู้พื้นฐานและแนวคิดในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับหน่วยงานภาครัฐ โดยอ้างอิงจากมาตรฐานสากลต่างๆ เช่น ISO 27000, ISO 17799, ISO 13335 เป็นต้น และปรับปรุงให้เหมาะสมกับสถานการณ์ของประเทศ

ยอดเยี่ยม เหล่านนท์ชัย (2551) [Online] สำนักงานคณะกรรมการการอาชีวศึกษา กระทรวงศึกษาธิการ ได้เล็งเห็นถึงความสำคัญของความมั่นคงปลอดภัยด้านระบบสารสนเทศจึงได้ส่งบุคลากรที่มีส่วนเกี่ยวข้องกับงานด้านความปลอดภัยของระบบสารสนเทศในหน่วยงานเข้าร่วมอบรมหัวข้อเรื่อง การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับหน่วยงานภาครัฐ สำนักงานคณะกรรมการการอาชีวศึกษา (Information Security of Vocational Education Commission) ในครั้งนี้โดยใช้มาตรฐาน ISO 17799:2005 เข้ามาใช้ในการปฏิบัติ

ดังนั้น ผู้วิจัยได้เล็งเห็นและตระหนักถึงภัยคุกคามที่มีผลต่อความมั่นคงในระบบสารสนเทศของสถานศึกษาดังกล่าว จึงมีความต้องการที่จะศึกษาในส่วนของการบริหารจัดการด้านความปลอดภัยในระบบเครือข่ายสารสนเทศของคณะกรรมการการอาชีวศึกษา โดยนำมาตรฐานด้านการปฏิบัติที่ถูกต้อง หรือ Best Practice โดยอิงกับ ISO17799 ทั้ง 11 หัวข้อหลักเข้ามาใช้ในการศึกษาในครั้งนี้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาการจัดการด้านความปลอดภัยในระบบสารสนเทศของสถานศึกษาสังกัดคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

1.3 กรอบแนวคิดของการวิจัย

การศึกษาวิจัยครั้งนี้เป็นการศึกษาการจัดการด้านความปลอดภัยในระบบสารสนเทศของสถานศึกษาของคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยใช้มาตรฐาน ISO17799: 2005 NECTEC (2550) [Online] ซึ่งประกอบไปด้วยหัวที่ต้องการศึกษา 11 หัวข้อใหญ่ ดังนี้

1.3.1 นโยบายความมั่นคงปลอดภัย

1.3.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

1.3.3 การบริหารจัดการทรัพย์สินขององค์กร

1.3.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

1.3.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

1.3.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

1.3.7 การควบคุมการเข้าถึง

1.3.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

1.3.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

1.3.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

1.3.11 การปฏิบัติตามข้อกำหนด

1.4 ขอบเขตของการวิจัย

การวิจัยในครั้งนี้ผู้ทำวิจัยการศึกษามุ่งที่จะศึกษาเกี่ยวกับความปลอดภัยในระบบสารสนเทศของสถานศึกษาของคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้งโดยมีขอบเขต ของการศึกษาดังนี้

1.4.1 ประชากร

ประชากรที่ใช้ในการศึกษา ได้แก่ บุคลากรที่เกี่ยวข้องกับระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะ กรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง มีจำนวนทั้งสิ้นจำนวน 204 คน

1.4.2 ตัวแปรที่ใช้ในการศึกษา

การจัดการด้านความปลอดภัยในระบบสารสนเทศ โดยใช้มาตรฐาน ISO17799:2005 ประกอบไปด้วย 11 หัวข้อใหญ่ ได้แก่

1.4.2.1 นโยบายความมั่นคงปลอดภัย

1.4.2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

1.4.2.3 การบริหารจัดการทรัพย์สินขององค์กร

1.4.2.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

1.4.2.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

1.4.2.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

1.4.2.7 การควบคุมการเข้าถึง

1.4.2.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

1.4.2.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

1.4.2.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

1.4.2.11 การปฏิบัติตามข้อกำหนด

1.5 นิยามศัพท์เฉพาะที่ใช้ในการวิจัย

1.5.1 มาตรฐานความปลอดภัยด้านระบบสารสนเทศ ISO 17799: 2005 หมายถึง มาตรฐานความปลอดภัยในระบบเครือข่ายสารสนเทศที่เป็นมาตรฐานกลางที่ทั่วโลกยอมรับประกอบไปด้วยหัวข้อใหญ่ๆ 11 ข้อดังนี้

1.5.1.1 นโยบายความมั่นคงปลอดภัย หมายถึง การกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

1.5.1.2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร หมายถึง การบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

1.5.1.3 การบริหารจัดการทรัพย์สินขององค์กร หมายถึง การป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

1.5.1.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร หมายถึงการให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษา อุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก

เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตนและเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

1.5.1.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม หมายถึง การป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

1.5.1.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร หมายถึง เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

1.5.1.7 การควบคุมการเข้าถึง หมายถึง การควบคุมการเข้าถึงสารสนเทศ

1.5.1.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ หมายถึง การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

1.5.1.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร หมายถึง เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบ สารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

1.5.1.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร หมายถึง การป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และ เพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

1.5.1.11 การปฏิบัติตามข้อกำหนด หมายถึง การปฏิบัติเพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

1.5.2 ระบบสารสนเทศ หมายถึง ระบบที่ประกอบไปด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง

1.5.3 สถานศึกษา หมายถึง สถานศึกษาในสังกัดคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

1.5.4 พนักงาน หมายถึง พนักงานและลูกจ้างที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบภายในองค์กร

1.5.5 ผู้บริหารองค์กร หมายถึง พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร

1.5.6 ผู้บริหารสารสนเทศ หมายถึง พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการและมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในองค์กร

1.5.7 ผู้ดูแลระบบและผู้พัฒนาระบบ หมายถึง พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account)

1.5.8 หัวหน้างานสารสนเทศ หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

1.5.9 หัวหน้างานบุคคล หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลการวางแผนทรัพยากรบุคคลทั้งคุณภาพ ปริมาณและสัดส่วนให้มีความเหมาะสมกับภารกิจ และแผนกลยุทธ์ของหน่วยงานระดับต่างๆ ทั้งในระยะสั้นและระยะยาว รวมถึงบริหารทรัพยากรบุคคลตามระเบียบ / หลักเกณฑ์ของสำนักงาน

1.5.10 หัวหน้างานอาคาร หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลและบริหารจัดการระบบสาธารณูปโภคต่างๆ และทรัพยากรสิ่งอำนวยความสะดวกภายในอาคาร รวมถึงดูแลความเป็นระเบียบเรียบร้อยและการรักษาความปลอดภัยของสำนักงาน

1.5.11 หัวหน้างานธุรการ หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลเกี่ยวกับงานธุรการและสารบรรณภายในองค์กร

1.5.12 หน่วยงานภายนอก หมายถึง องค์กรอื่นๆ ที่เกี่ยวข้อง เช่น บริษัทขายฮาร์ดแวร์หรือซอฟต์แวร์ บริษัทให้คำปรึกษาเกี่ยวกับระบบสารสนเทศ

1.5.13 หัวหน้างานนิติการ หมายถึง พนักงานที่มีหน้าที่ให้ความคิดเห็นหรือตีความเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ข้อบังคับ กฎหมาย พระราชบัญญัติ กฤษฎีกา หรือข้อความในเชิงระเบียบข้อบังคับอื่นๆ รวมทั้งจัดทำระเบียบ ข้อกำหนด กฎเกณฑ์ข้อบังคับ หรือคำสั่งสำหรับใช้ในองค์กร

1.5.14 หัวหน้างานพัสดุ หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลเกี่ยวกับงานด้านทรัพย์สินและบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กร

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การวิจัยครั้งนี้ผู้วิจัยได้ศึกษา รวบรวมเนื้อหาของทฤษฎีและงานวิจัยที่เกี่ยวข้องไว้หลายแนวคิด โดยศึกษาจาก ตำราเอกสาร วารสาร รายงานการวิจัยและวิทยานิพนธ์ที่เกี่ยวข้อง ทั้งนี้เพื่อให้สามารถกำหนดกรอบแนวคิดที่จะใช้เป็นแนวทาง ได้ครอบคลุมและชัดเจนขึ้นซึ่งประกอบด้วยสาระสำคัญตามลำดับ ดังนี้

2.1 ระบบสารสนเทศ

2.2 มาตรฐานเกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ISO/IEC 17799 (BS7799)

2.3 ข้อกำหนดและนโยบายด้านความปลอดภัยของ ISO 1779:2005

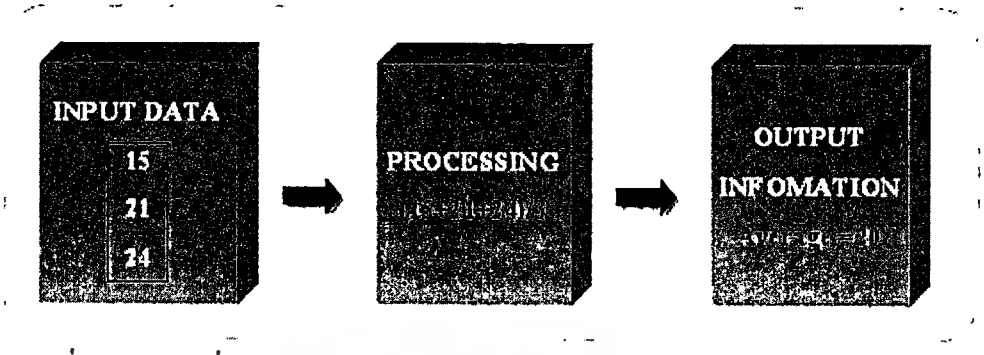
2.4 สถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

2.5 งานวิจัยที่เกี่ยวข้อง

2.1 ระบบสารสนเทศ

2.1.1 ระบบสารสนเทศ (Information system)

สุชาดา กีระนันทน์ (2541) [Online] กล่าวถึง ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร หรือ ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจ และการควบคุมในองค์กร ในการทำงานของระบบสารสนเทศประกอบไปด้วยกิจกรรม 3 อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และ การนำเสนอผลลัพธ์ (Output) ระบบสารสนเทศอาจจะมีการสะท้อนกลับ (Feedback) เพื่อการประเมินและปรับปรุงข้อมูลนำเข้า ระบบสารสนเทศอาจจะเป็นระบบที่ประมวลด้วยมือ(Manual) หรือระบบที่ใช้คอมพิวเตอร์ก็ได้ ดังแสดงในรูปที่ 2.1



รูปที่ 2.1 การเปลี่ยนรูปจากข้อมูลสู่สารสนเทศโดยผ่านการประมวลผลสารสนเทศ (วิเศษศักดิ์ โคตรอาษา. 2542 : 148)

2.1.2 ประเภทของระบบสารสนเทศ

สุชาดา กีระนันทน์ (2541) [Online] กล่าวว่า ปัจจุบันจะเห็นความสัมพันธ์ระหว่างองค์กร กับระบบสารสนเทศ และเทคโนโลยีสารสนเทศชัดเจนมากขึ้น และเนื่องจากการบริหารงานในองค์กรมีหลายระดับ กิจกรรมขององค์กรแต่ละประเภทอาจจะแตกต่างกัน ดังนั้น ระบบสารสนเทศของแต่ละองค์กรอาจแบ่งประเภทแตกต่างกันออกไป

ถ้าพิจารณาจำแนกระบบสารสนเทศตามการสนับสนุนระดับการทำงานในองค์กร จะแบ่งระบบสารสนเทศได้เป็น 4 ประเภท ดังนี้

2.1.2.1 ระบบสารสนเทศสำหรับระดับผู้ปฏิบัติงาน (Operational – level systems) ช่วยสนับสนุนการทำงานของผู้ปฏิบัติงานในส่วนปฏิบัติงานพื้นฐานและงานทำรายการต่างๆขององค์กร เช่นใบเสร็จรับเงิน รายการขาย การควบคุมวัสดุของหน่วยงาน เป็นต้น วัตถุประสงค์หลักของระบบนี้ก็เพื่อช่วยการดำเนินงานประจำแต่ละวัน และควบคุมรายการข้อมูลที่เกิดขึ้น

2.1.2.2 ระบบสารสนเทศสำหรับผู้ชำนาญการ (Knowledge-level systems) ระบบนี้สนับสนุนผู้ทำงานที่มีความรู้เกี่ยวข้องกับข้อมูล วัตถุประสงค์หลักของระบบนี้ก็เพื่อช่วยให้มีการนำความรู้ใหม่มาใช้ และช่วยควบคุมการไหลเวียนของงานเอกสารขององค์กร

2.1.2.3 ระบบสารสนเทศสำหรับผู้บริหาร (Management - level systems) เป็นระบบสารสนเทศที่ช่วยในการตรวจสอบ การควบคุม การตัดสินใจ และการบริหารงานของผู้บริหารระดับกลางขององค์กร

2.1.2.4 ระบบสารสนเทศระดับกลยุทธ์ (Strategic-level system) เป็นระบบสารสนเทศที่ช่วยการบริหารระดับสูง ช่วยในการสนับสนุนการวางแผนระยะยาว หลักการของระบบคือต้องจัดความสัมพันธ์ระหว่างสภาพแวดล้อมภายนอกกับความสามารถภายในที่องค์กรมีเช่นในอีก 5 ปีข้างหน้า องค์กรจะผลิตสินค้าใด

2.1.3 ระบบสารสนเทศที่ใช้สนับสนุนการทำงาน

สุชาดา กีระนันทน์ (2541) และ Laudon & Laudon (2001) [Online] กล่าวว่า ได้แบ่งประเภทของระบบสารสนเทศที่สนับสนุนการทำงานของผู้ปฏิบัติงาน ผู้บริหารระดับต่างๆไว้ดังตารางที่ 2.1

ตารางที่ 2.1 ประเภทของระบบสารสนเทศที่ใช้ในการสนับสนุนการทำงาน

ประเภทของระบบสารสนเทศ สุชาดา กีระนันทน์ (2541)	ประเภทของระบบสารสนเทศ Laudon & Laudon (2001)
ระบบประมวลผลรายการ (Transaction Processing Systems)	Transaction Processing System - TPS
ระบบสำนักงานอัตโนมัติ (Office Automation Systems)	Knowledge Work -KWS and office Systems
ระบบงานสร้างความรู้ (Knowledge Work Systems)	
ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems)	Management Information Systems - MIS
ระบบสนับสนุนการตัดสินใจ (Decision Support Systems)	Decision Support Systems – DSS
ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information Systems)	Executive Support System - ESS

2.1.3.1 ระบบประมวลผลรายการ (Transaction Processing Systems - TPS) เป็นระบบที่ทำหน้าที่ในการปฏิบัติงานประจำ ทำการบันทึกจัดเก็บ ประมวลผลรายการที่เกิดขึ้นในแต่ละวัน โดยใช้ระบบคอมพิวเตอร์ทำงานแทนการทำงานด้วยมือ ทั้งนี้เพื่อที่จะทำการสรุปข้อมูลเพื่อสร้างเป็นสารสนเทศ ระบบประมวลผลรายการนี้ ส่วนใหญ่จะเป็นระบบที่เชื่อมโยงกิจการกับลูกค้า ตัวอย่าง เช่น ระบบการจองบัตรโดยสารเครื่องบิน ระบบการฝากถอนเงินอัตโนมัติ เป็นต้น ในระบบต้องสร้างฐานข้อมูลที่จำเป็น ระบบนี้มักจัดทำเพื่อสนองความต้องการของผู้บริหารระดับต้นเป็นส่วนใหญ่เพื่อให้สามารถปฏิบัติงานประจำได้ ผลลัพธ์ของระบบนี้ มักจะอยู่ในรูปของรายงานที่มีรายละเอียด รายงานผลเบื้องต้น

2.1.3.2 ระบบสำนักงานอัตโนมัติ (Office Automation Systems- OAS) เป็นระบบที่สนับสนุนงานในสำนักงาน หรืองานธุรการของหน่วยงาน ระบบจะประสานการทำงานของบุคลากรรวมทั้งกับบุคคลภายนอก หรือหน่วยงานอื่น ระบบนี้จะเกี่ยวข้องกับการจัดการเอกสาร

