รายงานสหกิจศึกษาฉบับสมบูรณ์

การศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013

A STUDY OF GUIDELINES FOR IMPROVING INFORMATION SECURITY SYSTEMS ACCORDING TO ISO 27001:2013

เติมพันธ์ ช่วยนคร

TOEMPHAN CHUAYNAKORN

หลักสูตรวิศวกรรมสารสนเทศ

ภาควิชาวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

วิทยาเขตชุมพรเขตรอุดมศักดิ์ จังหวัดชุมพร

ปีการศึกษา 2564

รายงานสหกิจศึกษาฉบับสมบูรณ์

การศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013

A STUDY OF GUIDELINES FOR IMPROVING INFORMATION SECURITY SYSTEMS ACCORDING TO ISO 27001:2013

เติมพันธ์ ช่วยนคร

TOEMPHAN CHUAYNAKORN

หลักสูตรวิศวกรรมสารสนเทศ

ภาควิชาวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

วิทยาเขตชุมพรเขตรอุดมศักดิ์ จังหวัดชุมพร

ปีการศึกษา 2564

รายงานสหกิจศึกษาฉบับสมบูรณ์

ประจำปีการศึกษา 2564

โครงงาน	การศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 A study of guidelines for improving information security systems according to ISO 27001:2013
ผู้จัดทำ	นายเติมพันธ์ ช่วยนคร รหัสนักศึกษา 61515005
ปฏิบัติงาน	บริษัท อักษรเจริญทัศน์ อจท. (สนญ.) จำกัด
ที่อยู่	142 ถนนแพร่งสรรพศาสตร์ แขวงศาลเจ้าพ่อเสือ เขตพระนคร กรุงเทพมหานคร 10200
พนักงานที่ปรึกษา	คุณมนตรี พรวสันต์ ตำแหน่ง ผู้จัดการแผนกไอที

..... อาจารย์ที่ปรึกษา

(อาจารย์ อรรถศาสตร์ นาคเทวัญ)

หนังสือส่งรายงานสหกิจศึกษาฉบับสมบูรณ์

เรื่อง ขอส่งรายงานสหกิจศึกษา

เรียน อาจารย์ที่ปรึกษาสหกิจศึกษา สาขาวิชาวิศวกรรมสารสนเทศ

ตามที่กระผม นายเติมพันธ์ ช่วยนคร นักศึกษาสาขาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง วิทยาเขตชุมพรเขตรอุดมศักดิ์จังหวัดชุมพร ได้ปฏิบัติงานสหกิจศึกษาระหว่างวันที่ 1 สิงหาคม พ.ศ. 2564 ถึงวันที่ 30 พฤศจิกายน พ.ศ. 2564 ในตำแหน่ง ไอทีซัพพอร์ต ณ บริษัท อักษรเจริญทัศน์ อจท. (สนญ.) จำกัด และได้รับมอบหมายจากที่ปรึกษาสหกิจศึกษาให้ศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013

บัดนี้ การปฏิบัติงานสหกิจศึกษาได้เสร็จสิ้นลงแล้ว จึงใคร่ขอส่งรายงานสหกิจศึกษาฉบับ ดังกล่าว จำนวน 1 เล่ม เพื่อขอรับคำปรึกษาต่อไป

จึงเรียนมาเพื่อพิจารณา

ขอแสดงความเคารพอย่างสูง

นายเติมพันธ์ ช่วยนคร

นักศึกษาสหกิจศึกษาหลักสูตรวิศวกรรมสารสนเทศ

ภาควิชาวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

วิทยาเขตชุมพรเขตรอุดมศักดิ์ จังหวัดชุมพร

ใบรับรองสหกิจศึกษา

.....

หัวข้อสหกิจ	การศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013
Co-operative Title	A study of guidelines for improving information security systems according to ISO 27001:2013
ชื่อนักศึกษา	นายเติมพันธ์ ช่วยนคร รหัสประจำตัว 61515005
ปริญญา	วิศวกรรมศาสตรบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
อาจารย์ที่ปรึกษาสหกิจ	อาจารย์อรรถศาสตร์ นาคเทวัญ

คณะกรรมการสอบปริญานิพนธ์			**ลายมือชื่อ**
ดร.รัตติกร	สมบัติแก้ว	ประธานกรรมการสอบ	
ผศ.ดร.รัฐพงษ์	สุวลักษณ์	กรรมการสอบ	
อาจารย์นภัสรพี	สิทธิวัจน์	กรรมการสอบ	
อาจารย์อรรถศาสตร์	นาคเทวัญ	อาจารย์ที่ปรึกษา	

วัน/เดือน/ปี ที่สอบ 24 ธันวาคม 2564 เวลา 10.00 - 16.30 น.

สถานที่สอบ Online ด้วยโปรแกรม Microsoft Team

ภาควิชาวิศวกรรมศาสตร์ รับรองแล้ว

(ผศ.ดร.ปราโมทย์ กุศล)

หัวหน้าภาควิชาวิศวกรรมศาสตร์

วันที่ 21 กรกฎาคม พ.ศ. 2565

หัวข้อสหกิจ	การศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013
นักศึกษาผู้จัดทำ	นายเติมพันธ์ ช่วยนคร รหัสนักศึกษา 61515005
หลักสูตร	วิศวกรรมศาสตรบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์อรรถศาสตร์ นาคเทวัญ
พนักงานที่ปรึกษา	คุณมนตรี พรวสันต์
ปีการศึกษา	2564

บทคัดย่อ

โครงงานสหกิจศึกษาฉบับนี้แสดงข้อมูลเกี่ยวกับแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลขององค์กรตามมาตรฐานไอเอสโอ 27001 โดยศึกษานโยบายและแนวปฏิบัติด้านความปลอดภัยของข้อมูลขององค์กรในปัจจุบัน เปรียบเทียบกับมาตรฐานใหม่ (ISO/IEC 27001:2013) เพื่อปรับปรุงระบบรักษาความปลอดภัยข้อมูลขององค์กรในด้านต่าง ๆ ดังนี้ ด้านมาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์ ด้านระบบความปลอดภัยในการใช้งานระบบไอทีของผู้ใช้งาน และด้านการควบคุมการเข้ารหัสและการรักษาความลับข้อมูล ขั้นตอนของการศึกษาเริ่มต้นจากการเก็บรวมรวมข้อมูลระบบรักษาความปลอดภัยของข้อมูลขององค์ในแต่ละด้าน และนำมาวิเคราะห์ความเสี่ยงตามมาตรฐานไอเอสโอ 27001:2013 ซึ่งเป็นมาตรฐานใหม่ที่องค์กรต้องการปรับปรุง จากนั้นนำข้อมูลการประเมินความเสี่ยงที่ได้มากำหนดมาตรการเพื่อการควบคุมและลดความเสี่ยงให้มีน้อยที่สุดที่สามารถจะดำเนินการได้ โดยจากการศึกษาสามารถกำหนดหลักปฏิบัติเพื่อปรับปรุงระบบการรักษาความปลอดภัยข้อมูลขององค์กรได้ทั้งสามด้านในข้างต้น ซึ่งจากผลการศึกษาพบว่าเมื่อดำเนินการตามหลักปฏิบัติที่กำหนดขึ้นตามการศึกษานี้ จะมีความเสี่ยงของระบบรักษาความปลอดภัยของข้อมูลขององค์ที่ลดลงจากการประเมินความเสี่ยงก่อนการดำเนินการตามหลักปฏิบัติใหม่ที่กำหนดขึ้น และระบบรักษาความปลอดภัยของข้อมูลขององค์กรทั้งสามด้านที่กำหนดก็เป็นไปตามตามมาตรฐานไอเอสโอ 27001:2013 บรรลุตามวัตถุประสงค์ที่กำหนดไว้

คำสำคัญ: มาตรฐานไอเอสโอ 27001 มาตรฐานเครื่องคอมพิวเตอร์และซอฟต์แวร์ ความปลอดภัยการใช้งานระบบไอที การรักษาความปลอดภัยของข้อมูล

Co-operative Title	A study of guidelines for improving information security systems according to ISO 27001:2013
Student	Mr. Toemphan Chuaynakorn Student ID 61515005
Degree	Bachelor of Engineering
Program in	Information Engineering
Advisor	Mr. Athasart Narkthewan
Mentor	Mr. Montree Pornvasan
Academic Year	2021

ABTRACT

A guideline for improving corporate information security according to ISO 27001 was represented in the co-operative project report. The corporate information security management policies were compared with the new standard of information security ISO 27001:2013. The study aimed to improve three topics of information security management such as the standard of computer and software used, IT security for users, and encryption and data protection security controls. Firstly, the three topics of corporate IT security data were collected. Risk analysis was then used to the data following ISO 27001:2013 which was the new standard for the corporate. Subsequently, the risk data was used to improve three guidelines of information security management for reducing the corporate IT security risk. The study found that the corporate IT security risk was reduced after an operation following the new guidelines of information security management and the corporate was successful to improve its information security management according to ISO 27001:2013.

Keywords: ISO 27001:2013, Standard of Computer and Software, IT system security, Data protection security.

กิตติกรรมประกาศ

การที่ข้าพเจ้าได้มาปฏิบัติงานสหกิจศึกษา ณ บริษัท อักษรเจริญทัศน์ อจท. (สนญ.) จำกัด ตั้งแต่วันที่ 1 สิงหาคม พ.ศ. 2564 ถึงวันที่ 30 พฤศจิกายน พ.ศ. 2564 ส่งผลให้ข้าพเจ้าได้รับความรู้และประสบการณ์ต่าง ๆ ที่มีคุณค่าและประโยชน์อย่างมาก สำหรับรายงานวิชาสหกิจฉบับนี้ สำเร็จลุล่วงด้วยดีจากความช่วยเหลือและการสนับสนุนเป็นอย่างดีจากหลายฝ่าย

ขอขอบพระคุณคุณพ่อและคุณแม่และญาติพี่น้องผู้ซึ่งคอยให้การอบรมสั่งสอน เลี้ยงดูสนับสนุนเงินทุนในการศึกษา ตลอดจนให้กำลังใจเสมอมา

ขอขอบพระคุณอาจารย์อรรถศาสตร์ นาคเทวัญ อาจารย์ที่ปรึกษา และ ดร.รัตติกร สมบัติแก้ว อาจารย์ที่ปรึกษาร่วม ผู้ซึ่งให้คำแนะนำต่าง ๆ คำปรึกษาในการแก้ไขปัญหาที่เกิดขึ้นทั้งในการทำเอกสาร ปัญหาที่เกิดขึ้นในระหว่างการทำงานหน้างาน ตลอดจนการติดตามเกี่ยวกับงานโครงงานตลอดมา ข้าพเจ้าจึงขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณคณะอาจารย์ที่เคารพทุกท่าน ที่ให้ความเอาใจใส่แนะนำ คอยช่วยเหลือเสมอมา แม้ว่าจะไม่ใช่อาจารย์ที่ปรึกษาก็ตาม

ขอขอบพระคุณ คุณมนตรี พรวสันต์ ที่ปรึกษาและบริษัท อักษรเจริญทัศน์ อจท. (สนญ.) จำกัด ที่ได้เอื้อเฟื้อให้นักศึกษาได้มีโอกาสทำโครงงานร่วมกับบริษัท ตลอดจนสถานที่ใช้ในการทำงานและอุปกรณ์ที่ใช้ในการปฏิบัติงาน และการช่วยเหลือของพนักงานที่ปรึกษาในทุก ๆ ด้านที่มีให้เสมอมา

ขอน้อมรำลึกถึงคุณของทุก ๆ ท่านตอดไป และความรู้ที่ได้จากการทำโครงงานในครั้งนี้ ข้าพเจ้าจะใช้ให้เป็นประโยชน์สูงสุด รวมถึงแบ่งปันให้กับผู้ที่สนใจต่อไป

เติมพันธ์ ช่วยนคร

ธันวาคม 2564

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

ในบทนี้จะกล่าวถึง ความเป็นมาและความสำคัญ วัตถุประสงค์ของการทำโครงงาน ขอบเขตของการทำโครงงาน ประโยชน์ที่รับ แผนการดำเนินงาน และโครงสร้างของรายงานสหกิจศึกษา

1.1 ความเป็นมาและความสำคัญ

ในปัจจุบันบริษัท อักษรเจริญทัศน์ อจท. เป็นผู้ผลิต และจัดจำหน่ายหนังสือรวมไปถึงสื่อการเรียนการสอนไม่ว่าจะเป็นออนไลน์หรือออฟไลน์ครบวงจรชั้นนำของประเทศ ภายในองค์กรมีสาขาที่เป็นสำนักงานใหญ่ (Head Office) และในส่วนของสาขาต่าง ๆ ที่จัดแสดงสินค้า (Showroom) อีกทั้งภายในบริษัทมีฝ่ายคลังสินค้า (Warehouse) สำหรับจัดเก็บอุปกรณ์สื่อการเรียนการสอนทั้งหมด เช่น หนังสือ สมุด เป็นต้น โดยปัจจุบันบริษัท อักษรเจริญทัศน์ อจท. ได้จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย (SET) ในชื่อ บริษัท อักษร เอ็ดดูเคชั่น จำกัด และกลุ่มบริษัทในเครือ และเมื่อองค์กรอยู่ในตลาดหลักทรัพย์มีความจำเป็นต้องมีการอัปเดตมาตรฐานไอเอสโอ (ISO 27001) ให้เป็นปัจจุบัน โดยจะเป็นประโยชน์อย่างมากจากการได้รับการรับรองมาตรฐานระบบ ISMS ทั้งนี้เพื่อให้องค์กรมีมาตรฐานในการบริหารจัดการความเสี่ยงและความปลอดภัยของข้อมูลที่เป็นมาตรฐานสากลที่องค์กรต่าง ๆ เลือกใช้เมื่อต้องการเข้าตลาดหลักทรัพย์หรืออยู่ในตลาดหลักทรัพย์แล้ว เป็นต้น

1.2 วัตถุประสงค์ของการทำโครงงาน

เพื่อให้องค์กรมีมาตรฐานในการบริหารจัดการความเสี่ยงและความปลอดภัยของข้อมูล และการบริหารจัดการความต่อเนื่องทางธุรกิจ ที่เป็นมาตรฐานสากลซึ่งเป็นที่ยอมรับจากองค์กรต่าง ๆ และ ป้องกันการละเมิดทางกฎหมาย สังคม ศีลธรรม และกฎระเบียบข้อบังคับขององค์กร โดยอ้างอิงมาตรฐานของ ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศขององค์กร

โดยต้องจัดทำนโยบาย (Policy) และ วิธีปฏิบัติ (Procedure) และการประกาศนโยบายเป็นระเบียบ ข้อบังคับขององค์กร การนำมาใช้งาน การประเมินผลการใช้งานของนโยบายและกรอบการทำงาน รวมถึงการปรับปรุงนโยบาย และ วิธีปฏิบัติให้สอดคล้องกับความต้องการทางธุรกิจขององค์กร และการป้องกันการเข้าถึงและการใช้งานอย่างต่อเนื่องของข้อมูลสารสนเทศภายในองค์กร โดยมีวัตถุประสงค์ 3 อย่างคือ

- รักษาไว้ซึ่งความลับของข้อมูลสารสนเทศ (Confidentiality)

- มีความถูกต้องครบถ้วนของข้อมูลสารสนเทศ (Integrity)
- มีสภาพพร้อมใช้งานของข้อมูลสารสนเทศ (Availability)

1.3 ขอบเขตของการทำโครงงาน

1. ศึกษานโยบายของบริษัทปัจจุบัน (ISO/IEC 27001:2005)
   - โดยเก็บรวบรวมข้อมูลความต้องการจากผู้ใช้งานในหน่วยงานต่าง ๆ ภายในสำนักงานใหญ่ของบริษัท
   - นำไปเปรียบเทียบกับมาตรฐานใหม่ ISO/IEC 27001:2013
2. สรุปข้อมูลที่ต้องปรับเปลี่ยนเพื่อแจ้งให้ทางบริษัททราบ และดำเนินการปรับเปลี่ยนให้เป็นไปตามมาตรฐานใหม่
3. นำข้อมูลต่าง ๆ ที่ได้มาปรับใช้ให้สอดคล้องกับมาตรฐานใหม่ ISO27001:2013 โดยสรุปและจัดทำเป็นเอกสาร (Document) ให้พร้อมเพื่อส่งต่อให้บริษัทยื่นขอมาตรฐาน ISO 27001:2013 ซึ่งประกอบด้วย

   3.1 หัวข้อ ISO : ITSP-002 เรื่อง IT Asset Management (Vendor Selection Procedure)เกี่ยวกับการจัดซื้ออุปกรณ์ไอทีและซอฟต์แวร์ต่าง ๆ ภายในองค์กร

   3.2 หัวข้อ ISO : ITSP-005 เรื่อง User Management Procedure เกี่ยวกับระบบความปลอดภัยของการใช้งานระบบไอทีของผู้ใช้งานแต่ละในบริษัท

   3.3 หัวข้อ ISO : ITSP-005 เรื่อง Active Directory ในเครื่องแม่ข่ายของบริษัท

   3.4 หัวข้อ ISO : ITPO-07 เรื่อง Cryptographic Control Policy เกี่ยวกับการควบคุมการเข้ารหัสและการรักษาความลับของข้อมูล

1.4 ประโยชน์ที่ได้รับ

1. ได้พัฒนาทักษะการทำงาน IT Audit
2. ทำให้องค์กรมีมาตรฐานการบริหารจัดการความเสี่ยงและความปลอดภัยของข้อมูล
3. ทำให้องค์กรมีภาพลักษณ์และความน่าเชื่อถือขององค์กรสูงขึ้น จากภายในและภายนอกองค์กร
4. ทำให้องค์กรตระหนักถึงความปลอดภัยของข้อมูล
5. ได้โอกาสในการเรียนรู้ ศึกษาหาประสบการณ์ใหม่เพิ่มเติมจากงานที่ได้รับมอบหมาย และนำความรู้ความสามารถมาประยุกต์กับงานได้จริง
6. มีมนุษย์สัมพันธ์กับบุคคลทั่วไปภายในบริษัท สามารถเรียนรู้ชีวิตในวัยทำงาน และปรับตัวกับความเข้าใจในการทำงานของรูปแบบบริษัทจริง

7. ได้พัฒนาทักษะการวางแผน รูปแบบการทำงาน และมีความรับผิดชอบในการทำงานมากขึ้น

8. มีความกล้า และมั่นใจในการนำเสนอผลงานมากขึ้น

9. ได้เรียนรู้ข้อผิดพลาดที่ตนเองได้พบเจอ และนำมาปรับปรุงเพื่อพัฒนาตนเอง

10. มีความรู้และความเข้าใจเอกสารเรื่องมาตรฐานไอเอสโอ 27001 ที่สามารถนำไปปรับใช้งานได้จริง

1.5 ขั้นตอนการดำเนินงาน

ขั้นตอนการดำเนินงานที่ผู้จัดทำได้วางแผนและฝึกสหกิจศึกษาแสดงรายละเอียดไว้ในตารางดังนี้

ตารางที่ 1.1 ขั้นตอนและวิธีการดำเนินงาน

ขั้นตอนการดำเนินงาน	ระยะเวลาการดำเนินงาน																			
	กรกฎาคม				สิงหาคม				กันยายน				ตุลาคม				พฤศจิกายน			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. เรียนรู้การทำงานของบริษัท	←	→																		
2. ศึกษาการทำงานตามรูปแบบของบริษัท			←	→																
3. ศึกษานโยบายของบริษัทปัจจุบัน					←			→												
4. รวบรวมข้อมูล Requirement									←			→								
5. จัดทำหัวข้อ ISO : ITSP-002													←		→					
6. จัดทำหัวข้อ ISO : ITPO-07														←		→				

ตารางที่ 1.1 ขั้นตอนและวิธีการดำเนินงาน (ต่อ)

ขั้นตอนการดำเนินงาน	ระยะเวลาการดำเนินงาน																			
	กรกฎาคม				สิงหาคม				กันยายน				ตุลาคม				พฤศจิกายน			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
7. จัดทำหัวข้อ ISO : ITSP-005 ทั้งสองตัว													←	—	—	→				
8. นำงานส่งกับหัวหน้าพร้อมนำข้อเสนอแนะมาแก้ไข														←	—	→				
9. ตรวจความผิดพลาดและแก้ไข																	←	—	→	
10. ส่งงานให้หัวหน้าพร้อมส่งต่อเข้าที่ประชุม																		←	—	→

1.6 โครงสร้างของรายงานสหกิจศึกษา

ในรายงานสหกิจศึกษาฉบับนี้แบ่งออกเป็น 5 ส่วนหลัก ๆ คือ บทที่ 1-5 ซึ่งแต่ละบทจะอธิบายเนื้อหาที่เกี่ยวข้องกับการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 โดยแบ่งออกเป็นบทต่าง ๆ มีรายละเอียด ดังต่อไปนี้

บทที่ 1 บทนำ ในบทนี้กล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการทำโครงงาน ขอบเขตของการทำโครงงาน ประโยชน์ที่ได้รับ ขั้นตอนและวิธีการดำเนินงาน และโครงสร้างของรายงานสหกิจศึกษา

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง ในบทนี้กล่าวถึงทฤษฎีที่เกี่ยวข้องกับการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 ได้แก่ มาตรฐานไอเอสโอ 27001 (ISO/IEC 27001) International Organization for Standardization ความจำเป็นของการรักษาความปลอดภัยของข้อมูล มาตรฐานไอเอสโอ ISO/IEC 27001:2013 Information Security Management Systems การบริหารจัดการความเสี่ยง (Risk Management) การประเมินความเสี่ยง (Risk Assessment) การควบคุม / แก้ไขความเสี่ยง (Risk Treatment)

บทที่ 3 หลักการและกระบวนการทำงาน ในบทนี้กล่าวถึงขั้นตอนการดำเนินการของการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 เช่น การศึกษาข้อมูลเก่า การเก็บรวบรวมข้อมูล และขั้นตอนการทำงาน เป็นต้น

บทที่ 4 การทำโครงงานและการปรับใช้ข้อบังคับ ในบทนี้กล่าวถึงการทำเอกสารและการปรับใช้ข้อบังคับ ของอุปกรณ์ไอทีและระบบต่าง ๆ ให้เป็นไปตามมาตรฐานไอเอสโอ 27001:2013 ในหัวข้อที่ได้รับมอบหมาย การปรับเปลี่ยนอุปกรณ์ไอทีและซอฟต์แวร์ต่าง ๆ ภายในองค์กร ขั้นตอนการทำ Active Directory เป็นต้น

บทที่ 5 สรุปผลการทำโครงงานและข้อเสนอแนะ ในบทนี้กล่าวถึงการสรุปผลการวิจัย ปัญหาและอุปสรรคในการทำงาน และข้อเสนอแนะต่าง ๆ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

ในบทนี้กล่าวถึง ทฤษฎีที่เกี่ยวข้องกับการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตมาตรฐาน ไอเอสโอ 27001:2013 ได้แก่ มาตรฐานไอเอสโอ 27001 มาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์ ความปลอดภัยของการใช้งานระบบไอทีของผู้ใช้งาน การควบคุมการเข้ารหัสและการรักษาความลับของข้อมูล

2.1 ความสำคัญและความจำเป็นของการรักษาความปลอดภัยข้อมูล

ความจำเป็นและความสำคัญของการรักษาความปลอดภัยของข้อมูล [1] คือ ข้อบังคับที่ต้องรักษาข้อมูลความปลอดภัยทางสารสนเทศ ปัจจุบันเทคโนโลยีสารสนเทศ (IT) เป็นองค์ประกอบที่สำคัญและซับซ้อนของเกือบทุกองค์กร หมายรวมถึงทุกอย่างตั้งแต่อีเมล์ที่ส่ง เอกสารที่สร้างขึ้น จนถึงข้อมูลที่เก็บไว้กับลูกค้าและซัพพลายเออร์ ด้วยการขยายตัวของอุปกรณ์ที่เชื่อมต่อกันได้ จึงกลายเป็นเรื่องง่ายที่แต่ละคนจะสามารถเข้าถึงข้อมูลนี้ไม่ว่าอยู่ที่ใดของโลก และด้วยการเข้าถึงที่ง่ายขึ้น ก็กลายเป็นเรื่องง่ายเช่นกันสำหรับผู้ใช้ที่ไม่ได้รับอนุญาตที่จะเข้าถึงข้อมูลส่วนตัวขององค์กรได้

หลักสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การปกป้องทรัพย์สินสารสนเทศตามสภาพความเสี่ยงขององค์กร การสร้างความตระหนักรู้เกี่ยวกับความจำเป็น และความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ การกำหนดความรับผิดชอบ และนโยบายสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ความต่อเนื่องในการให้บริการข้อมูล สารสนเทศ ระบบ และทรัพย์สินสารสนเทศ พร้อมทั้งประสิทธิผลของมาตรการควบคุม ทั้งมาตรการด้านบริหารจัดการ (Administrative Security) มาตรการด้านเทคนิค (Technical Security) และมาตรการทางกายภาพ (Physical Security) ตอบสนองความต้องการทางธุรกิจและกลุ่มผู้มีส่วนได้เสีย และภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ขององค์กร

ข้อมูลสารสนเทศ เป็นสินทรัพย์สำคัญทางธุรกิจ ที่ต้องดูแลบำรุงรักษา และป้องกันอย่างดี ปัจจุบันบริษัท ได้กำหนดความปลอดภัยระบบข้อมูลสารสนเทศ โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงาน และลดความเสี่ยงด้านความปลอดภัย ในระดับที่เหมาะสม และเกิดประสิทธิภาพต่อการทำงานสูงสุด บริษัทได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศ โดยให้มีการบริหารจัดการให้ระบบข้อมูลมีลักษณะคงความเป็น C I A ดังรูปที่ 2.1

2.1.1 ความลับ (Confidentiality) เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษา

ความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้ ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี

2.1.2 ความสมบูรณ์ (Integrity) ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน ทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

2.1.3 ความพร้อมใช้ (Availability) ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

รูปที่ 2.1 ตัวอย่างองค์ประกอบของความมั่นคงปลอดภัยของข้อมูล

2.2 มาตรฐานไอเอสโอ

International Organization for Standardization [2] คือ หน่วยงานที่กำหนดและใช้มาตรฐาน ISO27001 โดยเวอร์ชั่นล่าสุดคือ ISO27001:2013 ประกาศเมื่อ 1 ต.ค. 2013 ส่วนเวอร์ชั่นแรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO27001:2005) หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification) ประเทศไทย มีหน่วยงานรัฐและ เอกชนเริ่มทำ ISO27001 และขอการรับรองได้สำเร็จ เช่น บริษัท อักษร เอ็ดดูเคชั่น

จำกัด และรัฐวิสาหกิจอีกหลายแห่ง องค์กรสามารถทำได้ มาตรฐานนี้ออกแบบมาให้ใช้ได้ประเภทธุรกิจ หน่วยราชการ สถานศึกษา และใช้ได้กับองค์กรทั้งขนาดเล็กและ ขนาดใหญ่อย่างบริษัทข้ามชาติ

2.2.1 มาตรฐานไอเอสโอ 27001 (ISO/IEC 27001)

มาตรฐาน ISO 27001 [3] คือ มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems : ISMS) มาตรฐานนี้ให้ต้นแบบสำหรับการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัยมาตรฐาน ISO 27001 ได้ระบุแนวทางการดำเนินงานและการบริหารจัดการที่จะช่วยในการเก็บรักษาข้อมูลของท่านได้อย่างปลอดภัย

- **Information Security Management Systems**

Information Security Management Systems [4] คือ ระบบการจัดการความปลอดภัยของข้อมูล นับจากอีเมล์ภายในองค์กร วัสดุ/อุปกรณ์ช่วยขาย ไปจนถึงรายงานทางการเงิน องค์กรทุกขนาดในทุกภาคอุตสาหกรรมต่างต้องมีการดำเนินการหรือการจัดการการกับข้อมูลจำนวนมากในแต่ละวัน สำหรับองค์กรหนึ่ง ๆ เช่นองค์กรที่ผู้จัดทำไปฝึกงาน ข้อมูลนี้ถือเป็นข้อได้เปรียบทางการแข่งขัน เพราะสิ่งนี้คือข้อมูลที่บอกว่าองค์กรแก้ปัญหาต่าง ๆ อย่างไร หรือองค์กรคว้าส่วนแบ่งของตลาดมาได้อย่างไร เป้าหมายของระบบการจัดการความปลอดภัยของข้อมูล (ISMS) คือเพื่อปกป้องข้อมูลที่สร้างความแตกต่างให้กับธุรกิจขององค์กร ทั้งในแบบออนไลน์และโดยตัวบุคคล

หลักการของระบบการจัดการความปลอดภัยของข้อมูล ในขณะที่การนำระบบ ISMS ไปปฏิบัตินั้นจะแตกต่างกันไปในแต่ละองค์กร แต่มีหลักการพื้นฐานของ ISMS ที่ทุกองค์กรจะต้องปฏิบัติตามเพื่อให้เกิดประสิทธิภาพในการปกป้องทรัพย์สินสารสนเทศขององค์กร ตัวอย่างหลักการด้านล่างนี้จะช่วยแนะแนวทางเพื่อไปสู่การได้รับการรับรองมาตรตรฐาน ISO/ IEC 27001 เพื่อให้ระบบ ISMS ขององค์กรมีประสิทธิผล องค์กรต้องทำการวิเคราะห์ความจำเป็นด้านการรักษาความปลอดภัยสำหรับแต่ละทรัพย์สินสารสนเทศ และนำการควบคุมที่เหมาะสมต่าง ๆ มาใช้เพื่อให้สามารถเก็บรักษาสินทรัพย์ดังกล่าวไว้ได้อย่างปลอดภัย

- **มาตรฐาน ISO 27001 ที่นิยมประกาศใช้กันในไทย**

ปัจจุบันประกอบด้วยเวอร์ชั่น ISO 27001:2005 และ ISO 27001:2013 โดยมาตรฐาน ISO 27001 ไม่ใช่มาตรฐานระบบ ISMS มาตรฐานแรก ในปี 1995 กลุ่ม BSI (British Standards Institution) ได้กำหนดมาตรฐาน BS 7799 โดยอธิบายเกี่ยวกับวิธีปฏิบัติสำหรับการจัดการความปลอดภัยของข้อมูล ในปี 1999 กลุ่ม BSI กำหนดส่วนที่สองของมาตรฐาน BS 7799 นั่นคือ BS 7799 -2 โดยมุ่งเน้นไปที่วิธีการนำระบบ ISMS ไปปฏิบัติ หลังจากมีการแก้ไขในปี 2002 มาตรฐาน BS 7799-2 ได้รวมเอาหลักการ Plan-Do-Check-Act เข้ามาประกอบ ซึ่งสอดคล้องกับมาตรฐานอื่น ๆ เช่น ISO 9000

มาตรฐาน BS 7799-2 นี้ ภายหลังได้ถูกนำมาประยุกต์ใช้โดย ISO จนในเดือนพฤศจิกายนปี 2005 จึงได้กลายเป็นมาตรฐาน ISO/IEC 27001

2.2.2 มาตรฐานไอเอสโอ ISO/IEC 27001:2013

มาตรฐานไอเอสโอ ISO/IEC 27001:2013 [5] คือ ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ (ISMS) เป็นมาตรฐานการจัดการความปลอดภัยของข้อมูลสารสนเทศ ซึ่งใช้หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Information Security) ที่มีองค์ประกอบ 3 ส่วน ได้แก่ C (Confidentiality) I (Integrity) A (Availability)

ระบบมาตรฐาน ISO/IEC 27001:2013 มีการประยุกต์ใช้หลักการ PDCA (Plan- Do - Check- Action) ซึ่งเป็นหลักการสำคัญในการบริหารจัดการที่ใช้กันแพร่หลาย หลักการ PDCA จึงกำหนดมาตรฐานการดำเนินการให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2013 เช่น การจัดทำนโยบาย กระบวนการ การกำหนดหน้าที่ความรับผิดชอบ การควบคุม การตรวจสอบ การประเมินความเสี่ยง การวางแผนความต่อเนื่องทางธุรกิจ

- **ISO 27001:2013 แตกต่าง/มีอะไรเพิ่มเติมจาก ISO 27001:2005**

ในเวอรชั่นใหม่ของ ISO 27001:2013 ส่วนระบบบริหารจัดการ (management system) จะถูกปรับเปลี่ยนให้เป็นไปตามโครงสร้างมาตรฐานใหม่ที่จะถูกใช้มาตรฐาน ISO ทั้งหมด โดยวัตถุประสงค์หลักเพื่ออัพเกรดข้อมูลสารสนเทศรวมไปถึงโปรแกรมและอุปกรณ์สารสนเทศให้มีความทันสมัย เพื่อทำให้โครงสร้างคำจำกัดความและนิยามของมาตรฐานต่าง ๆ ในระบบบริหารจัดการที่เป็น ISO เป็นไปในทิศทางเดียวกัน และสนับสนุนให้องค์กรที่มีการทำระบบบริหารจัดการ (management system) มากกว่าหนึ่งมาตรฐานสามารถควบรวมและทำงานประสานกันได้เป็นอย่างดี ในโครงสร้างใหม่มีข้อกำหนดทั้งหมด 14 ข้อจากเดิม 11 ข้อ

สิ่งที่เปลี่ยนไปในระบบบริหารจัดการ (ข้อกำหนด1-14) สรุปได้ดังนี้

- คำจำกัดความในเวอร์ชัน 2005 ทั้งหมดถูกย้ายไปอยู่ในมาตรฐานไอเอสโอ 27000:2013
- เปลี่ยนเทอมที่ใช้ จากเดิมชื่อ “ISMS Policy” เป็น “Information Security Policy” ให้ชื่อเป็นกลางมากขึ้น
- เปลี่ยนชื่อหัวข้อ ข้อกำหนดการบวนการประเมินความเสี่ยงก็ลงรายละเอียดน้อยลง นั่นหมายความว่าจะมีทางเลือก สำหรับวิธีการในการประเมินความเสี่ยงที่หลากหลายขึ้น
- เอกสารที่ต้องจัดทำ (Documentation) เวอร์ชันใหม่เน้นว่าต้องจัดทำเอกสารอะไรบ้าง

- เวอรชั่นใหม่ ISO 27000:2013 เน้นไปที่ผลลัพธ์ในการดำเนินงานของระบบ
- กำหนดคำใหม่ คือ “Documented information” แทนที่ เอกสาร และบันทึก แต่วิธีการควบคุมก็ไม่ต่างจากของเดิม
- ข้อกำหนดเรื่องการพัฒนา (Improvement) การป้องกันความเสียหายของข้อมูลและอุปกรณ์ เช่น การทำ PM อุปกรณ์สารสนเทศทั้งหมดในองค์กร และปรับเปลี่ยนอุปกรณ์ที่ชำรุดและล้าสมัย เพื่อลดความเสียหายการทำงานที่ราบรื่นขององค์กร
- การประเมินความเสี่ยง ต้องมีการประเมิณควบคุมและแก้ไขอยู่เสมอ เพราะการทำงานเชิงป้องกันนั้นถือเป็นกระบวนการหนึ่งในการประเมินความเสี่ยง

- **ประโยชน์ที่ได้รับจากการนำมาตรฐาน ISO/IEC 27001:2013 ไปใช้**

สร้างความมั่นใจให้กับลูกค้า พนักงาน คู่ค้า และผู้มีส่วนได้เสียเกี่ยวกับการจัดการข้อมูลและระบบสารสนเทศที่ปลอดภัย หรือการกำหนดนโยบายที่จะต่อสู่กับการละเมิดสิทธิ แสดงให้เห็นถึงความน่าเชื่อถือและความน่าไว้วางใจขององค์กร สามารถช่วยประหยัดค่าใช้จ่ายขององค์กร ช่วยให้ทราบถึงกฎหมายและกฎระเบียบที่เกี่ยวข้อง ทำให้มั่นใจได้ว่าองค์กรมุ่งมั่นที่จะรักษาความปลอดภัยของข้อมูลที่มีอยู่ในทุกระดับทั่วทั้งองค์กร

2.2.3 ข้อกำหนดด้านการรักษาความปลอดภัยตามมาตรฐาน ISO 27001:2013

- มาตรฐานไอเอสโอ 27001:2013 ประกอบด้วย

ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย 14 ข้อ			วัตถุประสงค์การควบคุม รวม 35 วัตถุประสงค์	การควบคุม 114 ข้อ
1	A.5	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)	1	2
2	A.6	โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)	2	7
3	A.7	ความมั่นคงปลอดภัยสำหรับบุคลากร (Human resource security)	3	6
4	A.8	การบริหารจัดการทรัพย์สิน (Asset management)	3	10
5	A.9	การควบคุมการเข้าถึง (Access control)	4	14
6	A.10	การเข้ารหัสข้อมูล (Cryptography)	1	2
7	A.11	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)	2	15
8	A.12	ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations security)	7	14
9	A.13	ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	2	7
10	A.14	การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)	3	13
11	A.15	ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)	2	5
12	A.16	การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)	1	7
13	A.17	ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)	2	4
14	A.18	ความสอดคล้อง (Compliance)	2	8

รูปที่ 2.2 ตัวอย่างหัวข้อที่มาตรฐานไอเอสโอ 27001:2013 กำหนด
(**ที่มา:** โครงสร้างของมาตรฐาน ISO 27001:2013 | ECS (ecs-support.github.io))

โครงสร้างของมาตรฐาน ISO 27001:2013 ดังรูปที่ 2.2 แบ่งเนื้อหาออกเป็น 14 หัวข้อ (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 35 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมันคงปลอดภัย แตกต่างกัน รวมแล้ว 114 ข้อ (Controls)

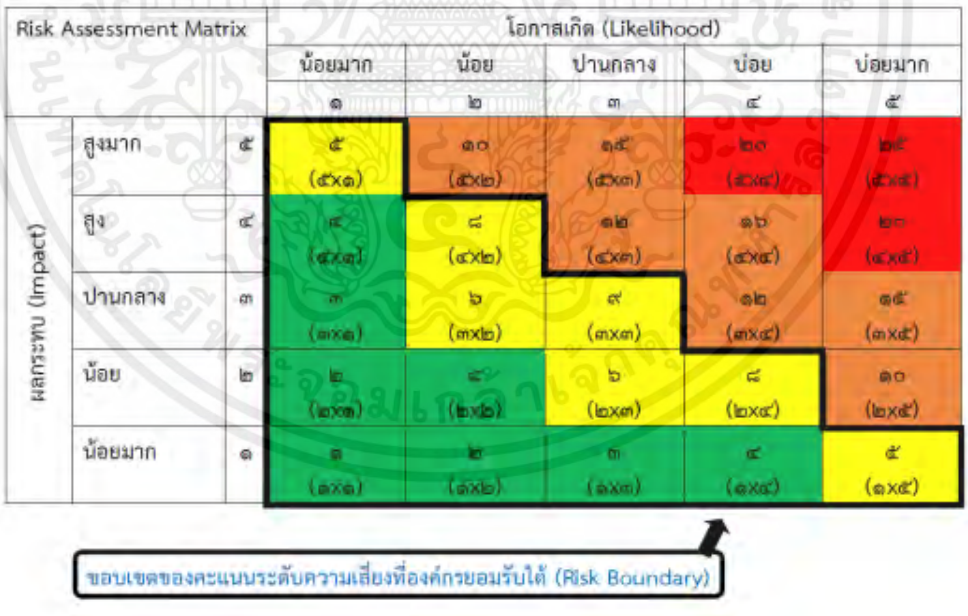
2.3 การบริหารจัดการความเสี่ยง (Risk Management)

การบริหารจัดการความเสี่ยง Risk Management [6] คือ กระบวนการในการบริหารจัดการความเสี่ยง จะประกอบด้วย 2 ส่วนหลัก ๆ

- คือ Risk Assessment (การประเมินความเสี่ยง)
- Risk Treatment (การควบคุมความเสี่ยง)

Risk Management ISO 27001

กระบวนการในการบริหารจัดการความเสี่ยงเป็น Requirement หนึ่งในการจัดทำระบบ ISMS (Information Security Management Systems) ตามมาตรฐาน ISO 27001 และถือเป็นส่วนสำคัญที่มีผลอย่างมากต่อความสำเร็จและความมีประสิทธิภาพ ของระบบ ISMS โดยตัวมาตรฐาน ISO 27001 นั้น เปิดกว้างและมิได้มีการระบุถึงวิธีการที่จะต้องใช้ในการจัดการความเสี่ยง แต่อย่างใด ซึ่งวิธีการในการบริหารจัดการความเสี่ยงของแต่ละองค์กรอาจมีความแตกต่างกันไปได้หลากหลายวิธี ขึ้นกับลักษณะการดำเนินธุรกิจ ขนาดขององค์กร นโยบายของผู้บริหาร เป็นต้น โดยในบทความนี้ จะกล่าวถึงหลักการและแนวความคิด ของการบริหารจัดการความเสี่ยงอย่างกว้าง ๆ โดยมิได้อ้างอิงถึงวิธีการของตำราใดโดยเฉพาะ โดยแสดงให้เห็นดังรูปที่ 2.3



รูปที่ 2.3 ตัวอย่างตารางการบริหารจัดการความเสี่ยง
(**ที่มา:** เอกสารไอเอสโอต้นฉบับของทางบริษัทอักษร)

2.3.1 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง Risk Assessment [7] คือ ความเสี่ยงรูปแบบต่าง ๆ ที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลสำคัญและระบบ / อุปกรณ์ต่าง ๆ ที่สนับสนุนการทำงานให้กับข้อมูลสำคัญนี้อยู่ โดยขั้นตอนนี้จะเป็นขั้นของการประเมินระดับของความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่าง ๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงในขั้นตอนต่อไป

ระดับของความเสี่ยง (Risk Level) โดยปกติระดับความเสี่ยงจะพิจารณาจาก 2 ปัจจัย คือ

- ความน่าจะเป็น (Probability) ในการที่จะเกิดภัยคุกคามใด ๆ ขึ้น และก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กร ซึ่งโดยปกติจะคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคาม / จุดอ่อน (Threat / Vulnerability Assessment) ที่มีต่อข้อมูลและทรัพย์สินขององค์กร ร่วมกับการพิจารณาถึงวิธีการควบคุมความเสี่ยง ที่มีอยู่ในปัจจุบัน (Existing Control)
- ความรุนแรง (Severity) ของความเสียหายที่อาจเกิดขึ้น ซึ่งโดยปกติจะคำนวณค่าโดยการพิจารณาจาก ระดับความสำคัญ ของข้อมูลหรือทรัพย์สินนั้น ๆ ที่มีต่อองค์กร

Quantitative vs. Qualitative

การประเมินความเสี่ยงโดยส่วนมาก จะทำการประเมินและแสดงค่าต่าง ๆ ในเชิง Qualitative เนื่องจากผลกระทบต่าง ๆ ที่อาจเกิดขึ้นต่อข้อมูลและทรัพย์สินขององค์กร อาจจะก่อให้เกิดความเสียหายในด้านของเม็ดเงิน (ที่สามารถวัดได้ในเชิง Quantitative) และยังมีความเสียหายบางอย่าง เช่น ชื่อเสียงและภาพลักษณ์ขององค์กร การเสียโอกาสในเชิงธุรกิจ ซึ่งอาจจะประเมินค่าเป็นตัวเงินได้ยาก หรือไม่สามารถประเมินค่าได้ ดังนั้นจึงนิยมใช้ การประเมินค่าแบบ Qualitative เป็น High Medium และ Low (3 ระดับ) หรืออาจใช้ถึง 5 ระดับ หรือ 7 ระดับ ตามความเหมาะสมขององค์กร

Threat (ภัยคุกคาม)

ภัยคุกคาม หมายถึง ปัจจัยจากภายนอกที่อาจเข้ามาทำร้ายหรือก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สิน ขององค์กร ภัยคุกคามนี้อาจแบ่งได้เป็นหลายประเภท ยกตัวอย่างเช่น ภัยคุกคามจากคน (ภายในองค์กร) เช่น การฉ้อโกง การทำงานผิดพลาด ภัยคุกคามจากคน (ภายนอกองค์กร) เช่น การ Hack Social (เช่น การหลอกถามข้อมูล) การก่อวินาศกรรม การโจรกรรม ภัยธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว ภัยคุกคามจากสภาพแวดล้อมที่ไม่เหมาะสม เช่น น้ำรั่ว ฝุ่นละออง สารเคมี

Vulnerability (จุดอ่อน)

การพิจารณาถึง จุดอ่อน หรือ Vulnerability จะพิจารณาจากปัจจัยภายในขององค์กร หรือจุดอ่อนของตัวข้อมูลและทรัพย์สิน โดยปกติ Threat และ Vulnerability จะต้องถูกพิจารณาควบคู่

กันไป เพราะถ้ามีภัยคุกคามจากปัจจัยภายนอกอยู่จริง แต่ตัวข้อมูล ทรัพย์สิน และระบบของเราไม่มีจุดอ่อน ภัยคุกคามก็ไม่สามารถทำอันตรายหรือก่อให้เกิดความเสียหายได้ เช่น ถ้าภัยคุกคามคือพนักงานที่ถูกเลิกจ้างหรือลาออกไปแล้วอาจใช้ User Account ของคนที่เคยมีอยู่มา Login เข้าเพื่อขโมยข้อมูลหรือกระทำการใด ที่ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์ขององค์กร จุดอ่อนในที่นี้ก็คือ การที่องค์กรไม่ลบหรือเพิกถอนสิทธิของบุคคล ที่ถูกเลิกจ้างหรือลาออกจากองค์กรไปแล้วโดยทันที ดังนั้นถ้าองค์กรมีกระบวนการในการเพิกถอนสิทธิการเข้าระบบทันทีที่พนักงาน ลาออก ภัยคุกคามนี้ก็ไม่สามารถทำอันตรายต่อระบบและข้อมูลขององค์กรได้ การค้นหาเพื่อระบุถึง จุดอ่อน หรือ Vulnerability ของระบบภายในองค์กรนั้น ในบางทีอาจต้องใช้วิธีทางเทคนิคเข้ามาช่วย เพื่อค้นหาจุดอ่อนในเชิง Logical ของระบบ เช่น การทำ Vulnerability Assessment ให้กับระบบ IT ขององค์กร

2.3.2 การควบคุมความเสี่ยง (Risk Treatment)

การควบคุมความเสี่ยง (Risk Treatment [7] คือ ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO 27001 นั้นมีอยู่ 4 ทาง คือ

1. การลดความเสี่ยง (Risk Reduction) คือ การพิจารณาหาวิธีในการควบคุม / แก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับที่องค์กรสามารถยอมรับได้ ซึ่งในมาตรฐาน ISO 27001 มีวิธีการในการแก้ไข / ควบคุมความเสี่ยงที่ได้แนะนำไว้ทั้งหมด 127 Controls
2. การยอมรับความเสี่ยง (Risk Acceptance) คือ การที่องค์กรพิจารณาแล้วพบว่า การดำเนินการแก้ไข / ควบคุมความเสี่ยงนั้น ไม่เหมาะสม ไม่สามารถกระทำได้ในทางปฏิบัติ หรือ ไม่คุ้มค่า เช่น ค่าใช้จ่ายในการดำเนินการแก้ไข / ควบคุม มีมูลค่า สูงกว่ามูลค่าของข้อมูลและทรัพย์สินที่จะทำการปกป้อง ทั้งนี้ ขึ้นอยู่กับดุลยพินิจของผู้บริหาร
3. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงโดยยกเลิกกระบวนการทำงาน หรือทรัพย์สิน ที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำเมื่อการแก้ไขความเสี่ยงด้วยวิธีการอื่นนั้น ไม่คุ้มกับผลประโยชน์ที่ได้ จากการทำงานด้วยกระบวนการหรือทรัพย์สินนั้น ๆ
4. การโอนความเสี่ยง (Risk Transfer) คือ การพิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย เป็นต้น

Control ที่สามารถเลือกใช้เพื่อการควบคุมความเสี่ยง อาจแบ่งออกเป็น 3 ประเภท ดังนี้

Physical Control คือ การจัดให้มีสภาพแวดล้อมทางกายภายที่เหมาะสม เช่น

- การจัดให้มี Access Control ควบคุมการเข้า – ออก
- การจัดแบ่งพื้นที่สำคัญ เช่น Data Center ออกจากพื้นที่ปฏิบัติงานปกติ
- การจัดเก็บสายเคเบิลต่าง ๆ ให้เรียบร้อย

Technical Control คือ การใช้ซอฟต์แวร์หรืออุปกรณ์ฮาร์ดแวร์มาช่วยควบคุมและจัดการด้าน Security เช่น

- Encryption
- Anit-virus
- Firewall
- Intrusion Detection System (IDS)

Administrative Control คือ การจัดให้มีนโยบาย ระเบียบ วิธีการปฏิบัติงาน (Procedure) การฝึกอบรมที่เหมาะสมสำหรับบุคลากรทั้งหมดที่เกี่ยวข้องกับการดำเนินงานขององค์กร รวมถึง Third Party และ Outsource