โดยการใช้ซอฟต์แวร์ด้านการพิมพ์ การติดต่อผ่านระบบไปรษณีย์อิเล็กทรอนิกส์ เป็นต้นผลลัพธ์ของระบบนี้ มักอยู่ในรูปของเอกสาร กำหนดการ สิ่งพิมพ์

2.1.3.3 ระบบงานสร้างความรู้ (Knowledge Work Systems - KWS) เป็นระบบที่ช่วยสนับสนุนบุคลากรที่ทำงานด้านการสร้างความรู้เพื่อพัฒนาการคิดค้น สร้างผลิตภัณฑ์ใหม่ๆ บริการใหม่ ความรู้ใหม่เพื่อนำไปใช้ประโยชน์ในหน่วยงาน หน่วยงานต้องนำเทคโนโลยีสารสนเทศเข้ามาสนับสนุนให้การพัฒนาเกิดขึ้นได้โดยสะดวก สามารถแข่งขันได้ทั้งในด้านเวลา คุณภาพ และราคา ระบบต้องอาศัยแบบจำลองที่สร้างขึ้น ตลอดจนการทดลองการผลิตหรือดำเนินการ ก่อนที่จะนำเข้ามาดำเนินการจริงในธุรกิจ ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของสิ่งประดิษฐ์ ตัวแบบ รูปแบบ

2.1.3.4 ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems-MIS) เป็นระบบสารสนเทศสำหรับผู้ปฏิบัติงานระดับกลาง ใช้ในการวางแผน การบริหารจัดการและการควบคุม ระบบจะเชื่อมโยงข้อมูลที่มีอยู่ในระบบประมวลผลรายการเข้าด้วยกัน เพื่อประมวลและสร้างสารสนเทศที่เหมาะสมและจำเป็นต่อการบริหารงาน ตัวอย่าง เช่น ระบบบริหารงานบุคลากร ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของรายงานสรุป รายงานของสิ่งผิดปกติ

2.1.3.5 ระบบสนับสนุนการตัดสินใจ (Decision Support Systems – DSS) เป็นระบบที่ช่วยผู้บริหารในการตัดสินใจสำหรับปัญหา หรือที่มีโครงสร้างหรือขั้นตอนในการหาคำตอบที่แน่นอนเพียงบางส่วน ข้อมูลที่ใช้ต้องอาศัยทั้งข้อมูลภายในกิจการและภายนอกกิจการประกอบกัน ระบบยังต้องสามารถเสนอทางเลือกให้ผู้บริหารพิจารณา เพื่อเลือกทางเลือกที่เหมาะสมที่สุดสำหรับสถานการณ์นั้น หลักการของระบบ สร้างขึ้นจากแนวคิดของการใช้คอมพิวเตอร์ช่วยการตัดสินใจ โดยให้ผู้ใช้โต้ตอบโดยตรงกับระบบ ทำให้สามารถวิเคราะห์ปรับเปลี่ยนเงื่อนไขและกระบวนการพิจารณาได้ โดยอาศัยประสบการณ์ และ ความสามารถของผู้บริหารเอง ผู้บริหารอาจกำหนดเงื่อนไขและทำการเปลี่ยนแปลงเงื่อนไขต่างๆ ไปจนกระทั่งพบสถานการณ์ที่เหมาะสมที่สุด แล้วใช้เป็นสารสนเทศที่ช่วยตัดสินใจ รูปแบบของผลลัพธ์ อาจจะอยู่ในรูปของ รายงานเฉพาะกิจ รายงานการวิเคราะห์เพื่อตัดสินใจ การทำนาย หรือ พยากรณ์เหตุการณ์

2.1.3.6 ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information System - EIS) เป็นระบบที่สร้างสารสนเทศเชิงกลยุทธ์สำหรับผู้บริหารระดับสูง ซึ่งทำหน้าที่กำหนดแผนระยะยาวและเป้าหมายของกิจการ สารสนเทศสำหรับผู้บริหารระดับสูงนี้จำเป็นต้องอาศัยข้อมูลภายนอกกิจกรรมเป็นอย่างมาก ยิ่งในยุคปัจจุบันที่เป็นยุค Globalization ข้อมูลระดับโลก แนวโน้มระดับสากลเป็นข้อมูลที่จำเป็นสำหรับการแข่งขันของธุรกิจ ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของการพยากรณ์/การคาดการณ์

ถึงแม้ว่าระบบสารสนเทศจะมีหลายประเภท แต่องค์ประกอบที่จำเป็นของระบบสารสนเทศทุกประเภท ก็คือต้องประกอบด้วยกิจกรรม 3 อย่างตามที่ Laudon & Laudon (2001[Online])ได้กล่าวไว้ คือ ระบบต้องมีการนำเข้าข้อมูล การประมวลผลข้อมูล และการแสดงผลลัพธ์ของข้อมูล

สุชาดา กีระนันทน์ (2541) [Online] สรุปไว้ว่า การพัฒนาระบบสารสนเทศในองค์กรนั้นเป็นสิ่งท้าทายผู้บริหารเป็นอย่างมาก การที่จะพัฒนาระบบสารสนเทศขึ้นในหน่วยงานเป็นสิ่งที่ผู้บริหารและผู้รับผิดชอบการพัฒนาระบบ ต้องร่วมกันตัดสินใจอย่างรอบคอบ เพราะการนำระบบสารสนเทศมาใช้อาจจะกระทบต่อกระบวนการดำเนินงานและการบริหารที่เป็นอยู่ หรืออาจจะมีผลก่อให้เกิดการเปลี่ยนแปลงในองค์กร

2.1.4 บทบาทของเทคโนโลยีสารสนเทศ

ฉัตรชัย เรืองมณี (2550) [Online] กล่าวว่า โลกเปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบันคงไม่มีใครปฏิเสธ ว่าเทคโนโลยีสารสนเทศ(Information Technology) หรือที่เรียกว่า IT ได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้นการสื่อสารข้อมูลเป็นไปด้วยความรวดเร็วและเชื่อมโยงกันอย่างทั่วถึงและกว้างขวาง(Globalization) เทคโนโลยีทางด้านการสื่อสาร(Communication) และ Computer ได้ถูกนำมาใช้เป็นเครื่องมือในการติดต่อแลกเปลี่ยนสารสนเทศ (Information) ที่มีประสิทธิภาพทำให้เกิดเครือข่ายข้อมูลที่เป็นเหมือนใยแมงมุมครอบคลุมทั่วโลกหรือ WWW(WorldWideWeb) ที่เราเห็น ได้จากการใช้งานในระบบInternet ซึ่งได้กลายมาเป็นส่วนหนึ่งในชีวิต ประจำวันไปเสียแล้วและกำลังขยายปริมาณจำนวนผู้ใช้มากขึ้นๆใน ทุกวันมีการใช้ Internet ในการสืบค้นข้อมูลความรู้ทั่วไปการติดต่อ สื่อสารในรูปแบบต่าง ๆ เช่น การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) การพูดคุย (Chat) หรือ การใช้ Video conference เป็นต้น การทำธุรกิจการค้า (e-commerce) การใช้เพื่อการบันเทิงต่างๆ เป็นการดูหนัง ฟังเพลง การอ่านนิตยสารอิเล็กทรอนิกส์ (e-Magazine) รวมทั้ง e-Book ที่อาจมาแทนที่กระดาษในอนาคตอันใกล้ อย่างไรก็ตามเทคโนโลยีสารสนเทศอาจมีทั้งคุณและโทษแต่ทั้งนี้ขึ้นอยู่กับว่าเราจะสามารถเลือกใช้ให้เป็นประโยชน์ในทางที่ดีได้อย่างไร ซึ่งเราสามารถนำระบบเทคโนโลยีสารสน เทศมาใช้เพื่อการพัฒนาทางด้านการศึกษาได้เป็นอย่างดี

2.1.4.1 บทบาทของเทคโนโลยีสารสนเทศเพื่อการศึกษา

การเรียนการสอนในปัจจุบันเราจัดในห้องเรียนมีครู-อาจารย์ เป็นผู้ถ่ายทอดความรู้แต่แนวโน้มของการปฏิรูปการศึกษาในอนาคตเน้นให้ผู้เรียนเป็นผู้ที่สามารถคิดเป็นทำเป็น (Con structive) ผู้เรียนเป็นศูนย์กลางของการเรียนรู้และเป็นองค์ความรู้ (Knowledge Body) ที่จะต้องได้รับการส่งเสริมให้พัฒนาได้เต็มศักยภาพที่แตกต่างกันของบุคคล (Individualdifferent) ครูจะกลายมามีบทบาทในการให้ความช่วยเหลือแนะนำ (Facilitator) ใน

การเรียนการสอน ดังนั้นด้วยในคุณสมบัติที่ดีของศึกษาระบบเทคโนโลยีสารสนเทศ ทำให้สามารถสร้างห้องเรียนทางอิเล็กทรอนิกส์ (e-Classroom) และการจัดการศึกษาแบบ e-Education ซึ่งสามารถออกแบบ หลักสูตร เนื้อหา กระบวนการเรียนการสอนและบทเรียนที่บรรจุข้อมูล ทั้งตัวอักษรและรูปภาพให้ผู้เรียนลงทะเบียนเข้ามาศึกษาได้และสามารถประเมินผลได้ด้วยตนเองหลังจากเรียนจบแต่ละหน่วย การเรียนและยังจะมีโอกาสฝึกฝนจนรู้จริงซึ่งขึ้นอยู่กับการออกแบบบทเรียนโดยนักออกแบบการเรียนการสอน (InstructionalDesigner) ซึ่งจะเป็นครูผู้เชี่ยวชาญพิเศษในยุคอนาคตที่สามารถจัดการเรียนรู้ ในรูปแบบ e-Learning นั่นเอง

ฉัตรชัย เรืองมณี (2550) [Online] กล่าวว่า ด้วยความเจริญก้าวหน้าทางด้านเทคโนโลยีสารสนเทศ และ Internet ทำให้การเผยแพร่และแลกเปลี่ยนข้อมูลสารสนเทศ เป็นไปด้วยความสะดวกและรวดเร็วกว้างขวางอย่างไร้พรมแดน ความรู้และการศึกษาเป็นสากล ภูมิปัญญาไทยโดยเฉพาะอย่างยิ่ง ด้านศิลปะ วัฒนธรรม ประเพณี สามารถทำเสนอเผยแพร่บน Websiteใดก็ได้เป็นการประกาศศักยภาพของความเป็นไทยให้กระจายไปทั่วโลกได้ในพริบตาแต่ในขณะเดียวกันก็ต้องตระหนักในการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและ Intetnet เพื่อการพัฒนาการศึกษาศิลปวัฒนธรรม และเศรษฐกิจ สังคม การเมืองของเราอย่างชาญฉลาดด้วยจึงจะทำให้สามารถ ใช้เทคโนโลยีสารสนเทศได้อย่างเกิดประสิทธิภาพ สูงสุดต่อการพัฒนาการศึกษาฯ ของประเทศในยุคปัจจุบันนี้

2.1.5 ลักษณะสำคัญของเทคโนโลยีสารสนเทศ

คณะบริหารธุรกิจ มหาวิทยาลัยพายัพ. (2547) [Online] กล่าวว่า โดยพื้นฐานของเทคโนโลยีย่อมมีประโยชน์ต่อการพัฒนาประเทศชาติให้เจริญก้าวหน้าได้ แต่เทคโนโลยีสารสนเทศเป็นเรื่องที่เกี่ยวข้องกับวิถีความเป็นอยู่ของสังคมสมัยใหม่อยู่มาก ลักษณะเด่นที่สำคัญของเทคโนโลยีสารสนเทศมีดังนี้

2.1.5.1 เทคโนโลยีสารสนเทศช่วยเพิ่มผลผลิต ลดต้นทุน และเพิ่มประสิทธิภาพในการทำงาน

ในการประกอบการทางด้านเศรษฐกิจ การค้า และการอุตสาหกรรม จำเป็นต้องหาวิธีในการเพิ่มผลผลิต ลดต้นทุน และเพิ่มประสิทธิภาพในการทำงานคอมพิวเตอร์และระบบสื่อสารเข้ามา ช่วยทำให้เกิดระบบอัตโนมัติ เราสามารถฝากถอนเงินสดผ่านเครื่องเอทีเอ็มได้ตลอดเวลา ธนาคารสามารถให้บริการได้ดีขึ้น ทำให้การบริการโดยรวมมีประสิทธิภาพ ในระบบการจัดการทุกแห่งต้องใช้ข้อมูลเพื่อการดำเนินการและการตัดสินใจ ระบบธุรกิจจึงใช้ เ ค รื่ อ ง มื อ เหล่านี้ช่วยในการทำงาน เช่น ใช้ในระบบจัดเก็บเงินสด จองตั๋วเครื่องบิน เป็นต้น

2.1.5.2 เทคโนโลยีสารสนเทศเปลี่ยนรูปแบบการบริการเป็นแบบกระจาย

เมื่อมีการพัฒนาระบบข้อมูล และการใช้ข้อมูลได้ดี การบริการต่าง ๆ จึงเน้นรูปแบบการบริการแบบกระจายผู้ใช้สามารถสั่งซื้อสินค้าจากที่บ้าน สามารถสอบถามข้อมูลผ่านทางโทรศัพท์ นิสิตนักศึกษาบางมหาวิทยาลัยสามารถใช้คอมพิวเตอร์สอบถามผลสอบจากที่บ้านได้

2.1.5.3 เทคโนโลยีสารสนเทศเป็นสิ่งที่จำเป็นสำหรับการดำเนินการในหน่วยงานต่างๆ

ปัจจุบันทุกหน่วยงานต่างพัฒนาระบบรวบรวมจัดเก็บข้อมูลเพื่อใช้ในองค์การประเทศไทยมีระบบทะเบียนราษฎร์ที่จัดทำด้วยระบบ ระบบเวชระเบียนในโรงพยาบาล ระบบการจัดเก็บข้อมูลภาษีในองค์การทุกระดับเห็นความสำคัญที่จะนำเทคโนโลยีสารสนเทศมาใช้

2.1.5.4 เทคโนโลยีสารสนเทศเกี่ยวข้องกับคนทุกระดับ

พัฒนาการด้านเทคโนโลยีสารสนเทศ ทำให้ชีวิตความเป็นอยู่ของคนเกี่ยวข้องกับเทคโนโลยี ดังจะเห็นได้จาก การพิมพ์ด้วยคอมพิวเตอร์ การใช้ตารางคำนวณ และใช้อุปกรณ์สื่อสารโทรคมนาคมแบบต่าง ๆ เป็นต้น

2.1.6 ผลของเทคโนโลยีสารสนเทศ

คณะบริหารธุรกิจ มหาวิทยาลัยพายัพ (2547) [Online] กล่าวว่า การกำเนิดของคอมพิวเตอร์เมื่อประมาณห้าสิบกว่าปีที่แล้ว เป็นก้าวสำคัญที่นำไปสู่ยุคสารสนเทศ ในช่วงแรกมีการนำเอาคอมพิวเตอร์มาใช้เป็นเครื่องคำนวณ แต่ต่อมาได้มีความพยายามพัฒนาให้คอมพิวเตอร์เป็นอุปกรณ์สำคัญสำหรับการจัดการข้อมูล เมื่อเทคโนโลยีอิเล็กทรอนิกส์ได้ก้าวหน้ามากขึ้น ทำให้สามารถสร้างคอมพิวเตอร์ที่มีขนาดเล็กลง แต่ประสิทธิภาพสูงขึ้น สภาพการใช้งานจึงใช้งานกันอย่างแพร่หลาย ผลของเทคโนโลยีสารสนเทศที่มีต่อชีวิตความเป็นอยู่และสังคมจึงมีมาก มีการเรียนรู้และใช้สารสนเทศกันอย่างกว้างขวาง ผลของเทคโนโลยีสารสนเทศโดยรวมกล่าวได้ดังนี้

2.1.6.1 การสร้างเสริมคุณภาพชีวิตที่ดีขึ้น สภาพความเป็นอยู่ของสังคมเมือง มีการพัฒนาใช้ระบบสื่อสารโทรคมนาคม เพื่อติดต่อสื่อสารให้สะดวกขึ้น มีการประยุกต์มาใช้กับเครื่องอำนวยความสะดวกภายในบ้าน เช่น ใช้ควบคุมเครื่องปรับอากาศ ใช้ควบคุมระบบไฟฟ้าภายในบ้าน เป็นต้น

2.1.6.2 เสริมสร้างความเท่าเทียมในสังคมและการกระจายโอกาส เทคโนโลยีสารสนเทศทำให้เกิดการกระจายไปทั่วทุกหนแห่ง แม้แต่ถิ่นทุรกันดาร ทำให้มีการกระจายโอกาสการเรียนรู้ มีการใช้ระบบการเรียนการสอนทางไกล การกระจายการเรียนรู้ไปยังถิ่นห่างไกล นอกจากนี้ในปัจจุบันมีความพยายามที่ใช้ระบบการรักษาพยาบาลผ่านเครือข่ายสื่อสาร

2.1.6.3 สารสนเทศกับการเรียนการสอนในโรงเรียน การเรียนการสอนในโรงเรียนมีการนำคอมพิวเตอร์และเครื่องมือประกอบช่วยในการเรียนรู้ เช่น วีทีทัศน์ เครื่องฉายภาพ

คอมพิวเตอร์ช่วยสอน คอมพิวเตอร์ช่วยจัดการศึกษา จัดตารางสอน คำนวณระดับคะแนน จัดชั้นเรียน ทำรายงานเพื่อให้ผู้บริหารได้ทราบถึงปัญหาและการแก้ปัญหาในโรงเรียน ปัจจุบันมีการเรียนการสอนทางด้านเทคโนโลยีสารสนเทศในโรงเรียนมากขึ้น

2.1.6.4 เทคโนโลยีสารสนเทศกับสิ่งแวดล้อม การจัดการทรัพยากรธรรมชาติหลายอย่างจำเป็นต้องใช้สารสนเทศ เช่น การดูแลรักษาป่า จำเป็นต้องใช้ข้อมูล มีการใช้ภาพถ่ายดาวเทียมการติดตามข้อมูลสภาพอากาศ การพยากรณ์อากาศ การจำลองรูปแบบสภาวะสิ่งแวดล้อมเพื่อปรับปรุงแก้ไข การเก็บรวมรวมข้อมูลคุณภาพน้ำในแม่น้ำต่าง ๆ การตรวจวัดมลภาวะ ตลอดจนการใช้ระบบการตรวจวัดระยะไกลมาช่วย ที่เรียกว่าโทรมาตร เป็นต้น

2.1.6.5 เทคโนโลยีสารสนเทศกับการป้องกันประเทศ กิจการทางด้านการทหารมีการใช้เทคโนโลยี อาวุธยุทโธปกรณ์สมัยใหม่ล้วนแต่เกี่ยวข้องกับคอมพิวเตอร์และระบบควบคุม มีการใช้ระบบป้องกันภัย ระบบเฝ้าระวังที่มีคอมพิวเตอร์ควบคุมการทำงาน

2.1.6.6 การผลิตในอุตสาหกรรม และการพาณิชยกรรม การแข่งขันทางด้านการผลิตสินค้าอุตสาหกรรมจำเป็นต้องหาวิธีการในการผลิตให้ได้มาก ราคาถูกลงเทคโนโลยีคอมพิวเตอร์เข้ามามีบทบาทมาก มีการใช้ข้อมูลข่าวสารเพื่อการบริหารและการจัดการ การดำเนินการและยังรวมไปถึงการให้บริการกับลูกค้า เพื่อให้ซื้อสินค้าได้สะดวกขึ้น

2.2 มาตรฐานเกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ISO/IEC 17799 (BS7799)

2.2.1 BS7799 (British Standard 7799)

จักรกฤษณ์ แร่ทอง (2547) [Online] กล่าวว่า เป็นมาตรฐานเกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ที่ออกโดย British Standards Institution ซึ่งถูกตีพิมพ์ครั้งแรกในเดือนเมษายน ค.ศ. 1991 โดยใช้ชื่อว่า BS7799:1999 มาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization)ต่อมาในเดือนตุลาคมปี ค.ศ.2000 ได้มีการปรับปรุงบางส่วนของมาตรฐาน และถูกตีพิมพ์เป็นครั้งที่ 2 ภายใต้ชื่อ ISO/IEC17799:2000 ในวันที่ 1 ธันวาคม ค.ศ. 2000 มาตรฐานนี้ถูกกำหนดขึ้นมาเพื่อเป็นแนวทางในการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยการกำหนดแนวทางสำหรับการพัฒนามาตรฐานความปลอดภัย และการปฏิบัติงานเพื่อให้เกิดการจัดการที่มีประสิทธิภาพ รวมไปถึงการสร้างความมั่นใจในการติดต่อระหว่างองค์กร เนื่องจากข้อมูลถือเป็นสินทรัพย์ที่มีความสำคัญเช่นเดียวกับสินทรัพย์ทางธุรกิจอื่นๆ ดังนั้นการรักษาความปลอดภัยข้อมูล,การประเมินและการบริหารความเสี่ยงที่เกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ หากกล่าวถึงความปลอดภัยข้อมูล จะต้องประกอบด้วย 3 องค์ประกอบ ดังนี้

2.2.1.1 ความลับ (Confidentiality) ในการรักษาความปลอดภัยข้อมูล สิ่งสำคัญที่ต้องคำนึงคือ สิทธิ์ในการเข้าถึงข้อมูลต่างๆ ในระบบงาน ดังนั้นผู้ที่จะสามารถเข้าถึงข้อมูลในระบบนั้น ๆ ได้ จะต้องได้รับการกำหนดสิทธิ์ในการเข้าใช้ ซึ่งเป็นไปตามหลัก need-to-know และ need-to-do basis ตัวอย่างเช่น ในการจัดการเกี่ยวกับข้อมูลเงินเดือนของพนักงานในองค์กร ก็จะมีเจ้าหน้าที่ของฝ่ายทรัพยากรบุคคลเท่านั้นที่จะสามารถเข้าถึงข้อมูลนี้ได้ เพราะข้อมูลดังกล่าวเป็นข้อมูลสำคัญและไม่สามารถเปิดเผยได้

2.2.1.2 ความมั่นคง (Integrity) ข้อมูลต่าง ๆ ในระบบจะต้องมีความถูกต้อง เช่น ข้อมูลที่เผยแพร่ทางอินเตอร์เน็ต ซึ่งเป็นข้อมูลที่ไม่ได้จำกัดสิทธิ์ในการเข้าถึง จึงส่งผลให้บุคคลภายนอกสามารถเข้าถึงข้อมูลดังกล่าวได้อย่างง่ายดาย ดังนั้นจะต้องมีการกำหนดมาตรการหรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลเพื่อป้องกันความผิดพลาดหรือการบิดเบือนข้อมูลหรือแม้กระทั่งผู้ที่มีสิทธิ์เข้าถึงระบบงานเพื่อทำการแก้ไขข้อมูลก็จะต้องได้รับการอนุมัติจากผู้บังคับบัญชาก่อน เช่น เจ้าหน้าที่ที่ทำการแก้ไขข้อมูล ดอกเบี้ยเงินฝากต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น

2.2.1.3 การใช้งาน(Availability) ผู้มีสิทธิ์สามารถที่จะเข้าถึงข้อมูลในระบบงานต่าง ๆ ได้ตามต้องการ โดยผ่านช่องทางที่องค์กรกำหนด เช่น เจ้าหน้าที่ที่มีสิทธิ์ในการเข้าถึงระบบซื้อขายหลักทรัพย์ของธนาคารสามารถเข้าใช้ข้อมูลในช่วงเวลาที่ต้องการได้อย่างต่อเนื่องโดยไม่เกิดเหตุขัดข้อง เช่น ระบบฐานข้อมูลมีปัญหา ไม่สามารถดึงข้อมูลออกมาได้

2.2.2 องค์ประกอบของมาตรฐาน ISO/IEC 17799 (BS7799):2000 First Edition

NECTEC (2547) [Online] กล่าวว่า สำหรับองค์ประกอบของมาตรฐานนี้ประกอบด้วย สิ่งจำเป็นสำหรับการเริ่มต้นสร้างมาตรฐานความมั่นคงปลอดภัยให้กับองค์กรในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ซึ่งแบ่งเป็น 10 หัวข้อดังนี้

2.2.2.1 นโยบายความมั่นคงปลอดภัยขององค์กร

2.2.2.2 โครงสร้างความมั่นคงปลอดภัยภายในองค์กร

2.2.2.3 การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร

2.2.2.4 มาตรฐานของบุคลากรเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร

2.2.2.5 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร

2.2.2.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

2.2.2.7 การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร

2.2.2.8 การพัฒนาและดูแลระบบสารสนเทศ

2.2.2.9 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

2.2.2.10 การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบาย

ปริญญา หอมอเนก (2548) [Online] กล่าวว่า มาตรฐาน ISO/IEC 17799 First Edition ถูกประกาศอย่างเป็นทางการในวันที่ 1 ธันวาคม ค.ศ. 2000 ประกอบด้วยหัวข้อใหญ่ๆ ของแนวทางที่องค์กรควรนำไปปฏิบัติเพื่อความปลอดภัยขององค์กร ทั้งหมด 10 หัวข้อ ล่าสุด ISO/IEC ได้ออกมาตรฐาน ISO/IEC 17799 Second Edition ฉบับปรับปรุงแก้ไข เพิ่มเติม ประกาศใช้ในวันที่ 15 มิถุนายน ค.ศ. 2005 มีการเพิ่มเติมหัวข้อใหม่ อีก 2 หัวข้อ เพิ่มเติมจาก First Edition

หัวข้อแรก เรื่อง Risk Assessment และ Risk Treatment คือ การประเมินความเสี่ยงและการบริหารจัดการเพื่อที่จะลดความเสี่ยงที่อาจเกิดขึ้นกับระบบ หัวข้อที่สองที่เพิ่มขึ้นมาจากมาตรฐาน ISO/IEC17799 First Edition ได้แก่ เรื่อง Information Security Incident Management คือ การเตรียมพร้อมรับเหตุการณ์ไม่คาดฝันที่อาจเกิดขึ้นกับระบบสารสนเทศ เช่น ระบบเกิดล่มโดยไม่ทราบสาเหตุองค์กรควรมีการเตรียมพร้อมรับเหตุการณ์ที่เกิดขึ้นในมาตรฐาน ISO/IEC 17799 Second Edition กล่าวถึง การรวบรวมเหตุการณ์ต่าง ๆ ที่เกิดขึ้นเกี่ยวกับระบบสารสนเทศอย่างเป็นระบบเพื่อรายงานให้กับผู้บริหารและการสร้างรายงานเพื่อแสดงให้เห็นถึงช่องโหว่ด้านการรักษาความปลอดภัย (Security Weakness) ของระบบสารสนเทศ อย่างสม่ำเสมอเมื่อมีเหตุการณ์เกี่ยวกับเรื่องความปลอดภัยเกิดขึ้นควรจะมีกระบวนการรองรับ (Incident Response Process) มีการกำหนดผู้รับชอบให้ชัดเจน นอกจากนี้มาตรฐาน ISO/IEC 17799 Second Edition ยังกล่าวถึงการเรียนรู้จากเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในอดีต เพื่อเป็นประสบการณ์และพัฒนาความรู้ และยังกล่าวถึงการเก็บหลักฐานอย่างเป็นระบบเพื่อการพิสูจน์หลักฐานทางด้านเทคนิคด้วยวิธี Digital Forensic จากหน่วยงานทางกฎหมายที่มีหน้าที่ด้านนี้โดยตรง เช่น กรมสอบสวนคดีพิเศษ เป็นต้น

นอกจากนี้ในมาตรฐาน ISO/IEC 17799 Second Edition ได้มีการแก้ไขชื่อหัวข้อให้แตกต่างจากมาตรฐาน ISO/IEC 17799 First Edition ได้แก่ หัวข้อ Personal Security เปลี่ยนเป็น Human Resource Security หัวข้อ Physical Security เปลี่ยนเป็น Physical and Environment Security และ หัวข้อ System Development and Maintenance เปลี่ยนเป็น Information System Acquisition , Development and Maintenance

บทความนี้มีจุดประสงค์เพื่อแสดงให้เห็นถึงความแตกต่างระหว่างมาตรฐาน ISO 17799 เวอร์ชันปี 2000 กับ ISO 17799 เวอร์ชันปี 2005 ที่เป็นเวอร์ชั่นภาษาอังกฤษ ว่ามีการแก้ไขปรับปรุงอย่างไร หลังจากประกาศใช้มาเป็นเวลาเกือบ 5 ปีแล้ว การแก้ไข ปรับปรุงดังกล่าวจัดทำโดยผู้เชี่ยวชาญในด้านความมั่นคงปลอดภัยจากหลายภูมิภาคทั่วโลกสำหรับภูมิภาคเอเชียแปซิฟิก มีการจัดประชุมกลุ่มย่อยชื่อว่า Regional Asia InformationSecurity Standards หรือ RAISS Forum ซึ่งจัดขึ้นเมื่อวันที่ 27-28 มิถุนายน 2548 ณ ประเทศสิงคโปร์เนื่องจากการประชุมดังกล่าวมีสาระสำคัญต่อภารกิจด้านความมั่นคงปลอดภัย ดังนั้น ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

จึงได้พิจารณาส่งผู้เชี่ยวชาญไปร่วมประชุม ในฐานะสมาชิกของกลุ่มความร่วมมือในภูมิภาคเอเชียแปซิฟิก และในการประชุมดังกล่าวผู้เชี่ยวชาญที่เป็นแกนนำหลักในการจัดทำมาตรฐาน ISO 17799 นี้ ได้แก่ Mr.Ted Humphreys และ Dr.Angelika Plate ได้มาบรรยายเกี่ยวกับเนื้อหาของ ISO 17799:2005 ที่ได้รับการปรับปรุง แก้ไข เพิ่มเติมดังรูปที่2.2 ซึ่งโครงการ ThaiCERTเห็นว่าเนื้อหาดังกล่าวเป็นประโยชน์อย่างยิ่งสำหรับผู้ที่ได้ติดตามเกี่ยวกับมาตรฐานความมั่นคงปลอดภัยในระดับสากล จึงแปลและเรียบเรียงเผยแพร่เป็นเอกสารฉบับนี้ขึ้น NECTEC(2548)[Online]

รูปที่ 2.2 แสดงหัวข้อในมาตรฐาน ISO 17799 เปรียบเทียบระหว่างเวอร์ชั่นเก่าและใหม่

แสดงจำนวนหัวข้อสำหรับเวอร์ชั่นเดิมปี 2000 (ทางซ้ายมือ) ซึ่งมีด้วยกันทั้งหมด 10 หัวข้อ และมี 11 หัวข้อ (สำหรับเวอร์ชั่นใหม่ปี 2005) หัวข้อที่เพิ่มขึ้นมาใหม่คือ หัวข้อ Information Security Incident Management

2.3 ข้อกำหนดและนโยบายด้านปลอดภัยของ ISO 17799:2005

2.3.1. นโยบายความมั่นคงปลอดภัย (Security policy)

2.3.1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการ ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

(1) เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information Security Policy Document) (ผู้บริหารองค์กร)ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร อย่างเป็นลายลักษณ์อักษรเอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่กี่ยวข้องได้รับทราบ

(2) การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

2.3.2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

2.3.2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)

มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

(1) การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทาง ด้านความมั่นคงปลอดภัย (Management Commitment to Information Security) (ผู้บริหารองค์กร)ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร การเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

(2) การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information Security Coordination) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับ

สารสนเทศขององค์กรโดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

(3) การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of Information Security Responsibilities)(ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

(4) กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ(Authorization Process for Information Processing Facilities)(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

(5) การลงนามมิให้เปิดเผยความลับขององค์กร (ConfidentialityAgreements)(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

(6) การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น(Contact with Authorities) (ผู้บริหารสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ.กสท. โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

(7) การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน(Contact with Special Interest Groups)(ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆที่มีความสนใจเป็นพิเศษในเรื่องเดียวกันกลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศหรือสมาคมต่างๆในอุตสาหกรรมที่องค์กรมีส่วนร่วม

(8) การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent Review of Information Security) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

2.3.2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึงถูกประมวลผลหรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

(1) การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก(Identification of Risks Related to External Parties) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

(2) การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security When Dealing With Customers) (หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

(3) การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing Security in Third Party Agreements) (หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.3.3 การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

2.3.3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for Assets)

มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

(1) การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

(2) การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets) (หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน

(3) การใช้งานทรัพย์สินที่เหมาะสม (Acceptable Use of Assets) (หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น

2.3.3.2 การจัดหมวดหมู่สารสนเทศ (Information Classification)

มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

(1) การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification Guidelines) (หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

(2) การจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศ (Information Labeling and Handling)(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

2.3.4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

2.3.4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษา อุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

(1) การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and Responsibilities)(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงานผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์ กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความ มั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

(2) การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณี

การจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคล หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึงประกอบการคัดเลือกด้วย

(3) การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญาและการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

2.3.4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During Employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบาย ความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

(1) หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management Responsibilities) (ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

(2) การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information Security Awareness, Education ,and Training) (หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกได้รับการอบรมเพื่อสร้างความตระหนัก และเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กร ตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

(3) กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืน หรือละเมิดนโยบาย หรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

2.3.4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

(1) การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination Responsibilities) (หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

(2) การคืนทรัพย์สินขององค์กร (Return of Assets) (หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

(3) การถอดถอนสิทธิในการเข้าถึง (Removal of Access Rights) (หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

2.3.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

2.3.5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตการก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

(1) การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter) (หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุมตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

(2) การควบคุมการเข้า-ออก (Physical Entry Controls) (หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

(3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms and Facilities) (หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ

(4) การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting Againstexternal and Environmental Threats) (หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัย

คุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหวการระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

(5) การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย(Working in Secure Areas)(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงาน ในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

(6) การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมาต่างหาก

2.3.5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมยหรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

(1) การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)(พนักงาน)ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

(2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรองระบบสายสื่อสารสำรอง เป็นต้น

(3) การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) (หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดย ไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้น เสียหาย

(4) การบำรุงรักษาอุปกรณ์ (Equipment maintenance) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

(5) การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment Off-Premises) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น

(6) การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

(7) การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Property)(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

2.3.6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)

2.3.6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

(1) ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงานปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

(2) การควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change Management)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

(3) การแบ่งหน้า ที่ความรับผิดชอบ (Segregation of Duties) (ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิด ชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

(4) การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Test, and Operational Facilities) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนาการทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

2.3.6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)

มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

(1) การให้บริการโดยหน่วยงานภายนอก (Service Delivery)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ

(2) การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and Review of Third Party Services)(หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการการศึกษาจากรายงานและข้อมูลต่างๆที่กำหนดให้บันทึกไว้ เป็นต้น

(3) การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing Changes to Third Party Services)(ผู้บริหารสารสนเทศ) ต้องกำหนด ให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยการเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อกาดำเนินงานของผู้ให้บริการจากภายนอก

2.3.6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

(1) การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity Management) (หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่ เหมาะสมและเพียงพอต่อการใช้งาน

(2) การตรวจรับระบบ (System Acceptance)(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติมหรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

2.3.6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code)

มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

(1) การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls Against Malicious Code)(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีรวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

(2) การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls Against Mobile Code)(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วย ความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

2.3.6.5 การสำรองข้อมูล (Back-up)

มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

(1) การสำรองข้อมูล (Information Back-up)(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

2.3.6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network Security Management)

มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือค่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

(1) มาตรการทางเครือข่าย (Network Controls) (ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่ายและดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่ายรวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

(2) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก

2.3.6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)

มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

(1) การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

(2) การกำจัดสื่อบันทึกข้อมูล(Disposal of Media) (หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

(3) ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ(Information Handling Procedures)(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

(4) การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation)(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of Information)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

(1) นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures)(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงาน ภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

(2) ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) (หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร

(3) การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical Media in Transit)(หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำ ให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

(4) การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) (หัวหน้างานสารสนเทศ)ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

(5) ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

2.3.6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Services)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

(1) การพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกงการปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(2) การทำธุรกรรมออนไลน์(On-line Transactions) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

(3) สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available information) (ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

2.3.6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

(1) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

(2) การตรวจสอบการใช้งานระบบ (Monitoring SystemUse) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

(3) การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of Log Information) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือ

เหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

(4) บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

(5) การบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

(6) การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock Synchronization) (ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

2.3.7. การควบคุมการเข้าถึง (Access Control)

2.3.7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ

(1) นโยบายการควบคุมการเข้าถึงระบบ (Access Control Policy) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

2.3.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(1) การลงทะเบียนพนักงาน (User Registration) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

(2) การบริหารจัดการสิทธิการใช้งานระบบ (Privilege Management) (ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

(3) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)(ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

(4) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

2.3.7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

(1) การใช้งานรหัสผ่าน (Password Use)(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

(2) การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended User Equipment)(พนักงาน) ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

(3) นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย(Clear Desk and Clear Screen Policy)(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

2.3.7.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

(1) นโยบายการใช้งานบริการเครือข่าย (Policy On Use of Network Services)(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

(2) การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections) (ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(3) การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)(ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือ สถานที่ที่ได้รับอนุญาตแล้ว

(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)(ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

(5) การแบ่งแยกเครือข่าย (Segregation in Networks) (ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) (ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรการเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางธุรกิจได้ระบุไว้

(7) การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network Routing Control)(ผู้ดูแลระบบ) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

2.3.7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(1) ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on Procedures)(ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

(2) การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User Identification and Authentication)(ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

(3) ระบบบริหารจัดการรหัสผ่าน (Password Management System) (ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

(4) การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) (ผู้ดูแลระบบ) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

(5) การหมดเวลาการใช้งานระบบสารสนเทศ (Session Time-Out) (ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) (ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

2.3.7.6 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอปพลิเคชันโดยไม่ได้รับอนุญาต

(1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) (ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

(2) การแยกระบบสารสนเทศที่มีความสำคัญสูง(Sensitive Systen. Isolation) (หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

2.3.7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

(1) การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communications)(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

(2) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) (ผู้บริหารสนเทศ) ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

2.3.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance)

2.3.8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

(1) การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements Analysis and Specification) (ผู้พัฒนาและผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

2.3.8.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (Correct Processing in Applications)

มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์

(1) การตรวจสอบข้อมูลนำเข้า (Input Data Validation)(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอปพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป

(2) การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing)(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุ จากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

(3) การตรวจสอบความถูกต้องของข้อความ (Message Integrity) (ผู้พัฒนาระบบ) ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

(4) การตรวจสอบข้อมูลนำออก(Output Data Validation) (ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอปพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

2.3.8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic Controls)

มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล

(1) นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy On the Use of Cryptographic Controls) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร

(2) การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร

2.3.8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of System Files)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้ บริการ

(1) การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of Perational Software) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติหรือไม่สามารถใช้งานได้

(2) การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of System test Data)(ผู้พัฒนาระบบ) ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือ ข้อมูลสำคัญ

(3) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ(Access Control to Program Source Code)(หัวหน้างานสารสนเทศ) ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

2.3.8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and Support Processes)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

(1) ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change Control Procedures)(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติหรือไม่สามารถใช้งานได้

(2) การตรวจสอบการทำงานของแอปพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ(Technical Review of Applications After Operating System

Changes)(ผู้ดูแลระบบ) ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอปพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้นทำงานผิดปกติไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

(3) การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on Changes to Software Packages)(หัวหน้างานสารสนเทศ) ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

(4) การป้องกันการรั่วไหลของสารสนเทศ (Information Leakage) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กรหรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหล ออกไป

(5) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

2.3.8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

(1) มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of Technical Vulnerabilities)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้ง กำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

2.3.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

2.3.9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses)

มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

(1) การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events) (พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่

เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

(2) การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting Security Weaknesses)(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

2.3.9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

(1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) (หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

(2) การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Security Incidents)(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัยโดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

(3) การเก็บรวบรวมหลักฐาน (Collection of Evidence)(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

2.3.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

2.3.10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร(Information Security Aspects of Business Continuity Management)

มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

(1) กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including Information Security in the Business Continuity Management Process)(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอกระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

(2) การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity and Risk Assessment)(หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัย สำหรับสารสนเทศขององค์กร

(3) การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and Implementing Continuity Plans Including Information Security) (ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

(4) การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity Planning framework)(ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆที่ต้องดำเนินการ

(5) การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing Maintaining and Re-Assessing Business Continuity Plans)(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

2.3.11. การปฏิบัติตามข้อกำหนด (Compliance)

2.3.11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements)

มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

(1) การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of Applicable Legislation)(หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมายทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอก อื่น)ที่เกี่ยวข้อง

กับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

(2) การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual Property Rights(IPR))(หัวหน้างานนิติการ) ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย

(3) การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of Organizational Records) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญาและข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

(4) การป้องกันข้อมูลส่วนตัว (Data Protection and Privacy of Personal Information)(หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมายระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง

(5) การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)(หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

(6) การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือต้องสอดคล้องกับข้อตกลงกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

2.3.11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with Security Policies and Standards, and TechnicalCompliance)

มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

(1) การปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

(2) การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technicalcompliance Checking)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอเพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

2.3.11.3 การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations)

มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

(1) มาตรการการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls) (หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน

(2) การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of Information Systems Audit Tools)(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

2.4 สถานศึกษาของคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

ประกอบไปด้วยสถานศึกษาจำนวนทั้งสิ้น 21 แห่งดังนี้

1. วิทยาลัยเทคนิคมีนบุรี
2. วิทยาลัยเทคนิคกาญจนาภิเษกมหานคร
3. วิทยาลัยพณิชยการบางนา
4. วิทยาลัยพณิชยการอินทราชัย
5. วิทยาลัยสารพัดช่างพระนคร
6. วิทยาลัยบริหารธุรกิจและการท่องเที่ยวกรุงเทพ
7. วิทยาลัยอาชีวศึกษาเอี่ยมละออ
8. วิทยาลัยศิลปหัตถกรรมกรุงเทพ
9. วิทยาลัยสารพัดช่างสี่พระยา
10. วิทยาลัยการอาชีพนวมินทราชูทิศ
11. วิทยาลัยการอาชีพกาญจนาภิเษกหนองจอก

12. วิทยาลัยเทคนิคราชสิทธาราม

13 วิทยาลัยเทคนิคดอนเมือง

14. วิทยาลัยเทคนิคดุสิต

15. กาญจนาภิเษกวิทยาลัยช่างทองหลวง

16. วิทยาลัยพณิชยการธนบุรี

17. วิทยาลัยพณิชยการเชตุพน

18. วิทยาลัยอาชีวศึกษาเสาวภา

19. วิทยาลัยอาชีวศึกษาธนบุรี

20. วิทยาลัยสารพัดช่างธนบุรี

21. วิทยาลัยสารพัดช่างนครหลวง

2.5 งานวิจัยที่เกี่ยวข้อง

ประวิทย์ คงฉาวรนันต์ (2550 : 161-170) โดยทำการศึกษาวิจัยเรื่อง ศักยภาพการแข่งขันของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์ด้วยระบบบริหารคุณภาพ ISO/TS16949 ในด้านกิจกรรมหลักในส่วนของโลจีสติกส์ขาเข้า กระบวนการผลิตและโลจีสติกส์ขาออกและในด้านกิจกรรมสนับสนุนในส่วนของโครงสร้างพื้นฐานขององค์กรเปรียบเทียบศักยภาพการแข่งขันของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์ตามรูปแบบระบบการบริหารการผลิต เปรียบเทียบศักยภาพการแข่งขันของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์ตามเหตุผลในการใช้ระบบการบริหารการผลิต ความสัมพันธ์ของศักยภาพการแข่งขันของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์ในด้านกิจกรรมสนับสนุนกับกิจกรรมหลัก

ศักยภาพการแข่งขันของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์อยู่ในระดับค่อนข้างสูงทั้งในด้านกิจกรรมหลักในส่วนของโลจีสติกส์ขาเข้ากระบวนการผลิตและโลจีสติกส์ขาออกและในด้านกิจกรรมสนับสนุนในส่วนของโครงสร้างพื้นฐานขององค์กร

ผลการเปรียบเทียบรูปแบบระบบการบริหารการผลิตต่างกันมีผลต่อศักยภาพการแข่งขันแตกต่างกัน ในด้านกิจกรรมหลักในส่วนของโลจีสติกส์ขาเข้ากระบวนการผลิตและโลจีสติกส์ขาออก และในด้านกิจกรรมสนับสนุนในส่วนของโครงสร้างพื้นฐานขององค์กร

ผลการเปรียบเทียบ เหตุผลในการใช้ระบบการบริหารการผลิตต่างกันมีผลต่อศักยภาพการแข่งขันแตกต่างกัน เฉพาะในด้านกิจกรรมหลักในส่วนของกระบวนการผลิตเท่านั้น

ความสัมพันธ์ระหว่างศักยภาพการแข่งขันในด้านกิจกรรมสนับสนุนขององค์กรและศักยภาพการแข่งขันในด้านกิจกรรมหลักพบว่า ศักยภาพการแข่งขันในด้านกิจกรรมสนับสนุนใน

ส่วนของโครงสร้างพื้นฐานขององค์กรมีความสัมพันธ์เชิงบวกกับศักยภาพการแข่งขันในด้านกิจกรรมหลัก

กรุณา เพียรวิชา (2550 : 149-166) ทำการศึกษาวิจัยเรื่องการศึกษาปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทย โดยมีวัตถุประสงค์ดังนี้ ศึกษาถึงระดับความคิดเห็นของผู้บริหารที่มีต่อปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000ในประเทศไทย ทั้ง 7 ประเภทได้แก่ การขาดงานของพนักงาน อุบัติเหตุในการทำงานของพนักงานความเชื่องช้าในการทำงานของพนักงาน การลาออกของพนักงาน การซ่อมบำรุงเครื่องจักรคุณภาพสินค้าต่ำกว่ามาตรฐาน การผลิตต่ำกว่ามาตรฐาน เปรียบเทียบความคิดเห็นของผู้บริหารที่มีต่อปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทย จากผลของการศึกษาวิจัยพบว่า

ระดับความคิดเห็นของผู้บริหารต่อปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลิตในด้านการซ่อมบำรุง ผู้บริหารให้ความสำคัญอยู่ในระดับมาก ส่วนปัจจัยในด้านคุณภาพสินค้าต่ำกว่ามาตรฐาน ความเชื่องช้าในการทำงานของพนักงาน อุบัติเหตุในการทำงานของพนักงาน การผลิตต่ำกว่ามาตรฐาน การขาดงานของพนักงาน การลาออกของพนักงาน ผู้บริหารให้ความสำคัญอยู่ในระดับปานกลาง

ผู้บริหารที่มีเพศ อายุ ระดับการศึกษา แตกต่างกันมีความคิดเห็นต่อปัจจัยที่เป็นตัวขัดขวางต่อการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทย ไม่แตกต่างกัน ส่วนผู้บริหารที่มีประสบการณ์ทำงานที่แตกต่างกันมีความคิดเห็นต่อปัจจัยที่เป็นตัวขัดขวางต่อการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทย แตกต่างกัน

ก้องเกียรติ ผลพิบูลสุนทร (2550 :104-117) ทำการศึกษาวิจัยเรื่องการศึกษาปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทยโดยการศึกษาวิจัยครั้งนี้มีวุตถุประสงค์ เพื่อศึกษาระดับความรู้และระดับเจตคติของพนักงาน ศึกษาอิทธิพลของปัจจัยส่วนบุคคลได้แก่ เพศ อายุ อายุงาน ระดับการศึกษา ตำแหน่งงาน และการได้รับการอบรมที่มีผลต่อความรู้และเจตคติ และศึกษาความสัมพันธ์ระหว่างความรู้และเจตคติของพนักงานที่มีต่อระบบการบริหารคุณภาพ ISO/TS 16949 ในกลุ่มอุตสาหกรรมผู้ผลิตชิ้นส่วนรถยนต์ ผลการวิจัยพบว่า

ด้านความรู้พนักงานในกลุ่มอุตสาหกรรมผู้ผลิตชิ้นส่วนรถยนต์ในนิคมอุตสาหกรรมบางปู ส่วนใหญ่มีระดับความรู้เกี่ยวกับระบบการบริหารคุณภาพ ISO/TS 16949 อยู่ในระดับมาก