บทที่ 3
การศึกษาและออกแบบกระบวนการ

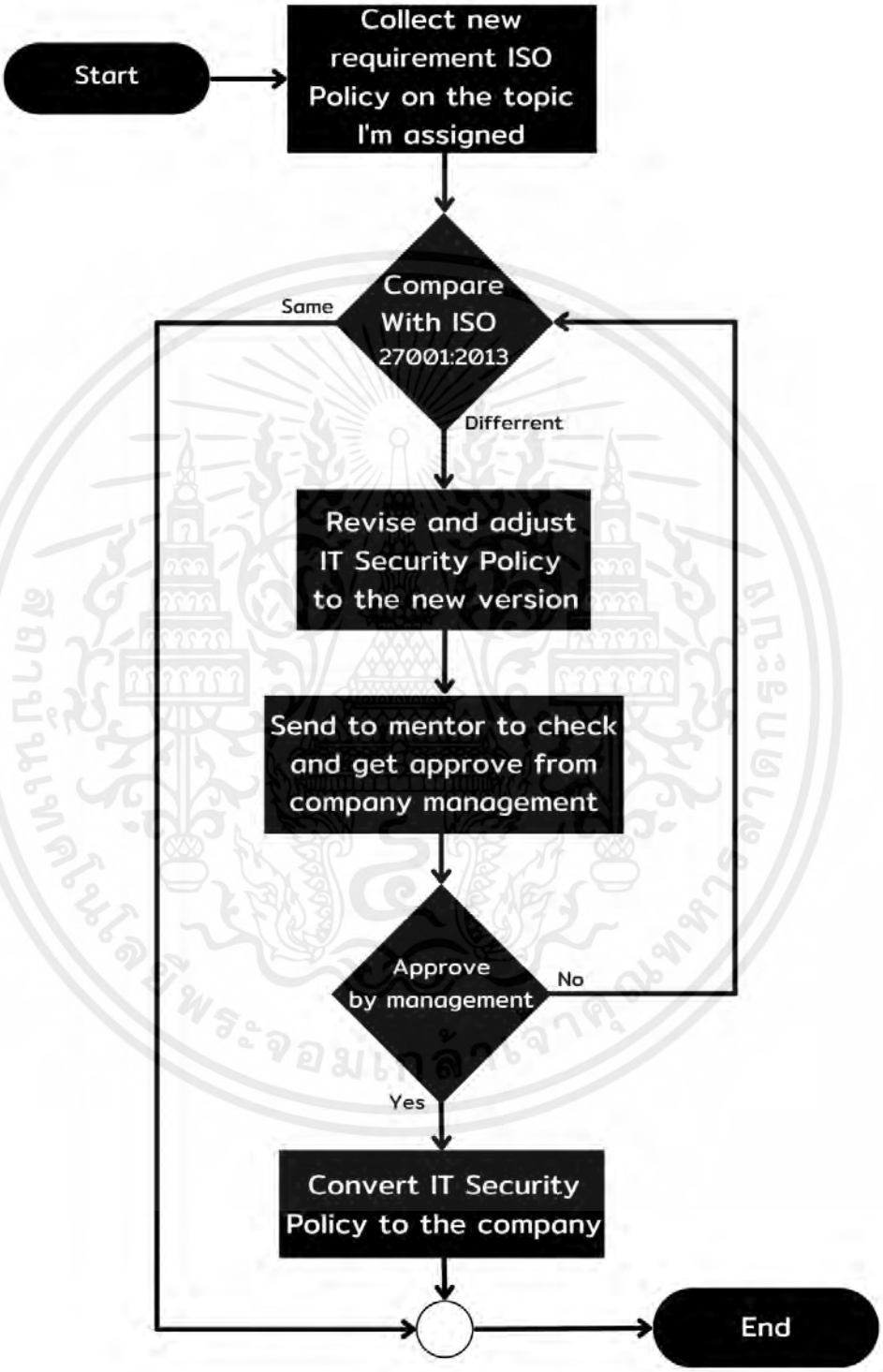
ในบทนี้จะกล่าวถึงขั้นตอนการดำเนินการของการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 เช่น การศึกษาข้อมูลเก่า การเก็บรวบรวมข้อมูล และขั้นตอนการทำงาน การทำเอกสารและการปรับใช้ข้อบังคับของอุปกรณ์ไอทีและระบบต่าง ๆ ให้เป็นไปตามมาตรฐานไอเอสโอ 27001:2013 ในหัวข้อที่ได้รับมอบหมาย การปรับเปลี่ยนอุปกรณ์ไอทีและซอฟต์แวร์ต่าง ๆภายในองค์กร การทำ Active Directory โดยผู้จัดทำดำเนินงานตามขั้นตอนดังต่อไปนี้

3.1 แนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001:2013

รูปที่ 3.1 ภาพรวมของการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013

ผู้จัดทำได้ออกแบบภาพรวมของวิธีการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 ดังรูปที่ 3.1 โดยผู้จัดทำจะเริ่มศึกษาข้อมูลมาตรฐานเก่าตามนโยบาย ISO 27001:2005 และ ออกไปเก็บรวบรวมข้อมูลทั้งหมดจากผู้ใช้งาน (User) จากนั้นจะนำข้อมูลมาปรับให้เข้ากับมาตรฐานใหม่ตามนโยบาย ISO 27001:2013 และดำเนินการปรับเปลี่ยนอุปกรณ์ไอทีและระบบบัญชีผู้ใช้ตามหัวข้อที่ได้รับมอบหมาย ให้สอดคล้องกับมาตรฐานใหม่และจัดทำเอกสารเพื่อส่งให้หัวหน้างานพิจารณตรวจสอบและส่งกลับมาแก้ไขก่อนที่จะส่งเข้าที่ประชุมขององค์กรต่อไป

3.2 การออกแบบกระบวนการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001:2013

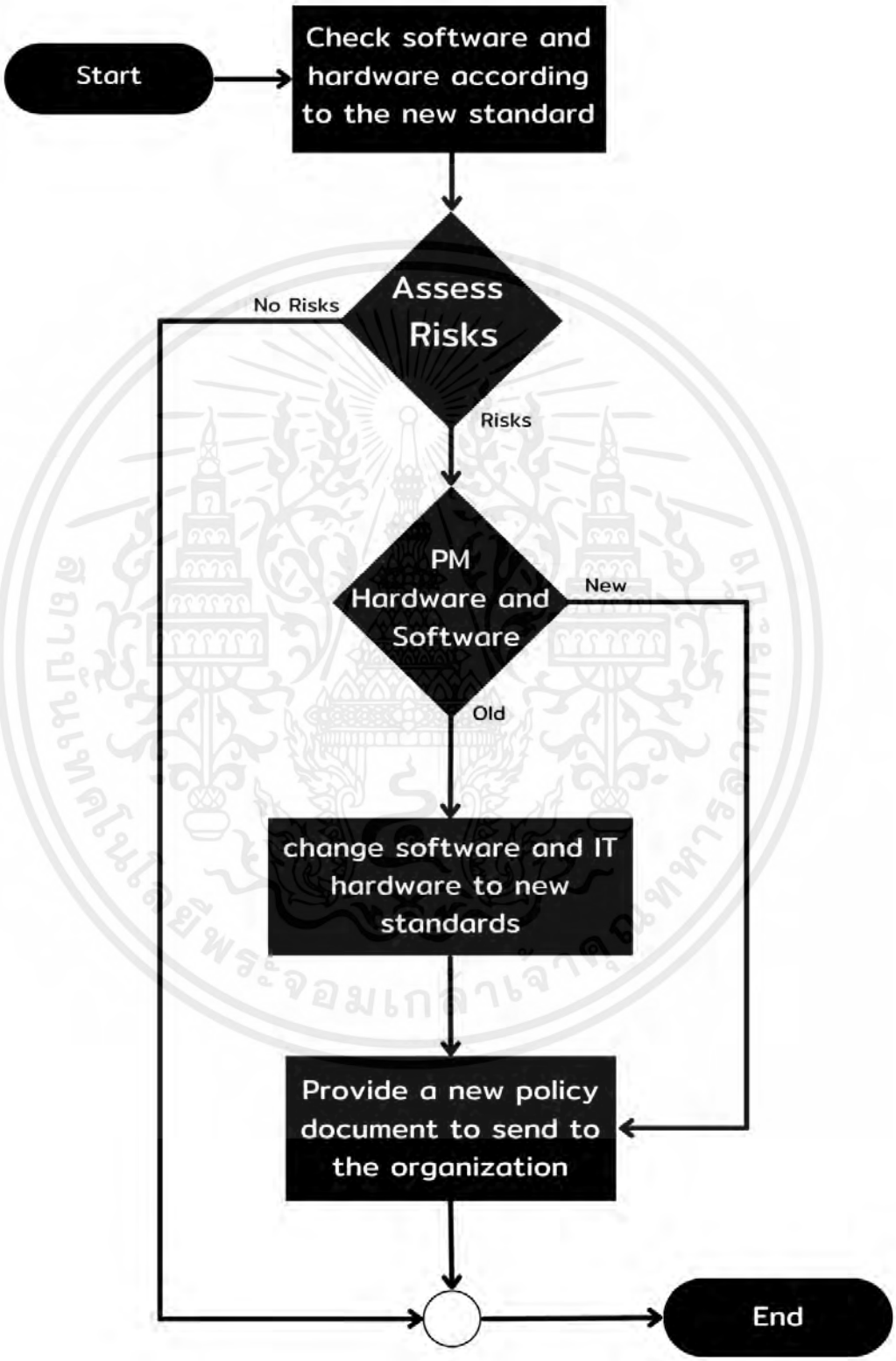


รูปที่ 3.2 การออกแบบกระบวนการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001:2013

การทำงานของการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 ดังรูปที่ 3.2 แบ่งการทำงานออกเป็น 4 ขั้นตอน ได้แก่ ขั้นตอนการเก็บรวบรวมข้อมูล ขั้นตอนการนำข้อมูลมาเปรียบเทียบและปรับให้เข้ากับมาตรฐานใหม่ ขั้นตอนการแก้ไขระบบและอุปกรณ์ให้สอดคล้องกับมาตรฐานใหม่ ขั้นตอนการจัดทำเอกสารและส่งต่อให้ผู้จัดการเพื่อนำส่งยื่นของมาตรฐานต่อไป ดังแสดงในรูปที่ 3.2 ซึ่งมีขั้นตอนการทำงานดังนี้

1. เก็บรวบรวมข้อมูลเกี่ยวกับมาตรฐานไอเอสโอ ในหัวข้อที่ได้รับมอบหมาย
2. นำข้อมูลเปรียบเทียบระหว่างไอเอสโอ 27001:2005 กับไอเอสโอ 27001:2013
3. หากข้อมูลใดที่มีการบังคับใช้หรือข้อกำหนดที่เหมือนเดิม ไม่แตกต่างจากมาตรฐานใหม่ ก็จบการทำงานสามารถจบนำมาทำเป็นเอกสารได้ทันที
4. หากข้อมูลมีการบังคับใช้หรือข้อกำหนดที่ไม่เหมือนเดิม หรือต่างออกไปจากมาตรฐานใหม่ ผู้จัดทำจะทำการแก้ไขข้อมูลเหล่านั้นให้เป็นปัจจุบันเพื่อให้สอดคล้องกับมาตรฐานใหม่
5. ส่งข้อมูลและเอกสารไปให้หัวหน้างานทำการตรวจสอบความถูกต้องของเอกสารและมาตรฐานทั้งหมด เพื่อนำไปปรับใช้กับองค์กร
6. หากผู้จัดการอนุมัติ ก็จะส่งต่อเอกสารให้องค์กร เพื่อนำไปยื่นขอมาตรฐานต่อไป
7. หากไม่ได้รับการอนุมัติจากผู้จัดการ ก็จะส่งเอกสารเหล่านั้นกลับมาให้ผู้จัดทำ แก้ไข้เพิ่มเติม เพื่อให้สอดคล้องกับความต้องการของผู้บริหารและมาตรฐานใหม่

3.2.1 การปรับปรุงหลักปฏิบัติการบริหารจัดการทรัพย์สิน



รูปที่ 3.3 กระบวนการปรับปรุงหลักปฏิบัติการบริหารจัดการทรัพย์สิน

การทำงานของการปรับปรุงหลักปฏิบัติการบริหารจัดการทรัพย์สิน ดังรูปที่ 3.3 แบ่งการทำงานออกเป็น 5 ขั้นตอน ได้แก่ ขั้นตอนการเก็บข้อมูลระบบและอุปกรณ์ไอทีทั้งหมด ขั้นตอนการนำข้อมูลมาประเมินความเสี่ยง ขั้นตอนการตรวจสอบระบบและอุปกรณ์ไอทีและทำการป้องกันเชิงรุก ขั้นตอนการเปลี่ยนระบบและอุปกรณ์ไอทีให้สอดคล้องกับมาตรฐานใหม่ ขั้นตอนการจัดทำเอกสารและส่งต่อให้องค์กรเพื่อนำส่งยื่นของมาตรฐานต่อไป ดังแสดงในรูปที่ 3.3 ซึ่งมีขั้นตอนการทำงานดังนี้

1. เก็บข้อมูลระบบและอุปกรณ์ไอทีทั้งหมดในหัวข้อและรายการที่ได้รับมอบหมาย
2. การนำข้อมูลมาประเมินความเสี่ยง
3. หากข้อมูลใดที่ไม่มีความเสี่ยง ไม่แตกต่างจากมาตรฐานใหม่ ก็จบการทำงานสามารถจบนำมาทำเป็นเอกสารได้ทันที
4. หากข้อมูลมีความเสี่ยงหรือข้อกำหนดที่ไม่เหมือนเดิม หรือต่างออกไปจากมาตรฐานใหม่ ผู้จัดทำจะทำการตรวจสอบระบบและอุปกรณ์ไอทีและทำการป้องกันเชิงรุกเพื่อให้สอดคล้องกับมาตรฐานใหม่
5. หากระบบและอุปกรณ์ไอทียังเป็นรุ่นเก่าผู้จัดทำจะทำการเปลี่ยนระบบและอุปกรณ์ไอทีให้สอดคล้องกับมาตรฐานใหม่
6. หากระบบและอุปกรณ์ไอทีเป็นรุ่นปัจจุบันหรือใหม่อยู่แล้ว ก็จบการทำงานสามารถจบนำมาทำเป็นเอกสารได้ทันที
7. ส่งข้อมูลและเอกสารไปให้ผู้จัดการทำการตรวจสอบความถูกต้องของเอกสารและมาตรฐานทั้งหมด เพื่อนำไปปรับใช้กับองค์กร
8. หากผู้จัดการอนุมัติ ก็จะส่งต่อเอกสารให้องค์กร เพื่อนำไปยื่นขอมาตรฐานต่อไป
9. หากไม่ได้รับการอนุมัติจากผู้จัดการ ก็จะส่งเอกสารเหล่านั้นกลับมาให้ผู้จัดทำแก้ไขเพิ่มเติม เพื่อให้สอดคล้องกับความต้องการของผู้บริหารและมาตรฐานใหม่

ITSP-002 : IT Asset Management (มาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์)

IT Standard Procedure

บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

ITSP-002: IT Asset Management
(มาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์)

แก้ไขครั้งที่ 1		วันที่ที่มีผลบังคับใช้ ตุลาคม 2564	
ผู้จัดทำ :	เดิมพันธ์ ช่วยบคร		
ผู้สอบทาน1 :			
ผู้อนุมัติ :			

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 1

รูปที่ 3.4 ตัวอย่างหน้าปกหัวข้อ ITSP-002 : IT Asset Management (มาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์

รูปที่ 3.4 เป็นหน้าปกของหัวข้อ ITSP-002 เครื่องคอมพิวเตอร์ และ อุปกรณ์ต่อเชื่อม หรือเครื่องอิเล็กทรอนิกส์อื่น ๆ ต้องเป็นทรัพย์สินขององค์กร ที่ใช้งานเชื่อมต่อกับเครือข่ายในองค์กร ห้ามนำเครื่องหรืออุปกรณ์ชนิดอื่นมาใช้งานโดยไม่ได้รับอนุญาติ โปรแกรมที่ใช้งานภายในองค์กรต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

ตารางที่ 3.1 ตารางแสดงความเสี่ยงของหัวข้อ ITSP-002

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 3.1 การทำ Risk Management พบว่า ก่อนทำการปรับแก้นโยบาย ITSP-002 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความเสี่ยงสูงและบ่อยครั้งในการเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุ

- **มาตรฐานการใช้เครื่องคอมพิวเตอร์**

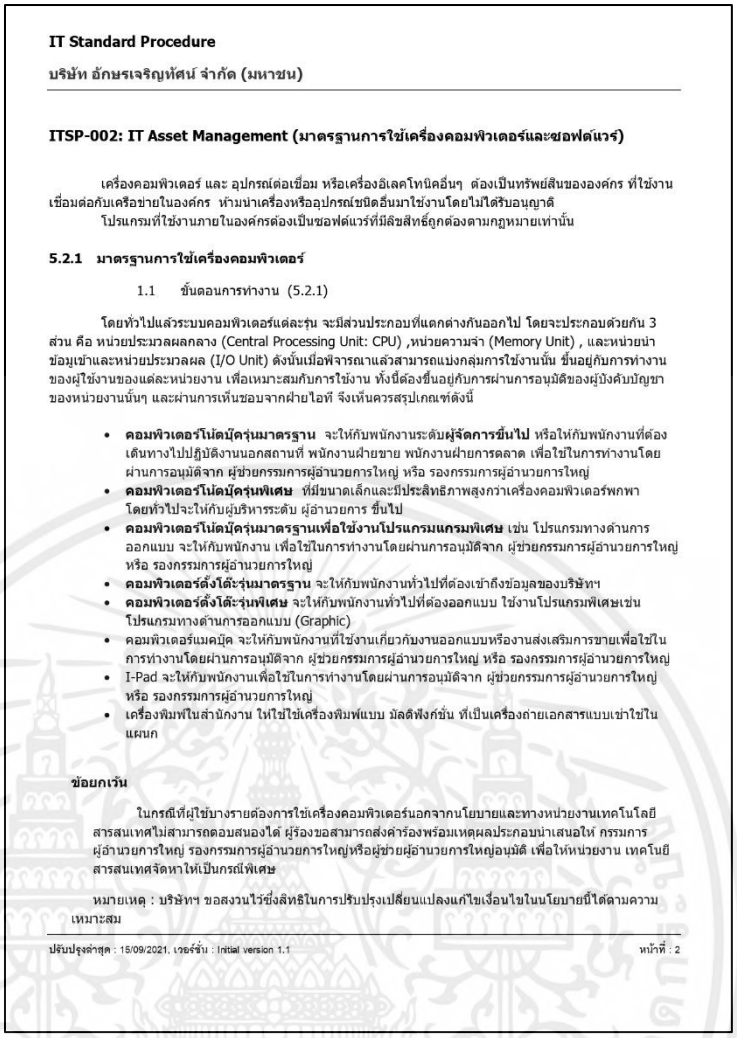
ขั้นตอนการทำงานดังรูปที่ 3.5 โดยทั่วไปแล้วระบบคอมพิวเตอร์แต่ละรุ่น จะมีส่วนประกอบที่แตกต่างกันออกไป โดยจะประกอบด้วยกัน 3 ส่วน คือ หน่วยประมวลผลกลาง (Central Processing Unit: CPU)หน่วยความจำ (Memory Unit) และหน่วยนำข้อมูลเข้าและหน่วยประมวลผล (I/O Unit) ดังนั้นเมื่อพิจารณาแล้วสามารถแบ่งกลุ่มการใช้งานนั้น ขึ้นอยู่กับการทำงานของผู้ใช้งานของแต่ละหน่วยงาน เพื่อเหมาะสมกับการใช้งาน ทั้งนี้ต้องขึ้นอยู่กับการผ่านการอนุมัติของผู้บังคับบัญชาของหน่วยงานนั้น ๆ และผ่านการเห็นชอบจากฝ่ายไอที จึงเห็นควรสรุปเกณฑ์ดังนี้

- **คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐาน** จะให้กับพนักงานระดับ**ผู้จัดการขึ้นไป** หรือให้กับพนักงานที่ต้องเดินทางไปปฏิบัติงานนอกสถานที่ พนักงานฝ่ายขาย พนักงานฝ่ายการตลาด เพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- **คอมพิวเตอร์โน้ตบุ๊ครุ่นพิเศษ** ที่มีขนาดเล็กและมีประสิทธิภาพสูงกว่าเครื่องคอมพิวเตอร์พกพาโดยทั่วไปจะให้กับผู้บริหารระดับ ผู้อำนวยการ ขึ้นไป
- **คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐานเพื่อใช้งานโปรแกรมแกรมพิเศษ** เช่น โปรแกรมทางด้านการออกแบบ จะให้กับพนักงาน เพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- **คอมพิวเตอร์ตั้งโต๊ะรุ่นมาตรฐาน** จะให้กับพนักงานทั่วไปที่ต้องเข้าถึงข้อมูลของบริษัทฯ
- **คอมพิวเตอร์ตั้งโต๊ะรุ่นพิเศษ** จะให้กับพนักงานทั่วไปที่ต้องออกแบบ ใช้งานโปรแกรมพิเศษเช่น โปรแกรมทางด้านการออกแบบ (Graphic)
- **คอมพิวเตอร์แมคบุ๊ค** จะให้กับพนักงานที่ใช้งานเกี่ยวกับงานออกแบบหรืองานส่งเสริมการขายเพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- I-Pad จะให้กับพนักงานเพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- **เครื่องพิมพ์ในสำนักงาน** ให้ใช้ใช้เครื่องพิมพ์แบบ มัลติฟังก์ชั่น ที่เป็นเครื่องถ่ายเอกสารแบบเช่าใช้ในแผนก

ข้อยกเว้น

ในกรณีที่ผู้ใช้บางรายต้องการใช้เครื่องคอมพิวเตอร์นอกจากนโยบายและทางหน่วยงานเทคโนโลยีสารสนเทศไม่สามารถตอบสนองได้ ผู้ร้องขอสามารถส่งคำร้องพร้อมเหตุผลประกอบนำเสนอให้ กรรมการผู้อำนวยการใหญ่ รองกรรมการผู้อำนวยการใหญ่หรือผู้ช่วยผู้อำนวยการใหญ่อนุมัติ เพื่อให้หน่วยงาน เทคโนยีสารสนเทศจัดหาให้เป็นกรณีพิเศษ

หมายเหตุ : บริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขในนโยบายนี้ได้ตามความเหมาะสม



IT Standard Procedure

บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

ITSP-002: IT Asset Management (มาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์)

เครื่องคอมพิวเตอร์ และ อุปกรณ์ต่อเชื่อม หรือเครื่องอิเลคโทนิคอื่นๆ ต้องเป็นทรัพย์สินขององค์กร ที่ใช้งานเชื่อมต่อกับเครือข่ายในองค์กร ห้ามนำเครื่องหรืออุปกรณ์ชนิดอื่นมาใช้งานโดยไม่ได้รับอนุญาติ
โปรแกรมที่ใช้งานภายในองค์กรต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

5.2.1 มาตรฐานการใช้เครื่องคอมพิวเตอร์

1.1 ขั้นตอนการทำงาน (5.2.1)

โดยทั่วไปแล้วระบบคอมพิวเตอร์แต่ละรุ่น จะมีส่วนประกอบที่แตกต่างกันออกไป โดยจะประกอบด้วยกัน 3 ส่วน คือ หน่วยประมวลผลกลาง (Central Processing Unit: CPU) ,หน่วยความจำ (Memory Unit) , และหน่วยนำข้อมูลเข้าและหน่วยประมวลผล (I/O Unit) ดังนั้นเมื่อพิจารณาแล้วสามารถแบ่งกลุ่มการใช้งานนั้น ขึ้นอยู่กับการทำงานของผู้ใช้งานของแต่ละหน่วยงาน เพื่อเหมาะสมกับการใช้งาน ทั้งนี้ต้องขึ้นอยู่กับการผ่านการอนุมัติของผู้บังคับบัญชาของหน่วยงานนั้นๆ และผ่านการเห็นชอบจากฝ่ายไอที จึงเห็นควรสรุปเกณฑ์ดังนี้

- **คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐาน** จะให้กับพนักงานระดับ**ผู้จัดการขึ้นไป** หรือให้กับพนักงานที่ต้องเดินทางไปปฏิบัติงานนอกสถานที่ พนักงานฝ่ายขาย พนักงานฝ่ายการตลาด เพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- **คอมพิวเตอร์โน้ตบุ๊ครุ่นพิเศษ** ที่มีขนาดเล็กและมีประสิทธิภาพสูงกว่าเครื่องคอมพิวเตอร์พกพา โดยทั่วไปจะให้กับผู้บริหารระดับ ผู้อำนวยการ ขึ้นไป
- **คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐานเพื่อใช้งานโปรแกรมแกรมพิเศษ** เช่น โปรแกรมทางด้านการออกแบบ จะให้กับพนักงาน เพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- **คอมพิวเตอร์ตั้งโต๊ะรุ่นมาตรฐาน** จะให้กับพนักงานทั่วไปที่ต้องเข้าถึงข้อมูลของบริษัทฯ
- **คอมพิวเตอร์ตั้งโต๊ะรุ่นพิเศษ** จะให้กับพนักงานทั่วไปที่ต้องออกแบบ ใช้งานโปรแกรมพิเศษเช่น โปรแกรมทางด้านการออกแบบ (Graphic)
- คอมพิวเตอร์แมคบุ๊ค จะให้กับพนักงานที่ใช้งานเกี่ยวกับงานออกแบบหรืองานส่งเสริมการขายเพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- I-Pad จะให้กับพนักงานเพื่อใช้ในการทำงานโดยผ่านการอนุมัติจาก ผู้ช่วยกรรมการผู้อำนวยการใหญ่ หรือ รองกรรมการผู้อำนวยการใหญ่
- เครื่องพิมพ์ในสำนักงาน ให้ใช้เครื่องพิมพ์แบบ มัลติฟังก์ชั่น ที่เป็นเครื่องถ่ายเอกสารแบบเข้าใช้ในแผนก

ข้อยกเว้น

ในกรณีที่ผู้ใช้บางรายต้องการใช้เครื่องคอมพิวเตอร์นอกจากนโยบายและทางหน่วยงานเทคโนโลยีสารสนเทศไม่สามารถตอบสนองได้ ผู้ร้องขอสามารถส่งคำร้องพร้อมเหตุผลประกอบนำเสนอให้ กรรมการผู้อำนวยการใหญ่ รองกรรมการผู้อำนวยการใหญ่หรือผู้ช่วยผู้อำนวยการใหญ่อนุมัติ เพื่อให้หน่วยงาน เทคโนยีสารสนเทศจัดหาให้เป็นกรณีพิเศษ

หมายเหตุ : บริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขในนโยบายนี้ได้ตามความเหมาะสม