ด้านเจตคติพนักงานในกลุ่มอุตสาหกรรมผู้ผลิตชิ้นส่วนรถยนต์ ในนิคมอุตสาหกรรม

บางปู ที่มีต่อระบบการบริหารคุณภาพ ISO/TS 16949 ในภาพรวมพบว่า มีเจตคติอยู่ในระดับเห็นด้วยมาก

ผลการเปรียบเทียบความรู้เกี่ยวกับระบบการบริหารคุณภาพ ISO/TS 16949 เมื่อพิจารณาปัจจัยส่วนบุคคลของพนักงานในกลุ่มอุตสาหกรรมผู้ผลิตชิ้นส่วนรถยนต์ ในนิคมอุตสาหกรรมบางปู พบว่า เพศ อายุ และอายุงาน เป็นปัจจัยที่มีผลทำให้ความรู้ของพนักงานไม่แตกต่างกัน ส่วนระดับการศึกษา และตำแหน่งงาน เป็นปัจจัยที่มีผลทำให้ความรู้ของพนักงานแตกต่างกัน

ผลการเปรียบเทียบเจตคติที่มีต่อระบบการบริหารคุณภาพ ISO/TS 16949 โดยแยกเป็นรายด้านต่างๆ ตามปัจจัยส่วนบุคคล พบว่า เพศต่างกัน มีผลทำให้เจตคติในด้านสภาพแวดล้อมภายในองค์การแตกต่างกัน อายุ มีผลทำให้เจตคติในด้านปัจจัยภายนอกองค์การแตกต่างกัน อายุงานมีผลทำให้เจตคติในด้านการบริหารจัดการแตกต่างกันและมีผลทำให้เจตคติในด้านปัจจัยภายนอกองค์การ แตกต่างกัน ระดับการศึกษา มีผลทำให้เจตคติในด้านการบริหารทรัพยากรบุคคลแตกต่างกัน และด้านงบประมาณ แตกต่างกัน ตำแหน่งงาน มีผลทำให้เจตคติในด้านการบริหารทรัพยากรบุคคล ด้านงบประมาณ และด้านสภาพแวดล้อมภายในองค์การ แตกต่างกัน การได้รับการอบรม มีผลทำให้เจตคติในด้านการบริหารจัดการ แตกต่างกัน

ความสัมพันธ์ระหว่างความรู้และเจตคติที่มีต่อระบบการบริหารคุณภาพ ISO/TS 16949 พบว่าความรู้เกี่ยวกับระบบการบริหารคุณภาพ ISO/TS 16949 ไม่มีความสัมพันธ์กันกับเจตคติที่มีต่อระบบการบริหารคุณภาพ ISO/TS 16949

มงคล พูนเพชรรัตน์ (2549 : 63-70) ได้ศึกษางานวิจัยเรื่องความรู้และระดับเจตคติที่มีต่อระบบมาตรฐาน ISO 14001 ของพนักงานปฏิบัติการในอุตสาหกรรมเครื่องปรับอากาศเพื่อการส่งออกครั้งนี้มีวัตถุประสงค์ เพื่อศึกษาระดับความรู้และระดับเจตคติที่มีต่อระบบมาตรฐาน ISO 14001 ของพนักงานปฏิบัติการในอุตสาหกรรมเครื่องปรับอากาศเพื่อการส่งออกเพื่อศึกษาเปรียบเทียบปัจจัยส่วนบุคคลที่มีต่อความรู้ต่อระบบมาตรฐาน ISO 14001 ของพนักงานปฏิบัติการในอุตสาหกรรมเครื่องปรับอากาศเพื่อการส่งออก ผลการวิจัยพบว่า

ระดับความรู้ต่อระบบมาตรฐาน ISO 14001 มีระดับสูงสุด ระดับเจตคติต่อระบบมาตรฐาน ISO 14001 มีระดับสูง ปัจจัยส่วนบุคคลทางด้านความแตกต่างทางด้านเพศ อายุ และระดับการศึกษามีผลต่อระดับความรู้ต่อระบบมาตรฐาน ISO 14001 อย่างมีนัยสำคัญทางสถิติ ปัจจัยส่วนบุคคลทางด้านความแตกต่างทางด้านระดับการศึกษา ประสบการณ์การทำงาน และฝ่ายที่สังกัด มีผลต่อระดับเจตคติต่อระบบมาตรฐาน ISO 14001 อย่างมีนัยสำคัญทางสถิติ ความสัมพันธ์ระหว่างระดับความรู้และเจตคติต่อระบบมาตรฐาน ISO 14001 มีความสัมพันธ์ในเชิงบวกอย่างมีนัยสำคัญทางสถิติ

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงสำรวจซึ่งมีวัตถุประสงค์ในการวิจัยเพื่อทำการศึกษาเกี่ยวกับความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยเทียบจากมาตรฐาน ISO 17799:2005 เนื่องจากปัจจัยเหล่านี้มีผลโดยตรงต่อความปลอดภัยในระบบสารสนเทศ ผู้วิจัยมีวิธีดำเนินการวิจัย ตามลำดับดังต่อไปนี้

3.1 ประชากร

3.2 เครื่องมือที่ใช้ในการวิจัย

3.3 การเก็บและรวบรวมข้อมูล

3.4 การวิเคราะห์ข้อมูล

3.1 ประชากร

ประชากรที่ใช้ในการศึกษาได้แก่ บุคลากรที่เกี่ยวข้องกับระบบสารสนเทศของสถานศึกษาในแต่ละสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง มีจำนวนทั้งสิ้นจำนวน 204 คน ประกอบด้วยบุคลากรกลุ่มต่างๆ รายละเอียดดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 แสดงจำนวนประชากรในแต่ละกลุ่มต่อ 1 สถานศึกษา

กลุ่ม	ประชากรต่อ 1 สถานศึกษา
1. ผู้บริหารองค์กร	1
2. ผู้บริหารสารสนเทศ	1
3. ผู้ดูแลระบบและผู้พัฒนาระบบ	1
4. หัวหน้างานสารสนเทศ	1
5. หัวหน้างานบุคคล	1
6. หัวหน้างานอาคาร	1
7. หัวหน้างานธุรการ	1
8. หัวหน้างานพัสดุ	1

ตารางที่ 3.1 (ต่อ)

กลุ่ม	ประชากรต่อ 1 สถานศึกษา
9. หัวหน้างานนิติการ	1 *
10. พนักงาน	1
รวม	**10**

*** หมายเหตุ สถานศึกษาบางแห่งไม่มีบุคคลากรในกลุ่มนี้**

3.2 เครื่องมือที่ใช้ในการวิจัย

3.2.1 ลักษณะเครื่องมือ

เครื่องมือที่ใช้ในการวิจัยครั้งนี้คือ แบบสอบถามที่ศึกษาปัจจัยเกี่ยวกับความปลอดภัยในระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยเทียบจากมาตรฐาน ISO 17799 : 2005 แบบสอบถามจะแบ่งเป็น 10 ชุด ได้แก่ ชุดของผู้บริหารองค์กร ผู้บริหารสารสนเทศ ผู้ดูแลระบบและผู้พัฒนาระบบ หัวหน้างานสารสนเทศ หัวหน้างานบุคคล หัวหน้างานอาคาร หัวหน้างานธุรการ หัวหน้างานพัสดุ หัวหน้างานนิติการและชุดของพนักงาน รวม 10 ชุดละ 3 ตอน โดยผู้วิจัยได้ทำการพัฒนาขึ้นมีลักษณะดังนี้

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนทั่วไปของผู้ตอบแบบสอบถามมีลักษณะเป็นแบบสำรวจรายการ (Check List) สอบถามเกี่ยวกับเพศ อายุ วุฒิการศึกษา และประสบการณ์ทำงาน จำนวน 4 ข้อ

ตอนที่ 2 เป็นคำถามเกี่ยวกับนโยบายด้านความปลอดภัยในระบบสารสนเทศ ตามมาตรฐาน ISO 17799 : 2005 ซึ่งเป็นแบบเลือกตอบ 2 ตัวเลือกคือ มี และไม่มี จำนวน 133 ข้อ นับเป็น 133 คะแนน

ตอบว่ามี แสดงว่าผู้ตอบแบบสอบถามสามารถปฏิบัติได้ตามข้อกำหนด จะได้คะแนน 1 คะแนน

ตอบว่าไม่มี แสดงว่าผู้ตอบแบบสอบถามไม่สามารถปฏิบัติได้ตามข้อกำหนด จะได้คะแนน 0 คะแนน

ตอนที่ 3 แบบสอบถามเกี่ยวกับข้อเสนอแนะ เกี่ยวกับมาตรฐาน ISO 17799:2005 ลักษณะของแบบสอบถามเป็นแบบปลายเปิด ให้ผู้ตอบเขียนได้อย่างอิสระ

3.2.2 การสร้างเครื่องมือที่ใช้ในการวิจัย

ในการสร้างเครื่องมือที่ใช้ในการวิจัย ผู้วิจัยได้ดำเนินการดังต่อไปนี้

1. ศึกษาทฤษฎี เอกสาร ตำรา และงานวิจัยที่เกี่ยวข้องกับงานวิจัยในครั้งนี้

2. ศึกษาวิธีการสร้างแบบสอบถามจากตำราและงานวิจัยที่เกี่ยวข้อง

3. กำหนดประเด็นและขอบข่ายของคำถามให้สอดคล้องกับวัตถุประสงค์ของงานวิจัย

4. สร้างแบบสอบถามฉบับร่าง แล้วนำแบบสอบถามที่สร้างขึ้นไปเสนออาจารย์ที่ปรึกษาวิทยานิพนธ์เพื่อตรวจสอบและแนะนำเพื่อการแก้ไขรวมทั้งปรับปรุงแบบสอบถามให้มีความเหมาะสมทั้งความครอบคลุมเนื้อหาและภาษาที่ใช้แล้วจัดพิมพ์

5. ผู้วิจัยนำแบบสอบถามที่ได้รับการปรับปรุงแล้ว ขอความอนุเคราะห์ผู้ทรงคุณวุฒิตรวจสอบความเที่ยงตรง ความเหมาะสม และความถูกต้องชัดเจนของภาษาที่ใช้ในแบบสอบถาม ซึ่งผู้ทรงคุณวุฒิทั้ง 3 ท่าน ประกอบด้วย

ตารางที่ 3.2 แสดงรายชื่อ ตำแหน่ง และสถานที่ปฏิบัติงานของผู้ทรงคุณวุฒิ

รายชื่อ	ตำแหน่ง	สถานที่ปฏิบัติงาน
ผศ.ดร.ฉันทนา วิริยเวชกุล	อาจารย์ประจำ คณะครุศาสตร์อุตสาหกรรม	คณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
นายสมณธร พุ่มพิมล	ครู คศ2. วิทยฐานะชำนาญการ	แผนกวิชาเทคโนโลยีโทรคมนาคม วิทยาลัยการอาชีพนวมินทราชูทิศ
นายรุ่งนิรันดร์ ผดุงพิทักษ์ชน	Assistant Technical Director	IT Consultant Division Universal Communication Systems Co.,Ltd

6. ผู้วิจัยนำแบบสอบถามที่ผู้ทรงคุณวุฒิเสนอแนะ มาปรับปรุงแก้ไข และนำเสนออาจารย์ที่ปรึกษาวิทยานิพนธ์อีกครั้งเพื่อแก้ไขให้ถูกต้อง เหมาะสมแล้วจัดพิมพ์

3.3 การเก็บรวบรวมข้อมูล

1. ขอหนังสือจากหน่วยงานบัณฑิตศึกษา คณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณลาดกระบัง ถึงผู้บริหารของแต่ละสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

2. นำแบบสอบถามที่ได้รับการตรวจสอบคุณภาพ พร้อมหนังสือขออนุญาตเก็บรวบรวมข้อมูลไปเก็บรวบรวมข้อมูลกับ บุคคลากรที่เกี่ยวข้องของในแต่ละสถานศึกษาของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร ทั้ง 21 แห่ง จำนวน 204 คน

3. นำแบบสอบถามที่ได้รับคืนจากการสำรวจที่สมบูรณ์แล้วทั้งสิ้น 204 ฉบับ คิดเป็นร้อยละ 100 ไปวิเคราะห์ข้อมูล

3.4 การวิเคราะห์ข้อมูล

ผู้วิจัยได้ดำเนินการวิเคราะห์ข้อมูลแบบสอบถามเรื่องความปลอดภัยในเครือข่ายสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยมาดำเนินการวิเคราะห์หาค่าความถี่ ร้อยละ

ร้อยละ (Percent) (พรรณี ลีกิจวัฒนะ. 2549)

$$pct = \frac{Ni}{Nt} \times 100$$

Pct หมายถึง ร้อยละ

Ni หมายถึง จำนวนส่วนย่อย

Nt หมายถึง จำนวนส่วนใหญ่

บทที่ 4
ผลการวิเคราะห์ข้อมูล

ผลการวิเคราะห์ข้อมูลในการวิจัยเรื่อง ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยเทียบจากมาตรฐาน ISO 17799:2005 ผู้วิจัยขอนำเสนอผลการวิเคราะห์ข้อมูลโดยแบ่งเป็น 3 ตอน ดังนี้

4.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

4.2 ผลการวิเคราะห์ข้อมูลนโยบายด้านความปลอดภัยในระบบสารสนเทศตามมาตรฐาน ISO 17799: 2005

4.3 ผลการวิเคราะห์ข้อเสนอแนะเกี่ยวกับมาตรฐาน ISO 17799:2005

4.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามมีลักษณะ เป็นแบบสำรวจรายการ (Check List) สอบถามเกี่ยวกับเพศ อายุ วุฒิการศึกษา และประสบการณ์ทำงาน วิเคราะห์ข้อมูลโดยวิธีการหา ความถี่ และ ร้อยละ ดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

รายการข้อมูลทั่วไป	จำนวน (N =204)	ร้อยละ
1. เพศ		
- ชาย	97	47.55
- หญิง	107	52.45
รวม	**204**	**100**
2. อายุ		
- น้อยกว่า 30 ปี	19	9.31
- 30 – 35 ปี	43	21.08
- 36 – 40 ปี	27	13.24
- มากกว่า 40 ปี	115	56.37
รวม	**204**	**100**

ตารางที่ 4.1 (ต่อ)

รายการข้อมูลทั่วไป	จำนวน (N =204)	ร้อยละ
3. ระดับการศึกษา		
- ต่ำกว่าปริญญาตรี	6	2.94
- ปริญญาตรี	83	40.69
- สูงกว่าปริญญาตรี	115	56.37
รวม	**204**	**100**
4. ประสบการณ์ทำงานด้านคอมพิวเตอร์ และเทคโนโลยีสารสนเทศ		
- น้อยกว่า 5 ปี	44	21.57
- 5 – 10 ปี	72	35.29
- มากกว่า 10 ปี	88	43.14
รวม	**204**	**100**
5. กลุ่มบุคลากร		
- ผู้บริหารองค์กร	21	10.29
- ผู้บริหารสารสนเทศ	21	10.29
- ผู้ดูแลระบบและผู้พัฒนาระบบ	21	10.29
- หัวหน้างานสารสนเทศ	21	10.29
- หัวหน้างานอาคาร	21	10.29
- หัวหน้างานพัสดุ	21	10.29
- หัวหน้างานบุคคล	21	10.29
- หัวหน้างานนิติการ	15	7.39
- หัวหน้างานธุรการ	21	10.29
- พนักงาน	21	10.29
รวม	**204**	**100**

จากตารางที่ 4.1แสดงบุคลากรในสถานศึกษาสังกัดสำนักงานคณะกรรมการอาชีวศึกษาที่ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิงจำนวนร้อยละ52.45 และเป็นเพศชายจำนวนร้อยละ 47.55

อายุส่วนใหญ่จะมากกว่า 40 ปี คิดเป็นร้อยละ 56.37 รองลงมาจะอยู่ในช่วง 30-35 ปี คิดเป็นร้อยละ21.08 ผู้มีอายุในช่วง 36-40 ปี คิดเป็นร้อยละ 13.24 และช่วงอายุที่น้อยที่สุดคือช่วงอายุที่น้อยกว่า 30 ปี คิดเป็นร้อยละ 9.31

ระดับการศึกษาของบุคลากรนั้นส่วนใหญ่จะสูงกว่าระดับปริญญาตรี คิดเป็นร้อยละ 56.37 รองลงมาคือระดับปริญญาตรี คิดเป็นร้อยละ 40.69 และต่ำกว่าระดับปริญญาตรีจะมีอยู่น้อยที่สุด หรือคิดเป็นร้อยละ 2.94

ด้านประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ นั้นผู้ที่มีมากกว่า 10 ปีนั้น คิดเป็นร้อยละ 43.14 ซึ่งถือว่ามากที่สุด รองลงมาจะอยู่ในช่วง 5-10 ปี มีอยู่ ร้อยละ 35.29 และที่น้อยกว่า 5 ปีนั้นคิดเป็นร้อยละ 21.57

กลุ่มบุคลากรจะเป็นระดับผู้บริหารองค์กรจำนวน 21 คน คิดเป็นร้อยละ 10.29 ผู้บริหารสารสนเทศจำนวน 21 คน คิดเป็นร้อยละ 10.29 ผู้ดูแลระบบและผู้พัฒนาระบบจำนวน 21คน คิดเป็นร้อยละ 10.29 หัวหน้างานสารสนเทศจำนวน 21 คน คิดเป็นร้อยละ 10.29 หัวหน้างานอาคาร จำนวน 21 คน คิดเป็นร้อยละ 10.29 หัวหน้างานพัสดุจำนวน 21 คน คิดเป็นร้อยละ 10.29 หัวหน้างานบุคคลจำนวน 21 คน คิดเป็นร้อยละ 10.29 หัวหน้างานนิติการจำนวน 15 คน คิดเป็นร้อยละ 7.39 หัวหน้างานธุรการจำนวน 21 คน คิดเป็นร้อยละ 10.29 และพนักงานจำนวน 21 คน คิดเป็นร้อยละ 10.29

4.2 ผลการวิเคราะห์ข้อมูลนโยบายด้านความปลอดภัยในระบบสารสนเทศตามมาตรฐาน ISO 17799: 2005

ผลการวิเคราะห์ข้อมูลนโยบายด้านความปลอดภัยในระบบสารสนเทศ ตามมาตรฐาน ISO 17799 : 2005 ซึ่งเป็นแบบเลือกตอบ 2 ตัวเลือกคือ มี และไม่มี จำนวน 11 รายการหลัก 133 ข้อย่อย วิเคราะห์ข้อมูลโดยวิธีการหาค่า ความถี่ ร้อยละ ดังแสดงในตารางที่ 4.2

ตารางที่ 4.2 จำนวนและสถานศึกษาที่ผ่านเกณฑ์และไม่ผ่านเกณฑ์ด้านความปลอดภัยในระบบสารสนเทศจำแนกตามรายการมาตรฐาน ISO 17799 : 2005

รายการมาตรฐาน ISO 17799:2005	สถานศึกษา			
	ผ่านเกณฑ์		ไม่ผ่านเกณฑ์	
	จำนวน	ร้อยละ	จำนวน	ร้อยละ
1. นโยบายความมั่นคงปลอดภัย	17	80.95	4	19.05
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร	1	4.76	20	95.24
3. การบริหารจัดการทรัพย์สินขององค์กร	11	52.38	10	47.62
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร	3	14.29	18	85.71

ตารางที่ 4.2 (ต่อ)

รายการมาตรฐาน ISO 17799:2005	สถานศึกษา			
	ผ่านเกณฑ์		ไม่ผ่านเกณฑ์	
	จำนวน	ร้อยละ	จำนวน	ร้อยละ
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	4	19.05	17	80.95
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร	1	4.76	20	95.24
7. การควบคุมการเข้าถึง	4	19.05	17	80.95
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	4	19.05	17	80.95
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร	5	23.81	16	76.19
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร	7	33.33	14	66.67
11. การปฏิบัติตามข้อกำหนด	3	14.29	18	85.71
รวมรายการมาตรฐาน ISO 17799:2005	**60**	**25.97**	**171**	**74.03**

จากตารางที่ 4.2 แสดงผลการวิเคราะห์ข้อมูลส่วนนโยบายด้านความปลอดภัยในระบบสารสนเทศตามมาตรฐาน ISO 17799: 2005 ครอบคลุมทั้ง 11 รายการหลักโดย

ด้านนโยบายความมั่นคงปลอดภัย ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 17 แห่ง คิดเป็นร้อยละ 80.9 และ ไม่ผ่านเกณฑ์ จำนวน 4 แห่ง คิดเป็นร้อยละ 19.05

ด้านโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 1 แห่ง คิดเป็นร้อยละ 4.76 ไม่ผ่านเกณฑ์ จำนวน 20 แห่ง คิดเป็นร้อยละ 95.24

ด้านการบริหารจัดการทรัพย์สินขององค์กร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 11 แห่ง คิดเป็นร้อยละ 52.38 ไม่ผ่านเกณฑ์ จำนวน 10 แห่ง คิดเป็นร้อยละ 47.62

ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 3 แห่ง คิดเป็นร้อยละ 14.29 ไม่ผ่านเกณฑ์ จำนวน 18 แห่ง คิดเป็นร้อยละ 85.71

ด้านการ สร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์จำนวน 4 แห่ง คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์ จำนวน 17 แห่ง คิดเป็นร้อยละ 80.95

ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 1 แห่ง คิดเป็นร้อยละ 4.76 ไม่ผ่านเกณฑ์ จำนวน 20 แห่ง คิดเป็นร้อยละ 95.24

ด้านการควบคุมการเข้า ถึง ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ผ่านเกณฑ์ จำนวน 4 แห่ง คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์จำนวน 17 แห่ง คิดเป็นร้อยละ 80.95

ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 4 แห่ง คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์ จำนวน 17 แห่ง คิดเป็นร้อยละ 80.95

ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 5 แห่ง คิดเป็นร้อยละ 23.81 ไม่ผ่านเกณฑ์ จำนวน 16 แห่ง คิดเป็นร้อยละ 76.19

ด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 7 แห่ง คิดเป็นร้อยละ 33.33 ไม่ผ่านเกณฑ์ จำนวน 14 แห่ง คิดเป็นร้อยละ 66.67

ด้านการปฏิบัติตามข้อกำหนด ในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาที่ ผ่านเกณฑ์ จำนวน 3 แห่ง คิดเป็นร้อยละ 14.29 ไม่ผ่านเกณฑ์ จำนวน 18 แห่ง คิดเป็นร้อยละ 85.71

ตารางที่ 4.3 จำนวนข้อที่สถานศึกษาผ่านเกณฑ์มาตรฐานด้านความปลอดภัยของระบบสารสนเทศแต่ละรายการจำแนกตามสถานศึกษา

รายการข้อกำหนด ISO 17799:2005	จำนวนข้อ	สถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1. นโยบายความมั่นคงปลอดภัย	2	2	2	2	2	1	2	2	2	2	2	2	1	0	2	2	2	2	1	2	2	2
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร	11	9	9	9	8	6	10	11	8	10	10	10	9	9	4	5	9	8	9	8	10	8
3. การบริหารจัดการทรัพย์สินขององค์กร	5	4	5	4	4	5	5	5	5	4	2	5	5	5	5	3	5	5	3	2	4	4
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร	9	7	6	6	4	2	8	9	4	8	5	9	6	7	6	5	8	9	8	6	5	7
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	12	9	11	12	9	4	9	12	13	13	6	11	4	10	12	5	13	13	10	10	9	11
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร	32	20	27	23	11	17	19	32	31	30	25	28	23	30	21	7	30	30	12	30	28	29
7. การควบคุมการเข้าถึง	25	22	17	11	15	23	24	25	25	25	21	21	19	20	16	8	22	18	20	23	21	25
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	16	8	13	9	3	10	9	16	16	16	12	14	11	13	6	2	15	10	9	15	14	16
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร	5	4	2	4	2	3	5	4	4	3	5	4	5	3	2	1	5	5	4	4	4	4
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร	5	1	5	4	4	1	4	5	4	5	5	5	4	2	0	1	5	3	4	4	3	5
11. การปฏิบัติตามข้อกำหนด	10	4	5	6	6	6	6	10	9	9	6	5	7	10	0	2	10	9	8	5	7	6
รวม	**133**	**90**	**102**	**90**	**68**	**78**	**101**	**131**	**121**	**125**	**99**	**114**	**94**	**109**	**74**	**41**	**124**	**112**	**88**	**109**	**107**	**117**

จากตารางที่ 4.3 ผลสรุปการจัดเก็บแบบสอบถามของสถานศึกษา 21 แห่งพบว่า

สถานศึกษาที่ 1 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 2 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 2 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย และด้านการบริหารจัดการทรัพย์สินขององค์กร

สถานศึกษาที่ 3 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 4 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 5 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านการบริหารจัดการทรัพย์สินขององค์กร

สถานศึกษาที่ 6 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 3 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการทรัพย์สินขององค์กร และด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

สถานศึกษาที่ 7 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 9 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย , ด้านโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร, ด้านการบริหารจัดการทรัพย์สินขององค์กร , ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร , ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร , ด้านการควบคุมการเข้าถึง , ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ , ด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร และด้านการปฏิบัติตามข้อกำหนด

สถานศึกษาที่ 8 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 5 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการทรัพย์สินขององค์กร, ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม, ด้านการควบคุมการเข้าถึง และด้านการจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

สถานศึกษาที่ 9 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 5 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม , ด้านการควบคุมการเข้าถึง , ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ และด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

สถานศึกษาที่ 10 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 3 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

สถานศึกษาที่ 11 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 4 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการทรัพย์สินขององค์กร, ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร และด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

สถานศึกษาที่ 12 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 2 ด้านคือ ด้านการบริหารจัดการทรัพย์สินขององค์กร และด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

สถานศึกษาที่ 13 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 2 ด้านคือ ด้านการบริหารจัดการทรัพย์สินขององค์กร และด้านการปฏิบัติตามข้อกำหนด

สถานศึกษาที่ 14 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 2 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย และด้านการบริหารจัดการทรัพย์สินขององค์กร

สถานศึกษาที่ 15 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 16 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 6 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการทรัพย์สินขององค์กร, ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม, ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร, ด้านการบริหารความต่อ เนื่องในการดำเนินงานขององค์กร และด้านการปฏิบัติตามข้อกำหนด

สถานศึกษาที่ 17 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 4 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการบริหารจัดการทรัพย์สินขององค์กร, ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม และด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

สถานศึกษาที่ 18 ไม่คะแนนในด้านใดที่สามารถผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005

สถานศึกษาที่ 19 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 20 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 1 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย

สถานศึกษาที่ 21 ผ่านเกณฑ์ตามมาตรฐาน ISO 17799:2005 จำนวน 3 ด้านคือ ด้านนโยบายความมั่นคงปลอดภัย, ด้านการควบคุมการเข้าถึง และด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

4.3 ผลการวิเคราะห์ข้อเสนอแนะเกี่ยวกับมาตรฐาน ISO 17799:2005

ผลการวิเคราะห์ข้อเสนอแนะเกี่ยวกับมาตรฐาน ISO 17799:2005 จากบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษา มีดังนี้

เรื่องของ ISO 17799:2005 นี้มีประโยชน์มากสำหรับการนำมาเป็นนโยบายในการบริหารการจัดการเกี่ยวกับระบบสารสนเทศของสถานศึกษาแต่ทางด้านบุคลากรเองนั้น มีความต้องการในเรื่องของการจัดอบรมพื้นฐานในด้านความรู้ความเข้าใจเกี่ยวกับระบบ ISO 17799:2005 ทั้งในด้านการนำไปใช้งานได้จริง และการให้ความรู้อย่างต่อเนื่องและสม่ำเสมอ เนื่องมาจากเทคโนโลยีด้านสารสนเทศในปัจจุบันนั้นมีความเปลี่ยนแปลงไปอย่างรวดเร็วตามสภาวะและเศรษฐกิจของโลกในยุค ปัจจุบัน จึงมีความประสงค์ที่จะให้มีเป็นนโยบายในการจัดฝึกอบรมเจ้าหน้าที่ในส่วนงานที่เกี่ยวข้อง ให้มีความรู้ใหม่ๆ ตามเทคโนโลยีที่เกิดขึ้นอย่างสม่ำเสมอ เพื่อให้เกิดความปลอดภัยในระบบสารสนเทศของทางสำนักงานคณะกรรมการการอาชีวศึกษาได้ อย่างมีประสิทธิภาพสูงสุดต่อไป

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาวิจัยเรื่อง ความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร ผู้วิจัยสรุปผลการวิจัย อภิปรายผลและข้อเสนอแนะได้ดังนี้

5.1 สรุปผลการวิจัย

5.1.1 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาการจัดการด้านความปลอดภัยในระบบสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร

5.1.2 ประชากร

ประชากรที่ใช้ในการศึกษาได้แก่ บุคลากรที่เกี่ยวข้องกับสถานศึกษาในแต่ละสถานศึกษาของสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง มีจำนวนทั้งสิ้นจำนวน 204 คน

5.1.3 เครื่องที่ใช้ในงานวิจัย

เครื่องมือที่ใช้ในการวิจัยครั้งนี้คือ แบบสอบถามที่ศึกษาเกี่ยวกับความปลอดภัยในระบบสารสนเทศของสถานศึกษาของสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยเทียบจากมาตรฐาน ISO 17799 : 2005 แบบสอบถามจะแบ่งเป็น 10 ชุด ได้แก่ ชุดของผู้บริหารองค์กร ผู้บริหารสารสนเทศ ผู้ดูแลระบบและผู้พัฒนาระบบ หัวหน้างานสารสนเทศ หัวหน้างานบุคคล หัวหน้างานอาคาร หัวหน้างานธุรการ หัวหน้างานพัสดุ หัวหน้างานนิติการและชุดของพนักงาน รวม 10 ชุดๆละ 3 ตอน โดยนำแบบสอบถามที่ได้รับการปรับปรุงแล้ว ขอความอนุเคราะห์ผู้ทรงคุณวุฒิตรวจสอบความเที่ยงตรง ความเหมาะสม และความถูกต้องชัดเจนของภาษาที่ใช้ในแบบสอบถาม

5.1.4 การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลทางผู้วิจัยได้ส่งแบบสอบถามไปด้วยกัน 2 วิธี คือการส่งแบบสอบถามด้วยตัวเอง และส่งแบบสอบถามทางไปรษณีย์ แบบสอบถามสามารถเก็บคืนได้ครบทุกชุด มีเพียงบางชุดที่ไม่มีบุคลากรที่รับผิดชอบดูแลก็จะไม่มีการตอบแบบสอบถาม โดยทางเจ้าหน้าที่จะทำการระบุไว้ที่หน้าแรกของแบบสอบถามว่าไม่มีผู้รับผิดชอบ

5.1.5 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูล ผู้วิจัยได้ดำเนินการวิเคราะห์ข้อมูลจากผู้ตอบแบบสอบถามเรื่อง ความปลอดภัยในเครือข่ายสารสนเทศของสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร โดยมาดำเนินการวิเคราะห์หาค่าจำนวน และ ร้อยละ

5.1.6 ผลการวิจัย

ผลการวิจัยพบว่าสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง ไม่มีสถานศึกษาแห่งใดในเขตกรุงเทพมหานคร ที่สามารถผ่านมาตรฐานความปลอดภัยในระบบสารสนเทศ ISO17799: 2005 เมื่อพิจารณาสามารถสรุปได้ดังนี้

1. นโยบายความมั่นคงปลอดภัย ผ่านเกณฑ์ คิดเป็นร้อยละ 80.9 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 19.05

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร ผ่านเกณฑ์ คิดเป็นร้อยละ 4.76 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 95.24

3. การบริหารจัดการทรัพย์สินขององค์กร ผ่านเกณฑ์ คิดเป็นร้อยละ 52.38 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 47.62

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ผ่านเกณฑ์ คิดเป็นร้อยละ 14.29 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 85.71

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ผ่านเกณฑ์ คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 80.95

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร ผ่านเกณฑ์ คิดเป็นร้อยละ 4.76 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 95.24

7. การควบคุมการเข้า ถึง ผ่านเกณฑ์ คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 80.95

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ ผ่านเกณฑ์ คิดเป็นร้อยละ 19.05 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 80.95