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 2

รูปที่ 3.5 ตัวอย่างมาตรฐานการใช้เครื่องคอมพิวเตอร์

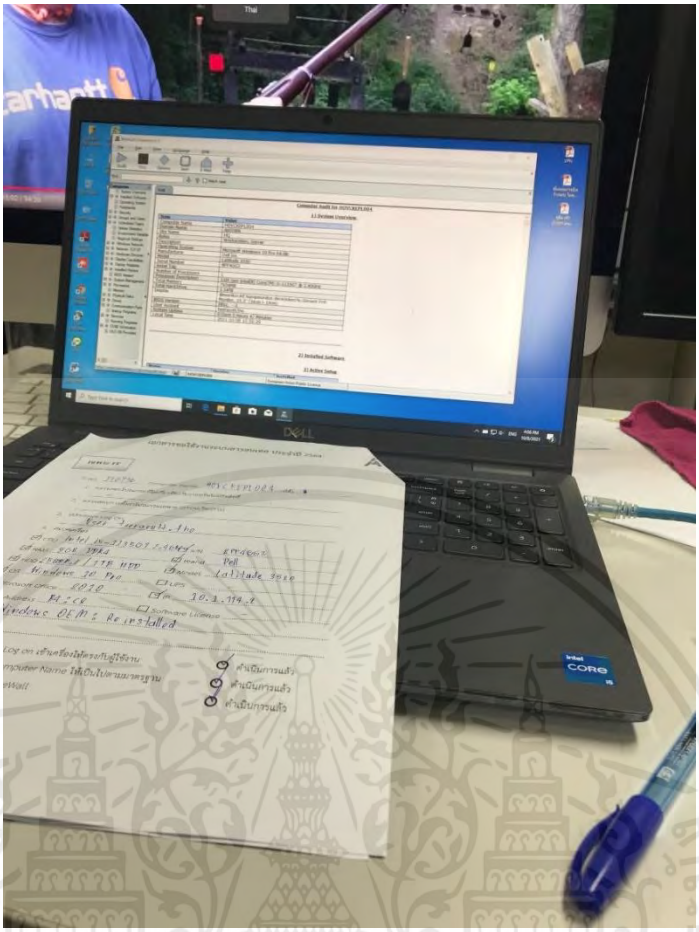
คุณสมบัติด้านเทคนิค บริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขคุณสมบัติทางด้านเทคนิคนี้ได้ตามความเหมาะสม เพื่อให้รองรับกับ Application ต่าง ๆ ของบริษัท และ technology ใหม่ ๆ ที่เกิดขึ้นโดยจะทำการปรับปรุงอย่างน้อย 1 ครั้งต่อปี

- คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐานจะมีรายละเอียดดังตารางที่ 3.2 และรูปภาพตัวอย่างดังรูปที่ 3.6

ตารางที่ 3.2 ตารางแสดงคุณสมบัติด้านเทคนิคของคอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐาน

Detail	Specification
CPU	Core i5 ความเร็วไม่ต่ำกว่า 1.7 GHz
Cache	ไม่ต่ำกว่า L3 Cache ขนาดไม่น้อยกว่า 4 MB
Ram	ชนิด DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 4GB
HDD	ขนาดความจุไม่น้อยกว่า 500 GB มีความเร็วรอบไม่ต่ำกว่า 7200 rpm
DVD	DVD +/-RW Drive
Graphic Adapter	ที่เทียบเท่า Intel® HD Graphics หรือดีกว่า
Pointing Device / Touch Pad	Multi TouchPad และแบบ TrackPoint หรือดีกว่า
Monitor	มีจอภาพขนาดไม่น้อยกว่า 15.6 นิ้ว ชนิด HD Anti-Glare LED backlight แบบ 16:9 ความละเอียดภาพอย่างน้อย 1366x768 pixels
Audio	มี Port สำหรับแบบ Combo mic/Headphone Jack อย่างน้อย 1 Port
Ethernet	ช่องสื่อสาร RJ-45 มาตรฐาน 10/100/1000 Gigabit Ethernet อย่างน้อย 1 ช่อง
WiFi	ไม่น้อยกว่ามาตรฐาน IEEE 802.11 แบบ a/b/g/n และ Bluetooth
I/O Interface	- ช่องเชื่อมต่อ VGA อย่างน้อย 1ช่อง - ช่องเชื่อมต่อ HDMI หรือ Display Port อย่างน้อย 1 ช่อง - ช่องสื่อสาร USB อย่างน้อย 3 ช่อง (USB 3.0 อย่างน้อย 1 ช่อง)
Expansion Slot	PCI Express 2.0x16 at Last 1 or more PCIe 2.0x1 at Last 1 or more
Keyboard	- มีระบบ Spill Resistant เพื่อป้องกันอุปกรณ์ภายในตัวเครื่องจากการทำน้ำหกใส่ - มีอักษรภาษาไทยพิมพ์ติดที่ Keyboard จากโรงงาน - มี Function keys 12 keys
Mouse	USB Optical Mouse
Chassis	Small From or Small Desktop
Power Supply	Not less than 240 watt
Operating System (OS)	Microsoft Windows Professional 64 bit
Web Camera	ความละเอียดไม่ต่ำกว่า HD 720p ที่มีระบบ Face Tracking

Battery	ชนิด Lithium Ion ไม่น้อยกว่า 3-Cell up to 6 hr. or more
Other	- มีโปรแกรมจัดการอุปกรณ์ ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดทำ Backup / Restore ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดการ Battery - สามารถดำเนินการทำ System Recovery ได้กรณี OS มีปัญหาการใช้งาน - อุปกรณ์ส่วนประกอบทั้งหมดต้องเป็นไปตามมาตราฐานสากล FCC UL EPEAT Gold Rating etc. - 3 Year Warranty and Onsite Service (Next Business Day) - Online Support and Download Utilities - มีช่องสำหรับ Express Card Slot ที่รองรับ Express Card /34 - มี Media Card Reader Slot แบบ 4 in 1 แบบติดตั้งภายใน หรือดีกว่า - มีระบบจัดการเรื่องเสียงและลำโพงแบบติดตั้งภายใน - ตัวเครื่องต้องเป็นวัสดุทนทานต่อแรงกระแทก เช่น Magnesium alloy หรือ Carbon-fiber - TPM 1.2 (Trusted Platform Module) - น้ำหนักไม่เกิน 2.8 Kg. - มีกระเป๋าสำหรับใส่เครื่องพร้อมอุปกรณ์ที่ออกแบบเพื่อให้ใส่คอมพิวเตอร์แบบ Notebook และมีวัสดุภายในที่ป้องกันการกระแทกจากภายนอก



รูปที่ 3.6 ตัวอย่างคอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐาน

- คอมพิวเตอร์โน้ตบุ๊ครุ่นพิเศษ ที่มีขนาดเล็กและมีประสิทธิภาพสูงกว่าเครื่องคอมพิวเตอร์พกพาโดยทั่วไปจะมีรายละเอียดดังตารางที่ 3.3

ตารางที่ 3.3 ตารางแสดงคุณสมบัติด้านเทคนิคของคอมพิวเตอร์โน้ตบุ๊ครุ่นพิเศษ

Detail	Specification
CPU	Core i5 ความเร็วไม่ต่ำกว่า 1.7 GHz
Cache	ไม่ต่ำกว่า L3 Cache ขนาดไม่น้อยกว่า 4 MB
BIOS	ต้องมีเครื่องหมายการค้าเดียวกันกับตัวเครื่อง
Ram	ชนิด DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 4GB
SDD	128 GB Solid State Drive or more
Graphic Adapter	ที่เทียบเท่า Intel® HD Graphics หรือดีกว่า
Display size	ไม่ต่ำกว่า 12" Hi-Def (720p)
Screen Type	LED-Backlit LCD
Weight	Not over 1.5 kg.
Webcam	1.3 MPixel with Microphone
Audio	Hi-Def audio
Battery	ชนิด Lithium Ion ไม่น้อยกว่า 3-Cell up to 6 hr. or more
OS	Windows 7 Professional 64-bit
Warranty	3 Year On Site service
Port & Interface	ช่องสื่อสาร USB อย่างน้อย 3 ช่อง (USB 3.0 อย่างน้อย 1 ช่อง) Display port อย่างน้อย 1 ช่อง
Connection	WiFi Bluetooth

- คอมพิวเตอร์โน้ตบุ๊ครุ่นมาตรฐานเพื่อใช้งานโปรแกรมแกรมพิเศษหรือโปรแกรมทางด้านการออกแบบจะมีรายละเอียดดังตารางที่ 3.4 และรูปภาพตัวอย่างดังรูปที่ 3.7

ตารางที่ 3.4 ตารางแสดงคุณสมบัติด้านเทคนิคของโน้ตบุ๊คเพื่อใช้งานโปรแกรมแกรมพิเศษ

Detail	Specification
CPU	Core i5 ความเร็วไม่ต่ำกว่า 1.7 GHz
Cache	ไม่ต่ำกว่า L3 Cache ขนาดไม่น้อยกว่า 4 MB
BIOS	ต้องมีเครื่องหมายการค้าเดียวกันกับตัวเครื่อง
Ram	ชนิด DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 4GB
HDD	ขนาดความจุไม่น้อยกว่า 500 GB มีความเร็วรอบไม่ต่ำกว่า 7200 rpm
DVD	DVD +/-RW Drive
Graphic Adapter	มีหน่วยควบคุมการแสดงผล ขนาดไม่น้อยกว่า 2 GB
Pointing Device / Touch Pad	Multi Touch Pad และแบบ TrackPoint หรือดีกว่า
Monitor	มีจอภาพขนาดไม่น้อยกว่า 15.6 นิ้ว TFT Wide Screen ชนิด HD Anti-Glare LED backlight แบบ 16:9 ความละเอียดไม่ต่ำกว่า 1366x768 หรือดีกว่า
Audio	มี Port สำหรับแบบ Combo mic/Headphone Jack อย่างน้อย 1 Port
Ethernet	ช่องสื่อสาร RJ-45 มาตรฐาน 10/100/1000 Gigabit Ethernet อย่างน้อย 1 ช่อง
WiFi	ไม่น้อยกว่ามาตรฐาน IEEE 802.11 แบบ a/b/g/n และ Bluetooth
I/O Interface	- ช่องเชื่อมต่อ VGA อย่างน้อย 1ช่อง - ช่องเชื่อมต่อ HDMI หรือ Display Port อย่างน้อย 1 ช่อง - ช่องสื่อสาร USB อย่างน้อย 3 ช่อง (USB 3.0 อย่างน้อย 1 ช่อง) - eSATA/USB at Last 1 or more - Media card reader
Keyboard	- มีระบบ Spill Resistant เพื่อป้องกันอุปกรณ์ภายในตัวเครื่องจากการทำน้ำหกใส่ - มีอักษรภาษาไทยพิมพ์ติดที่ Keyboard จากโรงงาน - มี Function keys 12 keys
Mouse	USB Optical Mouse
Chassis	Small From or Small Desktop

Power Supply	Not less than 240 watt
Operating System (OS)	Microsoft Windows Professional 64 bit
Web Camera	ความละเอียดไม่ต่ำกว่า HD 720p ที่มีระบบ Face Tracking
Battery	ชนิด Lithium Ion ไม่น้อยกว่า 3-Cell
Other	- มีโปรแกรมจัดการอุปกรณ์ ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดทำ Backup / Restore ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดการ Battery - สามารถดำเนินการทำ System Recovery ได้กรณี OS มีปัญหาการใช้งาน - อุปกรณ์ส่วนประกอบทั้งหมดต้องเป็นไปตามมาตราฐานสากล FCC UL EPEAT Gold Rating etc. - 3 Year Warranty and Onsite Service (Next Business Day) - Online Support and Download Utilities - มีช่องสำหรับ Express Card Slot ที่รองรับ Express Card /34 - มี Media Card Reader Slot แบบ 4 in 1 แบบติดตั้งภายใน หรือดีกว่า - External Monitor (VGA) อย่างน้อย 1 Port และแบบ Mini Display port จำนวนไม่น้อยกว่า 1 Port - ตัวเครื่องต้องเป็นวัสดุทนทานต่อแรงกระแทกเช่น Magnesium alloy หรือ Carbon-fiber - TPM 1.2 (Trusted Platform Module) - น้ำหนักไม่เกิน 2.8 Kg.
Bag	มีกระเป๋าสำหรับใส่เครื่องพร้อมอุปกรณ์ที่ออกแบบเพื่อให้ใส่คอมพิวเตอร์แบบ Notebook และมีวัสดุภายในที่ป้องกันการกระแทกจากภายนอก

รูปที่ 3.7 ตัวอย่างโน้ตบุ๊ครุ่นมาตรฐานเพื่อใช้งานโปรแกรมทางด้านการออกแบบ

- คอมพิวเตอร์ตั้งโต๊ะรุ่นมาตรฐานจะมีรายละเอียดดังตารางที่ 3.5 และรูปภาพตัวอย่างดังรูปที่ 3.8

ตารางที่ 3.5 ตารางแสดงคุณสมบัติด้านเทคนิคของคอมพิวเตอร์ตั้งโต๊ะรุ่นมาตรฐาน

Detail	Specification
CPU	Core i5 ความเร็วไม่ต่ำกว่า 1.7 GHz
Cache	ไม่ต่ำกว่า L3 Cache ขนาดไม่น้อยกว่า 4 MB
BIOS	ต้องมีเครื่องหมายเดียวกัน
Ram	ชนิด DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 4GB
HDD	ขนาดความจุไม่น้อยกว่า 500 GB มีความเร็วรอบไม่ต่ำกว่า 7200 rpm
DVD	DVD +/-RW Drive
Graphic Adapter	Intel® HD Graphics 2500 หรือดีกว่า

Monitor	LCD หรือ LED มีเครื่องหมายการค้าเดียวกับเครื่องคอมพิวเตอร์ มีความละเอียดไม่ต่ำกว่า 1366 x 768 pixels และมีขนาดไม่น้อยกว่า 19 inc. Wild Screen
Audio	Integrated High Definition
Ethernet	ช่องสื่อสาร RJ-45 มาตรฐาน 10/100/1000 Gigabit Ethernet อย่างน้อย 1 ช่อง
I/O Interface	- Serial Port at Last 1 or more - เชื่อมต่อ USB Port 2.0 more USB 3.0 รวมแล้วจำนวนไม่น้อยกว่า 5 Port - PS/2 Port (ถ้ามี) - VGA and DVI Port - eSATA/USB at Last 1 or more
Expansion Slot	PCI Express 2.0x16 at Last 1 or more PCIe 2.0x1 at Last 1 or more
Keyboard	- USB Keyboard 101 keys และ มีอักษรภาษาไทยพิมพ์ติดที่ Keyboard จากโรงงาน - มี Function keys 12 keys
Mouse	USB Optical Mouse
Chassis	Small From or Small Desktop
Power Supply	Not less than 240 watt
Operating System (OS)	Microsoft Windows Professional 64 bit
Other	- มีโปรแกรมจัดการอุปกรณ์ ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดทำ Backup / Restore ที่ถูกต้องตามกฎหมาย - สามารถดำเนินการทำ System Recovery ได้กรณี OS มีปัญหาการใช้งาน - อุปกรณ์ส่วนประกอบทั้งหมดต้องเป็นไปตามมาตราฐานสากล - 3 Year Warranty and Onsite Service (Next Business Day) - Online Support and Download Utilities

รูปที่ 3.8 ตัวอย่างคอมพิวเตอร์ตั้งโต๊ะรุ่นมาตรฐาน

- คอมพิวเตอร์ตั้งโต๊ะรุ่นพิเศษ ที่ใช้งานโปรแกรมแกรมพิเศษหรือโปรแกรมทางด้านการออกแบบจะมีรายละเอียดดังตารางที่ 3.6 และรูปภาพตัวอย่างดังรูปที่ 3.9

ตารางที่ 3.6 ตารางแสดงคุณสมบัติด้านเทคนิคของคอมพิวเตอร์ตั้งโต๊ะรุ่นพิเศษ

Detail	Specification
CPU	Core i5 ความเร็วไม่ต่ำกว่า 1.7 GHz
Cache	ไม่ต่ำกว่า L3 Cache ขนาดไม่น้อยกว่า 4 MB
BIOS	ต้องมีเครื่องหมายเดียวกัน
Ram	ชนิด DDR3 หรือดีกว่า ขนาดไม่น้อยกว่า 4GB
HDD	ขนาดความจุไม่น้อยกว่า 500 GB มีความเร็วรอบไม่ต่ำกว่า 7200 rpm
DVD	DVD +/-RW Drive

Graphic Adapter	มีหน่วยควบคุมการแสดงผล ขนาดไม่น้อยกว่า 2 GB
Monitor	LCD หรือ LED มีเครื่องหมายการค้าเดียวกับเครื่องคอมพิวเตอร์ มีความละเอียดไม่ต่ำกว่า 1366 x 768 pixels และมีขนาดไม่น้อยกว่า 19 inc. Wild Screen
Audio	Integrated High Definition
Ethernet	10/100/1000 Mbps.
I/O Interface	- Serial Port at Last 1 or more - เชื่อมต่อ USB Port 2.0 more USB 3.0 รวมแล้วจำนวนไม่น้อยกว่า 5 Port - PS/2 Port (ถ้ามี) - VGA and DVI Port - eSATA/USB at Last 1 or more
Expansion Slot	PCI Express 2.0x16 at Last 1 or more PCIe 2.0x1 at Last 1 or more
Keyboard	- USB Keyboard 101 และ มีอักษรภาษาไทยพิมพ์ติดที่ Keyboard จากโรงงาน - มี Function keys 12 keys
Mouse	USB Optical Mouse
Chassis	Small From or Small Desktop
Power Supply	Not less than 240 watt
Operating System (OS)	Microsoft Windows Professional 64 bit
Other	- มีโปรแกรมจัดการอุปกรณ์ ที่ถูกต้องตามกฎหมาย - มีโปรแกรมในการจัดทำ Backup / Restore ที่ถูกต้องตามกฎหมาย - สามารถดำเนินการทำ System Recovery ได้กรณี OS มีปัญหาการใช้งาน - อุปกรณ์ส่วนประกอบทั้งหมดต้องเป็นไปตามมาตราฐานสากล - 3 Year Warranty and Onsite Service (Next Business Day) - Online Support and Download Utilities

รูปที่ 3.9 ตัวอย่างคอมพิวเตอร์ตั้งโต๊ะรุ่นพิเศษ ที่ใช้งานโปรแกรมทางด้านการออกแบบ

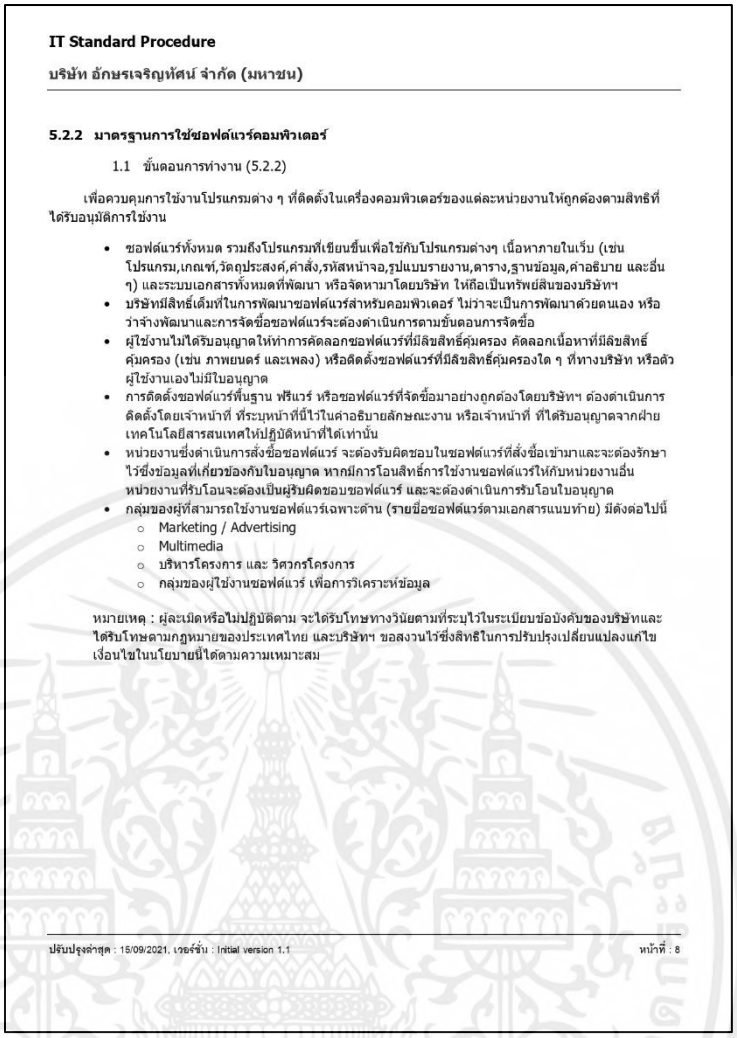
- **มาตรฐานการใช้ซอฟต์แวร์คอมพิวเตอร์**

ขั้นตอนการทำงานเพื่อควบคุมการใช้งานโปรแกรมต่าง ๆ ที่ติดตั้งในเครื่องคอมพิวเตอร์ของแต่ละหน่วยงานให้ถูกต้องตามสิทธิที่ได้รับอนุมัติการใช้งานดังรูปที่ 3.10

- ซอฟต์แวร์ทั้งหมด รวมถึงโปรแกรมที่เขียนขึ้นเพื่อใช้กับโปรแกรมต่าง ๆ เนื้อหาภายในเว็บ (เช่น โปรแกรม เกณฑ์ วัตถุประสงค์ คำสั่ง รหัสหน้าจอ รูปแบบรายงาน ตาราง ฐานข้อมูล คำอธิบาย) และระบบเอกสารทั้งหมดที่พัฒนา หรือจัดหามาโดยบริษัท ให้ถือเป็นทรัพย์สินของบริษัทฯ
- บริษัทมีสิทธิ์เต็มที่ในการพัฒนาซอฟต์แวร์สำหรับคอมพิวเตอร์ ไม่ว่าจะเป็นการพัฒนาด้วยตนเอง หรือว่าจ้างพัฒนาและการจัดซื้อซอฟต์แวร์จะต้องดำเนินการตามขั้นตอนการจัดซื้อ

- ผู้ใช้งานไม่ได้รับอนุญาตให้ทำการคัดลอกซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครอง คัดลอกเนื้อหาที่มีลิขสิทธิ์คุ้มครอง (เช่น ภาพยนตร์ และเพลง) หรือติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครองใด ๆ ที่ทางบริษัท หรือตัวผู้ใช้งานเองไม่มีใบอนุญาต
- การติดตั้งซอฟต์แวร์พื้นฐาน ฟรีแวร์ หรือซอฟต์แวร์ที่จัดซื้อมาอย่างถูกต้องโดยบริษัทฯ ต้องดำเนินการติดตั้งโดยเจ้าหน้าที่ ที่ระบุหน้าที่นี้ไว้ในคำอธิบายลักษณะงาน หรือเจ้าหน้าที่ ที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศให้ปฏิบัติหน้าที่ได้เท่านั้น
- หน่วยงานซึ่งดำเนินการสั่งซื้อซอฟต์แวร์ จะต้องรับผิดชอบในซอฟต์แวร์ที่สั่งซื้อเข้ามาและจะต้องรักษาไว้ซึ่งข้อมูลที่เกี่ยวข้องกับใบอนุญาต หากมีการโอนสิทธิ์การใช้งานซอฟต์แวร์ให้กับหน่วยงานอื่น หน่วยงานที่รับโอนจะต้องเป็นผู้รับผิดชอบซอฟต์แวร์ และจะต้องดำเนินการรับโอนใบอนุญาต
- กลุ่มของผู้ที่สามารถใช้งานซอฟต์แวร์เฉพาะด้าน (รายชื่อซอฟต์แวร์ตามเอกสารแนบท้าย) มีดังต่อไปนี้
  - Marketing / Advertising
  - Multimedia
  - บริหารโครงการ และ วิศวกรโครงการ
  - กลุ่มของผู้ใช้งานซอฟต์แวร์ เพื่อการวิเคราะห์ข้อมูล

หมายเหตุ : ผู้ละเมิดหรือไม่ปฏิบัติตาม จะได้รับโทษทางวินัยตามที่ระบุไว้ในระเบียบข้อบังคับของบริษัทและได้รับโทษตามกฎหมายของประเทศไทย และบริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขในนโยบายนี้ได้ตามความเหมาะสม



IT Standard Procedure

บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

5.2.2 มาตรฐานการใช้ซอฟต์แวร์คอมพิวเตอร์

1.1 ขั้นตอนการทำงาน (5.2.2)

เพื่อควบคุมการใช้งานโปรแกรมต่าง ๆ ที่ติดตั้งในเครื่องคอมพิวเตอร์ของแต่ละหน่วยงานให้ถูกต้องตามสิทธิที่ได้รับอนุมัติการใช้งาน

- ซอฟต์แวร์ทั้งหมด รวมถึงโปรแกรมที่เขียนขึ้นเพื่อใช้กับโปรแกรมต่างๆ เนื้อหาภายในเว็บ (เช่น โปรแกรม,เกณฑ์,วัดถุประสงค์,คำสั่ง,รหัสหน้าจอ,รูปแบบรายงาน,ตาราง,ฐานข้อมูล,คำอธิบาย และอื่น ๆ) และระบบเอกสารทั้งหมดที่พัฒนา หรือจัดหามาโดยบริษัท ให้ถือเป็นทรัพย์สินของบริษัทฯ
- บริษัทมีสิทธิ์เต็มที่ในการพัฒนาซอฟต์แวร์สำหรับคอมพิวเตอร์ ไม่ว่าจะเป็นการพัฒนาด้วยตนเอง หรือว่าจ้างพัฒนาและการจัดซื้อซอฟต์แวร์จะต้องดำเนินการตามขั้นตอนการจัดซื้อ
- ผู้ใช้งานไม่ได้รับอนุญาตให้ทำการคัดลอกซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครอง คัดลอกเนื้อหาที่มีลิขสิทธิ์คุ้มครอง (เช่น ภาพยนตร์ และเพลง) หรือติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครองใด ๆ ที่ทางบริษัท หรือตัวผู้ใช้งานเองไม่มีใบอนุญาต
- การติดตั้งซอฟต์แวร์พื้นฐาน ฟรีแวร์ หรือซอฟต์แวร์ที่จัดซื้อมาอย่างถูกต้องโดยบริษัทฯ ต้องดำเนินการติดตั้งโดยเจ้าหน้าที่ ที่ระบุหน้าที่นี้ไว้ในคำอธิบายลักษณะงาน หรือเจ้าหน้าที่ ที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศให้ปฏิบัติหน้าที่ได้เท่านั้น
- หน่วยงานซึ่งดำเนินการสั่งซื้อซอฟต์แวร์ จะต้องรับผิดชอบในซอฟต์แวร์ที่สั่งซื้อเข้ามาและจะต้องรักษาไว้ซึ่งข้อมูลที่เกี่ยวข้องกับใบอนุญาต หากมีการโอนสิทธิ์การใช้งานซอฟต์แวร์ให้กับหน่วยงานอื่น หน่วยงานที่รับโอนจะต้องเป็นผู้รับผิดชอบซอฟต์แวร์ และจะต้องดำเนินการรับโอนใบอนุญาต
- กลุ่มของผู้ที่สามารถใช้งานซอฟต์แวร์เฉพาะด้าน (รายชื่อซอฟต์แวร์ตามเอกสารแนบท้าย) มีดังต่อไปนี้
  - Marketing / Advertising
  - Multimedia
  - บริหารโครงการ และ วิศวกรโครงการ
  - กลุ่มของผู้ใช้งานซอฟต์แวร์ เพื่อการวิเคราะห์ข้อมูล

หมายเหตุ : ผู้ละเมิดหรือไม่ปฏิบัติตาม จะได้รับโทษทางวินัยตามที่ระบุไว้ในระเบียบข้อบังคับของบริษัทและได้รับโทษตามกฎหมายของประเทศไทย และบริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขในนโยบายนี้ได้ตามความเหมาะสม

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 8

รูปที่ 3.10 ตัวอย่างมาตรฐานการใช้ซอฟต์แวร์คอมพิวเตอร์

รายชื่อซอฟต์แวร์พื้นฐานและฟรีแวร์จะมีรายละเอียดดังตารางที่ 3.7 บริษัทฯ ขอสงวนไว้ซึ่งสิทธิในการปรับปรุงเปลี่ยนแปลงแก้ไขเงื่อนไขคุณสมบัติทางด้านเทคนิคนี้ได้ตามความเหมาะสม

ตารางที่ 3.7 ตารางแสดงรายชื่อซอฟต์แวร์พื้นฐานและฟรีแวร์

ลำดับ	รายการ	คุณสมบัติ	ซอฟต์แวร์
1	Windows 10 Professional	Operating System	ลิขสิทธิ์
2	trend micro apex one	Antivirus	ลิขสิทธิ์
3	Adobe Reader	เปิดไฟล์เอกสาร PDF เท่านั้น	ฟรีแวร์
4	PDF Converter	(แปลงเอกสารเป็น PDF)	ฟรีแวร์
5	7zip	Zip (ย่อขนาดข้อมูล)	ฟรีแวร์
6	Adobe Flash Player	เปิดไฟล์มีเดียนามสกุล .swf ผ่านบราวเซอร์	ฟรีแวร์
7	Adobe Shockwave Player	เปิดไฟล์มีเดียนามสกุล.dcr ผ่านบราวเซอร์	ฟรีแวร์
8	Nero Burner	โปรแกรมไรท์แผ่น CD DVD	ฟรีแวร์
9	Java Runtime	ปลั๊กอินให้รันโปรแกรมจาวาผ่านเว็บบราวเซอร์บนเครือข่าย	ฟรีแวร์
10	MS 2010 Tool (Picture Manager)	Edit Picture	ฟรีแวร์
11	Dot Net Framework	รองรับการใช้งานภาษาที่ใช้ในการเขียนโปรแกรม	ฟรีแวร์
12	Google Chrome	Internet Browser	ฟรีแวร์
13	Capture Tool	Sniping Tool (include Widnows 10)	ฟรีแวร์
14	Ultra VNC	Remote Tools	ฟรีแวร์
15	Microsoft Office 2010 หรือ สูงกว่า	Microsoft Office	ลิขสิทธิ์

รายชื่อซอฟต์แวร์เฉพาะด้านจะมีรายละเอียดดังตารางที่ 3.8

ตารางที่ 3.8 ตารางแสดงรายชื่อซอฟต์แวร์เฉพาะด้าน

ลำดับ	รายการ	คุณสมบัติ	ซอฟต์แวร์
1	AutoCAD	Graphic/Design	ลิขสิทธิ์
2	Photo Shop	Graphic/Design	ลิขสิทธิ์
3	Illustrator	Graphic/Design	ลิขสิทธิ์
4	Microsoft Visio	Flowchart/Design	ลิขสิทธิ์
4	Acrobat Professional	Document Editor (PDF)	ลิขสิทธิ์
6	Microsoft Project	Project Management	ลิขสิทธิ์
7	Sketchup	Graphic 3D	ลิขสิทธิ์
8	SPSS	วิเคราะห์ข้อมูลทางสถิติ	ลิขสิทธิ์
9	Mind Mapping	ไดอะแกรมที่แสดงให้เห็นถึงความเชื่องโยง	ลิขสิทธิ์
10	SAP GUI 7.2 + Gui720	โปรแกรมประเภท ERP	ลิขสิทธิ์

การจัดการลุจำหน่ายอุปกรณ์คอมพิวเตอร์ต่าง ๆ จะมีรายละเอียดดังตารางที่ 3.9 และรูปภาพตัวอย่างดังรูปที่ 3.11

เพื่อเป็นการควบคุมดูแลรายการทรัพย์สินอุปกรณ์ไอทีไม่ต้องการใช้แล้ว อุปกรณ์ชำรุด วัสดุสิ้นเปลือง เช่นคีย์บอร์ด เม้าส์ และเศษซากวัสดุทุกประเภททางด้านไอที ของกลุ่มบริษัทและในเครือให้มีความคล่องตัว มีการควบคุมดูและอย่างถูกต้อง กรณีของที่มีคุณภาพ ใช้งานได้ให้ทำการบริจาคเพื่อเป็นประโยชน์แก่สังคม

การลุจำหน่ายไม่น้อยกว่า 1 ปีต่อครั้ง ขั้นตอนการทำงาน

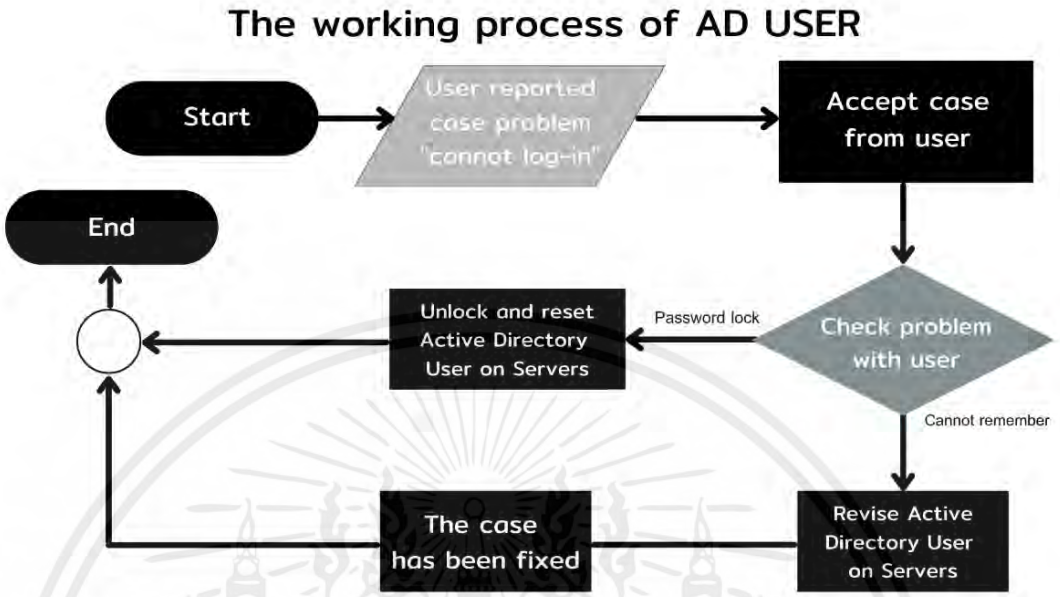
คัดแยกประเภท ถ่ายรูปและหารายละเอียดของอุปกรณ์เหล่านั้น บันทึกใน Excel File พร้อมแนบกับแบบฟอร์มการลุจำแนก และเสนอผู้บังคับบัญชาสูงสุดให้เซ็นอนุมัติทำการลุจำหน่ายส่งหาทรัพย์สิน

ตารางที่ 3.9 ตารางแสดงการจัดการลุจำหน่ายอุปกรณ์คอมพิวเตอร์ต่าง ๆ

Description	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง
คัดแยกประเภท ถ่ายรูป รายละเอียดรายการอุปกรณ์ บันทึกใน Excel File	IT Helpdesk	Excel File
กรอกเอกสารตัดจำหน่าย แล้วให้ ผู้บริหารทำการอนุมัติ เห็นชอบ	IT Helpdesk	ใบขอตัดจำหน่ายทรัพย์สิน
นัดฝ่ายทรัพย์สินเพื่อทำการตรวจเช็คเอกสาร และ จำนวนสิ่งของที่ลุจำหน่าย	ทรัพย์สิน IT Helpdesk	

รูปที่ 3.11 ตัวอย่างการจัดการลุจำหน่ายอุปกรณ์คอมพิวเตอร์เก่าต่าง ๆ

3.2.2 การปรับปรุงหลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ

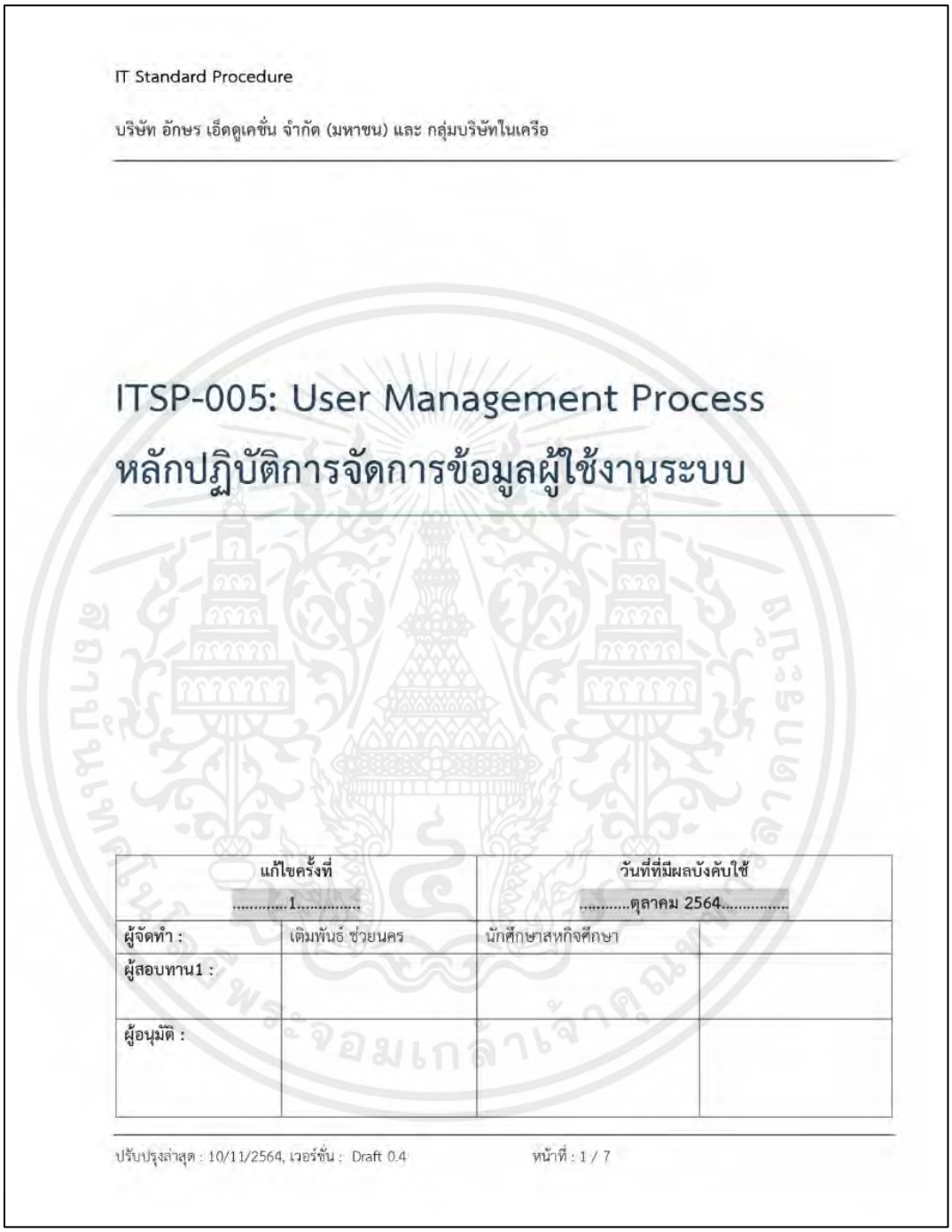


รูปที่ 3.12 กระบวนการการปรับปรุงหลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ Active Directory

การทำงานของการบริหารจัดการรหัสผู้งานโดยใช้ Active Directory แบ่งการทำงานออกเป็น 3 ขั้นตอน ได้แก่ ขั้นตอนการรับเคสจากผู้ใช้งาน (User) ขั้นตอนการตรวจสอบปัญหาที่ผู้ใช้งาน (User) แจ้งปัญหาเข้ามา ขั้นตอนการแก้ไขรหัสผู้งานโดยใช้ Active Directoryให้สอดคล้องกับมาตรฐานใหม่ ดังแสดงในรูปที่ 3.12 ซึ่งมีขั้นตอนการทำงานดังนี้

1. ผู้ใช้งาน (User) แจ้งเคสพบปัญหาไม่สามารถเข้าสู่ระบบ (Log-in) ได้
2. กดรับเคสที่ผู้ใช้งานแจ้งปัญหาเข้ามาใน IT Helpdesk
3. นำเคสที่ผู้ใช้งาน (user) แจ้งมาตรวจสอบปัญหา
4. หากไม่สามารถเข้าสู่ระบบได้เพราะรหัสผ่านหมดอายุตามนโยบาย จะทำการแก้ไขรหัสผ่านให้เป็นปัจจุบันเพื่อให้สอดคล้องกับมาตรฐานใหม่
5. ส่งข้อมูลรหัสผ่านที่ทำการกำหนดใหม่ตามมาตรฐานใหม่ ให้แก่ผู้ใช้งาน (User) เจ้าของเคส
6. หากไม่สามารถเข้าสู่ระบบได้เพราะผู้ใช้งาน (User) ลืมรหัสผ่าน และเข้ารหัสผิดซ้ำ ๆ จนระบบล็อค จะทำการปลดล็อครหัสผ่านให้ใหม่ โดยรีเซ็ตเป็นรูปแบบปัจจุบันเพื่อให้สอดคล้องกับมาตรฐานใหม่
7. ส่งข้อมูลรหัสผ่านที่ทำการปลดล็อคและรหัสผ่านที่กำหนดใหม่ตามมาตรฐานใหม่ให้แก่ผู้ใช้งาน (User) เจ้าของเคส

ITSP-005 : User Management Process (หลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ)



IT Standard Procedure

บริษัท อักษร เอ็ดดูเคชั่น จำกัด (มหาชน) และ กลุ่มบริษัทในเครือ

ITSP-005: User Management Process

หลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ

แก้ไขครั้งที่ 1		วันที่ที่มีผลบังคับใช้ ตุลาคม 2564	
ผู้จัดทำ :	เติมพันธ์ ช่วยนคร	นักศึกษาสหกิจศึกษา	
ผู้สอบทาน1 :			
ผู้อนุมัติ :			

ปรับปรุงล่าสุด : 10/11/2564, เวอร์ชั่น : Draft 0.4 หน้าที่ : 1 / 7

รูปที่ 3.13 ตัวอย่างหน้าปกหัวข้อ ITSP-005: User Management Process (หลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ)

รูปที่ 3.13 เป็นหน้าปกของหัวข้อ ITSP-005 ในหัวข้อนี้จะเป็นการจัดการบัญชีผู้ใช้งานระบบ Application ภายใน การจัดการบัญชีผู้ใช้งานระบบ One Account การใช้งาน Active Directory การบริหารจัดการรหัสผู้งานโดยใช้ Active Directory

ตารางที่ 3.10 ตารางแสดงความเสี่ยงของหัวข้อ ITSP-005

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 3.10 การทำ Risk Management พบว่า ก่อนทำการปรับแก้นโยบาย ITSP-005 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความเสี่ยงสูงมากและเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุอยู่สม่ำเสมอ

การจัดการบัญชีผู้ใช้งานระบบ Application ภายในจะมีรายละเอียดดังตารางที่ 3.11 การเปิดสิทธิ์การใช้งานบัญชีที่ควบคุมด้วย application ภายในบริษัท ทำได้โดยการเปิดผ่าน user request form

ตารางที่ 3.11 ตารางแสดงการจัดการบัญชีผู้ใช้งานระบบ Application ภายใน

ขั้นตอน	รายละเอียด
1) สร้างคำร้องจัดการบัญชีผู้ใช้งาน	หน่วยงานร้องขอจัดการบัญชีผู้ใช้งาน เพื่อสนับสนุนการทำงานของระบบนั้น ๆ
2) พิจารณาคำร้อง	ผู้บริหารของหน่วยงานพิจารณาอนุมัติ

3) ปรับปรุงบัญชีผู้ใช้งาน	ทีมเจ้าของระบบปรับปรุงข้อมูลบัญชีผู้ใช้งานตามที่ร้องขอ
4) ตรวจรับบัญชีผู้ใช้งาน	หน่วยงานร้องขอ ตรวจรับบัญชีผู้ใช้งาน

การจัดการบัญชีผู้ใช้งานระบบ One Accountจะมีรายละเอียดชี้แจงดังตารางที่ 3.12การเปิดสิทธิ์ One Account Admin สำหรับพนักงานภายในบริษัท การกำหนดสิทธิ์ให้พนักงานภายในบริษัท สามารถเข้าไปใช้งานระบบ Back Office ในการค้นหาข้อมูลผู้ใช้/ยกเลิกการใช้งานบัญชี One Account เพื่อสนับสนุนและแก้ไขปัญหาการใช้งานแก่ผู้ใช้งานทั่วไป

ตารางที่ 3.12 ตารางแสดงการจัดการบัญชีผู้ใช้งานระบบ One Account

ขั้นตอน	รายละเอียด
1) ร้องขอเปิดสิทธิ์	- ผู้ร้องขอ ต้องเป็นพนักงานภายในบริษัท และได้รับความเห็นชอบจากหัวหน้างานหรือผู้มีอำนาจ - ส่งอีเมลแจ้งวัตถุประสงค์ที่ต้องการเข้าใช้งานระบบ และรายชื่อผู้ใช้มายัง System Admin
2) ตรวจสอบข้อมูล	- System Admin ตรวจสอบวัตถุประสงค์และรายชื่อผู้ใช้ - ดำเนินการเปิดสิทธิ์ Admin ให้ตามรายชื่อผู้ใช้ที่มีการร้องขอ
3) แจ้งผลการเปิดสิทธิ์	System Admin แจ้งผลกลับไปยังผู้ร้องขอทางอีเมล พร้อมแนะนำการใช้งานระบบ Back Office เบื้องต้น

การเปิดสิทธิ์การมองเห็นสื่อฯ ทั้งหมดภายในระบบ Aksorn On-Learn (AOL) สำหรับพนักงานภายในบริษัท

ตารางที่ 3.12 ตารางแสดงการจัดการบัญชีผู้ใช้งานระบบ One Account (ต่อ)

ขั้นตอน	รายละเอียด
1) ร้องขอเปิดสิทธิ์	- ผู้ร้องขอ ต้องเป็นพนักงานภายในบริษัท และได้รับความเห็นชอบจากหัวหน้างานหรือผู้มีอำนาจ - ส่งอีเมลแจ้งรายชื่อผู้ใช้ และวัตถุประสงค์มายัง System Admin
2) ตรวจสอบข้อมูล	- System Admin ตรวจสอบข้อมูลผู้ใช้และวัตถุประสงค์ - ดำเนินการเปิดสิทธิ์การมองเห็นสื่อฯ ทั้งหมดภายในระบบ AOL ให้ตามรายชื่อผู้ใช้ที่มีการร้องขอ
3) แจ้งผลการเปิดสิทธิ์	System Admin แจ้งผลการเปิดสิทธิ์กลับไปยังผู้ร้องขอทางอีเมล ให้ผู้ใช้ลองเข้าสู่ระบบใหม่อีกครั้ง

ยกเลิกการใช้งานบัญชีผู้ใช้ One Account (กรณีพนักงานภายในบริษัท ลาออก)

ตารางที่ 3.12 ตารางแสดงการจัดการบัญชีผู้ใช้งานระบบ One Account (ต่อ)

ขั้นตอน	รายละเอียด
1) ร้องขอยกเลิกการใช้งานบัญชี One Account	HR หรือหัวหน้างาน ส่งอีเมลแจ้งรายชื่อผู้ใช้ ที่ต้องการยกเลิกการใช้งานบัญชี One Account มายัง System Admin
2) ตรวจสอบรายชื่อผู้ใช้	System Admin ตรวจสอบรายชื่อผู้ใช้ และดำเนินการยกเลิกการใช้งานบัญชี One Account
3) แจ้งผลยกเลิกการใช้งานบัญชี One Account	System Admin แจ้งผลการยกเลิกการใช้งานบัญชี One Account กลับไปยังผู้ร้องขอทางอีเมล

การบริหารจัดการรหัสผู้งานโดยใช้ Active Directory จะมีรายละเอียดชี้แจงดังตารางที่ 3.13 Active Directory (AD) ทำหน้าที่บริหารจัดการระบบ IT ในบริษัท (โดเมน) และพิสูจน์ตัวตนผู้ใช้เมื่อเข้ามาใช้งานระบบ รวมทั้งจัดเก็บรายละเอียดข้อมูลต่าง ๆ เช่น User Group Computer หรือ นโยบายรักษาความปลอดภัย เป็นต้น โดยจะเก็บข้อมูลต่าง ๆ เหล่านี้ไว้ใน Active Directory Database และมีเซิร์ฟเวอร์ที่ทำหน้าที่เป็น Domain Controller (DC) เป็นตัวจัดการอีกทีหนึ่ง Active Directory มีส่วนประกอบอยู่ 2 ส่วนที่สำคัญ ได้แก่

1. Active Directory Service คือ ส่วนประกอบที่ให้บริการแก่ผู้บริหารระบบและผู้ใช้
2. Active Directory Database คือ ฐานข้อมูลสำหรับจัดเก็บออบเจ็กต์ต่าง ๆ

ในการใช้งานระบบต่าง ๆ จึงต้องมีฐานข้อมูลผู้ใช้งาน ที่ประกอบอยู่ 2 ส่วนที่สำคัญ ได้แก่

1. AD ข้อมูลผู้ใช้งานระบบ IT ในบริษัท
2. HR Tiger ฐานข้อมูลพนักงานบริษัทของฝ่าย HR

การใช้งาน Active Directory

1. การใช้งานควบคุมสิทธิ์ ผ่านทาง AD ทำได้โดยการอ้างอิง ถึงชื่อ user หรือ group ของ AD
2. IT Support จะทำการทบทวนชื่อผู้ใช้งานที่ยัง Active กับทาง HR 1 ครั้งต่อ 1 ปี

ขั้นตอนการทำงานเมื่อมีพนักงานใหม่

ตารางที่ 3.13 ตารางแสดงการใช้งาน Active Directory

ขั้นตอน	รายละเอียด
1) HR บันทึกข้อมูล	- ฝ่าย HR บันทึกข้อมูลพนักงานลงใน HR Tiger แล้วแจ้งที่ IT Support ผ่านทาง Google Sheet
2) สร้างข้อมูล	- เจ้าหน้าที่ IT Support สร้างข้อมูลพนักงานลงใน Active Directory (AD)
3) แจ้งให้พนักงานใหม่ทราบ	- เมื่อพนักงานใหม่ เข้ามาทำงาน ทาง IT Support จะส่ง ข้อมูลให้แก่พนักงาน

เมื่อ User ต้องการมี Account AD/Group ใหม่

ตารางที่ 3.13 ตารางแสดงการใช้งาน Active Directory (ต่อ)

ขั้นตอน	รายละเอียด
1) เปิด IT Ticket	- ผู้ร้องขอ เปิด IT Ticket พร้อมแนบเอกสารที่ได้รับอนุมัติจากหัวหน้างาน
2) เปิดสิทธิ์ตามที่ขอ	- เจ้าหน้าที่ IT Support ทำการเปิด account/group ใหม่ตามที่ร้องขอ

เมื่อต้องการ เพิ่ม user เข้าไปใน Account AD/Group

ตารางที่ 3.13 ตารางแสดงการใช้งาน Active Directory (ต่อ)

ขั้นตอน	รายละเอียด
1) เปิด IT Ticket	- ผู้ร้องขอ เปิด IT Ticket พร้อมแนบเอกสารที่ได้รับอนุมัติจากหัวหน้างาน
2) เปิดสิทธิ์ตามที่ขอ	- เจ้าหน้าที่ IT Support ทำการเพิ่ม account/group ใหม่ตามที่ร้องขอ
3) แจ้งให้พนักงานทราบ	- เจ้าหน้าที่ IT Support แจ้งข้อมูลผ่านทาง Ticket

เมื่อมีพนักงานลาออก

ตารางที่ 3.13 ตารางแสดงการใช้งาน Active Directory (ต่อ)

ขั้นตอน	รายละเอียด
1) HR บันทึกข้อมูล	- ฝ่าย HR บันทึกข้อมูลพนักงานที่ลาออกลงใน HR Tiger แล้วแจ้งที่ IT Support ผ่านทาง Google Sheet
2) ปรับปรุงข้อมูล	- เจ้าหน้าที่ IT Support ทำการตั้งค่า Account expires End of: ที่ข้อมูลพนักงานลงใน Active Directory (AD) เพื่อ disable ตามวันเวลาดังกล่าว

การทบทวนชื่อผู้ใช้งาน

ตารางที่ 3.13 ตารางแสดงการใช้งาน Active Directory (ต่อ)

ขั้นตอน	รายละเอียด
1) HR ส่งข้อมูลจาก Tiger	- IT Support รับข้อมูล list รายชื่อ user จาก HR โดยการ dump ข้อมูลออกจาก Tiger
2) เปรียนเทียบรายชื่อพนักงาน	- เจ้าหน้าที่ IT Support เปรียบเทียบ ข้อมูลใน AD กับข้อมูลของ HR
3) ปรับค่าต่าง ๆ ตามข้อมูล HR	- เจ้าหน้าที่ IT Support ปรับปรุงข้อมูลบน AD ให้ตรงกับที่ทาง HR แจ้ง

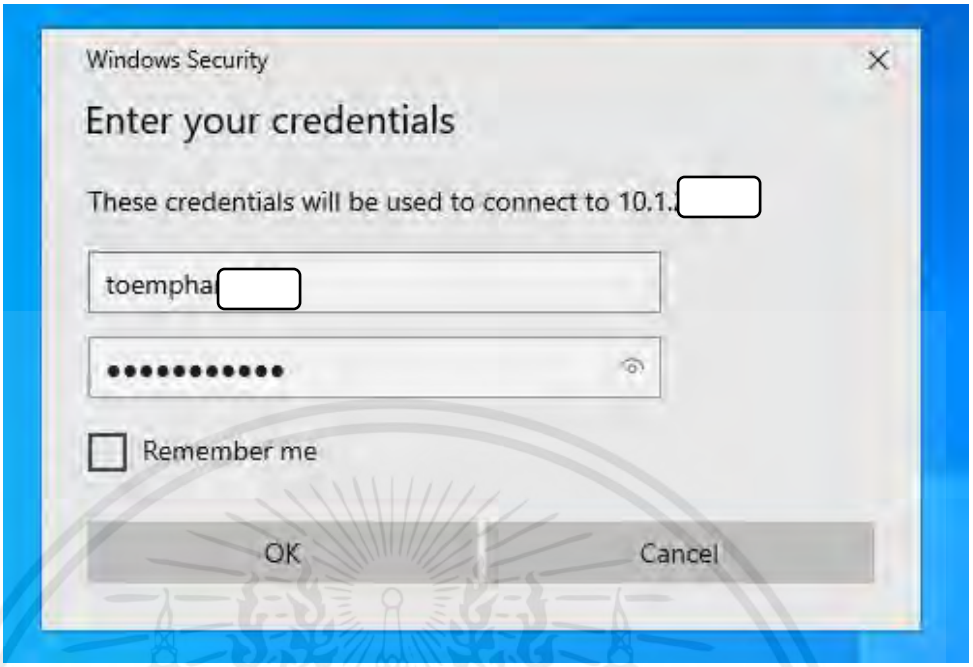
- **การทำงานของการบริหารจัดการรหัสผู้งานโดยใช้ Active Directory**

โดยผู้จัดทำจะแสดงให้เห็นถึงวิธีการบริหารจัดการรหัสผู้งานโดยใช้ Active Directory ดังต่อไปนี้

1. ใช้ Remote Desktop เพื่อ Connect เข้าไปยัง Servers ดังรูปที่ 3.14

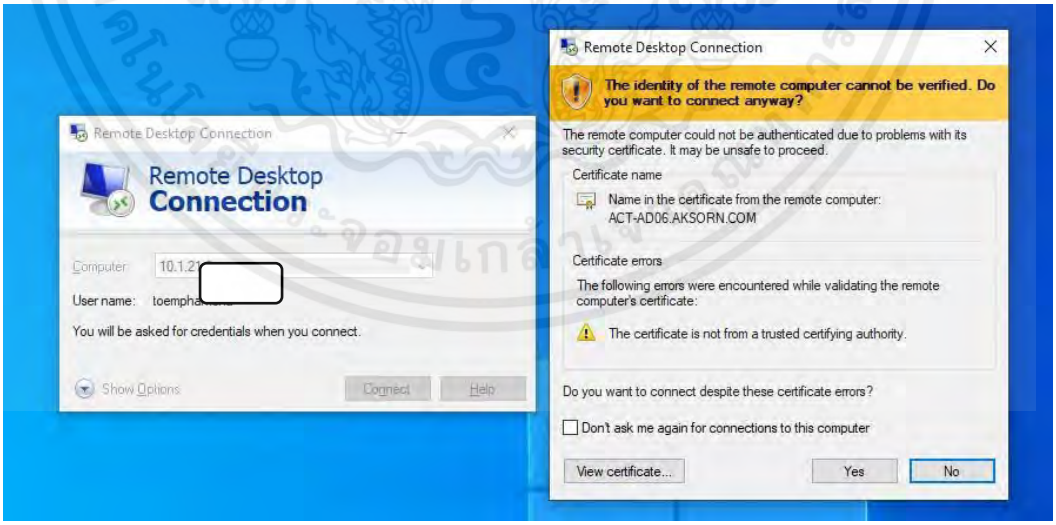
รูปที่ 3.14 ตัวอย่างการใช้ Remote Desktop เพื่อเข้าไปยัง Servers

2. Log-in เพื่อ Connect เข้าไปยัง Servers ดังรูปที่ 3.15



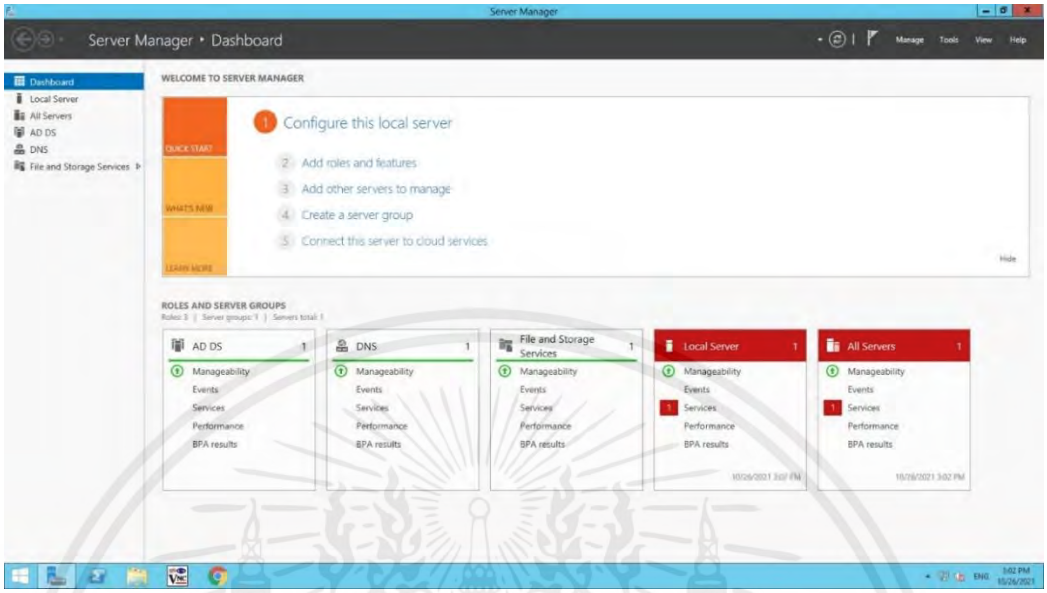
รูปที่ 3.15 ตัวอย่างการกรอก username และ password เพื่อ log-in เข้าสู่ Servers

3. ระบบจะแจ้งเตือน Certificate จาก Domain ของ Server ให้ทราบดังรูปที่ 3.16



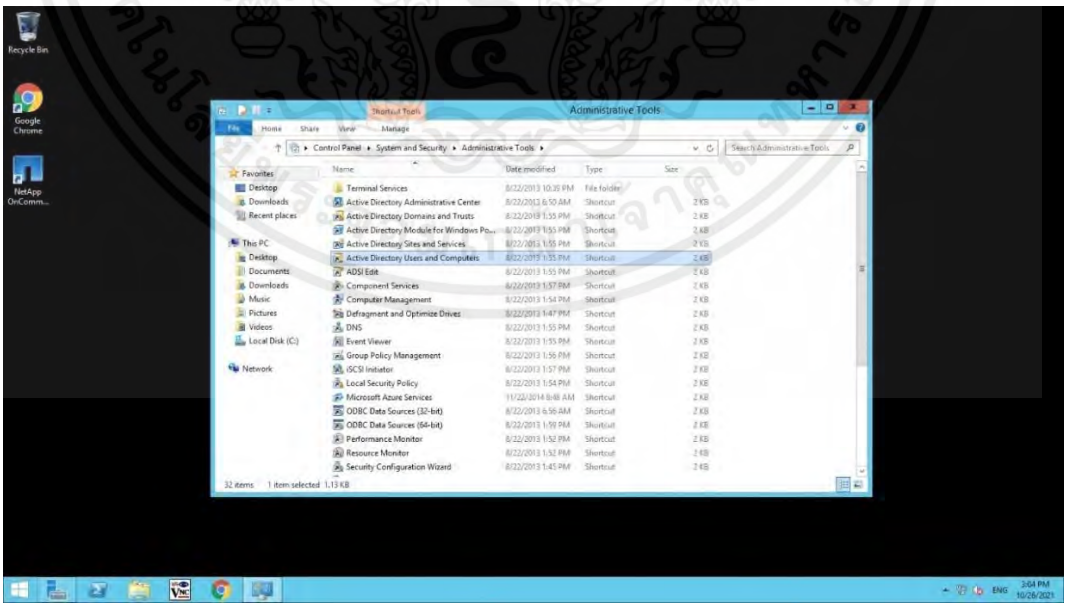
รูปที่ 3.16 ตัวอย่างการแจ้งเตือน Certificate ก่อนเข้าสู่ระบบ Servers

4. เมื่อ Log-in เข้ามาจะเจอหน้า Dashboard ของ Servers โดยจะมีเมนูแสดงการทำ AD บน Servers แสดงให้เราเห็นดังรูปที่ 3.17



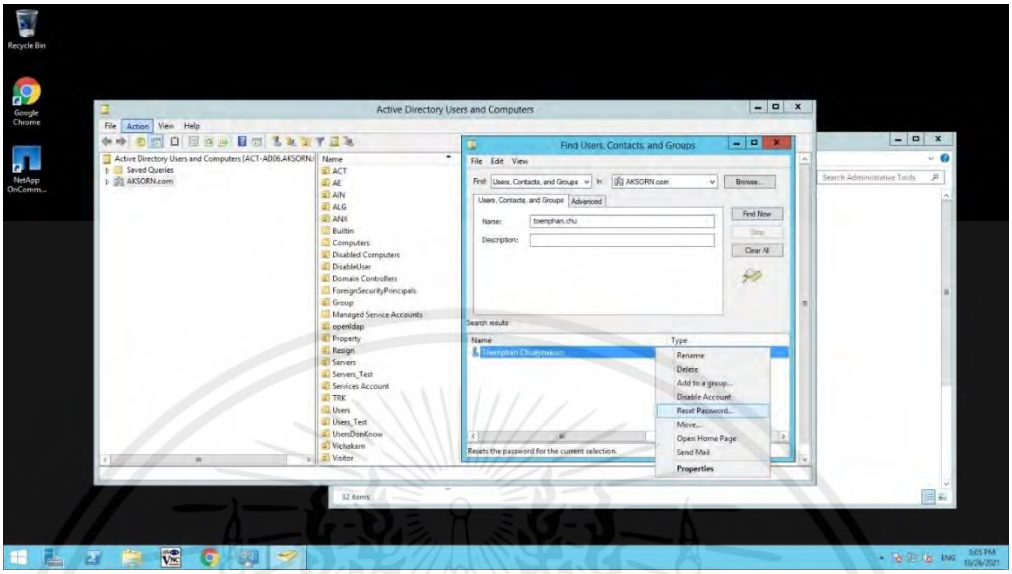
รูปที่ 3.17 ตัวอย่างแสดงหน้า Dashboard แรกของ Servers

5. เปิด Administrative Tools ขึ้นมาเพื่อทำ Active Directory Users and Computers ดังรูปที่ 3.18



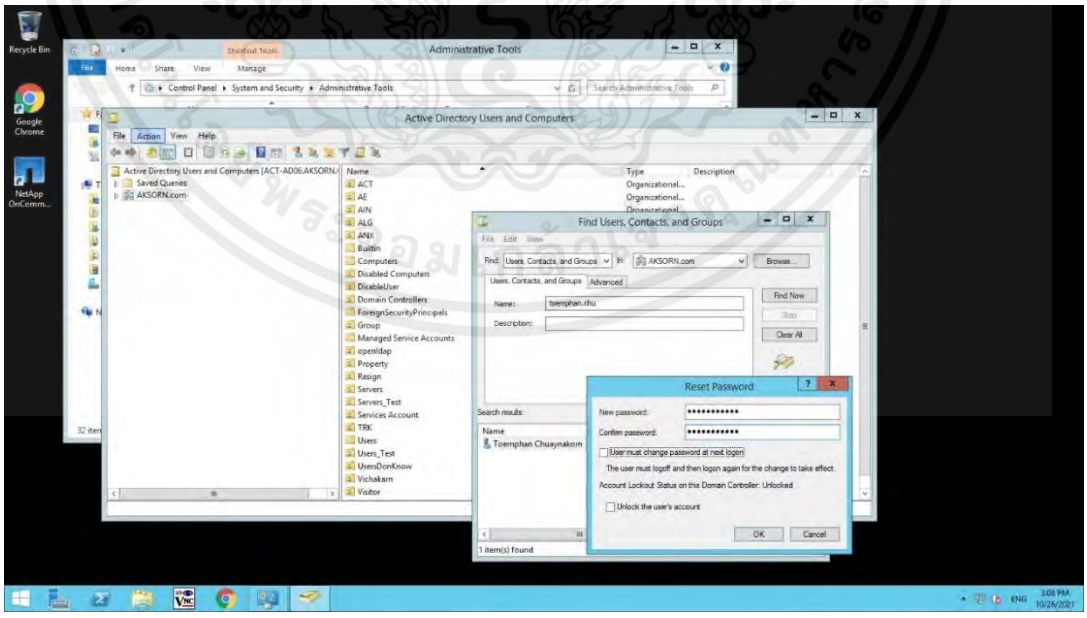
รูปที่ 3.18 ตัวอย่างแสดงการเปิด Administrative Tools เพื่อทำ Active Directory

6. ค้นหาชื่อของ User ที่ต้องการเปลี่ยน Password เมื่อครบ 90 วันตาม Policy ดังรูปที่ 3.19



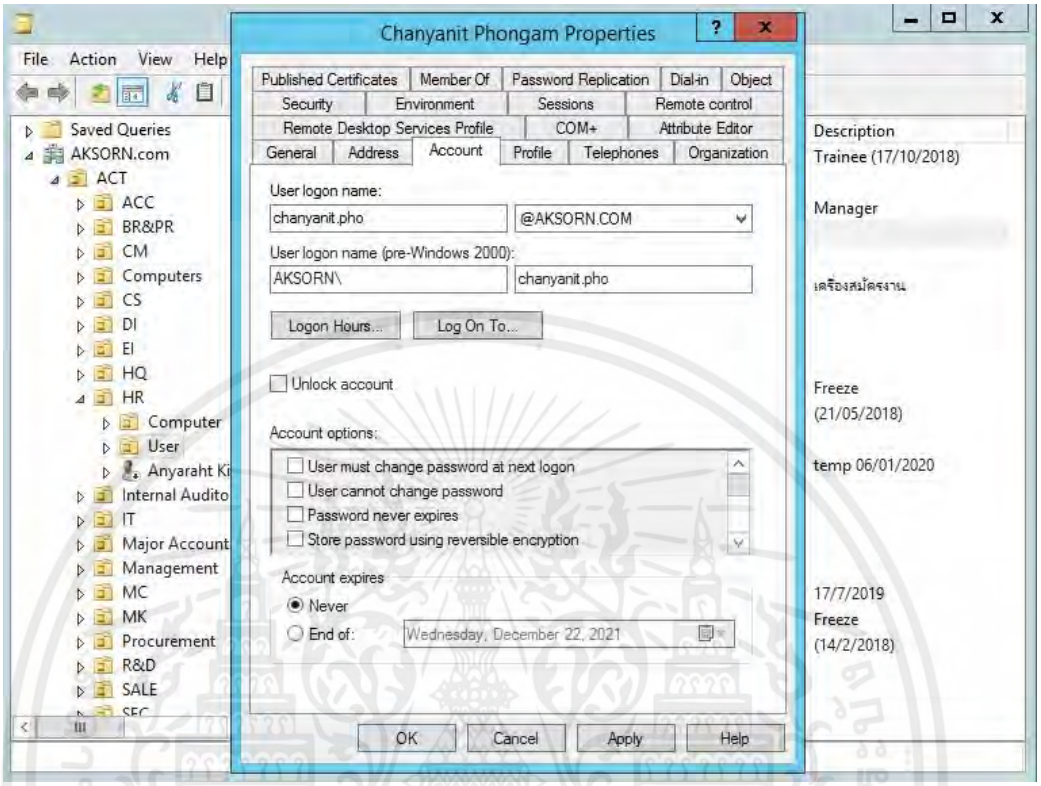
รูปที่ 3.19 ตัวอย่างแสดงการค้นหาชื่อของ User ที่ต้องการเปลี่ยน Password

7. ทำการเปลี่ยน Password ของ User ให้สอดคล้องกับมาตรฐานใหม่ขององค์กร ดังรูปที่ 3.20



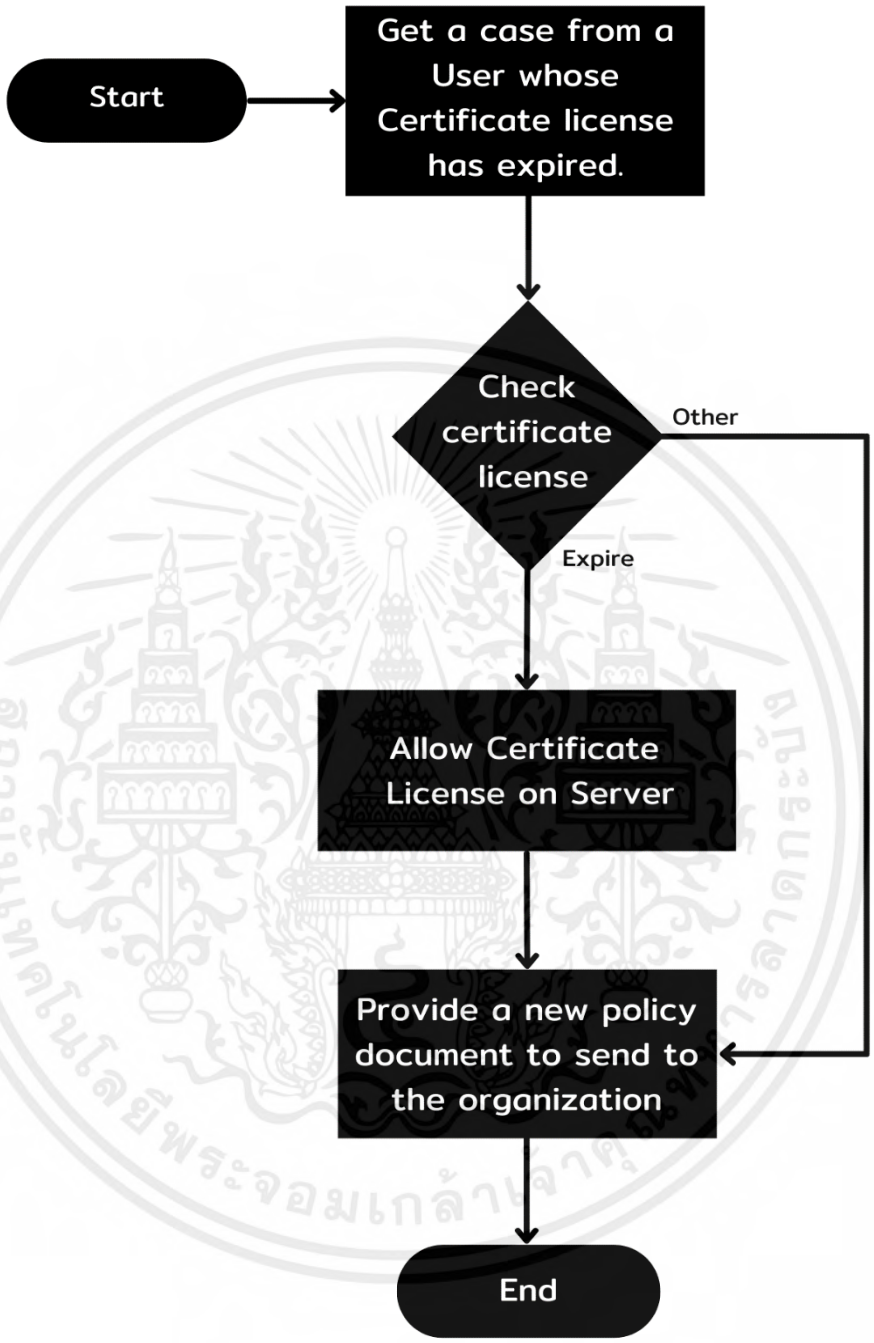
รูปที่ 3.20 ตัวอย่างแสดงการเปลี่ยน Password ของ User

8. ค้นหาชื่อของ User ที่ต้องการ Unlock เมื่อ User เข้ารหัสผิดซ้ำจนล็อก ดังรูปที่ 3.21



รูปที่ 3.21 ตัวอย่างแสดงการ unlock รหัสผ่านให้ user

3.2.3 การปรับปรุงหลักปฏิบัติการเข้ารหัสข้อมูล



รูปที่ 3.22 กระบวนการปรับปรุงหลักปฏิบัติการเข้ารหัสข้อมูล

การทำงานของการปรับปรุงหลักปฏิบัติการเข้ารหัสข้อมูล แบ่งการทำงานออกเป็น 4 ขั้นตอน ได้แก่ ขั้นตอนการรับเคสจาก User ที่ใบอนุญาต Certificate หมดอายุ ขั้นตอนการตรวจสอบใบอนุญาต Certificate ขั้นตอนการ Remote เข้าไป Servers เพื่อไป Allow ใบอนุญาต Certificate ขั้นตอนการจัดทำเอกสารและส่งต่อให้องค์กรเพื่อนำส่งยื่นของมาตรฐานต่อไป ดังแสดงในรูปที่ 3.22 ซึ่งมีขั้นตอนการทำงานดังนี้

1. รับเคสจาก User ที่ใบอนุญาต Certificate หมดอายุ Log-in แล้วไม่สามารถทำการเข้ารหัสสำเร็จ ไม่สามารถทำการถ่ายโอนไฟล์ได้

2. ตรวจสอบใบอนุญาต Certificate ว่าหมดอายุจริง หรือ User มีการเข้ารหัสของพนักงานเก่าเพื่อสิทธิ์การเข้าถึงข้อมูลที่สูงกว่า

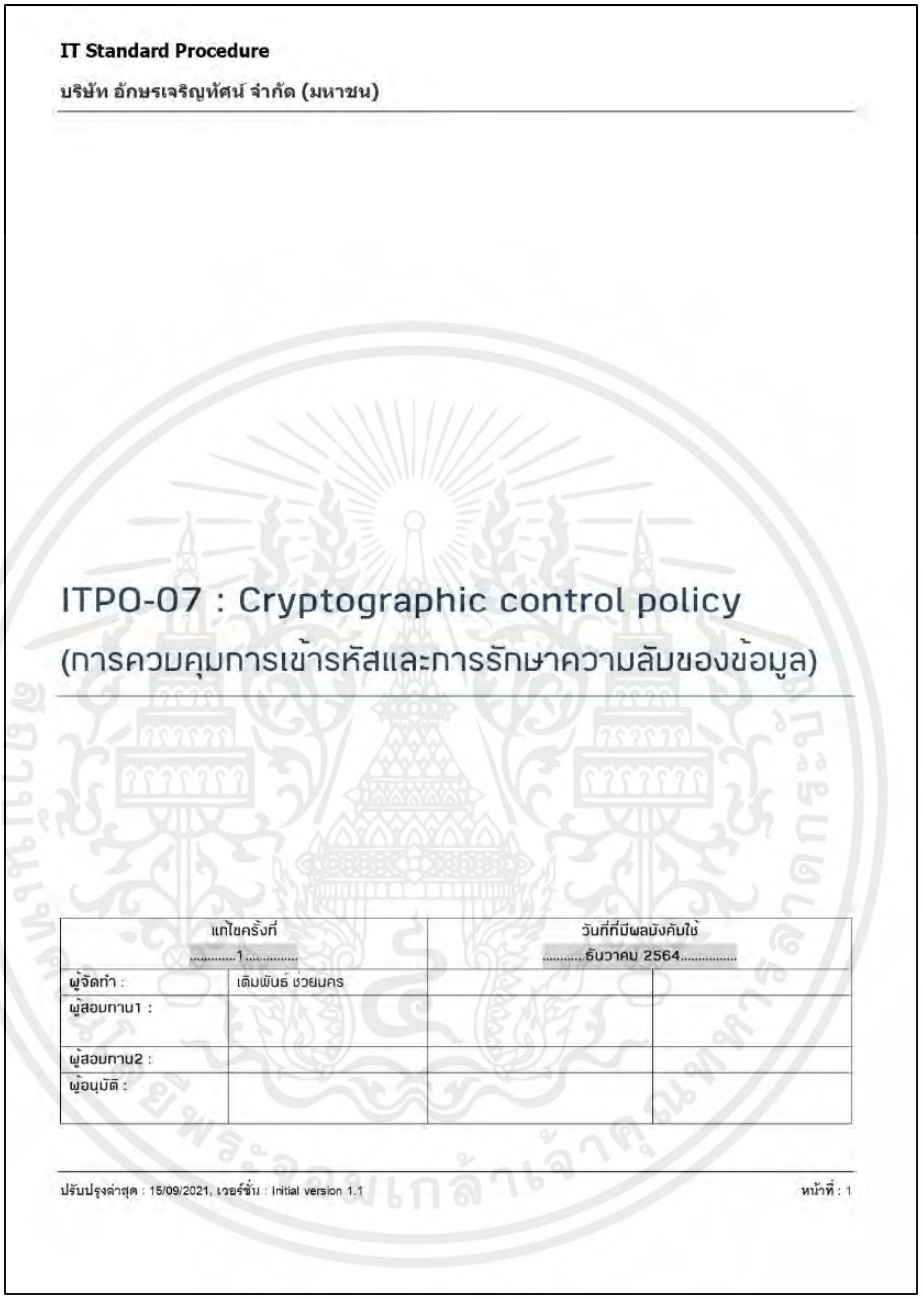
3. หากใบอนุญาต Certificate ไม่หมดอายุหรือมรกรณีอื่น ๆ ที่ User ผิดพลาด ก็จบการทำงาน สามารถจบนำมาทำเป็นเอกสารได้ทันที

4. หากใบอนุญาต Certificate หมดอายุจริง จะใช้ Remote Desktop Connection เข้าไปยัง Server เพื่อ Allow ใบอนุญาต Certificate

5. ถ้าพบว่าเป็นใบอนุญาต Certificate ของ User เก่าที่ลาออกไปแล้วจะทำการ Remove ใบอนุญาต Certificate ออกทันทีก่อนรอบทำการ PM ใหญ่

6. ส่งข้อมูลและเอกสารไปให้ผู้จัดการทำการตรวจสอบความถูกต้องของเอกสารและมาตรฐานทั้งหมด เพื่อนำไปปรับใช้กับองค์กร

ITPO-07 : Cryptographic control policy (การควบคุมการเข้ารหัสและการรักษาความลับของข้อมูล)



IT Standard Procedure

บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

ITPO-07 : Cryptographic control policy
(การควบคุมการเข้ารหัสและการรักษาความลับของข้อมูล)

แก้ไขครั้งที่		วันที่ที่มีผลบังคับใช้	
	1		ธันวาคม 2564
ผู้จัดทำ :	เติมพันธ์ ช่วยนคร		
ผู้สอบทาน1 :			
ผู้สอบทาน2 :			
ผู้อนุมัติ :			

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 1

รูปที่ 3.23 ตัวอย่างหน้าปกหัวข้อ ITPO-07 : Cryptographic control policy (การควบคุมการเข้ารหัสและการรักษาความลับของข้อมูล)

รูปที่ 3.23 เป็นหน้าปกของหัวข้อ ITPO-07 ในหัวข้อนี้จะเป็นการอธิบายนโยบายเกี่ยวกับการควบคุมการเข้ารหัสที่ได้รับการพัฒนาขึ้นด้วยกระบวนการและขั้นตอนเพื่อยกระดับการป้องกันที่เหมาะสมกับข้อมูลที่สำคัญและละเอียดอ่อน ในขณะเดียวกันก็รับประกันการปฏิบัติตามข้อกำหนดทางกฎหมาย

ตารางที่ 3.14 ตารางแสดงความเสี่ยงของหัวข้อ ITPO-07

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 3.14 การทำ Risk Management พบว่า ก่อนทำการปรับแก้นโยบาย ITPO-07 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความเสี่ยงสูงและเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุอยู่บ่อยครั้ง

- POLICY STATEMENT (นโยบายขององค์กร)

ในรูปที่ 3.24 จะเป็นการอธิบายระเบียบข้อบังคับ และสัญญา ขั้นตอนการจัดการข้อมูล กำหนดข้อกำหนดสำหรับการใช้เทคนิคการเข้ารหัสเพื่อปกป้องข้อมูลที่ละเอียดอ่อนทั้งที่เป็นข้อมูลดิบและข้อมูลที่อยู่ระหว่างการส่ง นโยบายนี้ควบคุมและขั้นตอนที่เกี่ยวข้องสำหรับพื้นที่ต่าง ๆ ที่มีการเข้ารหัสและใช้เทคนิคการเข้ารหัสอื่น ๆ

- **SCOPE AND APPLICATION OF THE POLICY (ขอบเขตและการบังคับใช้นโยบาย)**

การควบคุมการเข้ารหัสสามารถใช้เพื่อให้บรรลุวัตถุประสงค์ด้านความปลอดภัยของข้อมูลที่แตกต่างกัน เช่น

1. การรักษาความลับ : การใช้การเข้ารหัสข้อมูลเพื่อปกป้องข้อมูลที่ละเอียดอ่อนหรือสำคัญ ไม่ว่าจะจัดเก็บหรือส่ง

2. ความสมบูรณ์/ความถูกต้อง : ใช้ใบรับรองลายเซ็นดิจิทัลหรือรหัสการตรวจสอบข้อความเพื่อยืนยัน ความถูกต้องหรือความสมบูรณ์ของข้อมูลที่ละเอียดอ่อนหรือสำคัญที่จัดเก็บหรือส่งต่อ

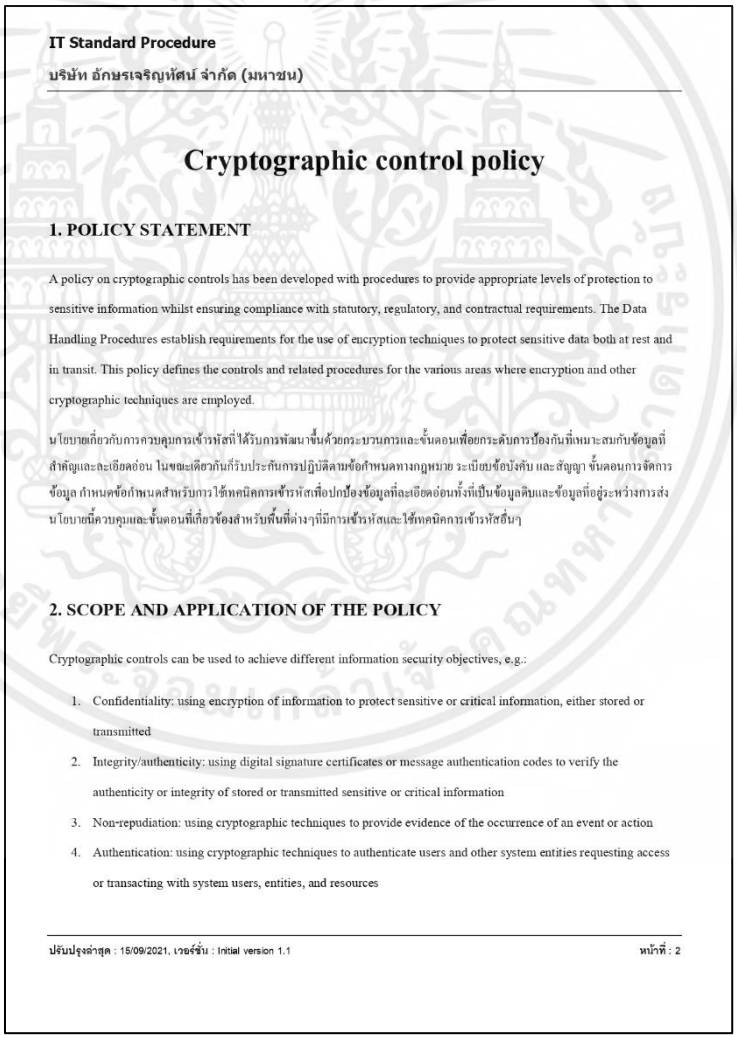
3. การไม่ปฏิเสธ : การใช้เทคนิคการเข้ารหัสเพื่อเก็บหลักฐานของเหตุการณ์หรือการกระทำเหล่านั้นที่เกิดขึ้น

4. การตรวจสอบความถูกต้อง : การใช้เทคนิคการเข้ารหัสเพื่อรับรองความถูกต้องของผู้ใช้และหน่วยงานระบบอื่น ๆ ที่ขอเข้าถึงหรือทำธุรกรรมกับ ผู้ใช้ระบบ หน่วยงาน และทรัพยากร

- **DEFINITIONS (คำจำกัดความ)**

1. การเข้ารหัสเชิงควอนตัม : วิธีการจัดเก็บและส่งข้อมูลในรูปแบบที่เฉพาะที่มีไว้สำหรับอ่านและประมวลผลเท่านั้น
2. การเข้ารหัส : กระบวนการแปลงข้อมูลจากข้อความธรรมดาเป็นรูปแบบที่ไม่สามารถอ่านได้กับบุคคลที่ไม่ได้รับอนุญาตหรือที่เรียกว่าการเข้ารหัส
3. กุญแจ : อินพุตที่ควบคุมกระบวนการเข้ารหัสและถอดรหัส มีทั้งคีย์ลับและคีย์สาธารณะที่ใช้ในการเข้ารหัส
4. ใบรับรองดิจิทัล : เอกสารอิเล็กทรอนิกส์ที่ใช้ในการตรวจสอบตัวตนของผู้ถือใบรับรองเมื่อทำธุรกรรมทางอิเล็กทรอนิกส์ ใบรับรอง SSL เป็นตัวอย่างทั่วไปที่ระบุข้อมูลเกี่ยวกับเซิร์ฟเวอร์บนอินเทอร์เน็ต รวมทั้งคีย์การเข้ารหัสลับสาธารณะของหน่วยงานที่เป็นเจ้าของ

5. ใบรับรองลายเซ็นดิจิทัล : ชนิดของใบรับรองดิจิทัลที่พิสูจน์ว่าผู้ส่งข้อความหรือเจ้าของเอกสารเป็นของแท้และความสมบูรณ์ของข้อความหรือเอกสารจะไม่เปลี่ยนแปลง
6. ใบรับรองลายเซ็นดิจิทัลใช้การเข้ารหัสแบบอสมมาตร และไม่ได้เป็นรุ่นที่สแกนของลายเซ็นที่เขียนด้วยลายมือของบุคคลอื่น หรือลายเซ็นที่เขียนด้วยลายมือที่สร้างโดยคอมพิวเตอร์ (a.k.a. เป็นลายเซ็นอิเล็กทรอนิกส์)
7. คีย์ SSH : คู่คีย์สาธารณะ / ส่วนตัวที่ใช้สำหรับการรับรองความถูกต้องของเซิร์ฟเวอร์ SSH และสร้างการเชื่อมต่อเครือข่ายที่ปลอดภัย



IT Standard Procedure
บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

Cryptographic control policy

1. POLICY STATEMENT

A policy on cryptographic controls has been developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory, and contractual requirements. The Data Handling Procedures establish requirements for the use of encryption techniques to protect sensitive data both at rest and in transit. This policy defines the controls and related procedures for the various areas where encryption and other cryptographic techniques are employed.

นโยบายเกี่ยวกับการควบคุมการเข้ารหัสที่ได้รับการพัฒนาขึ้นด้วยกระบวนการและขั้นตอนเพื่อยกระดับการป้องกันที่เหมาะสมกับข้อมูลที่สำคัญและละเอียดอ่อน ในขณะเดียวกันก็รับประกันการปฏิบัติตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา ขั้นตอนการจัดการข้อมูล กำหนดข้อกำหนดสำหรับการใช้เทคนิคการเข้ารหัสเพื่อปกป้องข้อมูลที่ละเอียดอ่อนทั้งที่เป็นข้อมูลดิบและข้อมูลที่อยู่ระหว่างการส่ง นโยบายนี้ควบคุมและขั้นตอนที่เกี่ยวข้องสำหรับพื้นที่ต่างๆที่มีการเข้ารหัสและใช้เทคนิคการเข้ารหัสอื่นๆ

2. SCOPE AND APPLICATION OF THE POLICY

Cryptographic controls can be used to achieve different information security objectives, e.g.:

1. Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted
2. Integrity/authenticity: using digital signature certificates or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information
3. Non-repudiation: using cryptographic techniques to provide evidence of the occurrence of an event or action
4. Authentication: using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities, and resources

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 2

รูปที่ 3.24 ตัวอย่างเอกสารหัวข้อ POLICY STATEMENT

- **USE OF CRYPTOGRAPHIC CONTROLS POLICY (นโยบายการควบคุมการเข้ารหัส)ดังแสดงให้เห็นในรูปที่ 3.25**

    1. วิธีการเข้ารหัสที่ได้รับการอนุมัติสำหรับข้อมูลที่เหลือ
    2. ขั้นตอนการจัดการข้อมูลกำหนดให้ต้องเข้ารหัสการจัดเก็บข้อมูลที่ละเอียดอ่อนในบางสถานที่ โปรดดูขั้นตอนการจัดการข้อมูลสำหรับความต้องการเฉพาะ
    3. ทำการดูขั้นตอนการเข้ารหัสข้อมูลสำหรับวิธีการเข้ารหัสที่ได้รับอนุมัติและขั้นตอนการจัดการคีย์
    4. วิธีการเข้ารหัสสำหรับข้อมูลที่มีการเคลื่อนไหว
    5. ขั้นตอนการจัดการข้อมูลต้องการถ่ายโอนข้อมูลที่ละเอียดอ่อนผ่านช่องทางที่ปลอดภัย ช่องสัญญาณที่ปลอดภัยคือการเชื่อมต่อเครือข่ายที่เข้ารหัสลับ
    6. มีวิธีการเข้ารหัสที่หลากหลายและโดยทั่วไปจะมีในตัวแอปพลิเคชัน ผู้ใช้ควรตระหนักถึงการเชื่อมต่อข้อมูลที่ใช้เพื่อส่งข้อมูลที่สำคัญและหากมีการเปิดใช้งานการเข้ารหัสสำหรับการเชื่อมต่อนั้น

- **ENCRYPTION IS REQUIRED FOR (ทำไมการเข้ารหัสถึงเป็นสิ่งจำเป็น)**

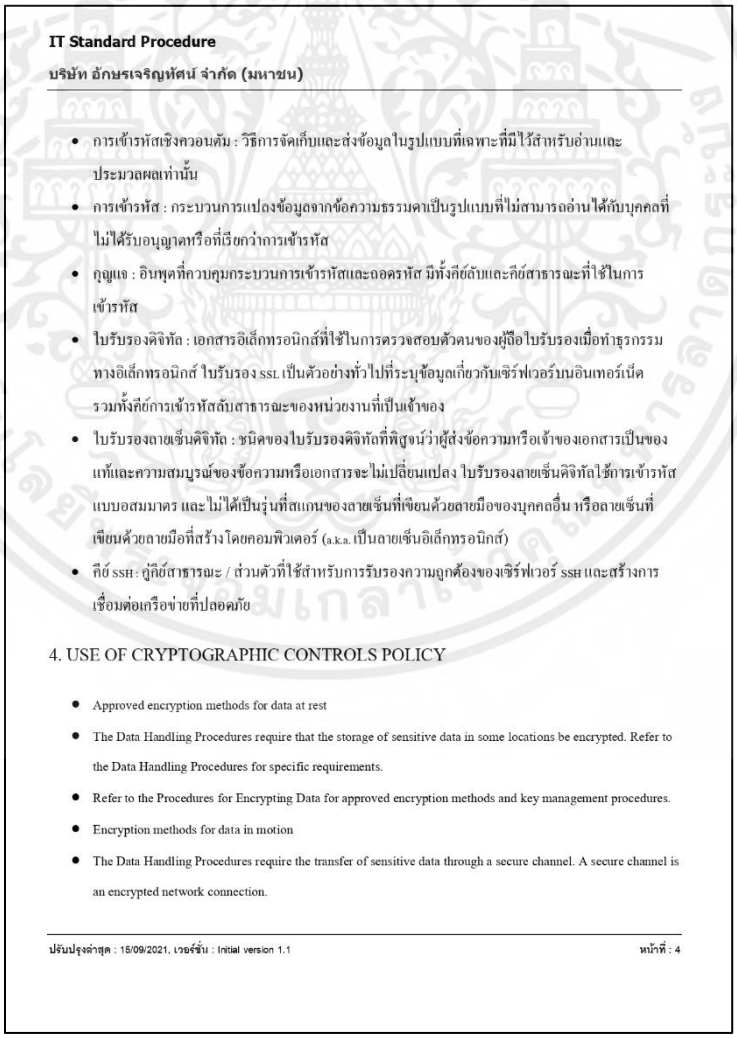
    1. การถ่ายโอนไฟล์ที่มีความละเอียดอ่อน (การใช้งาน FTP SCP หรือ VPN ที่ปลอดภัยเพื่อเข้ารหัสข้อมูลที่ละเอียดอ่อนสำหรับการเข้าถึงไฟล์เครือข่ายของไฟล์ที่ไม่ได้เข้ารหัส)
    2. การเข้าถึงข้อมูลที่ละเอียดอ่อนผ่านทางเว็บไซต์ เว็บแอปพลิเคชัน หรือแอปบนอุปกรณ์เคลื่อนที่ จำเป็นต้องมีการเข้ารหัสเพื่อเข้าถึงข้อมูลที่ละเอียดอ่อนจากทุกสิ่งด้วยอินเทอร์เฟซเว็บ รวมถึงอุปกรณ์มือถือ (เช่น การใช้ HTTPS เพื่อเข้ารหัสข้อมูลที่ละเอียดอ่อน)
    3. การรับส่งข้อมูลเครือข่ายทั้งหมดสำหรับการเข้าถึงระยะไกลไปยังเครื่องเดสก์ทอปเสมือน
    4. การถ่ายโอนข้อมูลที่ละเอียดอ่อนซึ่งเป็นส่วนหนึ่งของการสืบค้นฐานข้อมูลหรือการเรียกใช้บริการเว็บ (ตัวอย่าง การสืบค้น SQL เพื่อดึงหรือส่งข้อมูลจาก

ฐานข้อมูลหรือการเรียกบริการเว็บ Restful เพื่อดึงหรือส่งข้อมูลจากแอปพลิเคชันระบบคลาวด์)

5. สิทธิ์ในการเข้าถึงอุปกรณ์เครือข่ายหรือเซิร์ฟเวอร์เพื่อการจัดการระบบ

- **ENCRYPTION OF EMAIL (การเข้ารหัสอีเมล)**

1. ขั้นตอนการจัดการข้อมูล ที่กำหนดให้เมื่อส่งอีเมลที่มีข้อมูลที่ละเอียดอ่อน ข้อความและไฟล์แนบที่ต้องได้รับการเข้ารหัส
2. อ้างอิงถึงเอกสาร ขั้นตอนการเข้ารหัสข้อมูลสำหรับคำแนะนำในการเข้ารหัสอีเมล



IT Standard Procedure

บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

- การเข้ารหัสเชิงควอนตัม : วิธีการจัดเก็บและส่งข้อมูลในรูปแบบที่เฉพาะที่มีไว้สำหรับอ่านและประมวลผลเท่านั้น
- การเข้ารหัส : กระบวนการแปลงข้อมูลจากข้อความธรรมดาเป็นรูปแบบที่ไม่สามารถอ่านได้กับบุคคลที่ไม่ได้รับอนุญาตหรือที่เรียกว่าการเข้ารหัส
- กุญแจ : อินพุตที่ควบคุมกระบวนการเข้ารหัสและถอดรหัส มีทั้งคีย์ลับและคีย์สาธารณะที่ใช้ในการเข้ารหัส
- ใบรับรองดิจิทัล : เอกสารอิเล็กทรอนิกส์ที่ใช้ในการตรวจสอบตัวตนของผู้ถือใบรับรองเมื่อทำธุรกรรมทางอิเล็กทรอนิกส์ ใบรับรอง SSL เป็นตัวอย่างทั่วไปที่ระบุข้อมูลเกี่ยวกับเซิร์ฟเวอร์บนอินเทอร์เน็ต รวมทั้งคีย์การเข้ารหัสลับสาธารณะของหน่วยงานที่เป็นเจ้าของ
- ใบรับรองลายเซ็นดิจิทัล : ชนิดของใบรับรองดิจิทัลที่พิสูจน์ว่าผู้ส่งข้อความหรือเจ้าของเอกสารเป็นของแท้และความสมบูรณ์ของข้อความหรือเอกสารจะไม่เปลี่ยนแปลง ใบรับรองลายเซ็นดิจิทัลใช้การเข้ารหัสแบบอสมมาตร และไม่ได้เป็นรุ่นที่สแกนของลายเซ็นที่เขียนด้วยลายมือของบุคคลอื่น หรือลายเซ็นที่เขียนด้วยลายมือที่สร้างโดยคอมพิวเตอร์ (a.k.a. เป็นลายเซ็นอิเล็กทรอนิกส์)
- คีย์ SSH : คู่คีย์สาธารณะ / ส่วนตัวที่ใช้สำหรับการรับรองความถูกต้องของเซิร์ฟเวอร์ SSH และสร้างการเชื่อมต่อเครือข่ายที่ปลอดภัย

4. USE OF CRYPTOGRAPHIC CONTROLS POLICY

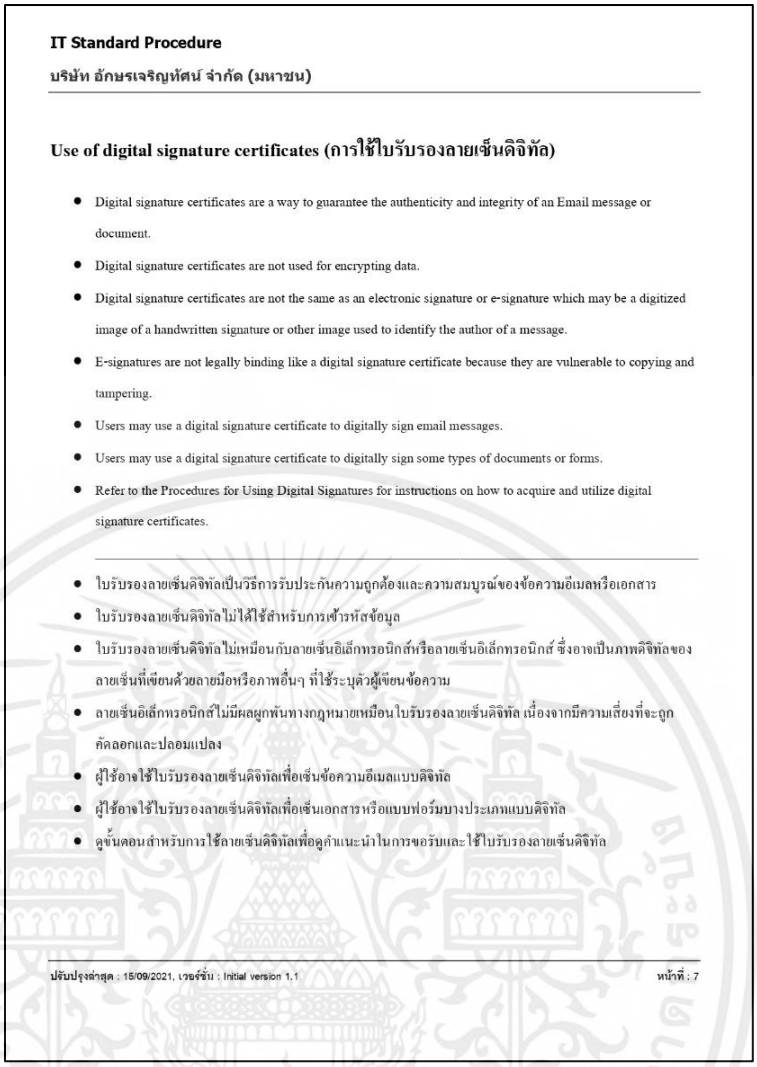
- Approved encryption methods for data at rest
- The Data Handling Procedures require that the storage of sensitive data in some locations be encrypted. Refer to the Data Handling Procedures for specific requirements.
- Refer to the Procedures for Encrypting Data for approved encryption methods and key management procedures.
- Encryption methods for data in motion
- The Data Handling Procedures require the transfer of sensitive data through a secure channel. A secure channel is an encrypted network connection.

ปรับปรุงล่าสุด : 15/09/2021, เวอร์ชั่น : Initial version 1.1 หน้าที่ : 4

รูปที่ 3.25 ตัวอย่างเอกสารหัวข้อ Use of cryptographic control policy

- **USE OF DIGITAL SIGNATURE CERTIFICATES (การใช้ใบรับรองลายเซ็นดิจิทัล) ดังแสดงให้เห็นตัวอย่างเอกสารในรูปที่ 3.26 และกระบวนการในรูปที่ 3.27**

1. ใบรับรองลายเซ็นดิจิทัลเป็นวิธีการรับประกันความถูกต้องและความสมบูรณ์ของข้อความอีเมลหรือเอกสาร
2. ใบรับรองลายเซ็นดิจิทัลไม่ได้ใช้สำหรับการเข้ารหัสข้อมูล
3. ใบรับรองลายเซ็นดิจิทัลไม่เหมือนกับลายเซ็นอิเล็กทรอนิกส์หรือลายเซ็นอิเล็กทรอนิกส์ ซึ่งอาจเป็นภาพดิจิทัลของลายเซ็นที่เขียนด้วยลายมือหรือภาพอื่น ๆ ที่ใช้ระบุตัวผู้เขียนข้อความ
4. ลายเซ็นอิเล็กทรอนิกส์ไม่มีผลผูกพันทางกฎหมายเหมือนใบรับรองลายเซ็นดิจิทัล เนื่องจากมีความเสี่ยงที่จะถูกคัดลอกและปลอมแปลง
5. ผู้ใช้อาจใช้ใบรับรองลายเซ็นดิจิทัลเพื่อเซ็นข้อความอีเมลแบบดิจิทัล
6. ผู้ใช้อาจใช้ใบรับรองลายเซ็นดิจิทัลเพื่อเซ็นเอกสารหรือแบบฟอร์มบางประเภทแบบดิจิทัล
7. ดูขั้นตอนสำหรับการใช้ลายเซ็นดิจิทัลเพื่อดูคำแนะนำในการขอรับและใช้ใบรับรองลายเซ็นดิจิทัล



IT Standard Procedure

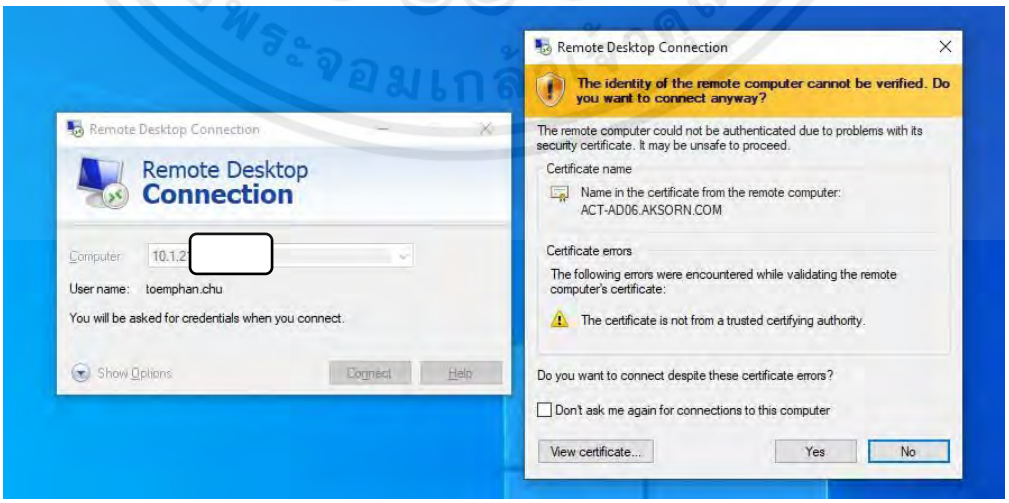
บริษัท อักษรเจริญทัศน์ จำกัด (มหาชน)

Use of digital signature certificates (การใช้ใบรับรองลายเซ็นดิจิทัล)

- Digital signature certificates are a way to guarantee the authenticity and integrity of an Email message or document.
- Digital signature certificates are not used for encrypting data.
- Digital signature certificates are not the same as an electronic signature or e-signature which may be a digitized image of a handwritten signature or other image used to identify the author of a message.
- E-signatures are not legally binding like a digital signature certificate because they are vulnerable to copying and tampering.
- Users may use a digital signature certificate to digitally sign email messages.
- Users may use a digital signature certificate to digitally sign some types of documents or forms.
- Refer to the Procedures for Using Digital Signatures for instructions on how to acquire and utilize digital signature certificates.

- ใบรับรองลายเซ็นดิจิทัลเป็นวิธีการรับประกันความถูกต้องและความสมบูรณ์ของข้อความอีเมลหรือเอกสาร
- ใบรับรองลายเซ็นดิจิทัลไม่ได้ใช้สำหรับการเข้ารหัสข้อมูล
- ใบรับรองลายเซ็นดิจิทัลไม่เหมือนกับลายเซ็นอิเล็กทรอนิกส์หรือลายเซ็นอิเล็กทรอนิกส์ ซึ่งอาจเป็นภาพดิจิทัลของลายเซ็นที่เขียนด้วยลายมือหรือภาพอื่นๆ ที่ใช้ระบุตัวผู้เขียนข้อความ
- ลายเซ็นอิเล็กทรอนิกส์ไม่มีผลผูกพันทางกฎหมายเหมือนใบรับรองลายเซ็นดิจิทัล เนื่องจากมีความเสี่ยงที่จะถูกคัดลอกและปลอมแปลง
- ผู้ใช้อาจใช้ใบรับรองลายเซ็นดิจิทัลเพื่อเซ็นข้อความอีเมลแบบดิจิทัล
- ผู้ใช้อาจใช้ใบรับรองลายเซ็นดิจิทัลเพื่อเซ็นเอกสารหรือแบบฟอร์มบางประเภทแบบดิจิทัล
- ดูขั้นตอนสำหรับการใช้ลายเซ็นดิจิทัลเพื่อดูคำแนะนำในการขอรับและใช้ใบรับรองลายเซ็นดิจิทัล

รูปที่ 3.26 ตัวอย่างเอกสารหัวข้อ Use of digital signature certificates



รูปที่ 3.27 ตัวอย่างใบรับรองลายเซ็นดิจิทัลที่แสดงขึ้นเมื่อ Log-in เข้าสู่ Servers

- **Use and management of SSH keys (การใช้และการจัดการคีย์ SSH)**

1. อ้างถึงเอกสารมาตรฐานสำหรับการใช้คีย์ SSH สำหรับคำแนะนำเกี่ยวกับเวลาและวิธีการใช้คีย์ SSH (https://upcloud.com/community/tutorials/use-ssh-keys-authentication/)
2. อ้างถึงเอกสารมาตรฐานการใช้และการจัดการใบรับรองดิจิทัล SSL (https://www.keyfactor.com/resources/what-is-certificate-management/)
3. เว็บเซิร์ฟเวอร์ AKSORN (หรืออุปกรณ์ที่มีเว็บอินเตอร์เฟส) ที่รองรับการเชื่อมต่อที่ปลอดภัย (HTTPS) จะต้องมีใบรับรอง SSL ติดตั้งอยู่
4. อ้างถึงเอกสารเมตริกซ์การตัดสินใจของใบรับรอง SSL (ภาคผนวก ก) สำหรับการเลือกประเภทใบรับรอง มาตรฐานใบรับรอง AKORN และขั้นตอนการจัดการใบรับรอง

- **USE OF ENCRYPTION (การใช้การเข้ารหัส)**

1. ข้อมูลที่เป็นความลับจะต้องนำไปใช้นอกองค์กรในรูปแบบที่เข้ารหัสเท่านั้น เว้นแต่จะสามารถรับประกันความลับได้เป็นอย่างอื่น ข้อมูลจำแนกประเภทที่นำออกจากองค์กรเพื่อใช้งานจะต้องเก็บไว้ในไดรฟ์ USB ที่เข้ารหัสซึ่งให้บริการโดย Computing and Media Services
2. ขั้นตอนต่าง ๆ จะต้องจัดทำขึ้นเพื่อให้แน่ใจว่าเจ้าหน้าที่ที่ได้รับอนุญาตอาจเข้าถึงข้อมูลทางธุรกิจที่สำคัญใด ๆ ที่เก็บไว้ในรูปแบบที่เข้ารหัสได้ เมื่อจำเป็น คีย์การเข้ารหัสที่ไม่ซ้ำกันจะรู้จักเฉพาะผู้ใช้และบริการคอมพิวเตอร์และสื่อ (อยู่ในที่เก็บที่ปลอดภัย)
3. ความลับของข้อมูลที่ถ่ายโอนบนสื่อแบบพกพาหรือข้ามเครือข่ายต้องได้รับการปกป้องโดยใช้เทคนิคการเข้ารหัสที่เหมาะสม VPN ให้ช่องสัญญาณที่เข้ารหัสระหว่างทรัพยากรในสถานที่และจุดเชื่อมต่อภายนอก ควรใช้ VPN มากกว่าการถ่ายโอนข้อมูลโดยสื่อมือถือ

4. การเข้ารหัสจะใช้เมื่อใดก็ตามที่เหมาะสมในการเชื่อมต่อการเข้าถึงระยะไกลทั้งหมดไปยังเครือข่ายและทรัพยากรขององค์กร คีย์การเข้ารหัสที่ไม่ซ้ำกันจะเป็นที่รู้จักเฉพาะกับผู้ใช้และบริการคอมพิวเตอร์และสื่อ (เก็บไว้ในที่เก็บที่ปลอดภัย)

Managing electronic keys (การจัดการกุญแจอิเล็กทรอนิกส์)

ต้องมีการกำหนดขั้นตอนสำหรับการจัดการกุญแจอิเล็กทรอนิกส์ เพื่อควบคุมทั้งการเข้ารหัสและถอดรหัสเอกสารที่มีความละเอียดอ่อนหรือลายเซ็นดิจิทัล เพื่อให้แน่ใจว่ามีการนำแนวทางปฏิบัติที่ดีที่สุดมาใช้และปฏิบัติตามข้อกำหนดทางกฎหมายและตามสัญญา บริการคอมพิวเตอร์และสื่อจะจัดการคีย์อิเล็กทรอนิกส์ทั้งหมดและให้บริการเข้ารหัสที่เหมาะสมแก่ผู้ใช้เมื่อมีการร้องขอ

Using and receiving digital signatures (การใช้และรับลายเซ็นดิจิทัล)

ข้อมูลทางธุรกิจที่สำคัญที่มีการสื่อสารทางอิเล็กทรอนิกส์จะต้องรับรองความถูกต้องโดยการใช้ลายเซ็นดิจิทัล ข้อมูลที่ได้รับโดยไม่มีลายเซ็นดิจิทัลจะไม่เป็นที่น่าเชื่อถือ บริการคอมพิวเตอร์และสื่อจะจัดการคีย์อิเล็กทรอนิกส์ทั้งหมดและให้บริการเข้ารหัสที่เหมาะสมแก่ผู้ใช้เมื่อมีการร้องขอ

- **REGULATION OF CRYPTOGRAPHIC CONTROLS (กฎระเบียบของการควบคุมการเข้ารหัส)**

กฎระเบียบของการควบคุม CRYPTOGRAPHIC การควบคุมการเข้ารหัสควรใช้ตามข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้องทั้งหมด รายการต่อไปนี้ต้องได้รับการพิจารณาเพื่อให้เป็นไปตามข้อกำหนด

1. ข้อจำกัดในการนำเข้าหรือส่งออกฮาร์ดแวร์คอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้เพื่อทำหน้าที่เข้ารหัส หรือได้รับการออกแบบให้มีฟังก์ชันการเข้ารหัสเพิ่มเข้าไป
2. ข้อจำกัดในการใช้การเข้ารหัสโดยเฉพาะในต่างประเทศ
3. วิธีการเข้าถึงข้อมูลที่เข้ารหัสซึ่งใช้โดยหน่วยงานของประเทศต่าง ๆ

ควรขอคำแนะนำทางกฎหมายเพื่อให้แน่ใจว่ามีการปฏิบัติตามข้อกำหนดก่อนที่ข้อมูลที่เข้ารหัสหรือการควบคุมการเข้ารหัสจะถูกย้ายข้ามเขตอำนาจศาล

บทที่ 4
ผลการศึกษาและการปรับใช้ข้อบังคับ

ในบทนี้กล่าวถึงผลการศึกษาและการปรับใช้ข้อบังคับของอุปกรณ์ไอทีและระบบต่าง ๆ ให้เป็นไปตามมาตรฐานไอเอสโอ 27001:2013 ในหัวข้อที่ได้รับมอบหมาย ผลการปรับเปลี่ยนอุปกรณ์ไอทีและซอฟต์แวร์ต่าง ๆ ภายในองค์กร ผลการทำ Active Directory

4.1 ผลการศึกษาการปรับปรุงหลักปฏิบัติการบริหารจัดการทรัพย์สิน

ผู้จัดทำจะแสดงผลการศึกษาการปรับปรุงหลักปฏิบัติการบริหารจัดการทรัพย์สิน ซึ่งเป็นตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานและตารางแสดงความเสี่ยง โดยแสดงให้เห็นดังตารางที่ 4.1 ต่อไปนี้

ตารางที่ 4.1 ตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานของหัวข้อ ITSP-002

หัวข้อ	รายละเอียด	มาตรฐาน
ITSP-002	- IT Asset Management	ผ่านมาตรฐาน √
ITSP-002	- มาตรฐานการใช้เครื่องคอมพิวเตอร์	ผ่านมาตรฐาน √
ITSP-002	- มาตรฐานการใช้ซอฟต์แวร์คอมพิวเตอร์	ผ่านมาตรฐาน √

ตารางที่ 4.2 ตารางแสดงสรุปความเสี่ยงของหัวข้อ ITSP-002

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 4.2 การทำ Risk Management พบว่า หลังการปรับแก้นโยบาย ITSP-002 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความเสี่ยงน้อยลงและลดความบ่อยครั้งในการเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุ ลงไปได้จาก (4,4) > (2,2)

4.2 ผลการศึกษาการปรับปรุงหลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบ

ผู้จัดทำจะแสดงผลการศึกษาการปรับปรุงหลักปฏิบัติการจัดการข้อมูลผู้ใช้งานระบบซึ่งเป็นตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานและตารางแสดงความเสี่ยง โดยแสดงให้เห็นดังตารางที่ 4.3 ต่อไปนี้

ตารางที่ 4.3 ตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานของหัวข้อ ITSP-005

หัวข้อ	รายละเอียด	มาตรฐาน
ITSP-005	- User Management Process	ผ่านมาตรฐาน √
ITSP-005	- การจัดการบัญชีผู้ใช้งานระบบ One Account	ผ่านมาตรฐาน √
ITSP-005	- การบริหารจัดการรหัสผู้งาน Active Directory	ผ่านมาตรฐาน √

ตารางที่ 4.4 ตารางแสดงสรุปความเสี่ยงของหัวข้อ ITSP-005

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 4.4 การทำ Risk Management พบว่า หลังทำการปรับแก้นโยบาย ITSP-005 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความเสี่ยงปานกลางและโอกาสเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุน้อยลงจาก (5,3) > (3,2)

4.3 ผลการศึกษาการปรับปรุงหลักปฏิบัติการเข้ารหัสข้อมูล

ผู้จัดทำจะแสดงผลการศึกษาการปรับปรุงหลักปฏิบัติการเข้ารหัสข้อมูล ซึ่งเป็นตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานและตารางแสดงความเสี่ยง โดยแสดงให้เห็นดังตารางที่ 4.5 ต่อไปนี้

ตารางที่ 4.5 ตารางแสดงรายละเอียดที่ต้องพิจารณาในมาตรฐานของหัวข้อ ITPO-07

หัวข้อ	รายละเอียด	มาตรฐาน
ITPO-07	- Cryptographic control policy	ผ่านมาตรฐาน √
ITPO-07	- USE OF DIGITAL SIGNATURE CERTIFICATES (การใช้ใบอนุญาตดิจิทัล)	ผ่านมาตรฐาน √
ITPO-07	- USE OF ENCRYPTION (การใช้การเข้ารหัส)	ผ่านมาตรฐาน √

ตารางที่ 4.6 ตารางแสดงสรุปความเสี่ยงของหัวข้อ ITPO-07

Risk Management	Likelihood (โอกาสเกิด)				
Impact (ผลกระทบ)	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	บ่อย (4)	บ่อยมาก (5)
สูงมาก (5)	Medium(5,1)	High(5,2)	Extreme(5,3)	Extreme(5,4)	Extreme(5,5)
สูง (4)	Medium(4,1)	Medium(4,2)	High(4,3)	Extreme(4,4)	Extreme(4,5)
ปานกลาง (3)	Low(3,1)	Medium(3,2)	Medium(3,3)	High(3,4)	Extreme(3,5)
น้อย (2)	Low(2,1)	Low(2,2)	Medium(2,3)	Medium(2,4)	High(2,5)
น้อยมาก (1)	Low(1,1)	Low(1,2)	Low(1,3)	Medium(1,4)	Medium(1,5)

ในตารางที่ 4.6 การทำ Risk Management พบว่า หลังทำการปรับแก้นโยบาย ITPO-07 ให้เป็นไปตามมาตรฐานใหม่ทางองค์กรมีความน้อยลงและลดโอกาสเกิดเหตุการณ์ฉุกเฉินและอุบัติเหตุได้ ลดลงจาก (4,4) > (2,2)

บทที่ 5
สรุปผลการศึกษาและข้อเสนอแนะ

ในบทนี้เป็นการสรุปผลการวิจัย ปัญหาและอุปสรรคในการทำงาน และข้อเสนอแนะต่าง ๆ ซึ่งมีรายละเอียดดังนี้

5.1 สรุปผลการศึกษา

จากการดำเนินงานของสหกิจศึกษาในการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013 ได้ทำเอกสารและปรับปรุงนโยบายข้อบังคับให้กับองค์กร รวมไปถึงการนำไปใช้ปรับเปลี่ยนระบบและอุปกรณ์ไอที ให้สอดคล้องกับนโยบายใหม่ตามมาตรฐานสากลควบคู่กับเอกสารใหม่ที่จัดทำขึ้นมา ช่วยให้องค์กรมีมาตรฐานการบริหารจัดการความเสี่ยงและความปลอดภัยของข้อมูล รวมไปถึงอุปกรณ์ไอทีต่าง ๆ ภายในองค์กรมีความทันสมัยมากยิ่งขึ้น และองค์กรมีภาพลักษณ์และความน่าเชื่อถือขององค์กรสูงขึ้น จากทั้งภายในและภายนอกองค์กร เพื่อองค์กรได้ยื่นขอปรับปรุงมาตรฐานไอเอสโอให้เป็นปัจจุบันตามมาตรฐานสากลต่อไป

5.2 ปัญหาและอุปสรรค

1. ต้องใช้ความรู้ความชำนาญในด้านการทำเอกสารมาตรฐานไอเอสโอ 27001

2. ไม่สามารถทำเอกสารได้อย่างถูกต้องมากนักในช่วงแรก เพราะเอกสารที่ทำเป็นเอกสารสำคัญและเป็นข้อมูลความลับขององค์กร

3. คำศัพท์บางคำเป็นคำศัพท์เฉพาะทางกฎหมายไอทีจึงทำให้ยากต่อการทำเอกสารในช่วงแรก เพราะไม่เคยมีความรู้และประสบการณ์ทางด้านนี้

5.3 วิธีการแก้ไขปัญหา

1. ผู้จัดทำได้ศึกษามาตรฐานไอเอสโอ 27001 จากทุกช่องทางอย่างละเอียด ไม่ว่าจะเป็นมาตรฐานเก่าปี 2005 และ มาตรฐานใหม่ปี 2013 เพื่อนำความรู้มาปฏิบัติและจัดทำเอกสารได้อย่างถูกต้อง เพื่อให้สอดคล้องกับการศึกษาแนวทางการปรับปรุงระบบรักษาความปลอดภัยของข้อมูลตามมาตรฐานไอเอสโอ 27001:2013

2. เนื่องจากผู้จัดทำไม่สามารถทำเอกสารให้ถูกต้องตามรูปแบบที่องค์กรต้องการได้ จำเป็นต้องสอบถามเจ้าหน้าที่ผู้มีประสบการณ์ โดยเจาะจงสอบถามเฉพาะข้อมูลที่จำเป็นต่อหัวข้อที่ได้รับมอบหมายเท่านั้น เพราะข้อมูลทั้งหมดคือข้อมูลสำคัญที่ใช้ภายในบริษัทเท่านั้น

3. ผู้จัดทำได้ศึกษาหาข้อมูลคำศัพท์เพิ่มเติมไม่ว่าจะเป็นคำศัพท์ไทยหรืออังกฤษ จากทุกช่องทางอย่างละเอียด ควบคู่ไปกับปรึกษาและสอบถามรุ่นพี่ที่ชำนาญการ

5.4 ข้อเสนอแนะ

คณะผู้บริหารและผู้จัดการฝ่ายสารสนเทศเสนอแนะว่า ผู้จัดทำควรมีการทำแบบฟอร์มที่เชื่อถือได้ในการสอบถามข้อมูลสารสนเทศจากพนักงาน เพื่อแก้ปัญหาต่าง ๆ ที่เกิดขึ้น เช่น ปัญหาข้อมูลที่ละเอียดอ่อนและเป็นความลับ ผู้จัดทำควรวางแผนและทำแบบฟอร์ม และทางผู้บริหารยินดีที่จะลงนามในแบบฟอร์มสอบถามข้อมูล เพื่อความน่าเชื่อถือและง่ายต่อผู้จัดทำในการประสานงานให้เป็นระบบ และการแบ่งหน้าที่ความรับผิดชอบให้ตรงตามงานที่ได้รับมอบหมาย เพื่อการทำงานจะได้มีประสิทธิภาพและรวดเร็วมากยิ่งขึ้น

บรรณานุกรม

[1] บทความเกี่ยวกับความจำเป็นของการรักษาความปลอดภัยของข้อมูล [3], [ออนไลน์], ค้นหาเมื่อ 15 ธันวาคม 2564, จาก https://www.pjrthailand.com/standards/iso-27001

[2] บทความเกี่ยวกับ International Organization for Standardization, [ออนไลน์], ค้นหาเมื่อ 15 ธันวาคม 2564, จาก https://op.mahidol.ac.th/ia/wp-content/uploads/2017/08/07KMISO27001.pdf

[3] บทความเกี่ยวกับมาตรฐาน ISO 27001, [ออนไลน์],ค้นหาเมื่อ 15 ธันวาคม 2564, จาก https://www.pjrthailand.com/standards/iso-27001

[4] บทความเกี่ยวกับ Information Security Management Systems, [ออนไลน์], ค้นหาเมื่อ 16 ธันวาคม 2564, จาก https://www.pjrthailand.com/standards/iso-27001

[5] บทความเกี่ยวกับมาตรฐานไอเอสโอ ISO/IEC 27001:2013, [ออนไลน์], ค้นหาเมื่อ 16 ธันวาคม 2564, จาก https://bit.ly/3pmNf5t

[6] บทความเกี่ยวกับการบริหารจัดการความเสี่ยง Risk Management, [ออนไลน์], ค้นหาเมื่อ 16 ธันวาคม 2564, จาก https://www.acinfotec.com/99/2006/10/06/policy-risk-management-the-key-process-for-iso-27001-implementation/

[7] บทความเกี่ยวกับการประเมินความเสี่ยง Risk Assessment, [ออนไลน์], ค้นหาเมื่อ 16 ธันวาคม 2564, จาก https://shorturl.asia/I4yQ7

[8] บทความเกี่ยวกับศัพท์เฉพาะทางเทคโนโลยีสารสนเทศ, [ออนไลน์], ค้นหาเมื่อ 23 ธันวาคม 2564, จาก https://bit.ly/3EuDoPC

ประวัติผู้เขียน

ชื่อ-นามสกุล นางเติมพันธ์ ช่วยนคร

วัน เดือน ปีเกิด 27 เมษายน พ.ศ. 2542

ที่อยู่ปัจจุบัน 48 หมู่ 3 ตำบลบางไทร อำเภอเมือง จังหวัดสุราษฎร์ธานี
รหัสไปรษณีย์ 84000

อีเมล 61515005@kmitl.ac.th

ประวัติการศึกษา ระดับมัธยมศึกษาตอนต้น โรงเรียนสุราษฎร์ธานี
ระดับมัธยมศึกษาตอนปลาย สายศิลป์คำนวณ
โรงเรียนสุราษฎร์ธานี จังหวัดสุราษฎร์ธานี
เบอร์โทรศัพท์ : 0994972167