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร ผ่านเกณฑ์ คิดเป็นร้อยละ 23.81 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 76.19

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร ผ่านเกณฑ์ คิดเป็นร้อยละ 33.33 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 66.67

11. การปฏิบัติตามข้อกำหนด ผ่านเกณฑ์ คิดเป็นร้อยละ 14.29 ไม่ผ่านเกณฑ์ คิดเป็นร้อยละ 85.71

สรุปภาพรวมของรายการมาตรฐาน ISO 17799:2005 ของสถานศึกษาสังกัดสำนักงานคณะ กรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครทั้ง 21 แห่ง ผ่านบางเกณฑ์คิดเป็น

ร้อยละ 25.97 ไม่ผ่าน บางเกณฑ์คิดเป็นร้อยละ 74.03 จากภาพรวมสรุปได้ว่าสถานศึกษาทั้งหมดไม่ผ่านเกณฑ์ของมาตรฐาน ISO 17799:2005 เนื่องจาก ISO 17799:2005 นั้นจะต้องผ่านเกณฑ์ทั้งหมด 11 ข้อใหญ่ หรือ 133 ข้อย่อย เท่านั้น หรือคิดเป็น 100 % จึงจะผ่านข้อกำหนด

5.2 อภิปรายผล

จากผลการวิจัยที่ออกมาจะเห็นได้ว่าสถาน ศึกษาต่างๆของทางสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานครนั้น ผลที่แสดงสรุปได้ว่าสถานศึกษาทั้งหมดไม่ผ่านเกณฑ์ของมาตรฐาน ISO 17799:2005 เนื่องจากอาจจะมีอุปสรรค์ใน ด้านการประสานงานในการดำเนินการเพื่อที่จะนำนโยบายไปใช้งานจริง เนื่องจากความปลอดภัยในระบบสารสนเทศนั้นจะต้องได้รับความร่วมมือจากบุคลากรที่เกี่ยวข้องกันทั่วทั้งองค์กรจึงอาจจะเกิดปัญหาเรื่องการสื่อสารและความรู้ความเข้าใจที่จะต้องเป็นไปในทิศทางเดียวกันทั้งหมดซึ่ง ยอดเยี่ยม เหล่านนท์ชัย (2551) [Online] กล่าวไว้ว่าสถาบันต่างๆสามารถปฏิบัติตามมาตรฐานด้านความปลอดภัย จะต้องได้รับความร่วมมือจากผู้บริหารระดับสูง จึงจะสามารถปฏิบัติได้ตามข้อกำหนด

เมื่อพิจารณาในสถานศึกษาที่ผ่านเกณฑ์สูงสุดคือข้อที่ 1. ว่าด้วยนโยบายความมั่นคงปลอดภัยเป็นรายการที่มีสถานศึกษาผ่านเกณฑ์สูงสุด คือร้อยละ 80.95 แสดงว่าผู้บริหารของแต่ละสถานศึกษามีนโยบายด้านความมั่นคงปลอดภัย ที่ชัดเจนแต่เมื่อมองถึงรายการในด้านอื่นๆนั้นออกมาต่ำมากๆเมื่อเทียบกัน เช่น ข้อที่ 2.เรื่องโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร และข้อที่ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร โดยมีสถานศึกษาที่ผ่านเกณฑ์ในระดับต่ำหรือเพียง ร้อยละ 4.76 เท่านั้น และมีตัวเลขบ่งชี้ได้ว่า สถานศึกษาของสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร นั้นมีนโยบายด้านความมั่นคงที่ดี แต่บุคลากรที่เกี่ยวข้องในแต่ละด้านของแต่ละสถานศึกษานั้นไม่สามารถนำไปใช้ ในการปฏิบัติงานได้ ดังข้อที่ 11. ที่ว่าด้วยเรื่องของการปฏิบัติตามข้อกำหนดนั้นมีสถานศึกษาผ่านเกณฑ์เพียงร้อยละ 14.29 แสดงให้เห็นว่าไม่สามารถนำนโยบายที่มีไปปฏิบัติตามข้อกำหนดได้

5.3 ข้อเสนอแนะ

5.3.1 ข้อเสนอแนะในการนำผลการวิจัยไปใช้งาน

5.3.1.1 ผลจากการวิจัยในครั้งนี้ทำให้ทางสำนักงานคณะกรรมการการอาชีวศึกษาสามารถเห็นถึงข้อบกพร่องต่างๆในการปฏิบัติตามเกณฑ์มาตรฐาน ISO17799:2005 เป็นข้อๆ ได้อย่างเฉพาะเจาะจงเพื่อการนำไปปรับใช้และแก้ปัญหาในด้านต่างๆได้ตรงจุด

5.3.1.2 เพื่อการนำไปสู่ความปลอดภัยของระบบสารสนเทศของทางสำนักงานคณะ กรรมการการอาชีวศึกษาที่สมบูรณ์และมีประสิทธิภาพนั้นจึงสมควรอย่างยิ่งที่จะมีการจัดอบรมและพัฒนาทักษะของบุคลากรที่มีส่วนเกี่ยวข้องในงานด้านสารสนเทศตามมาตรฐานกลางทางด้านความปลอดภัยที่ทั่วโลกยอมรับอย่างต่อเนื่องและสม่ำเสมอจึงจะทำให้เกิดความเสี่ยงจากภัยคุกคามต่างๆ ให้ลดลงได้และจะทำให้สามารถใช้งานระบบสารสนเทศได้เกิดประโยชน์สูงสุดต่อไป

5.3.2 ข้อเสนอแนะในการวิจัยครั้งต่อไป

หลังจากการจัดทำนโยบายด้านความปลอดภัยในระบบสารสนเทศ ตามมาตรฐาน ISO 17799 : 2005ไปแล้วนั้นจะทำให้ทราบว่ามีความบกพร่องในระบบสารสนเทศขององค์กรที่จุดใดบ้าง และสามารถเข้าไปแก้ปัญหาที่จุดนั้นๆได้ตรงจุด และควรหากรรมวิธีในการแก้ปัญหาของจุดบกพร่องนั้นๆที่พบ

โดยทางผู้วิจัยมีข้อเสนอแนะให้ใช้มาตรฐานหรือกระบวนการอื่นๆเข้ามาใช้งานร่วมกัน เช่น ISO/IEC27001:2005 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่างๆ กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO หลักการของการออกแบบโครงสร้างระบบ ISO/IEC27001:2005 จะใช้ อ้างอิง รูปแบบ PDCA Model (Plan Do Check Action) ซึ่งเป็นโครงสร้างเดียวกับ ระบบ การบริหารที่เป็นสากลที่ใช้กันทั่วโลก เข้ามาช่วยในการบริหารจัดการ

บรรณานุกรม

กรุณา เพียรวิชา .2550. "การศึกษาปัจจัยที่เป็นตัวขัดขวางการเพิ่มผลผลิตของอุตสาหกรรมสิ่งพิมพ์ที่ได้รับการรับรองระบบการบริหารงานคุณภาพ ISO 9001 : 2000 ในประเทศไทย" วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการจัดการอุตสาหกรรม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ก้องเกียรติ ผลพิบูลสุนทร .2550. "ความรู้และเจตคติของพนักงานที่มีต่อระบบการบริหารคุณภาพ ISO/TS16949ในกลุ่มอุตสาหกรรมผู้ผลิตชิ้นส่วนรถยนต์ในนิคมอุตสาหกรรมบางปู" วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการจัดการอุตสาหกรรม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

กิตติพงษ์ เกียรตินิยมรุ่ง.2550.ระบบมาตรฐานด้านความปลอดภัยของข้อมูล ISO 27001.[Online]. Available: http://www.tuv.com/th/_iso_27001.html

คณะบริหารธุรกิจ มหาวิทยาลัยพายัพ.2547. ความหมายของระบบสารสนเทศ.[Online]. Available: http://regelearning.payap.ac.th/docu/hm490/

จักรกฤษณ์ แร่ทอง.2547. ISO/IEC 17799 (BS7799) เกี่ยวข้องกับข้อมูลอย่างไร.[Online]. Available: http://www.nextproject.net/contents/default.aspx?00045

ฉัตรชัย เรืองมณี .2550. บทบาทเทคโนโลยีสารสนเทศเพื่อการศึกษา. [Online]. Available: http://gotoknow.org/blog/klick2know/106346

ณัฐพงศ์ โสภณาทรณ์ .2548. "ประโยชน์ที่ได้รับจากการจัดทำระบบการจัดการสิ่งแวดล้อม ISO 14001 ของอุตสาหกรรมยานยนต์." วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการจัดการอุตสาหกรรม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ดวงกมล ทรัพย์พิทยากร.2548. ISO 17799 อดีต ปัจจุบัน และอนาคต. [Online]. Available: http://www.thaicert.org/paper/basic/ISO17799PastPresentFuture.pdf

บรรจง หะรังสี และคณะ.2548.ความแตกต่างระหว่างมาตรฐาน BS ISO/IEC 17799:2000 กับ BS ISO/IEC 17799:2005 จากการประชุม Regional Asia Information Security Standards (RAISS Forum). [Online]. Available: http://www.thaicert.org/paper/basic/ISO17799-2005-WhatWereChanged _revised1.pdf

ประวิทย์ คงถาวรนันต์ .2550. "ศักยภาพการแข่งขันด้วยระบบบริหารคุณภาพ ISO/TS 16949 และระบบการผลิตแบบลีนของอุตสาหกรรมยานยนต์และชิ้นส่วนยานยนต์ในนิคมอุตสาหกรรมอีสเทิร์นซีบอร์ดจังหวัดระยอง" วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการจัดการอุตสาหกรรม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ปริญญา หอมอเนก.2548.**สถานการณ์ขององค์กรในประเทศไทยเกี่ยวกับการรับรองมาตรฐาน BS7799 Part 2 กับ บทวิเคราะห์มาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศ ISO/IEC 17799 Second Edition และ มาตรฐาน ISO/IEC FDIS 27001:2005** [Online] Available: http://www.acisonline.net/article_prinya_eweek_150748.htm

พรรณี ลีกิจวัฒนะ. 2549. **การวิจัยการศึกษา**. พิมพ์ครั้งที่ 2. กรุงเทพฯ : คณะครุศาสตร์อุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

มงคล พูนเพชรรัตน์.2549. "ความรู้และระดับเจตคติที่มีต่อระบบมาตรฐาน ISO 14001 ของพนักงานปฏิบัติการในอุตสาหกรรมเครื่องปรับอากาศเพื่อการส่งออก" วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการจัดการอุตสาหกรรม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ยอดเยี่ยม เหล่านนท์ชัย.2551.**การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับหน่วยงานภาครัฐ สำนักงานคณะกรรมการการอาชีวศึกษา (Information Security of Vocational Education Commission)** .[Online]. Available: http://info-sec.vec.go.th/index/index510504.htm

วิเศษศักดิ์ โคตรอายา.2542.**การเปลี่ยนรูปจากข้อมูลสู่สารสนเทศโดยผ่านการประมวลผลสารสนเทศ**.[Online]. Available: http://tsl.tsu.ac.th/file.php/1/courseware/aa_2/lesson02/lesson2-1.htm

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. 2547.**มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น1)** [Online]. Available: http://www.thaicert.org/event/SecurityStandard/SecurityStandardV1-2547.pdf

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.2550.**มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5).** [Online]. Available: http://www.thaicert.org/paper/basic/Book_2.5_FullVersion.pdf

เศรษฐพงค์ มะลิสุวรรณ และนันทณา หุ่นงาม.2549. **การจัดการเทคโนโลยีสารสนเทศ ด้านความปลอดภัยและความเสี่ยง**.[Online].
Available: http://doctorsettapong.edublogs.org/

สุชาดา กีระนันทน์ . 2541. **เทคโนโลยีสารสนเทศสฉิติ**.[Online].
Available: http://blog.eduzones.com/dena/4892

สำนักงานคณะกรรมการการอาชีวะศึกษา. 2551. **สถานศึกษาในสังกัดคณะกรรมการการอาชีวศึกษา**.[Online].
Available:http://www.vec.go.th/doc/DirectorStr/college_th.php

หนังสือพิมพ์ โลกวันนี้ ปีที่ 10 ฉบับที่ 2415 .2551.**ความปลอดภัยระบบสารสนเทศ** .[Online].
Available: http://www.dailyworldtoday.com/columblank.php?colum_id=16568

Laudon, K.C. & Laudon, J. P. (2001). Essentials of management information systems: Organization and technology in the enterprise. 4th ed. Upper Saddle River, NJ: Prentice Hall.
Available: http://blog.eduzones.com/dena/4892

ภาคผนวก

ภาคผนวก ก

แบบสอบถามสำหรับผู้บริหารองค์กร

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับผู้บริหารองค์กร

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005
คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. ผู้บริหารองค์กร ต้องจัดทำนโยบายความมั่นคงปลอดภัย สำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษรเอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ		
2. ผู้บริหารองค์กร ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร		
3. ผู้บริหารองค์กร ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ		
4. ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม		
5. ผู้บริหารองค์กร ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร		
6. ผู้บริหารองค์กร ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบาย หรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร		
7. ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร		
8. ผู้บริหารองค์กร ต้องกำหนดนโยบายขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงาน ภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ข

แบบสอบถามสำหรับผู้บริหารสารสนเทศ

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับผู้บริหารสารสนเทศ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. ผู้บริหารสารสนเทศ ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน		
2. ผู้บริหารสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน		
3. ผู้บริหารสารสนเทศ ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้		
4. ผู้บริหารสารสนเทศ ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆเช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ.กสท. โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้นเพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น		
5. ผู้บริหารสารสนเทศ ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร		
6. ผู้บริหารสารสนเทศ ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้นซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก		

ข้อกำหนด	มี	ไม่มี
7. ผู้บริหารสารสนเทศต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน		
8 .ผู้บริหารสารสนเทศ ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ		
9. ผู้บริหารสารสนเทศ ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัยเช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น		
10.ผู้บริหารสารสนเทศ ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้		
11. ผู้บริหารสารสนเทศ ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้		
12. ผู้บริหารสารสนเทศ ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร		
13.ผู้บริหารสารสนเทศ ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ		
14.ผู้บริหารสารสนเทศ ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว		
15. ผู้บริหารสารสนเทศ ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆที่ต้องดำเนินการ		

ข้อกำหนด	มี	ไม่มี
16. ผู้บริหารสารสนเทศ ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี		
17.ผู้บริหารสารสนเทศ ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร		
18. ผู้บริหารสารสนเทศ ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ค

แบบสอบถามสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ
เรื่องการใช้นโยบายความ
ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. ผู้ดูแลระบบ ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืน เพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย		
2. ผู้ดูแลระบบ ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้		
3. ผู้ดูแลระบบ ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย		
4. ผู้ดูแลระบบ ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ		
5. ผู้ดูแลระบบ ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก		
6. ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน		
7. ผู้ดูแลระบบ ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย		
8 .ผู้ดูแลระบบ ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน		
9. ผู้ดูแลระบบ ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้		

ข้อกำหนด	มี	ไม่มี
10. ผู้ดูแลระบบ ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว		
11. ผู้ดูแลระบบ ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย		
12. ผู้ดูแลระบบ ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ		
13.ผู้ดูแลระบบ ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรการเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางธุรกิจได้ระบุไว้		
14.ผู้ดูแลระบบ ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง		
15. ผู้ดูแลระบบ ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ		
16. ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ		
17.ผู้ดูแลระบบ ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ		
18.ผู้ดูแลระบบ ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว		
19. ผู้ดูแลระบบ ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้		
20.ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง		
21.ผู้ดูแลระบบ ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน		

ข้อกำหนด	มี	ไม่มี
22. ผู้ดูแลระบบ ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอปพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่		
23.ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า		
24.ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอปพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป		
25.ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น		
26. ผู้พัฒนาระบบ ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต		
27. ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอปพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม		
28. ผู้พัฒนาระบบ ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ		
29. ผู้พัฒนาระบบและผู้เป็นเจ้าของระบบ ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ง

แบบสอบถามสำหรับหัวหน้างานธุรการ

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานธุรการ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005
คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานธุรการและหัวหน้างานสารสนเทศต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก จ

แบบสอบถามสำหรับหัวหน้างานนิติการ
เรื่องการใช้นโยบายความ
ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานนิติการ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005
คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานนิติการและหัวหน้างานสารสนเทศ ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา		
2. หัวหน้างานนิติการ ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติและที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น)ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว		
3. หัวหน้างานนิติการ ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย		
4. หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง		
5. หัวหน้างานนิติการและหัวหน้างานสารสนเทศ ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ฉ

แบบสอบถามสำหรับหัวหน้างานบุคคล

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานบุคคล

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานบุคคล ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร		
2. หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคล หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึงประกอบการคัดเลือกด้วย		
3. หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญาและการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย		
4. หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย		
5. หัวหน้างานบุคคล ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว		
6. หัวหน้างานบุคคลและหัวหน้างานพัสดุ ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ช

แบบสอบถามสำหรับหัวหน้างานพัสดุ

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานพัสดุ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ		
2. หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน		
3. หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแล และเอาใจใส่เป็นต้น		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ซ

แบบสอบถามสำหรับหัวหน้างานสารสนเทศ

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานสารสนเทศ

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้		
2. หัวหน้างานสารสนเทศ ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้		
3. หัวหน้างานสารสนเทศ ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอกเมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้		
4. หัวหน้างานสารสนเทศ จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม		
5. หัวหน้างานสารสนเทศ จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว		
6. หัวหน้างานสารสนเทศ ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงานผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร		
7. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรองระบบสายสื่อสารสำรอง เป็นต้น		

ข้อกำหนด	มี	ไม่มี
8. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน		
9. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น		
10. หัวหน้างานสารสนเทศ ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง		
11. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการควบคุมการปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ		
12. หัวหน้างานสารสนเทศ ต้องจัดให้มีการแยกระบบสำหรับการพัฒนาการทดสอบและการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต		
13. หัวหน้างานสารสนเทศ ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ		
14. หัวหน้างานสารสนเทศ ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆที่กำหนดให้บันทึกไว้ เป็นต้น		
15. หัวหน้างานสารสนเทศ ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน		
16. หัวหน้างานสารสนเทศ ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน		
17. หัวหน้างานสารสนเทศ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร		

ข้อกำหนด	มี	ไม่มี
18. หัวหน้างานสารสนเทศ ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก		
19. หัวหน้างานสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้		
20. หัวหน้างานสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย		
21. หัวหน้างานสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์		
22. หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต		
23. หัวหน้างานสารสนเทศ ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร		
24. หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์		
25.หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกงการปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต		
26. หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต		
27. หัวหน้างานสารสนเทศ ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้		

ข้อกำหนด	มี	ไม่มี
28. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่		
29. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต		
30. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ		
31. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร		
32. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร		
33. หัวหน้างานสารสนเทศ ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้		
34. หัวหน้างานสารสนเทศ ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ		
35. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร		
36. หัวหน้างานสารสนเทศ ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้		
37. หัวหน้างานสารสนเทศ ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา		
38. หัวหน้างานสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้		

ข้อกำหนด	มี	ไม่มี
39. หัวหน้างานสารสนเทศ ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย		
40. หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป		
41. หัวหน้างานสารสนเทศ ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก		
42 หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว		
43. หัวหน้างานสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี		
44.หัวหน้างานสารสนเทศ ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร		
45. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง		
46. หัวหน้างานสารสนเทศต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต		
47. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร		
48. หัวหน้างานสารสนเทศ ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน		

ข้อกำหนด	มี	ไม่มี
49. หัวหน้างานสารสนเทศ ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ฌ

แบบสอบถามสำหรับพนักงาน

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับพนักงาน

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. พนักงาน ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต		
2. พนักงาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง		
3. พนักงาน ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล		
4. พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้		
5. พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ญ

แบบสอบถามสำหรับหัวหน้างานอาคาร

เรื่องการใช้นโยบายความ

ปลอดภัยสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

แบบสอบถามเรื่องการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กร เมื่อเทียบกับ ISO17799:2005

แบบสอบถามสำหรับหัวหน้างานอาคาร

เรื่อง การใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005
คำชี้แจง แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินผลนโยบายความปลอดภัยสารสนเทศในองค์กร

แบบสอบถามนี้มี 3 ตอน โดยขอให้ตอบทุกข้อ รายละเอียดมีดังนี้

ตอนที่ 1 : แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม เป็นคำถามปลายปิด

ตอนที่ 2 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ตอนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ น้อยกว่า 30 ปี ☐ 30 – 35 ปี
☐ 36 – 40 ปี ☐ มากกว่า 40 ปี

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ประสบการณ์ในการทำงานด้านคอมพิวเตอร์และเกี่ยวกับเทคโนโลยีสารสนเทศ

☐ น้อยกว่า 5 ปี ☐ 5-10 ปี ☐ มากกว่า 10 ปี

ตอนที่ 2 แบบสอบถามเกี่ยวกับข้อมูลการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005

คำชี้แจง โปรดทำเครื่องหมาย √ ลงในช่องสี่เหลี่ยมหน้าข้อความ ที่ตรงกับความเป็นจริงของท่าน

ข้อกำหนด	มี	ไม่มี
1. หัวหน้างานอาคาร ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ		
2. หัวหน้างานอาคาร ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ		
3. หัวหน้างานอาคาร ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงาน ในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย		
4. หัวหน้างานอาคาร ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น		
5. หัวหน้างานอาคารและหัวหน้างานสารสนเทศ ต้องมีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุมตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร		
6. หัวหน้างานอาคารและหัวหน้างานสารสนเทศ ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน		
7. หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก		
8. หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย		
9. หัวหน้างานอาคารและหัวหน้างานสารสนเทศ ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น		

ตอนที่ 3 : แบบสอบถามเกี่ยวกับการใช้นโยบายความปลอดภัยของระบบสารสนเทศในองค์กรเมื่อเทียบกับ ISO17799:2005 เป็นแบบสอบถามปลายเปิดสามารถแสดงความคิดเห็นได้อย่างอิสระ

ความคิดเห็นและข้อแนะนำเพิ่มเติม

.....

.....

.....

.....

.....

ภาคผนวก ฎ

เอกสารสรุปการจัดเก็บแบบสอบถามของบุคลากร

เอกสารสรุปการจัดเก็บแบบสอบถามของบุคลากร

บุคลากร	จำนวนข้อ	สถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
ส่วนของผู้บริหารองค์กร	8	6	8	8	5	7	8	8	8	6	8	8	5	3	8	8	4	8	4	6	4	6
ส่วนของผู้บริหารสารสนเทศ	18	12	14	15	18	9	16	18	14	18	18	18	17	10	4	8	14	9	17	11	16	18
ส่วนของผู้ดูแลระบบและผู้พัฒนาระบบ	29	29	18	5	12	29	29	29	29	29	18	25	20	24	20	3	29	20	24	29	25	28
ส่วนของหัวหน้างานสารสนเทศ	49	19	47	41	12	21	23	49	49	47	44	40	35	49	21	12	48	47	18	49	40	46
ส่วนของหัวหน้างานอาคาร	9	9	8	9	9	0	6	9	9	9	1	8	3	6	9	0	9	9	8	6	7	6
ส่วนของหัวหน้างานพัสดุ	3	3	3	2	3	3	3	3	3	2	0	3	3	3	3	2	3	3	3	0	3	2
ส่วนของหัวหน้างานบุคคล	6	4	2	4	3	0	6	6	0	6	2	6	4	6	3	4	6	6	6	2	4	5
ส่วนของหัวหน้างานนิติการ	5	3	0	0	4	3	5	5	3	4	2	0	3	5	0	0	5	4	5	0	5	0
ส่วนของหัวหน้างานธุรการ	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1
ส่วนของพนักงาน	5	4	2	5	1	5	4	3	5	3	5	5	4	2	5	4	5	5	2	5	2	5
รวม	**133**	**90**	**102**	**90**	**68**	**78**	**101**	**131**	**121**	**125**	**99**	**114**	**94**	**109**	**74**	**41**	**124**	**112**	**88**	**109**	**107**	**117**

ภาคผนวก ฎ

เอกสารและหนังสือทางราชการที่ใช้ในงานวิจัย

ประกาศคณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เรื่อง ผลการพิจารณาหัวข้อและเค้าโครงวิทยานิพนธ์

.....

คณะครุศาสตร์อุตสาหกรรม โดยความเห็นชอบของคณะกรรมการพิจารณาหัวข้อและเค้าโครงวิทยานิพนธ์ ขอประกาศรายชื่อหัวข้อและเค้าโครงวิทยานิพนธ์ หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ ซึ่งได้รับอนุมัติเมื่อวันที่ 8 ธันวาคม 2551 ให้ดำเนินการดังนี้

นายอรรถสิทธิ์ มีชัย รหัสประจำตัว 50063929 ให้ทำวิทยานิพนธ์เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษาสังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร (Security Information Systems of Vocational Education Commission in Bangkok) โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ทั้งนี้ให้นักศึกษาค้นคว้าและเขียนวิทยานิพนธ์ โดยปรึกษากับอาจารย์ที่ปรึกษาวิทยานิพนธ์ให้เสร็จสิ้นภายในเวลาที่กำหนดในระเบียบของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ประกาศ ณ วันที่ ๗ ธันวาคม พ.ศ. 2551

(รองศาสตราจารย์ พีระวุฒิ สุวรรณจันทร์)
คณบดี

บันทึกข้อความ

ส่วนราชการ คณะครุศาสตร์อุตสาหกรรม หน่วยบัณฑิตศึกษา งานทะเบียน โทร.3692

ที่ ศธ 0524.04 / 4313 วันที่ 12 ธันวาคม 2551

เรื่อง ขอเชิญเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามเพื่อการวิจัย

เรียน ผศ.ดร.ฉันทนา วิริยเวชกุล

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษา ในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม พิจารณาแล้วเห็นว่าท่านเป็นผู้มีความรู้ความสามารถเกี่ยวกับเรื่องดังกล่าวเป็นอย่างดี จึงขอเชิญท่านเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามดังที่แนบมาพร้อมนี้ว่ามีเนื้อหาถูกต้องและเหมาะสมมากน้อยเพียงใด ซึ่งผลการตรวจของท่านจะช่วยให้งานวิจัยของ นายอรรถสิทธิ์ มีชัย มีความสมบูรณ์ยิ่งขึ้น พร้อมกันนี้ได้แนบแบบสอบถามเพื่อการวิจัย

จึงเรียนมาเพื่อโปรดพิจารณาและหวังว่าจะได้รับความอนุเคราะห์จากท่านด้วยดีและขอขอบคุณเป็นอย่างยิ่งมา ณ โอกาสนี้ด้วย

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

ที่ ศธ 0524.04/ 4313

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

12 ธันวาคม 2551

เรื่อง ขอเชิญเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามเพื่อการวิจัย

เรียน นายสมณธร พุ่มพิมล

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษา ในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

คณะครุศาสตร์อุตสาหกรรม พิจารณาแล้วเห็นว่าท่านเป็นผู้มีความรู้ความสามารถเกี่ยวกับเรื่องดังกล่าวเป็นอย่างดี จึงขอเชิญท่านเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามดังที่แนบมาพร้อมนี้ว่ามีเนื้อหาถูกต้องและเหมาะสมมากน้อยเพียงใด ซึ่งผลการตรวจของท่านจะช่วยให้งานวิจัยของนายอรรถสิทธิ์ มีชัย มีความสมบูรณ์ยิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณาและหวังว่าจะได้รับความอนุเคราะห์จากท่านด้วยดีและขอขอบคุณเป็นอย่างยิ่งมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4313

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

๑๒ ธันวาคม 2551

เรื่อง ขอเชิญเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามเพื่อการวิจัย

เรียน นายรุ่งนิรันดร์ ผดุงพิทักษ์ชน

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษา ในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

คณะครุศาสตร์อุตสาหกรรม พิจารณาแล้วเห็นว่าท่านเป็นผู้มีความรู้ความสามารถเกี่ยวกับเรื่องดังกล่าวเป็นอย่างดี จึงขอเชิญท่านเป็นผู้ทรงคุณวุฒิตรวจแบบสอบถามดังที่แนบมาพร้อมนี้ว่ามีเนื้อหาถูกต้องและเหมาะสมมากน้อยเพียงใด ซึ่งผลการตรวจของท่านจะช่วยให้งานวิจัยของนายอรรถสิทธิ์ มีชัย มีความสมบูรณ์ยิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณาและหวังว่าจะได้รับความอนุเคราะห์จากท่านด้วยดีและขอขอบคุณเป็นอย่างยิ่งมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยเทคนิคมีนบุรี

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยเทคนิคกาญจนาภิเษกมหานคร

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยสารพัดช่างธนบุรี

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยพณิชยการบางนา

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยพณิชยการอินทราชัย

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาสารพัดช่างพระนคร

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยบริหารธุรกิจและการท่องเที่ยวกรุงเทพ

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยอาชีวศึกษาเอี่ยมละออ

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยการอาชีพนวมินทราชูทิศ

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยศิลปหัตถกรรมกรุงเทพ

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยสารพัดช่างสี่พระยา

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์. พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยการอาชีพกาญจนาภิเษกหนองจอก

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยเทคนิคราชสิทธาราม

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยเทคนิคดอนเมือง

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยเทคนิคดุสิต

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการกาญจนาภิเษกวิทยาลัยช่างทองหลวง

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยพณิชยการเชตุพน

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02-326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยพณิชยการธนบุรี

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยอาชีวศึกษาเสาวภา

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยอาชีวศึกษาธนบุรี

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ที่ ศธ 0524.04/ 4321

คณะครุศาสตร์อุตสาหกรรม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถนนฉลองกรุง เขตลาดกระบัง กรุงเทพฯ 10520

15 ธันวาคม 2551

เรื่อง ขอความอนุเคราะห์ให้นักศึกษาทดลองใช้แบบสอบถามเพื่อการวิจัย

เรียน ผู้อำนวยการวิทยาลัยสารพัดช่างนครหลวง

สิ่งที่ส่งมาด้วย แบบสอบถามเพื่อการวิจัย

ด้วย นายอรรถสิทธิ์ มีชัย นักศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กำลังทำวิทยานิพนธ์ เรื่อง "ความปลอดภัยของระบบสารสนเทศในสถานศึกษา สังกัดสำนักงานคณะกรรมการการอาชีวศึกษาในเขตกรุงเทพมหานคร" โดยมี ผศ.ดร.เลิศลักษณ์ กลิ่นหอม เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และ ผศ.ไพฑูรย์ พิมดี เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม คณะครุศาสตร์อุตสาหกรรม จึงขอความอนุเคราะห์จากท่านโปรดอนุญาตให้ นายอรรถสิทธิ์ มีชัย ทดลองใช้แบบสอบถามเพื่อการวิจัยภายในสถานศึกษาท่านได้

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาตและขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้ด้วย

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์จิระเสกข์ ตรีเมธสุนทร)
รองคณบดีกำกับดูแลงานด้านบัณฑิตศึกษา
ปฏิบัติราชการแทนคณบดี

หน่วยบัณฑิตศึกษา
โทร. 02-737-3000 ต่อ 3692
โทรสาร. 02- 326-4325

ประวัติผู้เขียน

ชื่อ - นามสกุล	นายอรรถสิทธิ์ มีชัย
วัน เดือน ปี เกิด	1 ธันวาคม 2525
สถานที่เกิด	กรุงเทพมหานคร
สถานที่อยู่ปัจจุบัน	2328 ซอยลาดพร้าว 71 ถนนลาดพร้าว แขวงลาดพร้าว เขตลาดพร้าว จังหวัดกรุงเทพมหานคร 10230
สถานที่ทำงาน	Universal Communication System Co.,Ltd. 64 ถนนปั้น แขวงสีลม เขตบางรัก กรุงเทพฯ 10500
ตำแหน่ง	IT Consultant Engineer
ประวัติการศึกษา	ปีการศึกษา 2548 สำเร็จการศึกษาอุตสาหกรรมศาสตรบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์ สถาบันเทคโนโลยีราชมงคล วิทยาเขตพระนครเหนือ ปีการศึกษา 2552 สำเร็จการศึกษาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการศึกษาวิทยาศาสตร์ (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง