กรณีศึกษาการจัดทำ ISO 27001:2013 ให้กับภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สจล.

THE CASE STUDY ON ISO 27001:2013 FOR DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF SCIENCE, KMITL

พรเทพ เกิดสมพงษ์
ภมรวิทย์ วรรณวิชิต

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตร์บัณฑิต

สาขาวิทยาการคอมพิวเตอร์

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2557

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

THE CASE STUDY ON ISO 27001:2013 FOR DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF SCIENCE, KMITL

Phornthep Kerdsompong
Pamonwit Wanwichit

SPECIAL PROBLEM SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF BACHELOR OF SCIENCE
IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2014

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปัญหาพิเศษ	กรณีศึกษาการจัดทำ ISO 27001:2013 ภาควิชาวิทยาการ-คอมพิวเตอร์ คณะวิทยาศาสตร์ สจล. The Case Study on ISO 27001:2013 for Department of Computer Science, Faculty of Science, KMITL
ชื่อนักศึกษา	นายพรเทพ เกิดสมพงษ์ 54050924 นายภมรวิทย์ วรรณวิชิต 54050942
ปริญญา	วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
ภาควิชา	วิทยาการคอมพิวเตอร์
ปีการศึกษา	2557
อาจารย์ที่ปรึกษา	อาจารย์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์

คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์) ประจำปีการศึกษา 2557

คณะกรรมการสอบ	ลายมือชื่อ
ผศ.กฤษฎา บุศรา ประธานกรรมการ	
ผศ.ดร.กรกช ประชุมรักษ์ กรรมการ	
อ.ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ กรรมการและอาจารย์ที่ปรึกษา	

ลิขสิทธิ์ของคณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปัญหาพิเศษ	กรณีศึกษาการจัดทำ ISO 27001:2013 ภาควิชาวิทยาการ-คอมพิวเตอร์ คณะวิทยาศาสตร์ สจล. The Case Study on ISO 27001:2013 for Department of Computer Science, Faculty of Science, KMITL
ชื่อนักศึกษา	นายพรเทพ เกิดสมพงษ์ 54050924 นายภมรวิทย์ วรรณวิชิต 54050942
ปริญญา	วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
ภาควิชา	วิทยาการคอมพิวเตอร์
ปีการศึกษา	2557
อาจารย์ที่ปรึกษา	อาจารย์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์

บทคัดย่อ

ปัญหาพิเศษนี้มีวัตถุประสงค์ในการจัดทำนโยบายเรื่องความปลอดภัยในการใช้งานอุปกรณ์คอมพิวเตอร์ ห้องปฏิบัติการคอมพิวเตอร์ และระบบสารสนเทศของภาควิชาวิทยาการคอมพิวเตอร์ให้เป็นไปตามมาตรฐาน ISO 27001:2013 ซึ่งประกอบไปด้วยสองส่วน คือ ส่วนในการสำรวจและตรวจสอบสถานะความเสี่ยงของระบบสารสนเทศของภาควิชา เพื่อผลักดันให้ภาควิชามีการจัดทำนโยบายด้านความปลอดภัยของระบบสารสนเทศ ที่เป็นไปตามมาตรฐาน ISO 27001:2013 และส่วนโปรแกรมในการจัดการการพิมพ์เอกสารของผู้ใช้งานให้เป็นไปตามโควตาที่ผู้ดูแลระบบได้กำหนดไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	The Case Study on ISO 27001:2013 for Department of Computer Science, Faculty of Science, KMITL
Students	Mr.Phornthep Kerdsompong 54050924
	Mr.Pamonwit Wanwichit 54050942
Degree	Bachelor of Science (Computer Science)
Department	Computer Science
Academic Year	2014
Advisor	Dr. Rungrat Wiangsripanawan

Abstract

This special problem aims to prepare the information security policies according to the international standard namely ISO 27001:2013 for the Department of Computer Science, Faculty of Science, KMITL. Therefore, the department's information security system such as the security for computer devices and computer laboratories, and information system is not only increased but also follows the international standards. The work is divided into two parts. The first part is to detect and analyze computer threats in the department so that it can be used to plan the set of Department's security policies that abide by the ISO 27001/2013. The second part is the print management program that the administrator can use to manage the users' print quota.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ในการทำปัญหาพิเศษฉบับนี้ จะสำเร็จไม่ได้หากไม่ได้ความกรุณาและความช่วยเหลือจากบุคคลผู้มีพระคุณหลายท่านดังนี้

ขอขอบพระคุณในความกรุณาของ อาจารย์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ อาจารย์สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อาจารย์ที่ปรึกษาปัญหาพิเศษที่ได้เสียสละให้คำแนะนำ ให้คำปรึกษาในการแก้ปัญหาต่างๆ ตลอดจนการตรวจแก้ปัญหาพิเศษฉบับนี้ให้สมบูรณ์มากยิ่งขึ้น

ขอขอบพระคุณ คณาจารย์ทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชาความรู้ ตลอดจนคุณธรรม จริยธรรม ตลอดระยะเวลา 4 ปี

สุดท้ายขอกราบขอบพระคุณบิดา มารดา และบุคคลในครอบครัว รวมทั้งเพื่อนๆที่ให้ความช่วยเหลือในด้านต่างๆ และเป็นกำลังใจตลอดการทำปัญหาพิเศษนี้

นายพรเทพ เกิดสมพงษ์
นายภมรวิทย์ วรรณวิชิต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่ หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูปภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ISO 27001:2013 (Information Security Management System-ISMS) มาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการจัดทำ นำไปปฏิบัติ ทบทวนและเฝ้าระวัง รักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้สอดคล้องกับสถานการณ์ ISO 27001:2013 ซึ่งเป็นแนวทางหรือวิธีการจัดการเกี่ยวกับเรื่องความเสี่ยงด้านสารสนเทศเพื่อกำหนดนโยบายและกระบวนการทำงาน รวมทั้งเพื่อเลือกการควบคุมที่เหมาะสมในการบริหารความเสี่ยง กล่าวได้ว่าเป็นมาตรฐานเชิงระบบเน้นการปฏิบัติ

จากการสำรวจและสัมภาษณ์เจ้าหน้าที่ที่ดูแลระบบคอมพิวเตอร์ พบว่านโยบายในการจัดการเกี่ยวกับอุปกรณ์คอมพิวเตอร์ และการเข้าใช้อุปกรณ์ของบุคลากรและนักศึกษาทางสาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ ไม่เป็นไปตามมาตรฐาน ISO 27001:2013 (Information Security Management Systems) ซึ่งอาจทำให้เกิดความไม่ปลอดภัยในการเข้าใช้ระบบคอมพิวเตอร์ได้

ผู้จัดทำได้เห็นถึงปัญหานี้จึงมีความสนใจในการนำมาตรฐาน ISO 27001:2013 มาทำการกำหนดนโยบายในการจัดการอุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่ายและการเข้าใช้อุปกรณ์คอมพิวเตอร์และห้องปฏิบัติการของบุคลากรและนักศึกษาของภาควิชาฯ รวมทั้งสร้างโปรแกรมเพื่อช่วยอำนวยความสะดวกให้เจ้าหน้าที่ประจำห้องปฏิบัติการ ในการจำกัดจำนวนหน้าการใช้เครื่องพิมพ์เอกสารของนักศึกษา

นอกจากนี้เพื่อให้การจัดการอุปกรณ์ต่างๆ เป็นได้อย่างมีระบบ ผู้จัดทำจะมีการจัดทำบัญชีทรัพย์สินของอุปกรณ์ต่างๆ ในห้องปฏิบัติการ และมีการจัดทำเว็บไซต์เพื่อให้ความรู้แก่ผู้ใช้งาน และผู้ดูแลระบบ ซึ่งผู้จัดทำหวังว่าการปรับปรุงขั้นตอนการทำงานเหล่านี้สามารถนำไปใช้อ้างอิงเพื่อการประเมินความปลอดภัยของระบบคอมพิวเตอร์ได้

1.2 วัตถุประสงค์ของหัวข้อปัญหาพิเศษ

1) เพื่อเพิ่มความปลอดภัยในการใช้งานคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ภายในภาควิชาวิทยาการคอมพิวเตอร์
2) เพื่อกำหนดนโยบายในการใช้งานคอมพิวเตอร์ให้เป็นไปตามมาตรฐาน ISO 2700:2013 ให้สาขาวิทยาการคอมพิวเตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3) เพื่อแนะนำให้ผู้ดูแลระบบรู้จักมาตรฐาน ISO 27001:2013
4) เพื่อตรวจสอบระบบคอมพิวเตอร์ในคณะวิทยาศาสตร์ว่าเป็นไปตามมาตรฐาน ISO 27001:2013

1.3 ขอบเขตของหัวข้อปัญหาพิเศษ

1) สร้างโปแกรมจำกัดจำนวนหน้าการใช้เครื่องพิมพ์เอกสารของนักศึกษา
2) กำหนดนโยบายความปลอดภัยให้ภาควิชาวิทยาการคอมพิวเตอร์
3) จัดทำบัญชีทรัพย์สินให้ภาควิชาวิทยาการคอมพิวเตอร์
4) จัดทำแผนผังระบบเครือข่ายให้ภาควิชาวิทยาการคอมพิวเตอร์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ผู้พัฒนา

1) ได้ศึกษามาตรฐาน ISO 27001:2013
2) ได้ฝึกการเขียนโปรแกรมด้วยภาษา C#
3) ได้ฝึกตรวจสอบการตั้งค่าเครื่องคอมพิวเตอร์

ผู้ใช้

1) ได้รู้จักกับมาตรฐาน ISO 27001:2013
2) สามารถใช้โปรแกรมในการจำกัดจำนวนหน้าการใช้เครื่องพิมพ์เอกสารของนักศึกษา
3) เครื่องคอมพิวเตอร์ของผู้ใช้มีความปลอดภัยมากขึ้น

1.5 ขั้นตอนในการดำเนินงาน

1) กำหนดและเลือกหัวข้อโครงงาน
2) ศึกษามาตรฐาน ISO 27001:2013
3) ศึกษานโยบายการใช้งานเครื่องคอมพิวเตอร์ของภาควิชาวิทยาการคอมพิวเตอร์
4) ทำการออกแบบพัฒนาและตรวจสอบนโยบายการใช้งานเครื่องคอมพิวเตอร์ของภาควิชาวิทยาการคอมพิวเตอร์ให้เป็นไปตามมาตรฐาน ISO 27001:2013
5) ทำการศึกษาเรียนรู้และพัฒนาการเขียนสคริปต์ การเขียนโปรแกรมเรียกใช้งานสคริปต์และการจัดการฐานข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6) ทำการทดลองและตรวจสอบสคริปต์และโปรแกรมเรียกใช้งานสคริปต์เพื่อหาข้อผิดพลาดในระบบแล้วทำการแก้ไขให้ใช้งานได้จริง
7) ทำการส่งโปรแกรมรุ่นทดลองไปให้ผู้ใช้ทดสอบ
8) ทำการแก้ไขและพัฒนาโปรแกรมให้เสร็จสมบูรณ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ISO 27001:2013 มาตรฐานระบบบริหารความมั่นคงความปลอดภัย (Information Security Management System)

Information Security Management System (ISMS) Standard หรือที่รู้จักกันในนาม ISO 27001: 2013 มาตรฐานการจัดการความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการ จัดทำ นำไปปฏิบัติ ทบทวนและเฝ้าระวัง รักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้สอดคล้องกับสถานการณ์ ผู้ที่ประยุกต์ใช้มาตรฐานนี้ต้องจัดทำเอกสารให้ครอบคลุมข้อกำหนดข้างต้น และระบบที่จัดทำขึ้นนี้จะต้องเหมาะสมกับความเสี่ยงเชิงธุรกิจขององค์กร [1]

การจัดทำระบบบริหารจัดการ (Management System) ต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง

- การบริหารคนภายในองค์กรและภายนอกองค์กร
- กระบวนการและเทคโนโลยี เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน
- บริหารงบประมาณ การลงทุนที่คุ้มค่า [2]

ความเป็นมาของ ISO 27001:2013

ISO 27001:2013 เป็นมาตรฐานที่เกิดจากความร่วมมือระหว่างหน่วยงาน ISO (The International Organization for Standardization) กับหน่วยงาน IEC (The International Electro technical Commission) ร่วมกับองค์กรระหว่างประเทศอื่นอีกหลายองค์กร ประกอบด้วยองค์กรรัฐบาลและองค์กรอิสระต่างๆ

เป้าหมายของการนำมาตรฐานมาใช้

มาตรฐาน ISO 27001:2013 เป็นมาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศที่ผ่านการอภิปราย และรับรองโดยประเทศที่เป็นสมาชิก นอกจากนี้มีในกระบวนการพัฒนามาตรฐานระดับสากลได้เปิดโอกาสให้ตัวแทนของแต่ละประเทศ องค์กรวิชาชีพ ได้เข้ามามีส่วนร่วม โดยมีเป้าหมายเพื่อให้เกิดการยอมรับในระดับสากล

องค์กรที่ต้องการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ หากต้องการสร้างระบบที่ได้รับการยอมรับอย่างแพร่หลาย ควรนำมาตรฐานสากลมาประยุกต์ใช้จะเป็นผลดีกว่าการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กำหนดมาตรฐานเอง ซึ่งต้องใช้เวลาและผู้เชี่ยวชาญในการพัฒนา นอกจากนี้ยังอาจมีปัญหาเรื่องการยอมรับจากภายนอก

ข้อดีของการประยุกต์ใช้มาตรฐาน ISO 27001:2013

- เป็นที่ยอมรับระดับสากล รู้จักแพร่หลายทั่วโลก
- มีการตรวจประเมินเพื่อรับรองมาตรฐาน โดยองค์กรที่ไม่มีส่วนได้เสีย (Third Party Certification Body)
- มีองค์ความรู้ หนังสือ การสัมมนา ที่ปรึกษาและผู้เชี่ยวชาญ
- เป็นมาตรฐานที่ไม่ผูกมัดกับเทคโนโลยี เทคนิค หรือ ขั้นตอนที่เฉพาะเจาะจง ผู้จัดทำระบบสามารถเลือกเทคโนโลยีได้ตามความเหมาะสมทำให้มาตรฐานมีความคล่องตัวสูง

สิ่งที่ควรทราบก่อนนำมาตรฐาน ISO 27001:2013 มาประยุกต์ใช้

- ISO/IEC 27001 เป็นภาษาอังกฤษ ส่วนของไทยก็มีมาตรฐานของคณะกรรมการธุรกรรมองค์กรที่จัดทำระบบนี้ต้องมีความรู้ในภาษาอังกฤษระดับที่สามารถตีความข้อกำหนดได้อย่างถูกต้อง
- การประยุกต์ใช้มาตรฐาน ต้องมาตีความข้อกำหนดและวางแนวทางปฏิบัติให้สอดคล้อง หากตีความผิดหรือไม่ครบถ้วนก็อาจเกิดปัญหาในการตรวจประเมินเพื่อขอการรับรองได้ [3]

ก่อนเริ่มต้นทำ ISO 27001:2013 ต้องมีความรู้และความเข้าใจ 2 เรื่องคือ

1. เข้าใจองค์กรตนเอง ต้องสำรวจข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ เข้าใจภารกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่างๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง เพื่อที่จะหามาตรการมาจัดการกำจัดจุดอ่อนทั้งนี้ก็แล้วแต่แนวทางและขีดความสามารถของแต่ละองค์กร

2. เข้าใจมาตรฐาน จะนำมาตรฐาน ISO 27001 มาใช้งาน ก็ต้องทำความเข้าใจในตัวมาตรฐานเสียก่อน ว่าต้องทำอะไรบ้าง ทั้งเรื่องเอกสาร (Documents) และการนำไปใช้งานจริง (Implementation) ข้อกำหนดของ ISO 27001:2013 ฉบับของ ISO-International Organization for Standardization นั้นเป็นภาษาอังกฤษ

วิธีการเริ่มต้นทำ ISO 27001:2013

ขั้นตอนที่ 1 กำหนดขอบเขต (Scope)ที่จะทำ ISO 27001:2013 หรือต้องการให้ระบบงานหรือกิจกรรมอะไรบ้างที่ถูกควบคุมดูแลภายใต้ ISO 27001:2013 เพื่อให้มั่นใจว่าสารสนเทศของระบบงาน หรือกิจกรรมนั้นๆ มีความมั่นคงปลอดภัย

ขั้นตอนที่ 2 ศึกษามาตรฐาน ISO 27001:2013 ให้เข้าใจหลักการพื้นฐานและแนวทางการนำไปใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนที่ 3 ทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรบ้างเมื่อเทียบกับ สิ่งที่ต้องมีตามมาตรฐาน ISO 27001:2013

การนำมาตรฐาน ISO 27001:2013 มาใช้งาน

การจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS) แบ่งเป็น 4 ขั้นตอน ดังนี้

1. การวางแผนจัดทำระบบ ISMS (Establish ISMS)
2. การนำไปปฏิบัติ (Implement and operate ISMS)
3. การเฝ้าระวังและทบทวน (Monitor an review ISMS)
4. การรักษามาตรฐานและพัฒนาปรับปรุง (Maintain and improve ISMS)

1. การวางแผนจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (Plan: Establish the ISMS)

เริ่มต้นด้วยการกำหนดขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศให้ชัดเจน โดยแสดงถึงลักษณะของธุรกิจ องค์กร ทำเลที่ตั้ง ทรัพย์สิน และเทคโนโลยี หากไม่ครอบคลุมส่วนงานใด ต้องระบุรายละเอียดและเหตุผลดังกล่าว จากนั้นผู้บริหารระดับสูงกำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System Policy : ISMS Policy) พร้อมทั้งอนุมัติและประกาศใช้นโยบายดังกล่าว เป็นกลไกให้มั่นใจว่าโครงการนี้ได้รับการสนับสนุนอย่างเป็นรูปธรรม และเป็นสัญญาณว่า ISMS ได้เริ่มอย่างเป็นทางการแล้ว

การกำหนดคณะทำงานให้เหมาะสมและเพียงพอเป็นเรื่องสำคัญที่ต้องพิจารณา ตัวแทนหน่วยงานที่อยู่ในขอบเขตการจัดทำระบบควรเข้าร่วมเป็นคณะทำงานเพื่อ ให้มีส่วนร่วมในการจัดทำระบบที่สอดคล้องกับลักษณะการทำงาน เมื่อได้คณะทำงานเรียบร้อยแล้วก็เริ่มสำรวจภัยคุกคามและช่องโหว่ที่ก่อให้ เกิดความเสี่ยงต่อสารสนเทศในขอบเขตการจัดทำระบบขององค์กร ตัวแทนหน่วยงานที่เป็นคณะทำงานก็รับผิดชอบสำรวจภัยคุกคามและช่องโหว่ในหน่วยงานของตนเอง ผลการประเมินความเสี่ยงจะบอกถึงระดับความเสี่ยงจากภัยคุกคามและช่องโหว่ในระบบสารสนเทศ คณะทำงานและผู้เกี่ยวข้องต้องกำหนดมาตรการจัดการกับความเสี่ยงนั้นให้ชัดเจนและมีประสิทธิภาพเพียงพอ

2. การนำไปปฏิบัติ (Do: Implement and Operate the ISMS)

ขั้นตอนการปฏิบัติ (Do) เป็นการนำผลลัพธ์ของขั้นตอนวางแผน (Plan) มาปฏิบัติให้เกิดผลตามวัตถุประสงค์ เช่น มาตรการป้องกันการบุกรุกระบบ มาตรการสำรองข้อมูล เป็นต้น ซึ่งก่อนจะปฏิบัติได้อย่างถูกต้องนั้น จำเป็นต้องมีการฝึกอบรม ถ่ายทอดความรู้แนวทางปฏิบัติที่ถูกต้องให้รับทราบทั่วกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. การเฝ้าระวังและทบทวน (Check: Monitoring and Review the ISMS)

หลังจากปฏิบัติตามมาตรการที่กำหนดแล้ว เราจะรู้ได้อย่างไรว่ามาตรการที่ปฏิบัตินั้นได้ผลตามเป้าหมายที่ต้องการ คำตอบคือต้องมีการวัดผลของมาตรการที่ใช้ควบคุมดูแล แนวทางการวัดผลและความถี่ในการเฝ้าระวังต้องสอดคล้องกับความเสี่ยง ดังนั้นกระบวนการ ระบบงาน หรือทรัพย์สินสารสนเทศที่มีความเสี่ยงสูงควรได้รับการเฝ้าระวังและวัดผลการปฏิบัติงานที่เข้มงวดกว่า เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ระบบการตรวจวัดและเฝ้าระวังสามารถรายงานผลได้ทันเวลา

4. การรักษามาตรฐานและปรับปรุงให้ดีขึ้น (Act: Maintain and Improve the ISMS)

หลังจากที่ตรวจพบปัญหาหรือสิ่งผิดปกติในขั้นตอนการตรวจสอบ (Check : Monitoring and Review the ISMS) ผู้ที่เกี่ยวข้องทุกระดับจำเป็นต้องร่วมกันแก้ไขปัญหาที่เกิดขึ้นและป้องกันปัญหาที่อาจเกิดซ้ำในอนาคต รวมถึงหาแนวทางปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศให้ มีประสิทธิภาพยิ่งขึ้น กลไกสำคัญที่ช่วยให้ผลักดันให้การแก้ไขปัญหาและปรับปรุงดำเนินการได้อย่าง เป็นรูปธรรม คือการมีส่วนร่วมของผู้บริหารระดับสูง บ่อยครั้งที่พบว่าปัญหาเกิดจากการขาดความชัดเจนในนโยบายการบริหารจัดการ ซึ่งผู้บริหารจะต้องให้ความกระจ่างและตัดสินใจแก้ไขปัญหาเชิงนโยบายให้เป็นรูปธรรม เพื่อให้คณะทำงานยึดถือเป็นแนวปฏิบัติต่อไป [4]

2.2 องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ ใน ISO 27001:2013 (Security Goal)

ทรัพย์สิน (Asset) ที่มีความมั่นคงปลอดภัยนั้นต้องประกอบด้วยองค์ประกอบทั้งสามอย่างครบถ้วน ไม่ว่าทรัพย์สินนั้นจะเป็นสิ่งที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย หรือทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล เป็นต้น

ความมั่นคงปลอดภัยของสารสนเทศนั้นมีองค์ประกอบด้วยกัน 3 ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability)

1. **ความลับ (Confidentiality)**

การรักษาความลับให้กับข้อมูลเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ หลักการสำคัญของการรักษาความลับคือ ผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ภาคธุรกิจให้ความสำคัญกับการรักษาความลับทางธุรกิจ ประชาชนทั่วไปก็ต้องการปกป้องข้อมูลส่วนตัวตามสิทธิขั้นพื้นฐานเช่นเดียวกัน

ข่าวการละเมิดมาตรการป้องกันของระบบคอมพิวเตอร์เข้าไปเจาะระบบทั้งในประเทศและต่างประเทศ แสดงให้เห็นว่ามาตรการที่มีอยู่ยังมีจุดอ่อนที่ ผู้ไม่ประสงค์ดีที่มีความรู้บุกรุกผ่านช่องโหว่ดังกล่าว แรงจูงใจของการกระทำดังกล่าวมีหลายเหตุปัจจัย เช่น ทำเพื่อเงิน เพื่อสร้างชื่อเสียง การยอมรับในกลุ่ม และทำไปด้วยความคึกคะนอง ปฏิเสธไม่ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ว่าแฮกเกอร์ที่สามารถเจาะทะลุระบบรักษาความปลอดภัยของหน่วยงานสำคัญระดับประเทศ จะกลายเป็นฮีโร่ในสายตาของแฮกเกอร์มือใหม่ทั่วโลก

ระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพ ต้องมีมาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันให้แน่ใจก่อนว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้ กลไกพื้นฐานที่คุ้นเคยกันเป็นอย่างดี คือการใช้รหัสผ่าน (Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต

นอกจากมาตรการตรวจสอบสิทธิแล้วการกำหนดชั้นความลับเป็นระดับต่างๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้นในบางหน่วยงานกำหนดชั้นความลับของสารสนเทศออกเป็น 4 ระดับ ประกอบด้วย ระดับชั้นความลับสุดยอด (Top Secret) ระดับชั้นความลับ (Secret) ระดับชั้นข้อมูลสำหรับใช้ภายในองค์กร (Internal Use) และระดับชั้นสารธารณะ (Public) ชั้นความลับนี้จะต้องมีเกณฑ์พิจารณาที่ชัดเจนว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับที่กำหนด พร้อมทั้งกำหนดแนวทางการระบุชั้นความลับ การจัดเก็บ และการสื่อสารข้อมูลสารสนเทศในแต่ละชั้นความลับอย่างชัดเจน มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวด

2. ความถูกต้องสมบูรณ์ (Integrity)

การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้นๆ ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น คำตอบในเชิงหลักการคือระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใดๆ ต่อข้อมูลนั้น

ยิ่งเทคโนโลยีสารสนเทศพัฒนาก้าวหน้าไปมากเท่าไร มนุษย์ก็ยิ่งจำเป็นต้องพึงพาเทคโนโลยีมากขึ้นตามไปด้วย บัตรประชาชนอัจฉริยะเป็นตัวอย่างใกล้ตัวเราที่ชี้ให้เห็นว่าประชาชนทุกคนไม่ว่าจะยากดีมีจนอย่างไร ก็ต้องเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเลี่ยงไม่ได้ อย่างน้อยข้อมูลส่วนตัวของเราก็ถูกจัดเก็บในฐานข้อมูลของรัฐบาล ลองนึกดูว่าจะเกิดอะไรขึ้นหากชื่อของนาย ก. ถูกลบออกจากบัญชีทะเบียนราษฎร์ นั่นหมายถึง นาย ก. ไม่มีตัวตนและไม่สามารถใช้สิทธิของประชาชนในการรับบริการรัฐได้ จะเห็นได้ว่าข้อมูลนี้มีความสำคัญมากเพราะเป็นหลักฐานในการพิสูจน์ตัวตนของเรา หากมองในแง่ความมั่นคงปลอดภัยของสารสนเทศแล้ว ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ความพร้อมใช้งาน (Availability)

การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ

- การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)
- ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)

ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ อาจเกิดจากการกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหายก็เป็นได้ องค์กรที่ตระหนักถึงภัยคุกคามดังกล่าวอาจเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan) ไว้รองรับ หน่วยงานรัฐที่ให้บริการสาธารณะต่างใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน เช่นไฟฟ้า ประปา โทรศัพท์ เป็นต้น หากคอมพิวเตอร์ที่ควบคุมระบบเหล่านี้เกิดความเสียหายไม่สามารถให้บริการได้ ทำให้บริการต่างๆ หยุดชะงักย่อมส่งผลเสียต่อประชาชนในวงกว้าง นอกจากนี้หากไฟฟ้าดับเป็นเวลานาน ระบบต่างๆ จะเกิดความเสียหายอย่างมาก ตัวอย่างจริงที่เคยเกิดขึ้นในต่างประเทศ เมื่อหลายปีก่อนระบบคอมพิวเตอร์ของศูนย์กระจายสินค้าเกิดความเสียหาย ไม่สามารถจ่ายกระแสไฟฟ้าไปยังคอนเทนเนอร์ที่ติดตั้งระบบทำความเย็นเป็นเวลาหลายวัน ส่งผลให้สินค้าในตู้คอนเทนเนอร์ดังกล่าวเสียหายทั้งหมด นอกจากนี้ยังทำให้ลูกค้าขอยกเลิกสัญญาเนื่องจากไม่ไว้วางใจในการบริการ เกิดความสูญเสียมูลค่ามหาศาล

การปกป้องข้อมูล (Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับความเสี่ยง หลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความ เสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username และ password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเว็บไซต์องค์กร เป็นต้น [5]

2.3 ภัยคุกคาม และช่องโหว่ (Threat and Vulnerability)

ภัยคุกคาม (Threat) อาจเป็นมนุษย์ ภัยธรรมชาติ หรือปัจจัยอื่นๆ ที่มีแนวโน้มที่จะก่อให้เกิดความเสียหายได้ ทั้งที่เจตนาสร้างความเสียหายหรือไม่ก็ตาม การทำความเข้าใจและตระหนักถึงภัยคุกคามจะช่วยให้เข้าใจองค์ประกอบที่เกี่ยวข้องกันทั้งระบบได้เป็นอย่างดี หากจำแนกแหล่งกำเนิดของภัยคุกคาม อาจแบ่งได้ดังนี้

- มนุษย์ เช่น แฮกเกอร์ สายลับ ผู้ก่อการร้าย ผู้ไม่ประสงค์ดีที่โจมตีระบบสารสนเทศ ไวรัส โปรแกรมไม่ประสงค์ดีต่างๆ เป็นต้น
- ภัยธรรมชาติ เช่นน้ำท่วม,ฟ้าผ่า,พายุ,แผ่นดินไหว เป็นต้น
- ข้อผิดพลาดทางเทคนิค เช่น อุปกรณ์ชำรุด,เสื่อมสภาพ หรือทำงานผิดพลาด เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ช่องโหว่ (Vulnerability) เป็นองค์ประกอบที่สำคัญของการศึกษาเรื่องความมั่นคงปลอดภัยของสารสนเทศ ภัยคุกคามที่กล่าวมาข้างต้นจะใช้ประโยชน์จากช่องโหว่นี้เพื่อสร้างความเสียหาย ดังนั้นหากช่องโหว่มีจำนวนมาก โอกาสที่ภัยคุกคามจะสร้างความเสียหายจากช่องโหว่ดังกล่าวก็มากตามไปด้วย กล่าวได้ว่าหากไม่มีช่องโหว่หรือจุดอ่อน ภัยคุกคามก็ไม่สามารถทำอันตรายแก่ระบบสารสนเทศได้ [5]

2.4 การบริหารจัดการความเสี่ยง (Risk Management)

กระบวนการในการบริหารจัดการความเสี่ยง จะประกอบด้วย 2 ส่วนหลักๆ คือ

1. การประเมินความเสี่ยง (Risk Assessment)
2. การควบคุม / แก้ไขความเสี่ยง (Risk Treatment)

2.4.1 Risk Management vs. ISO 27001:2013

กระบวนการในการบริหารจัดการความเสี่ยงเป็น Requirement หนึ่งในการจัดทำระบบ ISMS (Information Security Management Systems) ตามมาตรฐาน ISO 27001:2013 และถือเป็นส่วนสำคัญที่มีผลอย่างมากต่อความสำเร็จและความมีประสิทธิภาพของระบบ ISMS โดยตัวมาตรฐาน ISO 27001:2013 นั้น เปิดกว้างและมิได้มีการระบุถึงวิธีการที่จะต้องใช้ในการจัดการความเสี่ยงแต่อย่างใด ซึ่งวิธีการหรือ Approach ในการบริหารจัดการความเสี่ยงของแต่ละองค์กรอาจมีความแตกต่างกันไปได้หลากหลายวิธีขึ้นกับลักษณะการดำเนินธุรกิจ,ขนาดขององค์กร,นโยบายของผู้บริหาร เป็นต้น

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศขององค์กร เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกขโมยซึ่งอาจทาให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง

การประเมินความเสี่ยง (Risk assessment) หมายถึง การกำหนดเหตุการณ์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้ กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การประเมินความเสี่ยงมีจุดประสงค์เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศหนึ่ง และมีระดับความเสี่ยงมากน้อยเพียงใด ทั้งนี้เพื่อจะได้เตรียมการป้องกันไว้ก่อนก่อนที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นจริงและทำให้องค์กรเกิดความเสียหาย

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้นี้ จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องกับเหตุการณ์ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แผนการลดความเสี่ยง (Risk treatment plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานเพื่อพิจารณาอนุมัติก่อนดำเนินการ

2.4.2 การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยง (Risk) ที่กล่าวถึงในที่นี้จะหมายถึง ความเสี่ยงรูปแบบต่างๆ ที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลสำคัญและระบบ อุปกรณ์ต่างๆ ที่สนับสนุนการทำงานให้กับข้อมูลสำคัญนี้อยู่ โดยขั้นตอนนี้จะเป็นขั้นของการประเมินระดับของความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่างๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงในขั้นตอนต่อไป

2.4.3 ระดับของความเสี่ยง (Risk Level)

โดยปกติระดับของความเสี่ยงจะพิจารณาจาก 2 ปัจจัย คือ

1. ความน่าจะเป็น (Probability) ในการที่จะเกิดภัยคุกคามใดๆ ขึ้น และก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สิน ขององค์กร ซึ่งโดยปกติจะคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคาม (Threat) จุดอ่อน (Vulnerability Assessment) ที่มีต่อข้อมูลและทรัพย์สินขององค์กร ร่วมกับการพิจารณาถึงวิธีการควบคุม แก้ไขความเสี่ยง ที่มีอยู่ในปัจจุบัน (Existing Control)

2. ความรุนแรง (Severity) ของความเสียหายที่อาจเกิดขึ้น ซึ่งโดยปกติจะคำนวณค่าโดยการพิจารณาจาก ระดับความสำคัญ ของข้อมูลหรือทรัพย์สินนั้นๆ ที่มีต่อองค์กร [6]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.5 มาตรการจัดการความมั่นคงปลอดภัยของสารสนเทศ ตาม Annex A ของ ISO 27001:2013

ตารางที่ 2.1 Annex A [6] [7]

A.5 Information security policies นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ		
A.5.1 Management direction for information security ทิศทางการบริหารสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ		
วัตถุประสงค์ เพื่อกำหนดทิศทางและให้การสนับสนุนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศตามข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง		
A.5.1.1	Policies for information security นโยบายสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการกำหนด อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารไปยังพนักงานและหน่วยงานภายนอกที่เกี่ยวข้อง
A.5.1.2	Review of the policies for information security การทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญกับองค์กร เพื่อให้มั่นใจว่ามีความเหมาะสม เพียงพอ และประสิทธิผลที่คงไว้อย่างต่อเนื่อง
A.6 Organization of information security โครงสร้างด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร		
A.6.1 Internal organization โครงสร้างภายในองค์กร		
วัตถุประสงค์ เพื่อจัดตั้งโครงร่างการบริหารจัดการในการริเริ่มและควบคุมการนำไปปฏิบัติและการดำเนินงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร		
A.6.1.1	Information security roles and responsibilities บทบาทและหน้าที่ความรับผิดชอบด้านความ	มาตรการควบคุม หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	มั่นคงปลอดภัยสำหรับสารสนเทศ	สารสนเทศทั้งหมด ต้องมีการกำหนดและมอบหมายงาน
A.6.1.2	Segregation of duties การแบ่งงานและหน้าที่ความรับผิดชอบ	มาตรการควบคุม งานและหน้าที่รับผิดชอบที่ขัดกันต้องแบ่งแยกเพื่อลดโอกาสในการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือโดยไม่ได้ตั้งใจ หรือการใช้ทรัพย์สินขององค์กรผิดวัตถุประสงค์
A.6.1.3	Contact with authorities การติดต่อหน่วยงานผู้มีอำนาจ	มาตรการควบคุม การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องอย่างเหมาะสมต้องถูกรักษาไว้
A.6.1.4	Contact with special interest groups การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ	มาตรการควบคุม การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Specialist Security Forums) และสมาคมวิชาชีพต้องถูกรักษาไว้
A.6.1.5	Information security in project management ความมั่นคงปลอดภัยสำหรับสารสนเทศในการบริการโครงการ	มาตรการควบคุม ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีกำหนดไว้ในการบริหารโครงการไม่ว่าจะเป็นโครงการประเภทใดก็ตาม
A.6.2 Mobile devices and teleworking อุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล		
วัตถุประสงค์ เพื่อให้มั่นใจถึงความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและการใช้งานอุปกรณ์พกพา		
A.6.2.1	Mobile device policy นโยบายสำหรับอุปกรณ์พกพำ	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำมาใช้เพื่อบริหารจัดการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ความเสี่ยงที่มาจากการใช้งานอุปกรณ์พกพา
A.6.2.2	Teleworking การปฏิบัติงานจากระยะไกล	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำไปปฏิบัติเพื่อป้องกันข้อมูลที่ได้รับการเข้าถึง การประมวลผล หรือการจัดเก็บจากสถานที่ที่มีการปฏิบัติงานจากระยะไกล
A.7 Human resource security ความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์		
A.7.1 Prior to employment ก่อนการจ้างงาน		
วัตถุประสงค์ เพื่อให้มั่นใจว่าพนักงาน (Employees) และผู้ที่องค์กรทำสัญญาจ้าง (Contractors) เข้าใจความรับผิดชอบของตน และเหมาะสมต่อบทบาทที่ได้รับการพิจารณา		
A.7.1.1	Screening การคัดกรอง	มาตรการควบคุม การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมดต้องดำเนินการ โดยให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง
A.7.1.2	Terms and conditions of employment ข้อตกลงและเงื่อนไขการจ้างงาน	มาตรการควบคุม ข้อตกลงและเงื่อนไขในสัญญาจ้างงานของพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบของผู้รับการว่าจ้าง และขององค์กรในด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.7.2 During employment ในระหว่างการจ้างงาน		
วัตถุประสงค์ เพื่อให้มั่นใจว่าพนักงานและผู้ที่องค์กรทำสัญญาจ้างตระหนักถึงและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของตน		
A.7.2.1	Management responsibilities หน้าที่ความรับผิดชอบของผู้บริหาร	มาตรการควบคุม ผู้บริหารต้องกำหนดให้พนักงานและผู้ทำสัญญาจ้างทั้งหมดปฏิบัติตามนโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่องค์กรจัดทำขึ้น
A.7.2.2	Information security awareness, education and training ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม พนักงานขององค์กรทุกคนและผู้ทำสัญญาจ้างที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมอย่างเหมาะสม และรับทราบนโยบายและขั้นตอนปฏิบัติงานขององค์กรที่ปรับปรุง ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ
A.7.2.3	Disciplinary process กระบวนการทางวินัย	มาตรการควบคุม ต้องมีกระบวนการทางวินัยอย่างเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษพนักงานที่ฝ่าฝืน ละเมิดความมั่นคงปลอดภัยสำหรับสารสนเทศ
A.7.3 Termination and change of employment การสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน		
วัตถุประสงค์ เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนแปลงหรือสิ้นสภาพการว่าจ้าง		
A.7.3.1	Termination or change of employment responsibilities	มาตรการควบคุม ความรับผิดชอบและหน้าที่ด้าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	การสิ้นสภาพหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการว่าจ้าง	ความมั่นคงปลอดภัยสำหรับสารสนเทศที่ยังคงไว้ภายหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการว่าจ้างงาน ต้องมีกำหนดไว้และสื่อสารให้พนักงานและผู้ทำสัญญาจ้าง และนำไปบังคับใช้
A.8 Asset management การบริหารจัดการทรัพย์สิน		
A.8.1 Responsibility for assets หน้าที่ความรับผิดชอบต่อทรัพย์สิน		
วัตถุประสงค์ เพื่อระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม		
A.8.1.1	Inventory of assets บัญชีทะเบียนทรัพย์สิน	มาตรการควบคุม ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูลต้องถูกระบุและบัญชีทะเบียนทรัพย์สินต้องจัดทำขึ้นและรักษาไว้
A.8.1.2	Ownership of assets ความเป็นเจ้าของทรัพย์สิน	มาตรการควบคุม ทรัพย์สินในบัญชีทะเบียนทรัพย์สินต้องมีการระบุความเป็นเจ้าของ
A.8.1.3	Acceptable use of assets การใช้งานทรัพย์สินอย่างเหมาะสม	มาตรการควบคุม กฎการใช้งานอย่างเหมาะสมของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกกำหนดอย่างเป็นลายลักษณ์อักษรและนำไปปฏิบัติ
A.8.1.4	Return of assets การคืนทรัพย์สิน	มาตรการควบคุม พนักงานและผู้ใช้งานจากหน่วยงานภายนอกทุกคน ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ถือครองไว้ เมื่อสิ้นสภาพการว่าจ้างงาน สิ้นสุดสัญญาหรือข้อตกลง
A.8.2 Information classification การจัดหมวดหมู่สารสนเทศ		
วัตถุประสงค์ เพื่อให้มั่นใจได้ว่าสารสนเทศได้รับระดับของการป้องกันอย่างเหมาะสมตามความสำคัญที่มีต่อองค์กร		
A.8.2.1	Classification of information การจัดหมวดหมู่ของสารสนเทศ	มาตรการควบคุม สารสนเทศต้องได้รับการแยกหมวดหมู่ตามคุณค่า (Value) ข้อกำหนดทางกฎหมาย ความสำคัญ (Criticality) และความอ่อนไหว (Sensitivity) ต่อการถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
A.8.2.2	Labeling of information การทำป้ายชี้บ่งสารสนเทศ	มาตรการควบคุม ชุดขั้นตอนปฏิบัติงานที่เหมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
A.8.2.3	Handling of assets การจัดการทรัพย์สิน	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการจัดการทรัพย์สิน ต้องจัดทำและนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
A.8.3 Media handling การจัดการสื่อบันทึกข้อมูล		
วัตถุประสงค์ เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลง การกำจัด หรือการทำลายข้อมูลที่จัดเก็บบนสื่อบันทึกโดยไม่ได้รับอนุญาต		
A.8.3.1	Management of removable media การบริหารจัดการสื่อบันทึกที่สำมารถ	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	เคลื่อนย้ายได้	บริหารจัดการสื่อบันทึกที่สามารถเคลื่อนย้ายได้ ต้องมีการนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
A.8.3.2	Disposal of media การกำจัดสื่อบันทึกข้อมูล	มาตรการควบคุม สื่อบันทึกข้อมูลต้องถูกกำจัดอย่างมั่นคงปลอดภัย เมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป ตามขั้นตอนปฏิบัติงานอย่างเป็นทางการ
A.8.3.3	Physical media transfer การขนย้ายสื่อบันทึก	มาตรการควบคุม สื่อบันทึกที่มีข้อมูลต้องได้รับการป้องกันจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือการทำให้เกิดความเสียหายระหว่างขนย้าย
A.9 Access control การควบคุมการเข้าถึง		
A.9.1 Business requirements of access control ข้อกำหนดทางธุรกิจสำหรับควบคุมการเข้าถึง		
วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลข้อมูล		
A.9.1.1	Access control policy นโยบายควบคุมการเข้าถึง	มาตรการควบคุม นโยบายควบคุมการเข้าถึงต้องจัดทำขึ้นเป็นลายลักษณ์อักษร และทบทวนตามข้อกำหนดทางธุรกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
A.9.1.2	Access to networks and network services การเข้าถึงเครือข่ายและบริการเครือข่าย	มาตรการควบคุม ผู้ใช้งานต้องจัดให้เข้าถึงเครือข่ายและบริการเครือข่ายตามที่ได้รับการอนุญาตให้ใช้งานตามที่กำหนดไว้เท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.9.2 User access management การบริหารจัดการการเข้าถึงของผู้ใช้งาน		
วัตถุประสงค์ เพื่อให้แน่ใจว่าผู้ที่ได้รับอนุญาตสามารถเข้าถึง และเพื่อป้องกันผู้ไม่ได้รับอนุญาตในการเข้าถึงระบบและบริการ		
A.9.2.1	User registration and de-registration การลงทะเบียน และการถอนทะเบียนผู้ใช้งาน	มาตรการควบคุม กระบวนการลงทะเบียนและถอนทะเบียนผู้ใช้งานอย่างเป็นทางการต้องนำไปปฏิบัติเพื่อทำให้เกิดการมอบสิทธิในการเข้าถึง
A.9.2.2	User access provisioning การให้การเข้าถึงของผู้ใช้งาน	มาตรการควบคุม กระบวนการให้การเข้าถึงของผู้ใช้งานอย่างเป็นทางการ ต้องนำไปปฏิบัติ เพื่อมอบ หรือถอนสิทธิในการเข้าถึงสำหรับทุกประเภทผู้ใช้งานของทุกระบบและทุกบริการ
A.9.2.3	Management of privileged access rights การบริหารจัดการสิทธิการเข้าถึงพิเศษ	มาตรการควบคุม การให้และใช้งานของสิทธิการเข้าถึงพิเศษต้องถูกจำกัดและควบคุม
A.9.2.4	Management of secret authentication information of users การบริหารจัดการข้อมูลลับที่ใช้พิสูจน์ตัวตนของผู้ใช้งาน	มาตรการควบคุม การให้ข้อมูลลับที่ใช้พิสูจน์ตัวตนต้องถูกควบคุมผ่านกระบวนการบริหารจัดการอย่างเป็นทางการ
A.9.2.5	Review of user access rights การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน	มาตรการควบคุม เจ้าของทรัพย์สินต้องทบทวนสิทธิในการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนด
A.9.2.6	Removal or adjustment of access rights การลบหรือปรับเปลี่ยนสิทธิการเข้าถึง	มาตรการควบคุม สิทธิของพนักงานและผู้ใช้งานจากหน่วยงานภายนอกทุกคน สำหรับเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกถอน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		เมื่อสิ้นสภาพการว่าจ้าง สิ้นสุดสัญญา หรือข้อตกลง หรือปรับปรุงเมื่อมีการเปลี่ยนแปลง
A.9.3 User responsibilities หน้าที่ความรับผิดชอบของผู้ใช้งาน		
วัตถุประสงค์ เพื่อทำให้ผู้ใช้งานมีความรับผิดชอบในการปกป้องข้อมูลที่ใช้พิสูจน์ตัวตน		
A.9.3.1	Use of secret authentication information การใช้ข้อมูลลับของการพิสูจน์ตัวตน	มาตรการควบคุม ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติขององค์กรในการใช้ข้อมูลลับที่ใช้ในการพิสูจน์ตัวตน
A.9.4 System and application access control การควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (Application)		
วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบและโปรแกรมประยุกต์ (Application) โดยผู้ไม่ได้รับอนุญาต		
A.9.4.1	Information access restriction การจำกัดการเข้าถึงสารสนเทศ	มาตรการควบคุม การเข้าถึงสารสนเทศและฟังก์ชันของระบบของโปรแกรมประยุกต์ (Application) ต้องถูกจำกัดตามนโยบายควบคุมการเข้าถึง
A.9.4.2	Secure log-on procedures ขั้นตอนการเข้าสู่ระบบอย่างมั่นคงปลอดภัย	มาตรการควบคุม กรณีที่กำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบและโปรแกรมประยุกต์ (Application) ต่างๆ ต้องได้รับการควบคุมโดยขั้นตอนการเข้าสู่ระบบอย่างมั่นคงปลอดภัย
A.9.4.3	Password management system ระบบบริหารจัดการรหัสผ่าน	มาตรการควบคุม ระบบบริหารจัดการรหัสผ่าน ต้องมีปฏิสัมพันธ์ (Interactive) และต้องมั่นใจได้ถึงรหัสผ่านที่มีคุณภาพ
A.9.4.4	Use of privileged utility programs การใช้งานโปรแกรมยูทิลิตี้พิเศษ	มาตรการควบคุม การใช้งานโปรแกรมยูทิลิตี้อาจจะสามารถข้ามมาตรการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ควบคุมของระบบและแอพพลิเคชั่นได้ จึงต้องถูกจำกัดและควบคุมอย่างเคร่งครัด
A.9.4.5	Access control to program source code การควบคุมการเข้าถึง ซอร์สโค้ดของโปรแกรม	มาตรการควบคุม การเข้าถึงซอร์สโค้ดของโปรแกรมต้องถูกจำกัด
A.10 Cryptography การเข้ารหัสข้อมูล		
A.10.1 Cryptography controls มาตรการควบคุมการเข้ารหัสข้อมูล		
วัตถุประสงค์ เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิผล เพื่อป้องกันความลับ (Confidentiality) การพิสูจน์ตัวตน (Authentication) และ/หรือความถูกต้องครบถ้วน (Integrity) ของสารสนเทศ		
A.10.1.1	Policy on the use of cryptographic controls นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูล	มาตรการควบคุม นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูลเพื่อปกป้องสารสนเทศ ต้องจัดทำขึ้นและนำไปปฏิบัติ
A.10.1.2	Key management การบริหารจัดการกุญแจ	มาตรการควบคุม นโยบายการใช้งาน การป้องกัน และอายุการใช้งานกุญแจเข้ารหัสข้อมูล (Cryptographic Keys) ต้องจัดทำขึ้น และนำไปปฏิบัติตลอดวงจรชีวิตของกุญแจ
A.11 Physical and environmental security ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม		
A.11.1 Secure areas บริเวณที่ต้องรักษาความมั่นคงปลอดภัย		
วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย การแทรกแซงต่อสารสนเทศและอุปกรณ์ประมวลผลข้อมูลขององค์กร		
A.11.1.1	Physical security perimeter ความมั่นคงปลอดภัยของแนวกั้นทางกายภาพ	มาตรการควบคุม แนวกั้นเขตความมั่นคงปลอดภัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ทางกายภาพ ต้องถูกกำหนดและนำไปใช้เพื่อปกป้องพื้นที่ดังกล่าว ที่มีสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ทั้งที่มีความอ่อนไหว (Sensitive) และที่มีความสำคัญ (Critical) อยู่ภายใน
A.11.1.2	Physical entry controls มาตรการควบคุมการเข้า-ออกพื้นที่	มาตรการควบคุม บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมทางเข้า-ออกอย่างเหมาะสม เพื่อให้มั่นใจว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นจึงอนุญาตให้เข้าถึงได้
A.11.1.3	Securing offices, rooms and facilities ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และอาคารสถานที่	มาตรการควบคุม ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอาคารสถานที่ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้
A.11.1.4	Protecting against external and environmental threats การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม	มาตรการควบคุม การป้องกันทางกายภาพจากภัยพิบัติทางธรรมชาติ การบุกรุกที่ไม่พึงประสงค์ หรืออุบัติเหตุ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้
A.11.1.5	Working in secure areas การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย	มาตรการควบคุม ขั้นตอนปฏิบัติงานในบริเวณที่ต้องรักษาความปลอดภัย ต้องได้รับการออกแบบและนำไปประยุกต์ใช้
A.11.1.6	Delivery and loading area พื้นที่จัดส่งและรับของ	มาตรการควบคุม ตำแหน่งที่เข้าถึงได้ เช่น พื้นที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		จัดส่งและรับของ และตำแหน่งอื่นๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่องค์กรได้ ต้องถูกควบคุม และถ้าเป็นไปได้ ให้แยกออกจากบริเวณที่มีอุปกรณ์ประมวลผลข้อมูลตั้งอยู่ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
A.11.2 Equipment อุปกรณ์		
วัตถุประสงค์ เพื่อป้องกันการสูญหาย ความเสียหาย การขโมยหรือทำให้เป็นอันตราย (Compromise) ต่อทรัพย์สิน และทำให้เกิดการหยุดชะงักในการดำเนินงานขององค์กร		
A.11.2.1	Equipment siting and protection การจัดวางและการป้องกันอุปกรณ์	มาตรการควบคุม อุปกรณ์ต้องได้รับการจัดวางและป้องกัน เพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายจากสภาพแวดล้อม และโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต
A.11.2.2	Supporting utilities ระบบสาธารณูปโภคสนับสนุน	มาตรการควบคุม อุปกรณ์ต้องได้รับการป้องกันจากความล้มเหลวของกระแสไฟฟ้า (Power Failure) และการหยุดชะงักอื่นๆ (disruption) ที่มีสำเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน
A.11.2.3	Cabling security ความมั่นคงปลอดภัยของการเดินสายไฟฟ้า สายสื่อสาร และสายสัญญาณ	มาตรการควบคุม สายไฟฟ้าและสายโทรคมนาคมที่ส่งข้อมูลหรือสนับสนุนบริการทางข้อมูล ต้องได้รับการปกป้องจากการขัดขวางการทำงาน (Interception) การแทรกแซงสัญญาณ (Interference) หรือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		การทำให้เสียหาย (Damage)
A.11.2.4	Equipment maintenance การบำรุงรักษาอุปกรณ์	มาตรการควบคุม อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มั่นใจถึงความพร้อมใช้งานและความถูกต้องในการทำงาน
A.11.2.5	Removal of assets การนำทรัพย์สินออก	มาตรการควบคุม อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ต้องไม่นำออกนอกสถานที่โดยไม่ได้รับอนุญาต
A.11.2.6	Security of equipment and assets off-premises ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่นอกสำนักงาน	มาตรการควบคุม มาตรการด้านความปลอดภัยต้องนำมาใช้กับทรัพย์สินที่นำออกไปใช้งานนอกสำนักงาน โดยพิจารณาถึงความเสี่ยงต่างๆ ที่มีต่อทรัพย์สินเมื่อนำไปปฏิบัติงานนอกสถานที่
A.11.2.7	Secure disposal or reuse of equipment การกำจัดอุปกรณ์หรือนำมาใช้ซ้ำอย่างมั่นคงปลอดภัย	มาตรการควบคุม อุปกรณ์ทั้งหมด ที่มีสื่อบันทึกข้อมูล ต้องได้รับการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ ได้ถูกลบทิ้ง หรือบันทึกทับอย่างมั่นคงปลอดภัย ก่อนนำไปทำลายหรือนำไปใช้ซ้ำ
A.11.2.8	Unattended user equipment อุปกรณ์ที่ไม่มีผู้ดูแล	มาตรการควบคุม ผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ที่ไม่มีผู้ดูแลได้รับการป้องกันอย่างเหมาะสม
A.11.2.9	Clear desk and clear screen policy นโยบายการเก็บโต๊ะทำงาน และลบหน้าจอให้ว่าง	มาตรการควบคุม นโยบายการเก็บโต๊ะทำงานสำหรับกระดาษเอกสารและสื่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		บันทึกข้อมูลที่เคลื่อนย้ายได้ และนโยบายการลบหน้าจอให้ว่าง สำหรับอุปกรณ์ประมวลผลข้อมูลต้องมีการนำไปปฏิบัติ
A.12.1 Operation procedures and responsibilities ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ		
วัตถุประสงค์ เพื่อให้มั่นใจว่าการปฏิบัติงานของอุปกรณ์ประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย		
A.12.1.1	Documented operating procedures ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร	มาตรการควบคุม ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษร และมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้
A.12.1.2	Change management การบริหารจัดการความเปลี่ยนแปลง	มาตรการควบคุม การเปลี่ยนแปลงขององค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลข้อมูล และระบบต่างๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศต้องได้รับการควบคุม
A.12.1.3	Capacity management การบริหารจัดการขีดความสามารถ	มาตรการควบคุม การใช้งานทรัพยากร ต้องได้รับการเฝ้าระวัง ปรับแต่ง คาดการณ์ความต้องการของขีดความสามารถในอนาคต เพื่อให้มั่นใจในประสิทธิภาพของระบบตามที่ต้องการ
A.12.1.4	Separation of development, testing and operational environments การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทางานจริงออกจากกัน	มาตรการควบคุม สภาพแวดล้อมของการพัฒนา การทดสอบ และการทางานจริงต้องถูกแบ่งแยกออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงโดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงสภาพแวดล้อมของการปฏิบัติงานจริง
A.12.2 Protection from malware การป้องกันโปรแกรมไม่พึงประสงค์		
วัตถุประสงค์ เพื่อให้มั่นใจว่าสารสนเทศและอุปกรณ์ประมวลผลข้อมูลได้รับการป้องกันจากโปรแกรมไม่พึงประสงค์		
A.12.2.1	Controls against malware มาตรการควบคุมโปรแกรมไม่พึงประสงค์	มาตรการควบคุม มาตรการตรวจจับ การป้องกัน และการกู้คืน เพื่อป้องกันจากโปรแกรมไม่พึงประสงค์ ต้องนำไปปฏิบัติร่วมกับการสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม
A.12.3 Backup การสำรองข้อมูล		
วัตถุประสงค์ เพื่อป้องกันการสูญหาย หรือสูญเสียข้อมูล		
A.12.3.1	Information backup การสำรองข้อมูล	มาตรการควบคุม การสำรองสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการปฏิบัติ และทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายสำรองข้อมูลที่กำหนดไว้
A.12.4 Logging and monitoring การบันทึกล็อก และการเฝ้าระวัง		
วัตถุประสงค์ เพื่อบันทึกเหตุการณ์และการสร้าง (generate) หลักฐาน		
A.12.4.1	Event logging การบันทึกล็อกของเหตุการณ์	มาตรการควบคุม ล็อกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น (Exception) ข้อผิดพลาด (Fault) และเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการจัดทำขึ้น จัดเก็บ และ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ทบทวนอย่างสม่ำเสมอ
A.12.4.2	Protection of log information การป้องกันข้อมูลล็อก	มาตรการควบคุม อุปกรณ์บันทึกล็อกและข้อมูลล็อก ต้องได้รับการป้องกันจากการเปลี่ยนแปลงเพื่อทำลาย (Tempering) และเข้าถึงโดยไม่ได้รับอนุญาต
A.12.4.3	Administrator and operator logs ล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ	มาตรการควบคุม กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ ต้องได้รับการบันทึกล็อก และข้อมูลล็อกต้องได้รับการป้องกันและทบทวนอย่างสม่ำเสมอ
A.12.4.4	Clock synchronization การประสานเวลาของนาฬิกา	มาตรการควบคุม นาฬิกาของระบบทั้งหมดที่เกี่ยวข้องกับอุปกรณ์ประมวลผลข้อมูลภายในองค์กร หรือโดเมนความมั่นคง (Security Domain) ต้องได้รับการประสานเวลาให้ตรงกับแหล่งเทียบเวลาอ้างอิงเดียวกัน
A.12.5 Control of operation software การควบคุมซอฟต์แวร์ปฏิบัติการ		
วัตถุประสงค์ เพื่อให้มั่นใจว่าระบบปฏิบัติการมีความถูกต้องครบถ้วน		
A.12.5.1	Installation of software on operational systems การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ	มาตรการควบคุม ขั้นตอนปฏิบัติงานต้องนำมาปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ
A.12.6 Technical vulnerability management การบริหารจัดการช่องโหว่ทางเทคนิค		
วัตถุประสงค์ เพื่อป้องกันการแสวงหาประโยชน์จากช่องโหว่ทางเทคนิค		
A.12.6.1	Management of technical vulnerabilities การบริหารจัดการช่องโหว่ทางเทคนิค	มาตรการควบคุม ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ต้องได้รับภายในเวลาที่ทันท่วงที การเปิดเผยช่องโหว่ดังกล่าวขององค์กรต้องถูกประเมินและระบุมาตรการที่เหมาะสมเพื่อจัดการความเสี่ยงที่เกี่ยวข้อง
A.12.6.2	Restrictions on software installation การจำกัดการติดตั้งซอฟต์แวร์	มาตรการควบคุม กฎบริหารงานของการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน ต้องจัดทำขึ้นและนำไปปฏิบัติ
A.12.7 Information systems audit consideration การพิจารณาสำหรับการตรวจสอบระบบสารสนเทศ		
วัตถุประสงค์ เพื่อลดผลกระทบจากกิจกรรมการตรวจประเมินระบบการดำเนินงาน		
A.12.7.1	Information systems audit controls มาตรการควบคุมของการตรวจสอบระบบสารสนเทศ	มาตรการควบคุม ข้อกำหนดและกิจกรรมของการตรวจตรวจสอบที่เกี่ยวข้องกับการทวนสอบระบบปฏิบัติการ ต้องมีการวางแผนอย่างระมัดระวัง และได้รับความเห็นชอบเพื่อลดการหยุดชะงักต่อกระบวนการทางธุรกิจให้น้อยที่สุด
A.13 Communication security ความมั่นคงปลอดภัยด้านการสื่อสาร		
A.13.1 Network security management การบริหารจัดการความปลอดภัยสำหรับเครือข่าย		
วัตถุประสงค์ เพื่อให้มั่นใจถึงการป้องกันสารสนเทศบนเครือข่ายและอุปกรณ์ประมวลผลที่สนับสนุนเครือข่าย		
A.13.1.1	Network controls มาตรการควบคุมของเครือข่าย	มาตรการควบคุม เครือข่ายต้องได้รับการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศบนระบบและโปรแกรมประยุกต์ (Application)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.13.1.2	Security of network services ความมั่นคงปลอดภัยของบริการเครือข่าย	มาตรการควบคุม กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของการบริการจัดการของบริการเครือข่ายทั้งหมด ต้องได้รับการระบุ และรวมอยู่ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าจะเป็นการให้บริการโดยหน่วยงานภายใน (In-house) หรือหน่วยงานภายนอก (Outsourced)
A.13.1.3	Segregation in networks การแบ่งแยกเครือข่าย	มาตรการควบคุม กลุ่มของบริการด้านสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศต่างๆ ต้องได้รับการแบ่งแยกบนเครือข่าย
A.13.2 Information transfer การถ่ายโอนข้อมูล		
วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศที่ถูกถ่ายโอนภายในองค์กร และที่ถ่ายโอนไปยังหน่วยงานภายนอกให้คงไว้		
A.13.2.1	Information transfer policies and procedures นโยบายและขั้นตอนปฏิบัติงานในการถ่ายโอนข้อมูล	มาตรการควบคุม นโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมต่างๆ อย่างเป็นทางการ ต้องมีไว้เพื่อป้องกันการถ่ายโอนสารสนเทศผ่านการใช้อุปกรณ์สื่อสารทุกประเภท
A.13.2.2	Agreements on information transfer ข้อตกลงในการถ่ายโอนข้อมูล	มาตรการควบคุม ข้อตกลงต้องมีกำหนดถึงการถ่ายโอนสารสนเทศทางธุรกิจอย่างมั่นคงปลอดภัยระหว่างองค์กรและหน่วยงานภายนอก
A.13.2.3	Electronic messaging การส่งข้อความอิเล็กทรอนิกส์	มาตรการควบคุม ข้อมูลที่มีการส่งผ่านทางการส่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ข้อความอิเล็กทรอนิกส์ ต้องได้รับการปกป้องอย่างเหมาะสม
A.13.2.4	Confidentiality or nondisclosure agreements ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ	มาตรการควบคุม ข้อกำหนดสำหรับการรักษาความลับ หรือการไม่เปิดเผยความลับที่สะท้อนให้เห็นถึงความจำเป็นขององค์กรในการปกป้องข้อมูล ต้องได้รับการระบุ ทบทวนอย่างสม่ำเสมอ และจัดทำเป็นลายลักษณ์อักษร
A.14 System acquisition, development and maintenance การจัดหา การพัฒนา และการบำรุงรักษาระบบ		
A.14.1 Security requirements of information systems ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ		
วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศเป็นส่วนที่ได้ผนวกรวมเข้าไปในระบบสารสนเทศตลอดวงจรชีวิต และยังรวมถึงข้อกำหนดของระบบสารสนเทศที่ได้ให้บริการผ่านเครือข่ายสาธารณะ		
A.14.1.1	Information security requirements analysis and specification การวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องต้องรวมไว้ในข้อกำหนดของระบบสารสนเทศใหม่ หรือการพัฒนาปรับปรุงระบบสารสนเทศเดิม
A.14.1.2	Securing application services on public networks การรักษาความมั่นคงปลอดภัยของบริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ	มาตรการควบคุม สารสนเทศที่อยู่ในการให้บริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ ต้องได้รับการปกป้องจากการฉ้อโกง การโต้แย้งสัญญา (Contract dispute) และการเปิดเผยและการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.14.1.3	Protecting application services transactions การป้องกันธุรกรรมของบริการโปรแกรมประยุกต์ (Application)	มาตรการควบคุม สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการโปรแกรมประยุกต์ (Application) ต้องได้รับการป้องกันจากการสื่อสัญญาณที่ไม่สมบูรณ์ (Incomplete Transmission) การจัดเส้นทางผิด (Mis-routing) การปรับแก้ข้อความโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การทาสำเนาหรือเล่นข้อความซ้ำ (Replay) โดยไม่ได้รับอนุญาต
A.14.2 Security in development and support process ความมั่นคงปลอดภัยในกระบวนการพัฒนาและกระบวนการสนับสนุน		
วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศได้ถูกออกแบบและนำไปปฏิบัติตลอดวงจรชีวิตของการพัฒนาระบบสารสนเทศ		
A.14.2.1	Secure development policy นโยบายสำหรับการพัฒนาอย่างมั่นคงปลอดภัย	มาตรการควบคุม กฎสำหรับการพัฒนาซอฟต์แวร์และระบบงาน ต้องจัดทำขึ้นและนำไปประยุกต์ใช้กับการพัฒนาต่างๆ ภายในองค์กร
A.14.2.2	System change control procedures ขั้นตอนปฏิบัติงานการควบคุมความเปลี่ยนแปลงของระบบ	มาตรการควบคุม ความเปลี่ยนแปลงของระบบภายในวงจรชีวิตของการพัฒนาต้องได้รับการควบคุมโดยใช้ขั้นตอนปฏิบัติงานควบคุมความเปลี่ยนแปลงอย่างเป็นทางการ
A.14.2.3	Technical review of applications after operating platform changes การทบทวนทางเทคนิคของโปรแกรมประยุกต์ (Application) ภายหลังการเปลี่ยนแปลงแพลตฟอร์มปฏิบัติการ	มาตรการควบคุม เมื่อแพลตฟอร์มปฏิบัติการ (Operating Platforms) ถูกเปลี่ยนแปลง โปรแกรมประยุกต์ที่มีความสำคัญทางธุรกิจ ต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ได้รับการทบทวน และทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน (Operation) และความมั่นคงปลอดภัยขององค์กร
A.14.2.4	Restrictions on changes to software packages การจำกัดการเปลี่ยนแปลงกับซอฟต์แวร์สำเร็จรูป	มาตรการควบคุม การปรับปรุงซอฟต์แวร์สำเร็จรูปต้องได้รับการห้ามกระทำ การจำกัดการเปลี่ยนแปลงทั้งที่จำเป็นและทั้งหมดต้องถูกควบคุมอย่างเคร่งครัด
A.14.2.5	Secure system engineering principles หลักการทางวิศวกรรมระบบความมั่นคงปลอดภัย	มาตรการควบคุม หลักการของวิศวกรรมระบบความมั่นคงปลอดภัย ต้องมีการจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร รักษาให้คงไว้ และนำไปใช้กับการประยุกต์ใช้ระบบสารสนเทศใดๆ ก็ตาม
A.14.2.6	Secure development environment สภาพแวดล้อมการพัฒนาที่มั่นคงปลอดภัย	มาตรการควบคุม องค์กรต้องจัดตั้งและป้องกันสภาพแวดล้อมการพัฒนาอย่างเหมาะสม สำหรับการพัฒนาและบูรณาการระบบ โดยให้ครอบคลุมตลอดทั้งวงจรชีวิตของการพัฒนาระบบ
A.14.2.7	Outsourced development การพัฒนาโดยหน่วยงานภายนอก	มาตรการควบคุม องค์กรต้องกำกับดูแลและเฝ้าติดตามกิจกรรมการพัฒนาระบบที่ดำเนินการโดยหน่วยงานภายนอก
A.14.2.8	System security testing การทดสอบความมั่นคงปลอดภัยของระบบ	มาตรการควบคุม การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย (Security

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		Functionality) ต้องดำเนินการในระหว่างการพัฒนา
A.14.2.9	System acceptance testing การทดสอบตรวจรับระบบ	มาตรการควบคุม โปรแกรมการทดสอบตรวจรับและเกณฑ์ที่เกี่ยวข้อง ต้องจัดทาขึ้นสำหรับระบบสารสนเทศใหม่ ระบบที่ยกระดับขึ้น (Upgrade) และเวอร์ชันใหม่ของระบบ
A.14.3 Test data ข้อมูลทดสอบ		
วัตถุประสงค์ เพื่อให้มั่นใจว่าข้อมูลที่ใช้ในการทดสอบได้รับการปกป้อง		
A.14.3.1	Protection of test data การปกป้องข้อมูลทดสอบ	มาตรการควบคุม ข้อมูลทดสอบต้องถูกคัดเลือกอย่างระมัดระวัง และได้รับการปกป้องและควบคุม
A.15 Supplier relationships ความสัมพันธ์กับผู้ขาย		
A.15.1 Information security in supplier relationships ความมั่นคงปลอดภัยสำหรับสารสนเทศในความสัมพันธ์กับผู้ขาย		
วัตถุประสงค์ เพื่อให้มั่นใจว่าทรัพย์สินขององค์กรที่สำมารถเข้าถึงได้โดยหน่วยงานภายนอกได้รับการป้องกัน		
A.15.1.1	Information security policy for supplier relationships นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศสำหรับความสัมพันธ์กับผู้ขาย	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศเพื่อจัดการความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินองค์กรโดยหน่วยงานภายนอก ต้องได้รับการตกลงร่วมกันกับหน่วยงานภายนอก และจัดทำเป็นลายลักษณ์อักษร
A.15.1.2	Addressing security within supplier agreements การระบุข้อกำหนดในข้อตกลงกับผู้ขาย	มาตรการควบคุม ข้อกำหนดทั้งหมดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสำหรับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		สารสนเทศ ต้องจัดทำขึ้น และตกลงร่วมกันกับผู้ขายแต่ละรายที่อาจทำการเข้าถึง ประมวลผล จัดเก็บ สื่อสารกับสารสนเทศขององค์กร หรือให้บริการส่วนประกอบของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure Components) สำหรับสารสนเทศขององค์กร
A.15.1.3	Information and communication technology supply chain ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร	มาตรการควบคุม ข้อตกลงกับผู้ขาย ต้องรวมถึงข้อกำหนดที่ระบุถึงความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องกับสารสนเทศและบริการเทคโนโลยีการสื่อสารที่ก่อให้เกิดห่วงโซ่อุปทาน (Supply Chain)
A.15.2 Supplier service delivery management การบริหารจัดการการส่งมอบบริการของผู้ขาย		
วัตถุประสงค์ เพื่อรักษาระดับของความมั่นคงปลอดภัยสำหรับสารสนเทศ และระดับของการส่งมอบบริการ ที่เห็นชอบร่วมกันให้คงไว้ตามข้อตกลงกับผู้ขาย		
A.15.2.1	Monitoring and review of supplier services การติดตามและทบทวนบริการของผู้ขาย	มาตรการควบคุม องค์กรต้องติดตาม ทบทวน และตรวจประเมินการส่งมอบบริการของผู้ขายอย่างสม่ำเสมอ
A.15.2.2	Managing changes to supplier services การบริหารจัดการความเปลี่ยนแปลงบริการของผู้ขาย	มาตรการควบคุม การเปลี่ยนแปลงการให้บริการของผู้ขาย รวมถึงการรักษาให้คงไว้ และการปรับปรุงนโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่มีอยู่ ต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		ได้รับการบริหารจัดการ โดยพิจารณาถึงความสำคัญของสารสนเทศ ระบบ และกระบวนการทางธุรกิจที่เกี่ยวข้อง และต้องประเมินความเสี่ยงซ้ำ
A.16 Information security incident management การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ		
A.16.1 Management of information security incident and improvements การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและการปรับปรุงพัฒนา		
วัตถุประสงค์ เพื่อมั่นใจถึงวิธีการที่สม่ำเสมอและมีประสิทธิภาพในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ รวมถึงการสื่อสารเกี่ยวกับจุดอ่อนและสถานการณ์ด้านความมั่นคงปลอดภัย		
A.16.1.1	Responsibilities and procedures หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน	มาตรการควบคุม หน้าที่ความรับผิดชอบของผู้บริหารและขั้นตอนปฏิบัติงานต้องจัดทำขึ้นเพื่อให้มั่นใจถึงการตอบสนองได้อย่างรวดเร็ว (Quick) มีประสิทธิผล (Effective) และเป็นระเบียบแบบแผน (Orderly) ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
A.16.1.2	Reporting information security events การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม สถานการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกรายงานผ่านช่องทางการบริหารจัดการที่เหมาะสมอย่างรวดเร็วเท่าที่ทำได้
A.16.1.3	Reporting information security weaknesses การรายงานจุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม พนักงานและผู้ทำสัญญาจ้างที่ใช้งานระบบและบริการสารสนเทศขององค์กร ต้องทำการจดบันทึกและรายงานข้อสังเกตหรือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		จุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่น่าสงสัยใดๆ ในระบบหรือบริการต่างๆ
A.16.1.4	Assessment of and decision on information security events การประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม สถานการณ์ (Events) ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกประเมินและถูกตัดสินใจ ถ้าสถานการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ (Incidents) ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
A.16.1.5	Response to information security incidents การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม เหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการตอบสนองตามขั้นตอนปฏิบัติงานที่จัดทำเป็นลายลักษณ์อักษร
A.16.1.6	Learning from information security incidents การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ความรู้ที่ได้รับจากการวิเคราะห์และการแก้ปัญหาเหตุการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกนำไปใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต
A.16.1.7	Collection of evidence การเก็บรวบรวมหลักฐาน	มาตรการควบคุม องค์กรต้องกำหนดขั้นตอนปฏิบัติงานและนำมาใช้ในการระบุ (Identification), การเก็บรวบรวม (Collection) การจัดหา (Acquisition) การเก็บรักษา (Preservation) สารสนเทศที่สามารถนำมาเป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		หลักฐาน
A.17 Information security aspect of business continuity management ความมั่นคงปลอดภัยสำหรับสารสนเทศในแง่มุมของการบริหารจัดการความต่อเนื่องทางธุรกิจ		
A.17.1 Information security continuity ความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ		
วัตถุประสงค์ ความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกฝังลงไปในระบบบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร		
A.17.1.1	Planning information security continuity การวางแผนความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม องค์กรต้องระบุข้อกำหนดของตน สำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรและความต่อเนื่องของการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศภายใต้สถานการณ์ที่ไม่พึงประสงค์ เช่น ในช่วงวิกฤติ หรือภัยพิบัติ
A.17.1.2	Implementing information security continuity การนำไปปฏิบัติด้านความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม องค์กรต้องจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร นำไปปฏิบัติและรักษากระบวนการ ขั้นตอนปฏิบัติงาน และมาตรการควบคุมเพื่อให้มั่นใจถึงระดับความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศที่ต้องการในระหว่างสถานการณ์ที่ไม่พึงประสงค์
A.17.1.3	Verify, review and evaluate information security continuity ทวนสอบ ทบทวน และประเมินความต่อเนื่องด้านความมั่นคง	มาตรการควบคุม องค์กรต้องทวนสอบมาตรการความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่จัดทำขึ้นและนำไปปฏิบัติตาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	ปลอดภัยสำหรับสารสนเทศ	รอบระยะเวลาที่กำหนด เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังคงใช้ได้สมเหตุสมผล และมีประสิทธิผลในระหว่างสถานการณ์ที่ไม่พึงประสงค์
A.17.2 Redundancies การสำรองซ้ำซ้อน		
วัตถุประสงค์ เพื่อให้มั่นใจว่าอุปกรณ์ประมวลผลข้อมูลมีความพร้อมใช้งาน		
A.17.2.1	Availability of information processing facilities ความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล	มาตรการควบคุม อุปกรณ์ประมวลผลข้อมูล ต้องมีการสำรองซ้ำซ้อนไว้อย่างเพียงพอ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน
A.18 Compliance การปฏิบัติตามข้อกำหนด		
A.18.1 Compliance with legal and contractual requirements การปฏิบัติตามข้อกำหนดด้านกฎหมายและสัญญา		
วัตถุประสงค์ เพื่อหลีกเลี่ยงการละเมิดกฎหมาย ระเบียบข้อบังคับ ข้อกำหนด หรือข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ และข้อกำหนดด้านความมั่นคงปลอดภัยใดๆ ก็ตาม		
A.18.1.1	Identification of applicable legislation and contractual requirements การระบุข้อกำหนดด้านกฎหมายและสัญญาที่เกี่ยวข้อง	มาตรการควบคุม กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องทั้งหมด และวิธีการขององค์กรเพื่อให้เป็นไปตามข้อกำหนดดังกล่าว ต้องถูกระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบสารสนเทศ และสำหรับองค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.18.1.2	Intellectual property rights สิทธิในทรัพย์สินทางปัญญา	มาตรการควบคุม ขั้นตอนปฏิบัติที่เหมาะสมต้องนำไปปฏิบัติ เพื่อให้มั่นใจว่าสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับสิทธิในทรัพย์สินทางปัญญา และการใช้ซอฟต์แวร์ที่มีกรรมสิทธิ์ (Proprietary Software)
A.18.1.3	Protection of records การป้องกันบันทึก	มาตรการควบคุม บันทึกต้องได้รับการป้องกันจากการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพรออกไปโดยไม่ได้รับอนุญาตตามที่กฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญา และข้อกำหนดทางธุรกิจที่ได้กำหนดไว้
A.18.1.4	Privacy and protection of personally identifiable information ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล	มาตรการควบคุม การรักษาความเป็นส่วนตัว และการปกป้องข้อมูลส่วนบุคคลต้องมั่นใจว่าเป็นไปตามที่ระบุไว้ในกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง ถ้าเหมาะสม
A.18.1.5	Regulation of cryptographic controls ข้อบังคับของมาตรการควบคุมของการเข้ารหัสข้อมูล	มาตรการควบคุม มาตรการควบคุมการเข้ารหัสต้องนำไปใช้เพื่อให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด
A.18.2 Information security reviews การทบทวนความมั่นคงปลอดภัยด้านสารสนเทศ		

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศมีการนำไปปฏิบัติและมีการดำเนินงานตามนโยบายและขั้นตอนปฏิบัติงานขององค์กร		
A.18.2.1	Independent review of information security การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นอิสระ	มาตรการควบคุม วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ และการนำไปปฏิบัติ เช่น วัตถุประสงค์ของมาตรการ (Control objectives) มาตรการควบคุม (Controls) นโยบาย กระบวนการ และขั้นตอนปฏิบัติงานสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนด หรือเมื่อมีความเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น
A.18.2.2	Compliance with security policies and standards การปฏิบัติตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย	มาตรการควบคุม ผู้จัดการต้องทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลข้อมูล และขั้นตอนปฏิบัติงานที่อยู่ภายใต้ความรับผิดชอบของตน กับนโยบายและมาตรฐานความมั่นคงปลอดภัย และข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ ที่เหมาะสม
A.18.2.3	Technical compliance review การทบทวนความสอดคล้องทางเทคนิค	มาตรการควบคุม ระบบสารสนเทศต้องได้รับการทบทวนความสอดคล้องอย่างสม่ำเสมอกับนโยบายและมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.6 TCP/IP Port number [8]

สำหรับโปรแกรมประยุกต์ (Application) ที่ใช้ TCP (Transmission Control Protocol) หรือ UDP (User Datagram Protocol) จะใช้หมายเลขพอร์ต

หมายเลขพอร์ต คือเลขฐาน 16 บิต ตั้งแต่ 0 ถึง 65535 หมายเลขพอร์ตแต่ละหมายเลขจะถูกกำหนดโดยเฉพาะจาก OS (Operating Systems)

ทาง Internet Assigned Numbers Authority (IANA) เป็นหน่วยงานกลางในการประสานการเลือกใช้พอร์ต ว่าพอร์ตหมายเลขใดควรเหมาะสำหรับ Service ใด เช่น เลือกใช้ TCP Port หมายเลข 23 กับ Service Telnet และเลือกใช้ UDP Port หมายเลข 69 สำหรับ Service Trivial File transfer Protocol (TFTP)

หมายเลข Port ถูกจัดแบ่งเป็น 2 ประเภทคือ well known Ports และ Registered Ports

Well Known Ports คือ พอร์ตที่ระบบส่วนใหญ่ กำหนดให้ใช้โดย Privileged User (ผู้ใช้ที่มีสิทธิพิเศษ) โดยพอร์ตเหล่านี้ ใช้สำหรับการติดต่อระหว่างเครื่องที่มีระบบเวลาที่ยาวนาน วัตถุประสงค์เพื่อให้ service แก่ผู้ใช้ (ที่ไม่รู้จักหรือคุ้นเคย) แปลกหน้า จึงจำเป็นต้องกำหนดพอร์ตติดต่อสำหรับ Service นั้นๆ Registered Ports จะเป็น Port หมายเลข 1024 ขึ้นไป

ตัวอย่างการใช้ Port

Transport layer segment ที่ประกอบไปด้วยหมายเลขพอร์ต ของเครื่องปลายทาง โดยที่เครื่องปลายทาง (Destination host) จะใช้ Port นี้ในการส่งข้อมูลให้กับ Application ได้ถูกต้อง หมายเลขพอร์ต จะอยู่ใน 32 bit แรกของ TCP และ UDP header โดยที่ 16 bit แรกเป็นหมายเลขพอร์ต ของเครื่องต้นทาง ขณะที่ 16 bit ต่อมาเป็นหมายเลขพอร์ตของ เครื่องปลายทาง Well know Ports เป็นพอร์ตที่ค่อนข้างมาตรฐาน ทำให้เครื่อง Remote Computer สามารถรู้ได้ว่าจะติดต่อกับทางพอร์ตหมายเลขอะไรสำหรับ Service นั้นๆ

กลุ่มของหมายเลขพอร์ตและ หมายเลข IP เราเรียกว่า Socket ที่ประกอบด้วย Socket หนึ่งตัว สำหรับต้นทาง และอีกตัว สำหรับปลายทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
วิธีการดำเนินงาน

3.1 ขั้นตอนการดำเนินงาน

หลังจากเลือกหัวข้อในการทำปัญหาพิเศษแล้ว ทางผู้จัดทำได้แบ่งขั้นตอนการดำเนินงานดังนี้

3.1.1 ศึกษาและค้นคว้าเกี่ยวกับ ISO 27001:2013

3.1.2 สำรวจนโยบายของทางภาควิชาวิทยาการคอมพิวเตอร์

3.1.3 สำรวจและจัดทำบัญชีทรัพย์สินของภาควิชาวิทยาการคอมพิวเตอร์

3.1.4 สัมภาษณ์ผู้บริหาร สรุปและนำเสนอให้ทางภาควิชาวิทยาการคอมพิวเตอร์

3.1.5 ศึกษาการเขียนโปรแกรม

3.1.6 จัดทำโปรแกรม

3.2 รายละเอียดของขั้นตอนการดำเนินงาน

3.2.1 ศึกษาค้นคว้าข้อมูลต่างๆเกี่ยวกับมาตรฐาน ISO 27001:2013 เช่น ความหมายของ ISO 27001:2013 หัวข้อต่างๆในมาตรฐาน และขั้นตอนการจัดทำ

3.2.2 สำรวจนโยบายในสาขาว่ามีนโยบายใดบ้างที่เป็นไปตามมาตรฐาน หรือยังไม่ได้จัดทำนโยบายใดบ้างเพื่อนำมาทำเป็น check list ต่อไป

3.2.3 สำรวจทรัพย์สินต่างๆภายในห้องปฏิบัติการของสาขาเพื่อรวบรวมข้อมูลมาจัดทำบัญชีทรัพย์สิน

3.2.4 สัมภาษณ์ผู้บริหารเกี่ยวกับนโยบายที่ต้องมีการดำเนินการก่อน สรุปและนำเสนอให้ทางภาควิชาวิทยาการคอมพิวเตอร์พิจารณา

3.2.5 ศึกษาการเขียนโปรแกรมเพื่อนสร้างโปรแกรมกำจำกัดจำนวนหน้าการใช้เครื่องพิมพ์เอกสารของนักศึกษา

3.2.6 สร้างโปรแกรมเพื่อให้ผู้ดูแลสามารถนำไปใช้ในการจำกัดจำนวนหน้าการใช้เครื่องพิมพ์เอกสารของนักศึกษา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 ตารางเปรียบเทียบนโยบายของสาขา

ตารางที่ 3.1 แสดงการเปรียบเทียบของนโยบายหัวข้อต่างๆของทางสาขา

Control	ธนาคารกรุงไทย	ม.กรุงเทพ	สาขาวิชา
A5. Information security policies	✓	✓	
A6. Organization of information	✓	✓	
A7. Human resource security	✓	✓	
A8. Asset Management	✓	✓	✓
A9. Access control	✓	✓	✓
A10. Cryptography	✓		
A11. Physical and environmental security	✓	✓	✓
A12. Operations security	✓	✓	
A13. Communications security	✓	✓	
A14. System acquisition, development and maintenance	✓	✓	
A15. Supplier relationships	✓	✓	
A16. Information security incident management	✓	✓	
A17. Information security aspects of business continuity management	✓	✓	
A18. Compliance	✓	✓	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4 ตารางแสดงนโยบาย

ตารางที่ 3.2 แสดงถึงนโยบายที่สามารถทำได้ทางด้าน Policy

Policy
A.8.1.3 การใช้งานทรัพย์สินที่เหมาะสม
A.8.1.4 การคืนทรัพย์สินขององค์กร
A.9.1.1 นโยบายการควบคุมการเข้าถึงระบบ
A.9.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน
A.9.2.6 การถอดถอนสิทธิในการเข้าถึง
A.9.4.1 การจำกัดการเข้าถึงสารสนเทศ
A.9.4.2 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย
A.11.1.1 การจัดทำบริเวณล้อมรอบ
A.11.1.2 การควบคุมการเข้า - ออก
A.11.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ
A.11.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม
A.11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย
A.11.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก
A.11.2.1 การจัดวางและการป้องกันอุปกรณ์
A.11.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน
A.11.2.4 การบำรุงรักษาอุปกรณ์
A.11.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน
A.11.2.7 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง
A.11.2.9 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย
A.13.1.1 มาตรการทางเครือข่าย
A.13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย
A.18.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย
A.18.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.3 แสดงถึงนโยบายที่สามารถทำได้ทางด้าน Physical

Physical
A.8.1.1 การจัดทำบัญชีทรัพย์สิน
A.8.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน
A.8.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ
A.8.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ
A.9.2.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
A.9.3.1 การใช้งานรหัสผ่าน
A.9.4.3 ระบบบริหารจัดการรหัสผ่าน
A.11.2.3 การเดินสายไฟ สายสื่อสารและสายเคเบิลอื่นๆ

3.5 ตารางแสดงบัญชีทรัพย์สิน

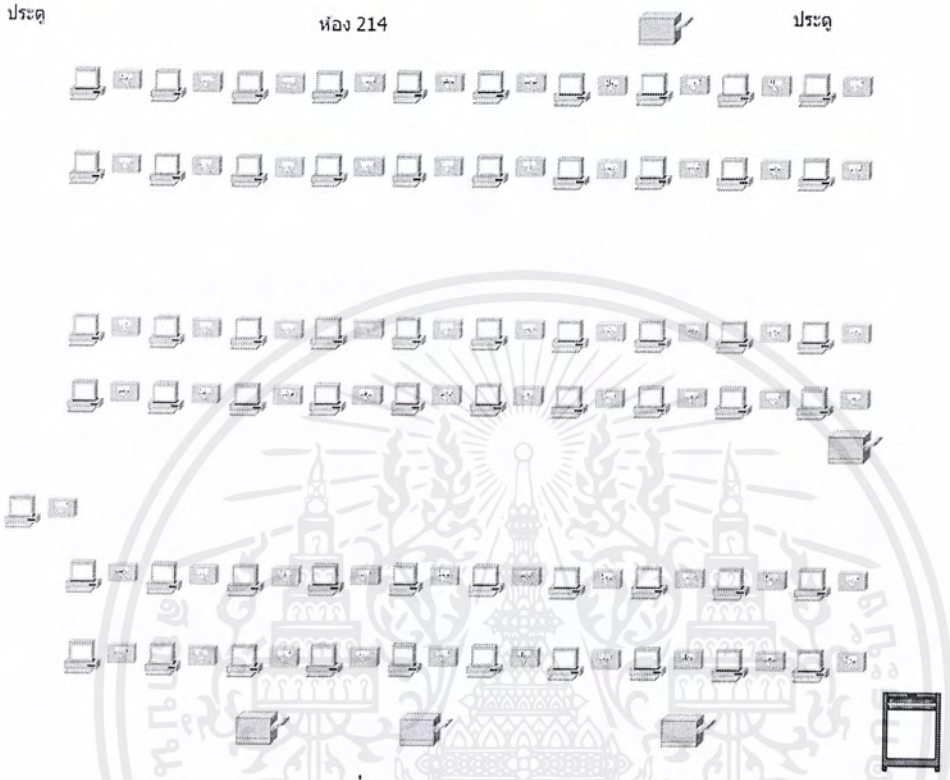
ตารางที่ 3.4 แสดงถึงอุปกรณ์ภายในห้องปฏิบัติ 214

ชนิดของอุปกรณ์	ยี่ห้อ	ชื่อรุ่น	จำนวน
computer PC	DELL	optiplex 3020	18
	HP	Pravilion HPE	42
	HP	compaq pro 6300	1
scanner	HP	Scanjet G4010	1
printer	HP	officejet 7000 Wide format	1
		laserjet p3015	1
		officejet pro 8100	1
		laserjet 4300	1
		laserjet 4250 dtn	1
LCD	Infocus		1
monitor	DELL	E2214hb	18
	Acer	T231H	1
	HP	w2072b	42
UPS	cleanline		62
switch	D-Link	DGS 1210-48	2
	SMC	EZ1024dt	2
	Bellcomms	cat 6E	3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.1 แผนผังห้องปฏิบัติการ 214

แผนผังนี้แสดงให้เห็นถึงตำแหน่งเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการ 214



รูปที่ 3. 1 แผนผังห้องปฏิบัติการ 214

ตารางที่ 3.5 แสดงถึงอุปกรณ์ภายในห้องปฏิบัติ 224

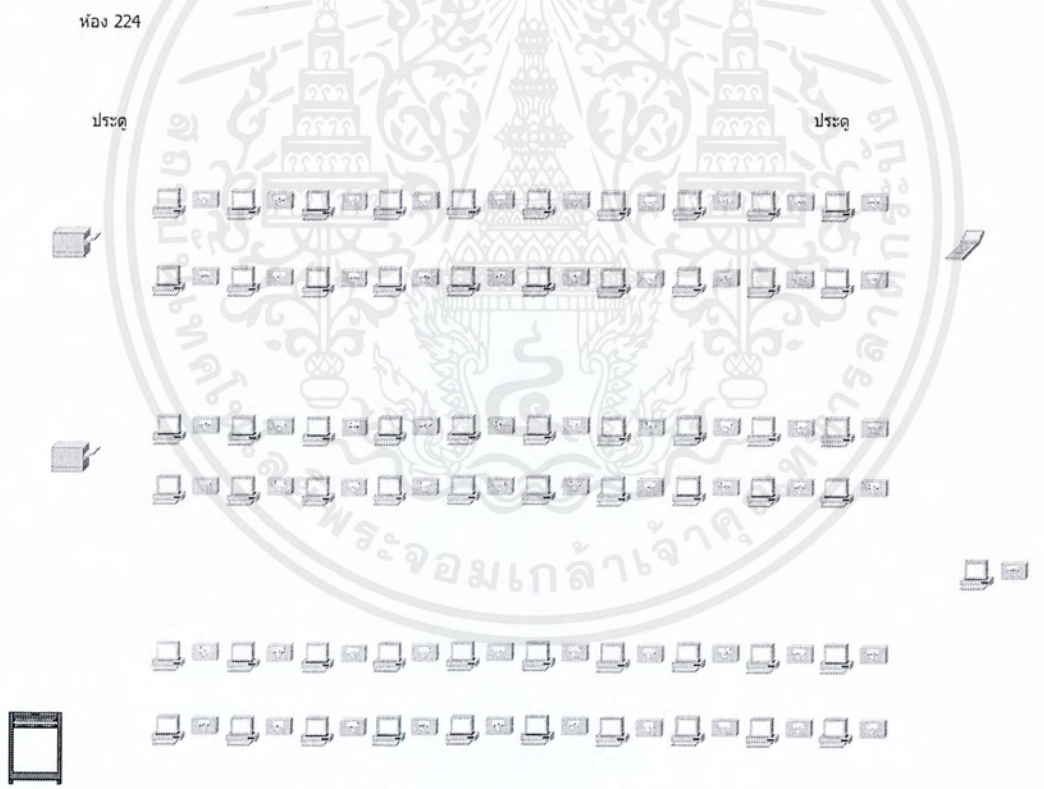
ชนิดของอุปกรณ์	ยี่ห้อ	ชื่อรุ่น	จำนวน
Computer PC	HP	compaq dc 5800	37
		compaq dc 7900	14
		Pravilion HPE	7
		compaq pro 6300	1
	Lenovo	thinkcenter	2
scanner	scanjet	5370c	1
printer	HP	laserjet 2430 dtn	1
LCD	Infocus		1
monitor	Philips	196v3l	1
	HP	x20led	1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชนิดของอุปกรณ์	ยี่ห้อ	ชื่อรุ่น	จำนวน
monitor	HP	L1908 wm	37
		w2072b	7
		L1910	14
	EliteDisplay	E231	1
UPS	cleanline		61
switch	D-Link	DGS 1210-48	2
	Bellcomms	cat 6E	3

3.5.2 แผนผังห้องปฏิบัติการ 224

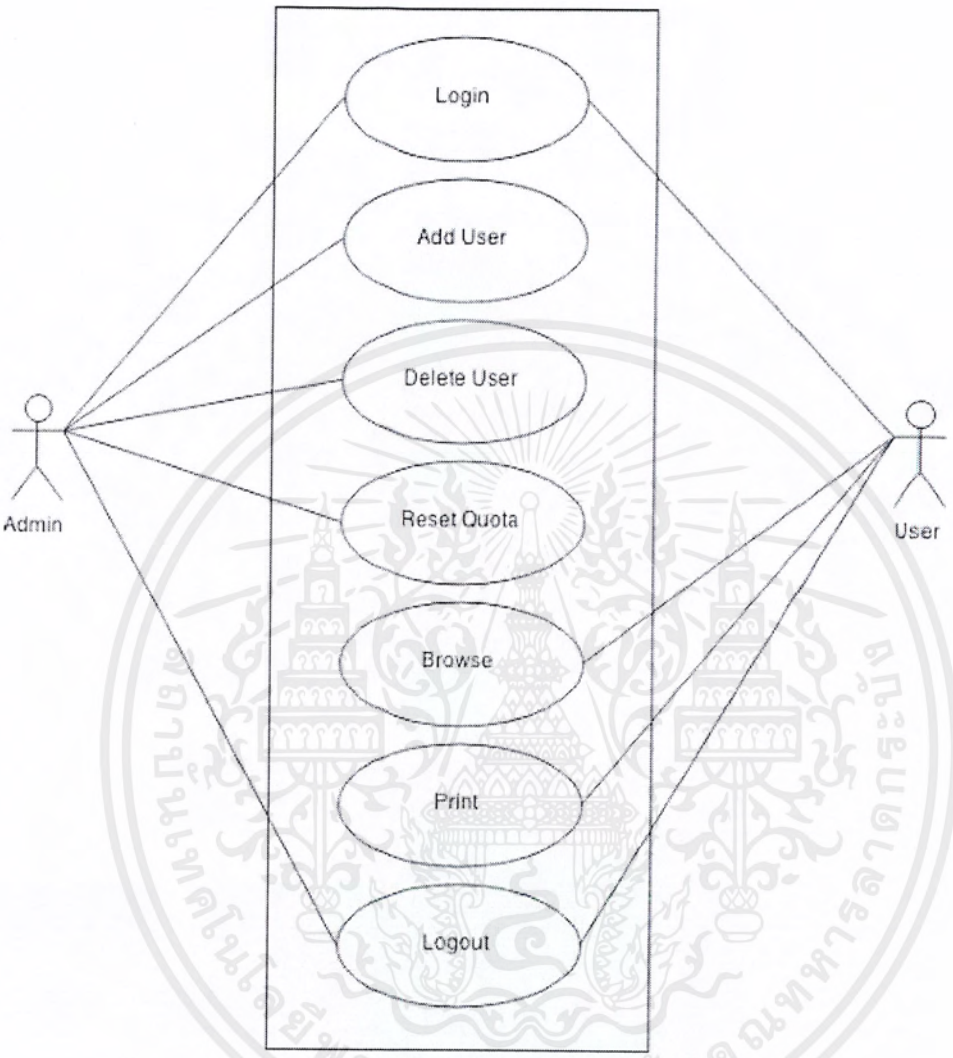
แผนผังนี้แสดงให้เห็นถึงตำแหน่งเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการ 224



รูปที่ 3. 2 แผนผังห้องปฏิบัติการ 224

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.6 Use case Diagram



รูปที่ 3. 3 Use case ของโปรแกรม

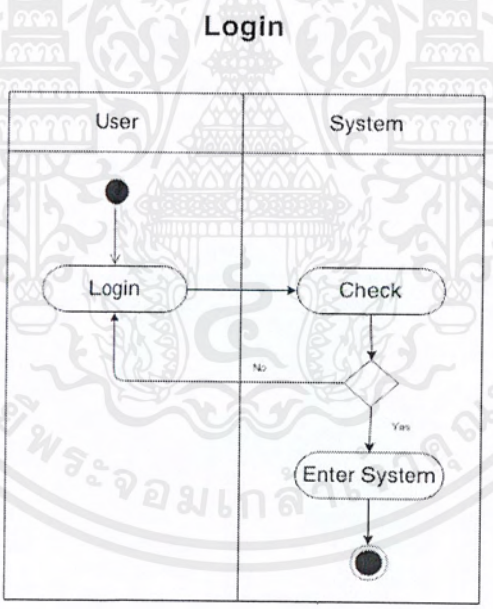
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.6 แสดงการทำงานของแต่ละ Use case

ชื่อ Use case	**คำอธิบาย**
Login	เข้าสู่ระบบ
Add User	เพิ่มข้อมูลของผู้ใช้
Delete User	ลบข้อมูลของผู้ใช้
Reset Quota	รีเซตจำนวนหน้า
Browse	เลือกไฟล์ที่ต้องการ
Print	สั่งให้พิมพ์ไฟล์ที่ต้องการ
Logout	ออกจากระบบ

3.7 Activity Diagram

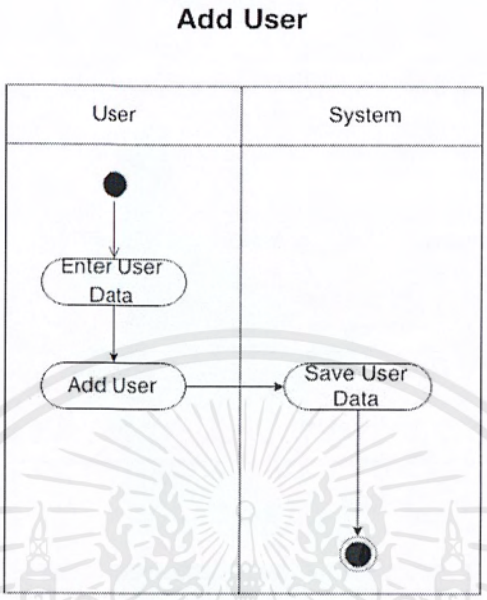
3.7.1 Login Activity Diagram



รูปที่ 3. 4 Login Activity Diagram

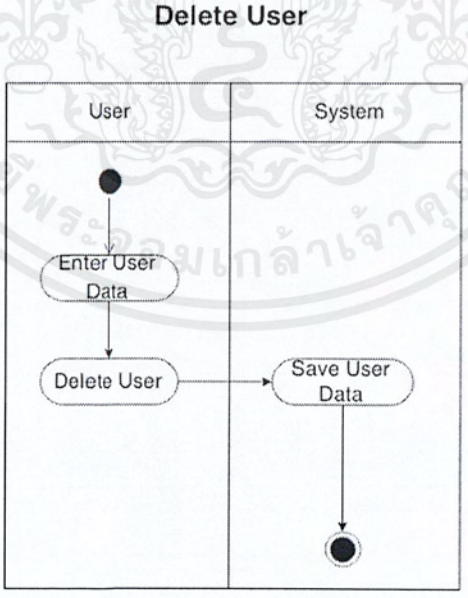
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.7.2 Add User Activity Diagram



รูปที่ 3. 5 Add User Activity Diagram

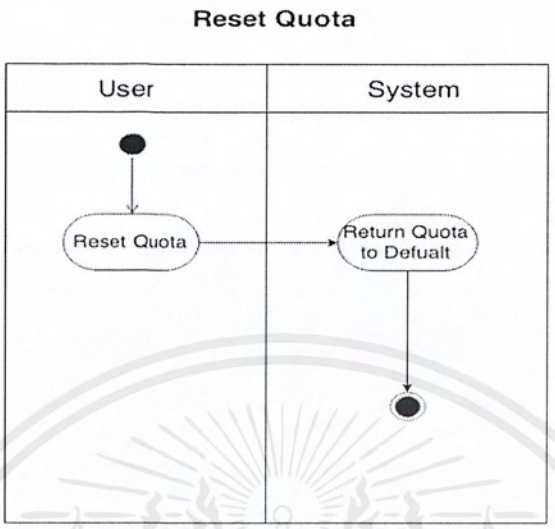
3.7.3 Delete User Activity Diagram



รูปที่ 3. 6 Delete User Activity Diagram

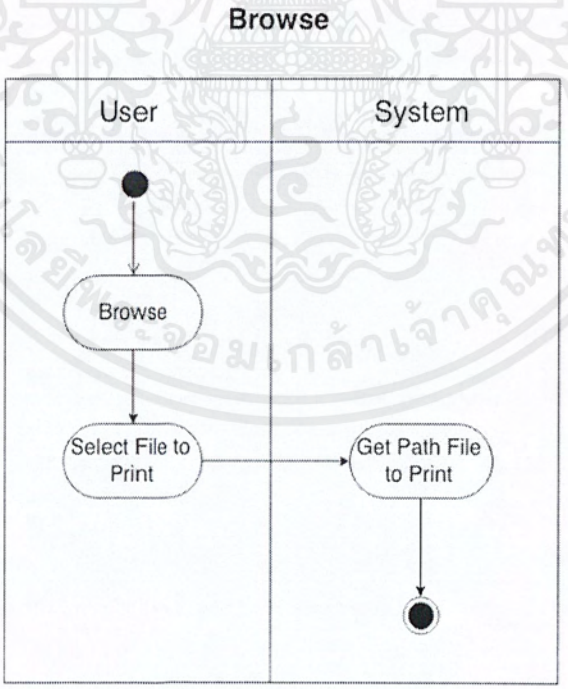
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.7.4 Reset User Activity Diagram



รูปที่ 3. 7 Reset User Activity Diagram

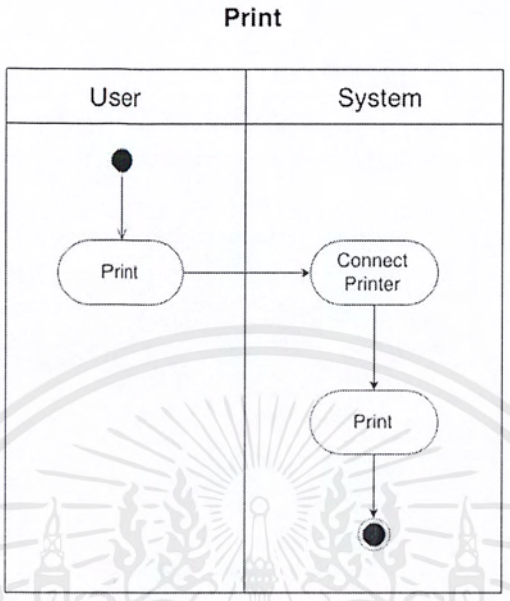
3.7.5 Browse Activity Diagram



รูปที่ 3. 8 Browse Activity Diagram

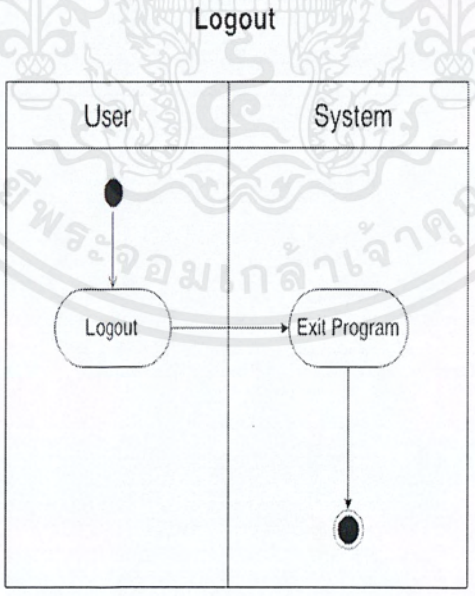
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.7.6 Print Activity Diagram



รูปที่ 3. 9 Print Activity Diagram

3.7.7 Logout Activity Diagram

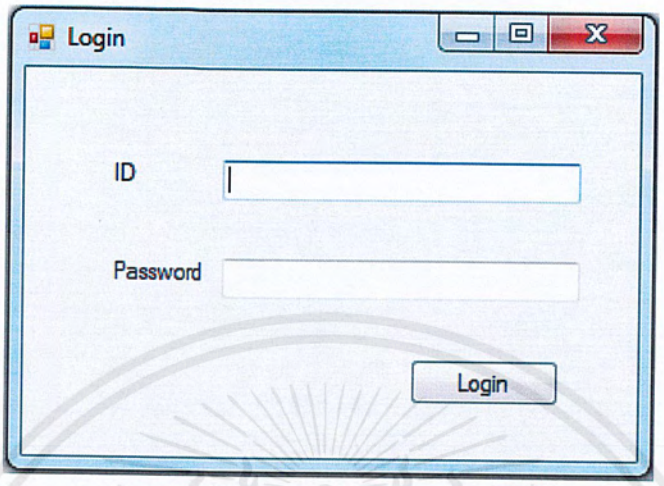


รูปที่ 3. 10 Logout Activity Diagram

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

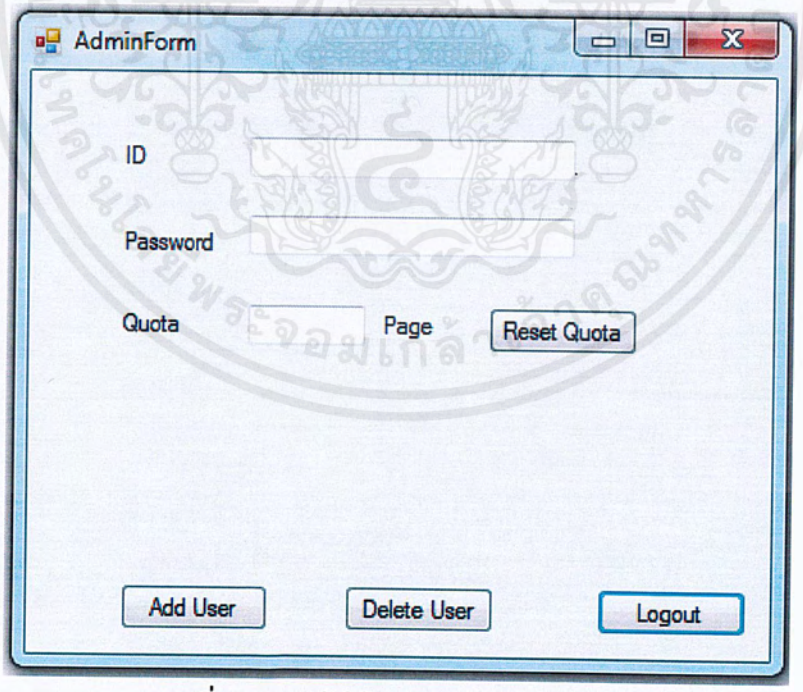
3.8 ตัวอย่างโปรแกรม

3.8.1 หน้า Login ของโปรแกรม



รูปที่ 3. 11 หน้า Login ของโปรแกรม

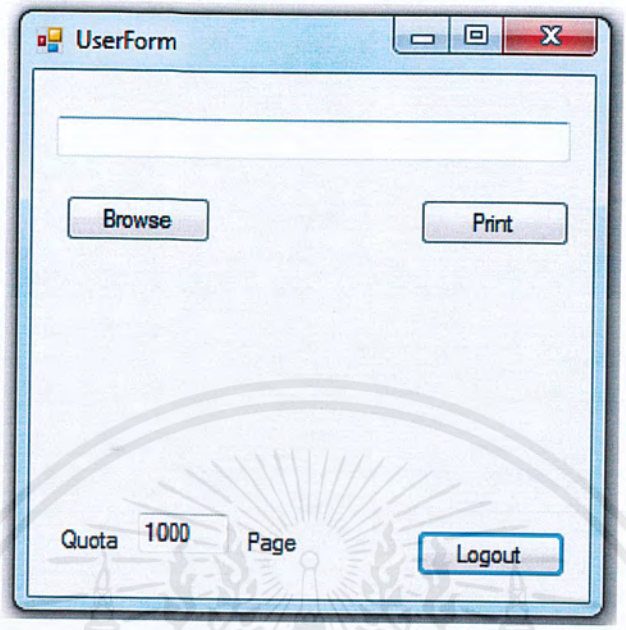
3.8.2 หน้าสำหรับ Admin



รูปที่ 3. 12 หน้าใช้งานสำหรับผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.8.3 หน้าสำหรับ User



รูปที่ 3. 13 หน้าใช้งานสำหรับนักศึกษา

3.9 การแบ่ง Phase การดำเนินงาน

ตารางที่ 3.7 แสดงจำนวนหัวข้อในแต่ละ phase

Phase 1			
ลำดับ	ข้อ	ชื่อหัวข้อ	รายละเอียด
1	A.5.1.1	นโยบายสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการกำหนด อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารไปยังพนักงาน และหน่วยงานภายนอกที่เกี่ยวข้อง
2	A.5.1.2	การทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Review of the policies for information security)	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการ
3	A.8.1.1	บัญชีทะเบียนทรัพย์สิน (Inventory of assets)	มาตรการควบคุม ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูลต้องถูกระบุ และบัญชีทะเบียนทรัพย์สินต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

			จัดทำขึ้นและรักษาไว้
4	A.8.1.2	ความเป็นเจ้าของทรัพย์สิน (Ownership of assets)	มาตรการควบคุม ทรัพย์สินในบัญชีทะเบียนทรัพย์สินต้องมีการระบุความเป็นเจ้าของ
5	A.8.1.3	การใช้งานทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)	มาตรการควบคุม กฎการใช้งานอย่างเหมาะสมของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกกำหนดอย่างเป็นลายลักษณ์อักษรและนำไปปฏิบัติ
6	A.8.1.4	การคืนทรัพย์สิน (Return of assets)	มาตรการควบคุม พนักงานและผู้ใช้งานจากหน่วยงาน ภายนอกทุกคน ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนถือครองไว้ เมื่อสิ้นสภาพการว่าจ้างงาน สิ้นสุดสัญญาหรือข้อตกลง
7	A.8.2.1	การจัดหมวดหมู่ของสารสนเทศ (Classification of information)	มาตรการควบคุม สารสนเทศต้องได้รับการแยกหมวดหมู่ตามคุณค่า (Value) ข้อกำหนดทางกฎหมาย ความสำคัญ (Criticality) และความอ่อนไหว (Sensitivity) ต่อการถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
8	A.9.1.1	นโยบายควบคุมการเข้าถึง (Access control policy)	มาตรการควบคุม นโยบายควบคุมการเข้าถึงต้องจัดทำขึ้นเป็นลายลักษณ์อักษร และทบทวนตามข้อกำหนดทาง ธุรกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
9	A.9.2.1	การลงทะเบียน และการถอนทะเบียนผู้ใช้งาน (User registration and de-registration)	มาตรการควบคุม กระบวนการลงทะเบียนและถอนทะเบียนผู้ใช้งานอย่างเป็นทางการต้องนำไปปฏิบัติเพื่อทำให้เกิดการมอบสิทธิในการเข้าถึง
10	A.9.2.4	การบริหารจัดการข้อมูลลับที่ใช้พิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	มาตรการควบคุม การให้ข้อมูลลับที่ใช้พิสูจน์ตัวตน ต้องถูกควบคุมผ่านกระบวนการบริหารจัดการอย่างเป็นทางการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

11	A.9.2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	มาตรการควบคุม เจ้าของทรัพย์สินต้องทบทวนสิทธิในการเข้าถึงของผู้ใช้งานตามรอบ ระยะเวลาที่กำหนด
12	A.9.2.6	การลบหรือปรับเปลี่ยนสิทธิการเข้าถึง (Removal or adjustment of access rights)	มาตรการควบคุม สิทธิของพนักงานและผู้ใช้งานจากหน่วยงานภายนอกทุกคนสำหรับเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกถอนเมื่อสิ้นสภาพการว่าจ้าง สิ้นสุดสัญญา หรือข้อตกลง หรือปรับปรุงเมื่อมีการเปลี่ยนแปลง
13	A.9.3.1	การใช้ข้อมูลลับของการพิสูจน์ตัวตน (Use of secret authentication information)	มาตรการควบคุม ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติขององค์กรในการใช้ข้อมูลลับที่ใช้ในการพิสูจน์ตัวตน
14	A.9.4.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	มาตรการควบคุม การเข้าถึงสารสนเทศและฟังก์ชันของระบบของโปรแกรมประยุกต์ (Application) ต้องถูกจำกัดตามนโยบายควบคุมการเข้าถึง
15	A.9.4.2	ขั้นตอนการเข้าสู่ระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	มาตรการควบคุม กรณีที่กำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบและโปรแกรมประยุกต์ (Application) ต่างๆ ต้องได้รับการควบคุมโดยขั้นตอนการเข้าสู่ระบบอย่างมั่นคง ปลอดภัย
16	A.9.4.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	มาตรการควบคุม ระบบบริหารจัดการรหัสผ่าน ต้องมีปฏิสัมพันธ์ (Interactive) และต้องมั่นใจได้ถึงรหัสผ่านที่มี คุณภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

17	A.11.1.1	ความมั่นคงปลอดภัยของแนวกั้นทางกายภาพ (Physical security perimeter)	มาตรการควบคุม แนวกั้นเขตความมั่นคงปลอดภัยทางกายภาพ ต้องถูกกำหนด และนำไปใช้เพื่อปกป้องพื้นที่ดังกล่าว ที่มีสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ทั้งที่มีความอ่อนไหว (Sensitive) และที่มีความสำคัญ (Critical) อยู่ภายใน
18	A.11.1.2	มาตรการควบคุมการเข้า-ออกพื้นที่ (Physical entry controls)	มาตรการควบคุม บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมทางเข้า-ออกอย่างเหมาะสม เพื่อให้มั่นใจว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น จึงอนุญาตให้เข้าถึงได้
19	A.11.1.3	ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และอาคารสถานที่ (Securing offices, rooms and facilities)	มาตรการควบคุม ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอาคารสถานที่ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้
20	A.11.1.4	การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats)	มาตรการควบคุม การป้องกันทางกายภาพจากภัยพิบัติทางธรรมชาติ การบุกรุกที่ไม่พึงประสงค์ หรืออุบัติเหตุ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้
21	A.11.1.5	การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	มาตรการควบคุม ขั้นตอนปฏิบัติงานในบริเวณที่ต้องรักษาความปลอดภัย ต้องได้รับการออกแบบและนำไปประยุกต์ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

22	A.11.1.6	พื้นที่จัดส่งและรับของ (Delivery and loading area)	มาตรการควบคุม ตำแหน่งที่เข้าถึงได้ เช่น พื้นที่จัดส่งและรับของ และตำแหน่งอื่นๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่องค์กรได้ ต้องถูกควบคุม และถ้าเป็นไปได้ให้แยกออกจากบริเวณที่มีอุปกรณ์ประมวลผลข้อมูลตั้งอยู่ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
23	A.11.2.1	การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)	มาตรการควบคุม อุปกรณ์ต้องได้รับการจัดวางและป้องกัน เพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายจากสภาพแวดล้อม และโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต
24	A.11.2.2	ระบบสาธารณูปโภคสนับสนุน (Supporting utilities)	มาตรการควบคุม อุปกรณ์ต้องได้รับการป้องกันจากความล้มเหลวของกระแสไฟฟ้า (Power Failure) และการหยุดชะงักอื่นๆ (disruption) ที่มีสำเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน
25	A.11.2.3	ความมั่นคงปลอดภัยของการเดินสายไฟฟ้า สายสื่อสาร และสายสัญญาณ (Cabling security)	มาตรการควบคุม สายไฟฟ้าและสายโทรคมนาคมที่ส่งข้อมูลหรือสนับสนุนบริการทางข้อมูล ต้องได้รับการปกป้องจากการขัดขวางการทำงาน (Interception) การแทรกแซงสัญญาณ (Interference) หรือการทำให้เสียหาย (Damage)
26	A.11.2.4	การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	มาตรการควบคุม อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มั่นใจถึงความพร้อมใช้งานและความถูกต้องในการทำงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

27	A.11.2.5	การนำทรัพย์สินออก (Removal of assets)	มาตรการควบคุม อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ต้องไม่นำออกนอกสถานที่โดยไม่ได้รับอนุญาต
28	A.11.2.7	การกำจัดอุปกรณ์หรือนำมาใช้ซ้ำอย่างมั่นคงปลอดภัย (Secure disposal or reuse of equipment)	มาตรการควบคุม อุปกรณ์ทั้งหมด ที่มีสื่อบันทึกข้อมูล ต้องได้รับการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ ได้ถูกลบทิ้ง หรือบันทึกทับอย่างมั่นคงปลอดภัย ก่อนนำไปทาลายหรือนำไปใช้ซ้ำ
29	A.11.2.9	นโยบายการเก็บโต๊ะทำงาน และลบหน้าจอให้ว่าง (Clear desk and clear screen policy)	มาตรการควบคุม นโยบายการเก็บโต๊ะทำงานสำหรับกระดาษเอกสารและสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ และนโยบายการลบหน้าจอให้ว่าง สำหรับอุปกรณ์ประมวลผลข้อมูล ต้องมีการนำไปปฏิบัติ
30	A.18.1.1	การระบุข้อกำหนดด้านกฎหมายและสัญญาที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)	มาตรการควบคุม กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องทั้งหมด และวิธีการขององค์กรเพื่อให้เป็นไปตามข้อกำหนดดังกล่าว ต้องถูกระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์ อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบสารสนเทศ และสำหรับองค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

31	A.18.1.2	สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)	มาตรการควบคุม ขั้นตอนปฏิบัติที่เหมาะสมต้องนำไปปฏิบัติ เพื่อให้มั่นใจว่าสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับสิทธิในทรัพย์สินทางปัญญา และการใช้ซอฟต์แวร์ที่มีกรรมสิทธิ์ (Proprietary Software)
Phase 2			
ลำดับ	ข้อ	ชื่อหัวข้อ	รายละเอียด
32	A.6.1.1	บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security roles and responsibilities)	มาตรการควบคุม หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศทั้งหมด ต้องมีการกำหนดและมอบหมายงาน
33	A.6.1.2	การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)	มาตรการควบคุม งานและหน้าที่รับผิดชอบที่ขัดกันต้องแบ่งแยกเพื่อลดโอกาสในการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือโดยไม่ได้ตั้งใจ หรือการใช้ทรัพย์สินขององค์กรผิดวัตถุประสงค์
34	A.6.1.3	การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)	มาตรการควบคุม การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องอย่างเหมาะสม ต้องถูกรักษาไว้
35	A.6.1.4	การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)	มาตรการควบคุม การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Specialist Security Forums) และสมาคมวิชาชีพต้องถูกรักษาไว้
36	A.6.1.5	ความมั่นคงปลอดภัยสำหรับสารสนเทศในการบริการโครงการ (Information security in project management)	มาตรการควบคุม ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีกำหนดไว้ในการบริหาร โครงการไม่ว่าจะเป็นโครงการประเภทใดก็ตาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

37	A.6.2.1	นโยบายสำหรับอุปกรณ์พกพา (Mobile device policy)	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำมาใช้เพื่อบริหารจัดการความเสี่ยงที่มาจากการใช้งานอุปกรณ์พกพา
38	A.6.2.2	การปฏิบัติงานจากระยะไกล (Teleworking)	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำไปปฏิบัติเพื่อป้องกันข้อมูลที่ได้รับการเข้าถึง การประมวลผล หรือการจัดเก็บจากสถานที่ที่มีการปฏิบัติงานจากระยะไกล
39	A.7.1.1	การคัดกรอง (Screening)	มาตรการควบคุม การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมดต้องดำเนินการ โดยให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง
40	A.7.1.2	ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)	มาตรการควบคุม ข้อตกลงและเงื่อนไขในสัญญาจ้างงานของพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบของผู้รับการว่าจ้าง และขององค์กรในด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
41	A.8.2.2	การทำป้ายชี้บ่งสารสนเทศ(Labelling of information)	มาตรการควบคุม ชุดขั้นตอนปฏิบัติงานที่เหมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
42	A.8.2.3	การจัดการทรัพย์สิน (Handling of assets)	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการจัดการทรัพย์สิน ต้องจัดทำและนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
43	A.8.3.1	การบริหารจัดการสื่อบันทึกที่สำมารถเคลื่อนย้ายได้ (Management of	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการสื่อบันทึกที่สามารถ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		removable media)	เคลื่อนย้ายได้ ต้องมีการนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้
44	A.8.3.2	การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	มาตรการควบคุม สื่อบันทึกข้อมูลต้องถูกกำจัดอย่างมั่นคง ปลอดภัย เมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป ตามขั้นตอนปฏิบัติงานอย่างเป็นทางการ
45	A.8.3.3	การขนย้ายสื่อบันทึก (Physical media transfer)	มาตรการควบคุม สื่อบันทึกที่มีข้อมูลต้องได้รับการป้องกันจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือการทำให้เกิดความเสียหายระหว่างขนย้าย
46	A.9.1.2	การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)	มาตรการควบคุม ผู้ใช้งานต้องจัดให้เข้าถึงเครือข่ายและบริการเครือข่ายตามที่ได้รับการอนุญาตให้ใช้งานตามที่กำหนดไว้เท่านั้น
47	A.9.2.2	การให้การเข้าถึงของผู้ใช้งาน (User access provisioning)	มาตรการควบคุม กระบวนการให้การเข้าถึงของผู้ใช้งานอย่างเป็นทางการ ต้องนำไปปฏิบัติ เพื่อมอบ หรือถอนสิทธิในการเข้าถึงสำหรับทุกประเภทผู้ใช้งานของทุกระบบและทุกบริการ
48	A.9.2.3	การบริหารจัดการสิทธิการเข้าถึงพิเศษ (Management of privileged access rights)	มาตรการควบคุม การให้และใช้งานของสิทธิการเข้าถึงพิเศษต้องถูกจำกัดและควบคุม
49	A.9.4.4	การใช้งานโปรแกรมยูทิลิตี้พิเศษ (Use of privileged utility programs)	มาตรการควบคุม การใช้งานโปรแกรมยูทิลิตี้อาจจะสามารถข้ามมาตรการควบคุมของระบบ และแอพพลิเคชั่นได้ จึงต้องถูกจำกัดและควบคุมอย่างเคร่งครัด
50	A.9.4.5	การควบคุมการเข้าถึงซอสโค้ดของโปรแกรม (Access control to	มาตรการควบคุม การเข้าถึงซอสโค้ดของโปรแกรมต้องถูกจำกัด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		program source code)	
51	A.11.2.6	ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่นอกสำนักงาน (Security of equipment and assets off-premises)	มาตรการควบคุม มาตรการด้านความปลอดภัย ต้องนำมาใช้กับทรัพย์สินที่นำออกไปใช้งานนอกสำนักงาน โดยพิจารณาถึงความเสี่ยงต่างๆ ที่มีต่อทรัพย์สินเมื่อนำไปปฏิบัติงานนอกสถานที่
52	A.11.2.8	อุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)	มาตรการควบคุม ผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ที่ไม่มีผู้ดูแลได้รับการป้องกันอย่างเหมาะสม
53	A.12.1.1	ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	มาตรการควบคุม ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษร และมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้
54	A.12.1.2	การบริหารจัดการความเปลี่ยนแปลง (Change management)	มาตรการควบคุม การเปลี่ยนแปลงขององค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลข้อมูล และระบบต่างๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการควบคุม
55	A.12.1.3	การบริหารจัดการขีดความสามารถ (Capacity management)	มาตรการควบคุม การใช้งานทรัพยากร ต้องได้รับการเฝ้าระวัง ปรับแต่ง คาดการณ์ความต้องการของขีดความสามารถในอนาคต เพื่อให้มั่นใจในประสิทธิภาพของระบบตามที่ต้องการ
56	A.12.2.1	มาตรการควบคุมโปรแกรมไม่พึงประสงค์ (Controls against malware)	มาตรการควบคุม มาตรการตรวจจับ การป้องกัน และการกู้คืน เพื่อป้องกันจากโปรแกรมไม่พึงประสงค์ ต้องนำไปปฏิบัติร่วมกับการสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม
57	A.12.3.1	การสำรองข้อมูล (Information backup)	มาตรการควบคุม การสำรองสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการปฏิบัติ และทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายสำรองข้อมูลที่กำหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

			ไว้
58	A.12.4.1	การบันทึกล็อกของเหตุการณ์ (Event logging)	มาตรการควบคุม ล็อกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น (Exception) ข้อผิดพลาด (Fault) และเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการจัดทำขึ้น จัดเก็บ และทบทวนอย่างสม่ำเสมอ
59	A.12.4.2	การป้องกันข้อมูลล็อก (Protection of log information)	มาตรการควบคุม อุปกรณ์บันทึกล็อกและข้อมูลล็อก ต้องได้รับการป้องกันจากการเปลี่ยนแปลงเพื่อทำลาย (Tempering) และเข้าถึงโดยไม่ได้รับอนุญาต
60	A.12.4.3	Administrator and operator logs ล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ	มาตรการควบคุม กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ ต้องได้รับการบันทึกล็อก และข้อมูลล็อกต้องได้รับการป้องกันและทบทวนอย่างสม่ำเสมอ
61	A.12.7.1	มาตรการควบคุมของการตรวจสอบระบบสารสนเทศ (Information systems audit controls)	มาตรการควบคุม ข้อกำหนดและกิจกรรมของการตรวจตรวจสอบที่เกี่ยวข้องกับการทวนสอบระบบปฏิบัติการ ต้องมีการวางแผนอย่างระมัดระวัง และได้รับความเห็นชอบเพื่อลดการหยุดชะงักต่อกระบวนการทางธุรกิจให้น้อยที่สุด
62	A.13.1.1	มาตรการควบคุมของเครือข่าย (Network controls)	มาตรการควบคุม เครือข่ายต้องได้รับการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศบนระบบและโปรแกรมประยุกต์ (Application)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

63	A.13.1.2	ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)	มาตรการควบคุม กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของการบริการจัดการของบริการเครือข่ายทั้งหมด ต้องได้รับการระบุ และรวมอยู่ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าจะเป็นการให้บริการโดยหน่วยงานภายใน (In-house) หรือหน่วยงานภายนอก (Outsourced)
64	A.13.1.3	การแบ่งแยกเครือข่าย (Segregation in networks)	มาตรการควบคุม กลุ่มของบริการด้านสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศต่างๆ ต้องได้รับการแบ่งแยกบนเครือข่าย
65	A.16.1.1	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Responsibilities and procedures)	มาตรการควบคุม หน้าที่ความรับผิดชอบของผู้บริหารและขั้นตอนปฏิบัติงาน ต้องจัดทำขึ้นเพื่อให้มั่นใจถึงการตอบสนองได้อย่างรวดเร็ว (Quick) มีประสิทธิผล (Effective) และเป็นระเบียบแบบแผน (Orderly) ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
66	A.16.1.2	การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Reporting information security events)	มาตรการควบคุม สถานการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกรายงานผ่านช่องทางการบริหารจัดการที่เหมาะสมอย่างรวดเร็วเท่าที่ทำได้
67	A.16.1.3	การรายงานจุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Reporting information security weaknesses)	ระบบและบริการสารสนเทศขององค์กร ต้องทำการจดบันทึก และรายงานข้อสังเกตหรือจุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่น่าสงสัยใดๆ ในระบบหรือบริการต่างๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

68	A.17.1.1	การวางแผนความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ (Planning information security continuity)	มาตรการควบคุม องค์กรต้องระบุข้อกำหนดของตน สำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร และความต่อเนื่องของการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศภายใต้สถานการณ์ที่ไม่พึงประสงค์ เช่น ในช่วงวิกฤติ หรือภัยพิบัติ
69	A.18.1.3	การป้องกันบันทึก (Protection of records)	มาตรการควบคุม บันทึกต้องได้รับการป้องกันจากการสูญหาย การทำลาย การปลอม แปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพรออกไปโดยไม่ได้รับอนุญาต ตามที่กฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญา และข้อกำหนดทางธุรกิจที่ได้กำหนดไว้
70	A.18.1.4	ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)	มาตรการควบคุม การรักษาความเป็นส่วนตัว และการปกป้องข้อมูลส่วนบุคคล ต้องมั่นใจว่าเป็นไปตามที่ระบุไว้ในกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง ถ้าเหมาะสม
71	A.18.1.5	ข้อบังคับของมาตรการควบคุมของการเข้ารหัสข้อมูล (Regulation of cryptographic controls)	มาตรการควบคุม มาตรการควบคุมการเข้ารหัส ต้องนำไปใช้เพื่อให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

72	A.18.2.1	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นอิสระ (Independent review of information security)	มาตรการควบคุม วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ และการนำไปปฏิบัติ เช่น วัตถุประสงค์ของมาตรการ (Control objectives) มาตรการควบคุม (Controls) นโยบาย กระบวนการ และขั้นตอนปฏิบัติงานสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนด หรือเมื่อมีความเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น
73	A.18.2.2	การปฏิบัติตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)	มาตรการควบคุม ผู้จัดการต้องทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลข้อมูล และขั้นตอนปฏิบัติงานที่อยู่ภายใต้ความรับผิดชอบของตน กับนโยบายและมาตรฐานความมั่นคงปลอดภัย และข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ ที่เหมาะสม
74	A.18.2.3	การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)	มาตรการควบคุมระบบสารสนเทศต้องได้รับการทบทวนความสอดคล้องอย่างสม่ำเสมอกับนโยบายและมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
Phase 3			
ลำดับ	**ข้อ**	**ชื่อหัวข้อ**	**รายละเอียด**
75	A.7.2.1	หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)	มาตรการควบคุม ผู้บริหารต้องกำหนดให้พนักงานและผู้ทำสัญญาจ้างทั้งหมดปฏิบัติตามนโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่องค์กรจัดทำขึ้น
76	A.7.2.2	ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม พนักงานขององค์กรทุกคน และผู้ทำสัญญาจ้างที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก การให้ความรู้ และ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		(Information security awareness, education and training)	การฝึกอบรมอย่างเหมาะสม และรับทราบนโยบายและขั้นตอนปฏิบัติงานขององค์กรที่ปรับปรุง ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ
77	A.7.2.3	กระบวนการทางวินัย (Disciplinary process)	มาตรการควบคุม ต้องมีกระบวนการทางวินัยอย่างเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษพนักงานที่ฝ่าฝืน ละเมิดความมั่นคงปลอดภัยสำหรับสารสนเทศ
78	A.7.3.1	การสิ้นสภาพหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการว่าจ้าง (Termination or change of employment responsibilities)	มาตรการควบคุม ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่ยังคงไว้ภายหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการว่าจ้างงาน ต้องมีกำหนดไว้และสื่อสารให้พนักงานและผู้ทำสัญญาจ้าง และนำไปบังคับใช้
79	A.10.1.1	นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)	มาตรการควบคุม นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูลเพื่อปกป้องสารสนเทศ ต้องจัดทำขึ้นและนำไปปฏิบัติ
80	A.10.1.2	การบริหารจัดการกุญแจ (Key management)	มาตรการควบคุม นโยบายการใช้งาน การป้องกัน และอายุการใช้งานกุญแจเข้ารหัสข้อมูล (Cryptographic Keys) ต้องจัดทำขึ้น และนำไปปฏิบัติตลอดวงจรชีวิตของกุญแจ
81	A.12.1.4	การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทางานจริงออกจากกัน (Separation of development, testing and operational environments)	มาตรการควบคุมสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง ต้องถูกแบ่งแยกออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาตหรือการเปลี่ยนแปลงสภาพแวดล้อมของการปฏิบัติงานจริง
82	A.12.4.4	Clock synchronization การประสานเวลาของนาฬิกา	มาตรการควบคุม นาฬิกาของระบบทั้งหมดที่เกี่ยวข้องกับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

			อุปกรณ์ประมวลผลข้อมูลภายในองค์กรหรือโดเมนความมั่นคง (Security Domain) ต้องได้รับการประสานเวลาให้ตรงกับแหล่งเทียบเวลาอ้างอิงเดียวกัน
83	A.12.5.1	การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Installation of software on operational systems)	มาตรการควบคุม ขั้นตอนปฏิบัติงานต้องนำมาปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ
84	A.12.6.1	การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	มาตรการควบคุม ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน ต้องได้รับภายในเวลาที่ทันท่วงที การเปิดเผยช่องโหว่ดังกล่าวขององค์กรต้องถูกประเมินและระบุมาตรการที่เหมาะสมเพื่อจัดการความเสี่ยงที่เกี่ยวข้อง
85	A.12.6.2	การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)	มาตรการควบคุม กฎบริหารงานของการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน ต้องจัดทำขึ้นและนำไปปฏิบัติ
86	A.13.2.1	นโยบายและขั้นตอนปฏิบัติงานในการถ่ายโอนข้อมูล (Information transfer policies and procedures)	มาตรการควบคุม นโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมต่างๆ อย่างเป็นทางการ ต้องมีไว้เพื่อป้องกันการถ่ายโอนสารสนเทศผ่านการใช้อุปกรณ์สื่อสารทุกประเภท
87	A.13.2.2	ข้อตกลงในการถ่ายโอนข้อมูล (Agreements on information transfer)	มาตรการควบคุม ข้อตกลงต้องมีกำหนดถึงการถ่ายโอนสารสนเทศทางธุรกิจอย่างมั่นคงปลอดภัยระหว่างองค์กรและหน่วยงานภายนอก
88	A.13.2.3	การส่งข้อความอิเล็กทรอนิกส์ (Electronic messaging)	มาตรการควบคุม ข้อมูลที่มีการส่งผ่านทางการส่งข้อความอิเล็กทรอนิกส์ ต้องได้รับการปกป้องอย่างเหมาะสม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

89	A.13.2.4	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or nondisclosure agreements)	มาตรการควบคุม ข้อกำหนดสำหรับการรักษาความลับ หรือการไม่เปิดเผยความลับที่สะท้อนให้เห็นถึงความจำเป็นขององค์กรในการปกป้องข้อมูล ต้องได้รับการระบุ ทบทวนอย่างสม่ำเสมอ และจัดทำเป็นลายลักษณ์อักษร
90	A.14.1.1	การวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security requirements analysis and specification)	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องต้องรวมไว้ในข้อกำหนดของระบบสารสนเทศใหม่ หรือการพัฒนาปรับปรุงระบบสารสนเทศเดิม
91	A.14.1.2	การรักษาความมั่นคงปลอดภัยของบริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ (Securing application services on public networks)	มาตรการควบคุม สารสนเทศที่อยู่ในการให้บริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ ต้องได้รับการปกป้องจากการฉ้อโกง การ โต้แย้งสัญญา (Contract dispute) และการเปิดเผยและการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
92	A.14.1.3	การป้องกันธุรกรรมของบริการโปรแกรมประยุกต์ (Application) (Protecting application services transactions)	มาตรการควบคุม สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการโปรแกรมประยุกต์ (Application) ต้องได้รับการป้องกันจากการสื่อสัญญาณที่ไม่สมบูรณ์ (Incomplete Transmission) การจัดเส้นทางผิด (Mis-routing) การปรับแก้ข้อความโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การทาสำเนาหรือ เล่นข้อความซ้ำ (Replay) โดยไม่ได้รับอนุญาต
93	A.14.2.1	นโยบายสำหรับการพัฒนาอย่างมั่นคงปลอดภัย (Secure (Secure development policy)	มาตรการควบคุม กฎสำหรับการพัฒนาซอฟต์แวร์และ ระบบงาน ต้องจัดทำขึ้นและนำไปประยุกต์ใช้กับการพัฒนาต่างๆ ภายในองค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

94	A.14.2.2	ขั้นตอนปฏิบัติงานการควบคุมความเปลี่ยนแปลงของระบบ (System change control procedures)	มาตรการควบคุม ความเปลี่ยนแปลงของระบบภายในวงจรชีวิตของการพัฒนา ต้องได้รับการควบคุมโดยใช้ขั้นตอนปฏิบัติงานควบคุมความเปลี่ยนแปลงอย่างเป็นทางการ
95	A.14.2.3	การทบทวนทางเทคนิคของโปรแกรมประยุกต์ (Application) ภายหลังการเปลี่ยนแปลงแพลตฟอร์มปฏิบัติการ (Technical review of applications after operating platform changes)	มาตรการควบคุม เมื่อแพลตฟอร์มปฏิบัติการ (Operating Platforms) ถูกเปลี่ยนแปลง โปรแกรมประยุกต์ที่มีความสำคัญทางธุรกิจ ต้องได้รับการทบทวนและทดสอบ เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน (Operation) และความมั่นคงปลอดภัยขององค์กร
96	A.14.2.4	การจำกัดการเปลี่ยนแปลงกับซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)	มาตรการควบคุม การปรับปรุงซอฟต์แวร์สำเร็จรูป ต้องได้รับการห้ามกระทำ การจำกัดการเปลี่ยนแปลงทั้งที่จำเป็นและทั้งหมดต้องถูกควบคุมอย่างเคร่งครัด
97	A.14.2.5	หลักการทางวิศวกรรมระบบความมั่นคงปลอดภัย (Secure system engineering principles)	มาตรการควบคุม หลักการของวิศวกรรมระบบความมั่นคงปลอดภัย ต้องมีการจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร รักษาให้คงไว้ และนำไปใช้กับการประยุกต์ใช้ระบบสารสนเทศใดๆ ก็ตาม
98	A.14.2.6	สภาพแวดล้อมการพัฒนาที่มั่นคงปลอดภัย (Secure development environment)	มาตรการควบคุม องค์กรต้องจัดตั้งและป้องกันสภาพแวดล้อมการพัฒนาอย่างเหมาะสม สำหรับการพัฒนาและบูรณาการระบบ โดยให้ครอบคลุมตลอดทั้งวงจรชีวิตของการพัฒนาระบบ
99	A.14.2.7	การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)	มาตรการควบคุม องค์กรต้อง กำกับดูแลและเฝ้าติดตามกิจกรรมการพัฒนาระบบที่ดำเนินการโดยหน่วยงานภายนอก
100	A.14.2.8	การทดสอบความมั่นคงปลอดภัยของระบบ (System security testing)	มาตรการควบคุม การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย (Security Functionality) ต้องดำเนินการในระหว่างการพัฒนา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

101	A.14.2.9	การทดสอบตรวจรับระบบ (System acceptance testing)	มาตรการควบคุม โปรแกรมการทดสอบตรวจรับและเกณฑ์ที่เกี่ยวข้อง ต้องจัดทาขึ้นสำหรับระบบสารสนเทศใหม่ ระบบที่ยกระดับขึ้น (Upgrade) และเวอร์ชันใหม่ของระบบ
102	A.14.3.1	การปกป้องข้อมูลทดสอบ (Protection of test data)	มาตรการควบคุม ข้อมูลทดสอบต้องถูกคัดเลือกอย่างระมัดระวัง และได้รับการปกป้องและควบคุม
103	A.15.1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศสำหรับความสัมพันธ์กับผู้ขาย (Information security policy for supplier relationships)	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศเพื่อจัดการความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินองค์กรโดยหน่วยงานภายนอก ต้องได้รับการตกลงร่วมกันกับหน่วยงาน ภายนอก และจัดทำเป็นลายลักษณ์อักษร
104	A.15.1.2	การระบุข้อกำหนดในข้อตกลงกับผู้ขาย (Addressing security within supplier agreements)	มาตรการควบคุม ข้อกำหนดทั้งหมดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องจัดทำขึ้น และตกลงร่วมกันกับผู้ขายแต่ละราย ที่อาจทำการเข้าถึง ประมวลผล จัดเก็บ สื่อสารกับสารสนเทศขององค์กร หรือให้บริการส่วนประกอบของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure Components) สำหรับสารสนเทศขององค์กร
105	A.15.1.3	ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and communication technology supply chain)	มาตรการควบคุม ข้อตกลงกับผู้ขาย ต้องรวมถึงข้อกำหนดที่ระบุถึงความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องกับสารสนเทศและบริการเทคโนโลยีการสื่อสารที่ก่อให้เกิดห่วงโซ่อุปทาน (Supply Chain)
106	A.15.2.1	การติดตามและทบทวนบริการของผู้ขาย (Monitoring and review of supplier services)	มาตรการควบคุม องค์กรต้องติดตาม ทบทวน และตรวจประเมินการส่งมอบบริการของผู้ขายอย่างสม่ำเสมอ
107	A.15.2.2	การบริหารจัดการความเปลี่ยนแปลง	มาตรการควบคุม การ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		บริการของผู้ขาย (Managing changes to supplier services)	เปลี่ยนแปลงการให้บริการของผู้ขาย รวมถึงการรักษาให้คงไว้ และการปรับปรุงนโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่มีอยู่ ต้องได้รับการบริหารจัดการ โดยพิจารณาถึงความสำคัญของสารสนเทศ ระบบ และกระบวนการทางธุรกิจที่เกี่ยวข้อง และต้องประเมินความเสี่ยงซ้ำ
108	A.16.1.4	การประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Assessment of and decision on information security events)	มาตรการควบคุม สถานการณ์ (Events) ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกประเมินและถูกตัดสินใจ ถ้าสถานการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ (Incidents) ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
109	A.16.1.5	การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Response to information security incidents)	มาตรการควบคุม เหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการตอบสนองตามขั้นตอนปฏิบัติงานที่จัดทำเป็นลายลักษณ์อักษร
110	A.16.1.6	การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Learning from information security incidents)	มาตรการควบคุม ความรู้ที่ได้รับจากการวิเคราะห์และการแก้ปัญหาเหตุการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกนำไปใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต
111	A.16.1.7	การเก็บรวบรวมหลักฐาน (Collection of evidence)	มาตรการควบคุม องค์กรต้องกำหนดขั้นตอนปฏิบัติงานและนำมาใช้ในการระบุ (Identification), การเก็บรวบรวม (Collection) การจัดหา (Acquisition) การเก็บรักษา (Preservation) สารสนเทศที่สามารถนำมาเป็นหลักฐาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

112	A.17.1.2	การนำไปปฏิบัติด้านความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ (Implementing information security continuity)	มาตรการควบคุม องค์กรต้องจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร นำไปปฏิบัติ และรักษากระบวนการ ขั้นตอนปฏิบัติงาน และมาตรการควบคุม เพื่อให้มั่นใจถึงระดับความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศที่ต้องการในระหว่างสถานการณ์ที่ไม่พึงประสงค์
113	A.17.1.3	ทวนสอบ ทบทวน และประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Verify, review and evaluate information security continuity)	มาตรการควบคุม องค์กรต้องทวนสอบมาตรการความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่จัดทำขึ้นและนำไปปฏิบัติตามรอบระยะเวลาที่กำหนด เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังคงใช้ได้สมเหตุสมผลและมีประสิทธิผลในระหว่างสถานการณ์ที่ไม่พึงประสงค์
114	A.17.2.1	ความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Availability of information processing facilities)	มาตรการควบคุม อุปกรณ์ประมวลผลข้อมูลต้องมีการสำรองซ้ำซ้อนไว้อย่างเพียงพอเพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
ผลการสำรวจและการจัดทำนโยบาย

ในโครงงานปัญหาพิเศษนี้ทางคณะผู้จัดทำได้แบ่งงานออกเป็น 2 ส่วน โดยส่วนแรกจะเป็นการตรวจสอบและกำหนดนโยบายให้เป็นไปตามมาตรฐาน ISO 27001-2013 ตรวจสอบถึงสถานะความเสี่ยงปัจจุบันทางด้านระบบสารสนเทศของสาขาวิทยาการคอมพิวเตอร์ เพื่อที่จะปรับปรุงระบบสารสนเทศปัจจุบันให้มีความเสี่ยงลดลงและผลักดันให้มีการจัดทำนโยบายด้านความปลอดภัยของระบบสารสนเทศ เพื่อให้สาขาวิทยาการคอมพิวเตอร์มีความเป็นมาตรฐานสากล และส่วนที่สองจะเป็นโปรแกรมที่ใช้ในการกำหนดจำนวนหน้าในการพิมพ์เอกสารของผู้ใช้งาน

เนื่องจากมาตรฐาน ISO 27001:2013 มีหัวข้อเป็นจำนวนมาก จากตารางที่ 2.1 ทางผู้จัดทำได้เลือกมาทำเพียงบางหัวข้อ

4.1 การสำรวจนโยบายด้านความปลอดภัยของสาขาวิชาวิทยาการคอมพิวเตอร์

ทางผู้จัดทำได้ทำการสำรวจนโยบายทางด้านความปลอดภัยของระบบสารสนเทศของ สาขาวิทยาการคอมพิวเตอร์เพื่อหาจุดที่มีความเสี่ยงและทำการปิดจุดเสี่ยงนั้น

A.5 นโยบายความมั่นคงปลอดภัย (Security policy)

A.5.1 ทิศทางการบริหารสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ (Management direction for information security)

วัตถุประสงค์ เพื่อกำหนดทิศทางและให้การสนับสนุนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศตามข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

ตารางที่ 4.1 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.5.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.5.1.1	นโยบายสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ (Policies for information security)	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการกำหนด อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารไปยังพนักงาน	ไม่มีเอกสารเป็นลายลักษณ์อักษร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.1 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.5.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		และหน่วยงาน ภายนอกที่เกี่ยวข้อง	
A.5.1.2	การทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	มาตรการควบคุม ชุดนโยบายด้านความมั่นคงปลอดภัยสำหรับ	ไม่มีการทบทวน เนื่องจากยังไม่มีนโยบายความมั่นคง
	(Review of the policies for information security)	สารสนเทศ ต้องถูกทบทวนตามรอบระยะเวลาที่กำหนด หรือเมื่อมีการ	ปลอดภัย

A.6 โครงสร้างด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Organization of information security)

A.6.1 โครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อจัดตั้งโครงร่างการบริหารจัดการในการริเริ่มและควบคุมการนำไปปฏิบัติและการดำเนินงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร

ตารางที่ 4.2 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.6.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.6.1.1	บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security roles and responsibilities)	มาตรการควบคุม หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศทั้งหมด ต้องมีการกำหนดและมอบหมายงาน	ยังไม่มี
A.6.1.2	การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)	มาตรการควบคุม งานและหน้าที่รับผิดชอบที่ขัดกันต้องแบ่งแยกเพื่อลดโอกาสในการ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.2 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.6.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		เปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือโดยไม่ได้ตั้งใจ หรือการใช้ทรัพย์สินขององค์กรผิดวัตถุประสงค์	
A.6.1.3	การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)	มาตรการควบคุม การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องอย่างเหมาะสม ต้องถูกรักษาไว้	ยังไม่มี
A.6.1.4	การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with	มาตรการควบคุม การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่อง	ยังไม่มี
	special interest groups)	เดียวกัน กลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย (Specialist Security Forums) และสมาคมวิชาชีพต้องถูกรักษาไว้	
A.6.1.5	ความมั่นคงปลอดภัยสำหรับสารสนเทศในการบริการโครงการ (Information security in project management)	มาตรการควบคุม ความมั่นคงปลอดภัยสำหรับสารสนเทศต้องมีกำหนดไว้ในการบริหารโครงการไม่ว่าจะเป็นโครงการประเภทใดก็ตาม	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.6.2 อุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

วัตถุประสงค์ เพื่อให้มั่นใจถึงความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและการใช้งานอุปกรณ์พกพา

ตารางที่ 4.3 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.6.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.6.2.1	นโยบายสำหรับอุปกรณ์พกพา (Mobile device policy)	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำมาใช้เพื่อบริหารจัดการความเสี่ยงที่มาจากการใช้งานอุปกรณ์พกพา	ยังไม่มี
A.6.2.2	การปฏิบัติงานจากระยะไกล (Teleworking)	มาตรการควบคุม นโยบายและมาตรการสนับสนุนด้านความมั่นคงปลอดภัย ต้องมีการนำไปปฏิบัติเพื่อป้องกันข้อมูลที่ได้รับการเข้าถึง การประมวลผล หรือการจัดเก็บจากสถานที่ที่มีการปฏิบัติงานจากระยะไกล	ยังไม่มี

A.7 ความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

A.7.1 ก่อนการจ้างงาน (Prior to employment)

วัตถุประสงค์ เพื่อให้มั่นใจว่าพนักงาน (Employees) และผู้ที่องค์กรทำสัญญาจ้าง (Contractors) เข้าใจความรับผิดชอบของตน และเหมาะสมต่อบทบาทที่ได้รับการพิจารณา

ตารางที่ 4.4 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.7.1.1	การคัดกรอง (Screening)	มาตรการควบคุม การตรวจสอบประวัติความเป็นมาของผู้สมัครงานทั้งหมด	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.4 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		ต้องดำเนินการ โดยให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึง และความเสี่ยงที่เกี่ยวข้อง	
A.7.1.2	ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)	มาตรการควบคุม ข้อตกลงและเงื่อนไขในสัญญาจ้างงานของพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบของผู้รับการว่าจ้างและขององค์กรในด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	มีแล้ว

A.7.2 ในระหว่างการจ้างงาน (During employment)

วัตถุประสงค์ เพื่อให้มั่นใจว่าพนักงานและผู้ที่องค์กรทำสัญญาจ้างตระหนักถึงและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของตน

ตารางที่ 4.5 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.7.2.1	หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)	มาตรการควบคุม ผู้บริหารต้องกำหนดให้พนักงานและผู้ทำสัญญาจ้างทั้งหมดปฏิบัติตามนโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่องค์กรจัดทำขึ้น	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.5 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.7.2.2	ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security awareness, education and training)	มาตรการควบคุม พนักงานขององค์กรทุกคนและผู้ทำสัญญาจ้างที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมอย่างเหมาะสม และรับทราบนโยบายและขั้นตอนปฏิบัติงานขององค์กรที่ปรับปรุง ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ	ยังไม่มี
A.7.2.3	กระบวนการทางวินัย (Disciplinary process)	มาตรการควบคุม ต้องมีกระบวนการทางวินัยอย่างเป็นทางการและสื่อสารให้รับทราบ เพื่อลงโทษพนักงานที่ฝ่าฝืน ละเมิดความมั่นคงปลอดภัยสำหรับสารสนเทศ	มีแล้ว

A.7.3 การสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนแปลง

ตารางที่ 4.6 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.3

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.7.3.1	การสิ้นสภาพหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการว่าจ้าง (Termination or change of employment responsibilities)	มาตรการควบคุม ความรับผิดชอบและหน้าที่ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่ยังคงไว้ภายหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการว่าจ้างงาน ต้องมีกำหนดไว้และสื่อสารให้	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.6 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.7.3 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		พนักงานและผู้ทำสัญญาจ้าง และนำไปบังคับใช้	

A.8 การบริหารจัดการทรัพย์สิน (Asset management)

A.8.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

วัตถุประสงค์ เพื่อระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

ตารางที่ 4.7 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.8.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.8.1.1	บัญชีทะเบียนทรัพย์สิน (Inventory of assets)	มาตรการควบคุม ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูลต้องถูกระบุ และบัญชีทะเบียนทรัพย์สินต้องจัดทำขึ้นและรักษาไว้	ยังไม่มี
A.8.1.2	ความเป็นเจ้าของทรัพย์สิน (Ownership of assets)	มาตรการควบคุม ทรัพย์สินในบัญชีทะเบียนทรัพย์สินต้องมีการระบุความเป็นเจ้าของ	ยังไม่มี
A.8.1.3	การใช้งานทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)	มาตรการควบคุม กฎการใช้งานอย่างเหมาะสมของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกกำหนดอย่างเป็นลายลักษณ์อักษรและนำไปปฏิบัติ	ยังไม่มี
A.8.1.4	การคืนทรัพย์สิน (Return of assets)	มาตรการควบคุม พนักงานและผู้ใช้งานจากหน่วยงานภายนอกทุกคน ต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนถือครองไว้ เมื่อสิ้นสภาพ	มีแล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.7 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.8.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		การว่าจ้างงาน สิ้นสุดสัญญา หรือข้อตกลง	

A.8.2 การจัดหมวดหมู่สารสนเทศ (Information classification)

วัตถุประสงค์ เพื่อให้มั่นใจได้ว่าสารสนเทศได้รับระดับของการป้องกันอย่างเหมาะสมตามความสำคัญที่มีต่อองค์กร

ตารางที่ 4.8 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.8.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.8.2.1	การจัดหมวดหมู่ของสารสนเทศ (Classification of information)	มาตรการควบคุม สารสนเทศต้องได้รับการแยกหมวดหมู่ตามคุณค่า (Value) ข้อกำหนดทางกฎหมาย ความสำคัญ (Criticality) และความอ่อนไหว (Sensitivity) ต่อการถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ยังไม่มี
A.8.2.2	การทำป้ายชี้บ่งสารสนเทศ (Labelling of information)	มาตรการควบคุม ชุดขั้นตอนปฏิบัติงานที่เหมาะสมสำหรับการทำป้ายชี้บ่งสารสนเทศต้องจัดทำและนำไปปฏิบัติตามให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้	มีแล้ว แต่ยังไม่เป็นระบบ
A.8.2.3	การจัดการทรัพย์สิน (Handling of assets)	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการจัดการทรัพย์สิน ต้องจัดทำและนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.8.3 การจัดการสื่อบันทึกข้อมูล (Media handling)

วัตถุประสงค์ เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลง การกำจัด หรือการทำลายข้อมูลที่จัดเก็บบนสื่อบันทึกโดยไม่ได้รับอนุญาต

ตารางที่ 4.9 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.8.3

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.8.3.1	การบริหารจัดการสื่อบันทึกที่สำมารถเคลื่อนย้ายได้ (Management of removable media)	มาตรการควบคุม ขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการสื่อบันทึกที่สามารถเคลื่อนย้ายได้ ต้องมีการนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดหมวดหมู่สารสนเทศที่องค์กรกำหนดไว้	ยังไม่มี
A.8.3.2	การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	มาตรการควบคุม สื่อบันทึกข้อมูลต้องถูกกำจัดอย่างมั่นคงปลอดภัย เมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไปตามขั้นตอนปฏิบัติงานอย่างเป็นทางการ	ยังไม่มี
A.8.3.3	การขนย้ายสื่อบันทึก (Physical media transfer)	มาตรการควบคุม สื่อบันทึกที่มีข้อมูลต้องได้รับการป้องกันจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือการทำให้เกิดความเสียหายระหว่างขนย้าย	ยังไม่มี

A.9 การควบคุมการเข้าถึง (Access control)

A.9.1 ข้อกำหนดทางธุรกิจสำหรับควบคุมการเข้าถึง (Business requirements of access control)

วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.10 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.1.1	นโยบายควบคุมการเข้าถึง (Access control policy)	มาตรการควบคุม นโยบายควบคุมการเข้าถึงต้องจัดทำขึ้นเป็นลายลักษณ์อักษร และทบทวนตามข้อกำหนดทางธุรกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	ยังไม่มี
A.9.1.2	การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)	มาตรการควบคุม ผู้ใช้งานต้องจัดให้เข้าถึงเครือข่ายและบริการเครือข่ายตามที่ได้รับการอนุญาตให้ใช้งานตามที่กำหนดไว้เท่านั้น	ยังไม่มี

A.9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์ เพื่อให้แน่ใจว่าผู้ที่ได้รับอนุญาตสามารถเข้าถึง และเพื่อป้องกันผู้ไม่ได้รับอนุญาตในการเข้าถึงระบบและบริการ

ตารางที่ 4.11 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.2.1	การลงทะเบียน และการถอนทะเบียนผู้ใช้งาน (User registration and de-registration)	มาตรการควบคุม กระบวนการลงทะเบียนและถอนทะเบียนผู้ใช้งานอย่างเป็นทางการ ต้องนำไปปฏิบัติเพื่อทำให้เกิดการมอบสิทธิในการเข้าถึง	ยังไม่มี
A.9.2.2	การให้การเข้าถึงของผู้ใช้งาน (User access provisioning)	มาตรการควบคุม กระบวนการให้การเข้าถึงของผู้ใช้งานอย่างเป็นทางการ ต้องนำไปปฏิบัติเพื่อมอบ หรือถอนสิทธิในการเข้าถึงสำหรับทุกประเภทผู้ใช้งานของทุกระบบและทุกบริการ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.11 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.2.3	การบริหารจัดการสิทธิการเข้าถึงพิเศษ (Management of privileged access rights)	มาตรการควบคุม การให้และใช้งานของสิทธิการเข้าถึงพิเศษต้องถูกจำกัดและควบคุม	ยังไม่มี
A.9.2.4	การบริหารจัดการข้อมูลลับที่ใช้พิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)	มาตรการควบคุม การให้ข้อมูลลับที่ใช้พิสูจน์ตัวตน ต้องถูกควบคุมผ่านกระบวนการบริหารจัดการอย่างเป็นทางการ	ยังไม่มี
A.9.2.5	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	มาตรการควบคุม เจ้าของทรัพย์สินต้องทบทวนสิทธิในการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนด	ยังไม่มี
A.9.2.6	การลบหรือปรับเปลี่ยนสิทธิการเข้าถึง (Removal or adjustment of access rights)	มาตรการควบคุม สิทธิของพนักงานและผู้ใช้งานจากหน่วยงานภายนอกทุกคนสำหรับเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ต้องถูกถอนเมื่อสิ้นสภาพการว่าจ้าง สิ้นสุดสัญญา หรือข้อตกลง หรือปรับปรุงเมื่อมีการเปลี่ยนแปลง	ยังไม่มี

A.9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์ เพื่อทำให้ผู้ใช้งานมีความรับผิดชอบในการปกป้องข้อมูลที่ใช้พิสูจน์ตัวตน

ตารางที่ 4.12 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.3

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.3.1	การใช้ข้อมูลลับของการพิสูจน์ตัวตน (Use of secret authentication information)	มาตรการควบคุม ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติขององค์กรในการใช้ข้อมูลลับที่ใช้ในการพิสูจน์ตัวตน	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.9.4 การควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (Application) (System and application access control)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบและโปรแกรมประยุกต์ (Application) โดยผู้ไม่ได้รับอนุญาต

ตารางที่ 4.13 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.4

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.4.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	มาตรการควบคุม การเข้าถึงสารสนเทศและฟังก์ชันของระบบของโปรแกรมประยุกต์ (Application) ต้องถูกจำกัดตามนโยบายควบคุมการเข้าถึง	ยังไม่มี
A.9.4.2	ขั้นตอนการเข้าสู่ระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	มาตรการควบคุม กรณีที่กำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบและโปรแกรมประยุกต์ (Application) ต่างๆ ต้องได้รับการควบคุมโดยขั้นตอนการเข้าสู่ระบบอย่างมั่นคงปลอดภัย	มีแล้ว
A.9.4.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	มาตรการควบคุม ระบบบริหารจัดการรหัสผ่าน ต้องมีปฏิสัมพันธ์ (Interactive) และต้องมั่นใจได้ถึงรหัสผ่านที่มีคุณภาพ	ยังไม่มี
A.9.4.4	การใช้งานโปรแกรมยูทิลิตี้พิเศษ (Use of privileged utility programs)	มาตรการควบคุม การใช้งานโปรแกรมยูทิลิตี้ อาจจะสามารถข้ามมาตรการควบคุมของระบบและแอพพลิเคชั่นได้ จึงต้องถูกจำกัดและควบคุมอย่างเคร่งครัด	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.13 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.9.4 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.9.4.5	การควบคุมการเข้าถึงซอสโค้ดของโปรแกรม (Access control to program source code)	มาตรการควบคุม การเข้าถึงซอสโค้ดของโปรแกรมต้องถูกจำกัด	ยังไม่มี

A.10 การเข้ารหัสข้อมูล (Cryptography)

A.10.1 มาตรการควบคุมการเข้ารหัสข้อมูล (Cryptography controls)

วัตถุประสงค์ เพื่อให้มั่นใจได้ว่าการใช้งานการเข้ารหัสข้อมูลเป็นไปอย่างเหมาะสมและมีประสิทธิผล เพื่อป้องกันความลับ (Confidentiality) การพิสูจน์ตัวตน (Authentication) และ/หรือ ความถูกต้องครบถ้วน (Integrity) ของสารสนเทศ

ตารางที่ 4.14 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.10.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.10.1.1	นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)	มาตรการควบคุม นโยบายการใช้มาตรการควบคุมการเข้ารหัสข้อมูลเพื่อปกป้องสารสนเทศ ต้องจัดทำขึ้นและนำไปปฏิบัติ	ยังไม่มี
A.10.1.2	การบริหารจัดการกุญแจ (Key management)	มาตรการควบคุม นโยบายการใช้งาน การป้องกัน และอายุการใช้งานกุญแจเข้ารหัสข้อมูล (Cryptographic Keys) ต้องจัดทำขึ้น และนำไปปฏิบัติตลอดวงจรชีวิตของกุญแจ	ยังไม่มี

A.11 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

A.11.1 บริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย การแทรกแซงต่อสารสนเทศและอุปกรณ์ประมวลผลข้อมูลขององค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.15 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.11.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.11.1.1	ความมั่นคงปลอดภัยของแนวกั้นทางกายภาพ (Physical security perimeter)	มาตรการควบคุม แนวกั้นเขตความมั่นคงปลอดภัยทางกายภาพ ต้องถูกกำหนด และนำไปใช้เพื่อปกป้องพื้นที่ดังกล่าว ที่มีสารสนเทศและอุปกรณ์ประมวลผลข้อมูล ทั้งที่มีความอ่อนไหว (Sensitive) และที่มีความสำคัญ (Critical) อยู่ภายใน	ยังไม่มี
A.11.1.2	มาตรการควบคุมการเข้า-ออกพื้นที่ (Physical entry controls)	มาตรการควบคุม บริเวณที่ต้องรักษาความมั่นคงปลอดภัยต้องได้รับการปกป้องโดยมาตรการควบคุมทางเข้า-ออกอย่างเหมาะสม เพื่อให้มั่นใจว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นจึงอนุญาตให้เข้าถึงได้	ยังไม่มี
A.11.1.3	ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และอาคารสถานที่ (Securing offices, rooms and facilities)	มาตรการควบคุม ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอาคารสถานที่ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้	ยังไม่มี
A.11.1.4	การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats)	มาตรการควบคุม การป้องกันทางกายภาพจากภัยพิบัติทางธรรมชาติ การบุกรุกที่ไม่พึงประสงค์ หรืออุบัติเหตุ ต้องได้รับการออกแบบและนำไปประยุกต์ใช้	ยังไม่มี
A.11.1.5	การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	มาตรการควบคุม ขั้นตอนปฏิบัติงานในบริเวณที่ต้องรักษาความปลอดภัย ต้องได้รับ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.15 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.11.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		การออกแบบและนำไปประยุกต์ใช้	
A.11.1.6	พื้นที่จัดส่งและรับของ (Delivery and loading area)	มาตรการควบคุม ตำแหน่งที่เข้าถึงได้ เช่น พื้นที่จัดส่งและรับของ และตำแหน่งอื่นๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่องค์กรได้ ต้องถูกควบคุม และถ้าเป็นไปได้ ให้แยกออกจากบริเวณที่มีอุปกรณ์ประมวลผลข้อมูลตั้งอยู่ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต	ยังไม่มี

A.11.2 อุปกรณ์ (Equipment)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย ความเสียหาย การขโมยหรือทำให้เป็นอันตราย (Compromise) ต่อทรัพย์สิน และทำให้เกิดการหยุดชะงักในการดำเนินงานขององค์กร

ตารางที่ 4.16 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.11.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.11.2.1	การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)	มาตรการควบคุม อุปกรณ์ต้องได้รับการจัดวางและป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายจากสภาพแวดล้อม และโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต	ยังไม่มี
A.11.2.2	ระบบสาธารณูปโภคสนับสนุน (Supporting utilities)	มาตรการควบคุม อุปกรณ์ต้องได้รับการป้องกันจากความล้มเหลวของกระแสไฟฟ้า (Power Failure) และการหยุดชะงักอื่นๆ (disruption)	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.16 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.11.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		ที่มีสำเหตุมาจากความผิดพลาดของระบบสาธารณูปโภคสนับสนุน	
A.11.2.3	ความมั่นคงปลอดภัยของการเดินสายไฟฟ้า สายสื่อสาร และสายสัญญาณ (Cabling security)	มาตรการควบคุม สายไฟฟ้าและสายโทรคมนาคมที่ส่งข้อมูลหรือสนับสนุนบริการทางข้อมูล ต้องได้รับการปกป้องจากการขัดขวางการทำงาน (Interception) การแทรกแซงสัญญาณ (Interference) หรือการทำให้เสียหาย (Damage)	ยังไม่มี
A.11.2.4	การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	มาตรการควบคุม อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มั่นใจถึงความพร้อมใช้งานและความถูกต้องในการทำงาน	ยังไม่มี
A.11.2.5	การนำทรัพย์สินออก (Removal of assets)	มาตรการควบคุม อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ต้องไม่นำออกนอกสถานที่โดยไม่ได้รับอนุญาต	มีแล้ว
A.11.2.6	ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่นอกสำนักงาน (Security of equipment and assets off-premises)	มาตรการควบคุม มาตรการด้านความปลอดภัย ต้องนำมาใช้กับทรัพย์สินที่นำออกไปใช้งานนอกสำนักงาน โดยพิจารณาถึงความเสี่ยงต่างๆ ที่มีต่อทรัพย์สินเมื่อนำไปปฏิบัติงานนอกสถานที่	ยังไม่มี
A.11.2.7	การกำจัดอุปกรณ์หรือนำมาใช้ซ้ำอย่างมั่นคงปลอดภัย (Secure disposal or reuse of equipment)	มาตรการควบคุม อุปกรณ์ทั้งหมด ที่มีสื่อบันทึกข้อมูล ต้องได้รับการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.16 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.11.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		และซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ ได้ถูกลบทิ้ง หรือบันทึกทับอย่างมั่นคงปลอดภัย ก่อนนำไปทาลายหรือนำไปใช้ซ้ำ	
A.11.2.8	อุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)	มาตรการควบคุม ผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ที่ไม่มีผู้ดูแลได้รับการป้องกันอย่างเหมาะสม	ยังไม่มี
A.11.2.9	นโยบายการเก็บโต๊ะทำงาน และลบหน้าจอให้ว่าง (Clear desk and clear screen policy)	มาตรการควบคุม นโยบายการเก็บโต๊ะทำงานสำหรับกระดาษเอกสารและสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ และนโยบายการลบหน้าจอให้ว่าง สำหรับอุปกรณ์ประมวลผลข้อมูล ต้องมีการนำไปปฏิบัติ	ยังไม่มี

A.12 ความมั่นคงปลอดภัยด้านการปฏิบัติงาน (Operations security)

A.12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation procedures and responsibilities)

วัตถุประสงค์ เพื่อให้มั่นใจว่าการปฏิบัติงานของอุปกรณ์ประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย

ตารางที่ 4.17 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.1.1	ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	มาตรการควบคุม ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษร และมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้	ยังไม่มี
A.12.1.2	การบริหารจัดการความเปลี่ยนแปลง	มาตรการควบคุม	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.17 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
	(Change management)	การเปลี่ยนแปลงขององค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลข้อมูล และระบบต่างๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการควบคุม	
A.12.1.3	การบริหารจัดการขีดความสามารถ (Capacity management)	มาตรการควบคุม การใช้งานทรัพยากร ต้องได้รับการเฝ้าระวัง ปรับแต่ง คาดการณ์ความต้องการของขีดความสามารถในอนาคต เพื่อให้มั่นใจในประสิทธิภาพของระบบตามที่ต้องการ	ยังไม่มี
A.12.1.4	การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทางานจริงออกจากกัน (Separation of development, testing and operational environments)	มาตรการควบคุม สภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง ต้องถูกแบ่งแยกออกจากกัน เพื่อลดความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงสภาพแวดล้อมของการปฏิบัติงานจริง	ยังไม่มี

A.12.2 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection from malware)

วัตถุประสงค์ เพื่อให้มั่นใจว่าสารสนเทศและอุปกรณ์ประมวลผลข้อมูลได้รับการป้องกันจากโปรแกรมไม่พึงประสงค์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.18 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.2.1	มาตรการควบคุมโปรแกรมไม่พึงประสงค์ (Controls against malware)	มาตรการควบคุม มาตรการตรวจจับ การป้องกัน และการกู้คืน เพื่อป้องกันจากโปรแกรมไม่พึงประสงค์ ต้องนำไปปฏิบัติร่วมกับการสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม	ยังไม่มี

A.12.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย หรือสูญเสียข้อมูล

ตารางที่ 4.19 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.3

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.3.1	การสำรองข้อมูล (Information backup)	มาตรการควบคุม การสำรองสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการปฏิบัติ และทดสอบอย่างสม่ำเสมอ สอดคล้องกับนโยบายสำรองข้อมูลที่กำหนดไว้	ยังไม่มี

A.12.4 การบันทึกล็อก และการเฝ้าระวัง (Logging and monitoring)

วัตถุประสงค์ เพื่อบันทึกเหตุการณ์และการสร้าง (generate) หลักฐาน

ตารางที่ 4.20 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.4

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.4.1	การบันทึกล็อกของเหตุการณ์ (Event logging)	มาตรการควบคุม ล็อกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น (Exception) ข้อผิดพลาด	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.20 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.4 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		(Fault) และเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องมีการจัดทำขึ้น จัดเก็บ และทบทวนอย่างสม่ำเสมอ	
A.12.4.2	การป้องกันข้อมูลล็อก (Protection of log information)	มาตรการควบคุม อุปกรณ์บันทึกล็อกและข้อมูลล็อก ต้องได้รับการป้องกันจากการเปลี่ยนแปลงเพื่อทำลาย (Tempering) และเข้าถึงโดยไม่ได้รับอนุญาต	ยังไม่มี

A.12.5 การควบคุมซอฟต์แวร์ปฏิบัติการ (Control of operation software)

วัตถุประสงค์ เพื่อให้มั่นใจว่าระบบปฏิบัติการมีความถูกต้องครบถ้วน

ตารางที่ 4.21 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.5

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.5.1	การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Installation of software on operational systems)	มาตรการควบคุม ขั้นตอนปฏิบัติงานต้องนำมาปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ	ยังไม่มี

A.12.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

วัตถุประสงค์ เพื่อป้องกันการแสวงหาประโยชน์จากช่องโหว่ทางเทคนิค

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.22 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.6

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.6.1	การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	มาตรการควบคุม ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งานต้องได้รับภายในเวลาที่ทันท่วงที การเปิดเผยช่องโหว่ดังกล่าวขององค์กรต้องถูกประเมินและระบุมาตรการที่เหมาะสมเพื่อจัดการความเสี่ยงที่เกี่ยวข้อง	ยังไม่มี
A.12.6.2	การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)	มาตรการควบคุม กฎบริหารงานของการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน ต้องจัดทำขึ้นและนำไปปฏิบัติ	ยังไม่มี

A.12.7 การพิจารณาสำหรับการตรวจสอบระบบสารสนเทศ (Information systems audit consideration)

วัตถุประสงค์ เพื่อลดผลกระทบจากกิจกรรมการตรวจประเมินระบบการดำเนินงาน

ตารางที่ 4.23 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.12.7

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.12.7.1	มาตรการควบคุมของการตรวจสอบระบบสารสนเทศ (Information systems audit controls)	มาตรการควบคุม ข้อกำหนดและกิจกรรมของการตรวจตรวจสอบที่เกี่ยวข้องกับการทวนสอบระบบปฏิบัติการ ต้องมีการวางแผนอย่างระมัดระวังและได้รับความเห็นชอบเพื่อลดการหยุดชะงักต่อกระบวนการทางธุรกิจให้น้อยที่สุด	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.13 ความมั่นคงปลอดภัยด้านการสื่อสาร (Communication security)

A.13.1 การบริหารจัดการความปลอดภัยสำหรับเครือข่าย (Network security management)

วัตถุประสงค์ เพื่อให้มั่นใจถึงการป้องกันสารสนเทศบนเครือข่ายและอุปกรณ์ประมวลผลที่สนับสนุนเครือข่าย

ตารางที่ 4.24 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.13.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.13.1.1	มาตรการควบคุมของเครือข่าย (Network controls)	มาตรการควบคุม เครือข่ายต้องได้รับการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศบนระบบและโปรแกรมประยุกต์ (Application)	ยังไม่มี
A.13.1.2	ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)	มาตรการควบคุม กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของการบริการจัดการของบริการเครือข่ายทั้งหมด ต้องได้รับการระบุ และรวมอยู่ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าจะเป็นการให้บริการโดยหน่วยงานภายใน (In-house) หรือหน่วยงานภายนอก (Outsourced)	ยังไม่มี
A.13.1.3	การแบ่งแยกเครือข่าย (Segregation in networks)	มาตรการควบคุม กลุ่มของบริการด้านสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศต่างๆ ต้องได้รับการแบ่งแยกบนเครือข่าย	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.13.2 การถ่ายโอนข้อมูล (Information transfer)

วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศที่ถูกถ่ายโอนภายในองค์กร และที่ถ่ายโอนไปยังหน่วยงานภายนอกให้คงไว้

ตารางที่ 4.25 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.13.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.13.2.1	นโยบายและขั้นตอนปฏิบัติงานในการถ่ายโอนข้อมูล (Information transfer policies and procedures)	มาตรการควบคุม นโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมต่างๆ อย่างเป็นทางการ ต้องมีไว้เพื่อป้องกันการถ่ายโอนสารสนเทศผ่านการใช้อุปกรณ์สื่อสารทุกประเภท	ยังไม่มี
A.13.2.2	ข้อตกลงในการถ่ายโอนข้อมูล (Agreements on information transfer)	มาตรการควบคุม ข้อตกลงต้องมีกำหนดถึงการถ่ายโอนสารสนเทศทางธุรกิจอย่างมั่นคงปลอดภัยระหว่างองค์กรและหน่วยงานภายนอก	ยังไม่มี
A.13.2.3	การส่งข้อความอิเล็กทรอนิกส์ (Electronic messaging)	มาตรการควบคุม ข้อมูลที่มีการส่งผ่านทางการส่งข้อความอิเล็กทรอนิกส์ ต้องได้รับการปกป้องอย่างเหมาะสม	ยังไม่มี
A.13.2.4	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or nondisclosure agreements)	มาตรการควบคุม ข้อกำหนดสำหรับการรักษาความลับ หรือการไม่เปิดเผยความลับที่สะท้อนให้เห็นถึงความจำเป็นขององค์กรในการปกป้องข้อมูล ต้องได้รับการระบุ ทบทวนอย่างสม่ำเสมอ และจัดทำเป็นลายลักษณ์อักษร	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.14 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

A.14.1 ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Security requirements of information systems)

วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศเป็นส่วนที่ได้ผนวกรวมเข้าไปในระบบสารสนเทศตลอดวงจรชีวิต และยังรวมถึงข้อกำหนดของระบบสารสนเทศที่ได้ให้บริการผ่านเครือข่ายสาธารณะ

ตารางที่ 4.26 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.14.1.1	การวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security requirements analysis and specification)	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่เกี่ยวข้องต้องรวมไว้ในข้อกำหนดของระบบสารสนเทศใหม่ หรือการพัฒนาปรับปรุงระบบสารสนเทศเดิม	ยังไม่มี
A.14.1.2	การรักษาความมั่นคงปลอดภัยของบริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ (Securing application services on public networks)	มาตรการควบคุม สารสนเทศที่อยู่ในการให้บริการโปรแกรมประยุกต์ (Application) บนเครือข่ายสาธารณะ ต้องได้รับการปกป้องจากการฉ้อโกง การโต้แย้งสัญญา (Contract dispute) และการเปิดเผยและการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	ยังไม่มี
A.14.1.3	การป้องกันธุรกรรมของบริการโปรแกรมประยุกต์ (Application) (Protecting application services transactions)	มาตรการควบคุม สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการโปรแกรมประยุกต์ (Application) ต้องได้รับการป้องกันจากการสื่อสัญญาณที่ไม่สมบูรณ์ (Incomplete -	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.26 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		Transmission) การจัดเส้นทางผิด (Mis-routing) การปรับแก้ข้อความโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การทาสำเนาหรือเล่นข้อความซ้ำ (Replay) โดยไม่ได้รับอนุญาต	

A.14.2 ความมั่นคงปลอดภัยในกระบวนการพัฒนาและกระบวนการสนับสนุน (Security in development and support process)

วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศได้ถูกออกแบบและนำไปปฏิบัติตลอดวงจรชีวิตของการพัฒนาระบบสารสนเทศ

ตารางที่ 4.27 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.14.2.1	นโยบายสำหรับการพัฒนาอย่างมั่นคงปลอดภัย (Secure (Secure development policy)	มาตรการควบคุม กฎสำหรับการพัฒนาซอฟต์แวร์และระบบงาน ต้องจัดทำขึ้นและนำไปประยุกต์ใช้กับการพัฒนาต่างๆ ภายในองค์กร	ยังไม่มี
A.14.2.2	ขั้นตอนปฏิบัติงานการควบคุมความเปลี่ยนแปลงของระบบ (System change control procedures)	มาตรการควบคุม ความเปลี่ยนแปลงของระบบภายในวงจรชีวิตของการพัฒนาต้องได้รับการควบคุมโดยใช้ขั้นตอนปฏิบัติงานควบคุมความเปลี่ยนแปลงอย่างเป็นทางการ	ยังไม่มี
A.14.2.3	การทบทวนทางเทคนิคของโปรแกรมประยุกต์ (Application) ภายหลังการเปลี่ยนแปลง	มาตรการควบคุม เมื่อแพลตฟอร์มปฏิบัติการ (Operating Platforms) ถูก	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.27 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
	แพลตฟอร์มปฏิบัติการ (Technical review of applications after operating platform changes)	เปลี่ยนแปลง โปรแกรมประยุกต์ที่มีความสำคัญทางธุรกิจ ต้องได้รับการทบทวนและทดสอบ เพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน (Operation) และความมั่นคงปลอดภัยขององค์กร	
A.14.2.4	การจำกัดการเปลี่ยนแปลงกับซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)	มาตรการควบคุม การปรับปรุงซอฟต์แวร์สำเร็จรูป ต้องได้รับการห้ามกระทำ การจำกัดการเปลี่ยนแปลงทั้งที่จำเป็นและทั้งหมดต้องถูกควบคุมอย่างเคร่งครัด	ยังไม่มี
A.14.2.5	หลักการทางวิศวกรรมระบบความมั่นคงปลอดภัย (Secure system engineering principles)	มาตรการควบคุม หลักการของวิศวกรรมระบบความมั่นคงปลอดภัย ต้องมีการจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร รักษาให้คงไว้ และนำไปใช้กับการประยุกต์ใช้ระบบสารสนเทศใดๆ ก็ตาม	ยังไม่มี
A.14.2.6	สภาพแวดล้อมการพัฒนาที่มั่นคงปลอดภัย (Secure development environment)	มาตรการควบคุม องค์กรต้องจัดตั้งและป้องกันสภาพแวดล้อมการพัฒนาอย่างเหมาะสม สำหรับการพัฒนาและบูรณาการระบบ โดยให้ครอบคลุมตลอดทั้งวงจรชีวิตของการพัฒนาระบบ	ยังไม่มี
A.14.2.7	การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)	มาตรการควบคุม องค์กรต้องกำกับดูแลและเฝ้าติดตามกิจกรรมการพัฒนาระบบที่	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.27 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.2 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		ดำเนินการโดยหน่วยงานภายนอก	
A.14.2.8	การทดสอบความมั่นคงปลอดภัยของระบบ (System security testing)	มาตรการควบคุม การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย (Security Functionality) ต้องดำเนินการในระหว่างการพัฒนา	ยังไม่มี
A.14.2.9	การทดสอบตรวจรับระบบ (System acceptance testing)	มาตรการควบคุม โปรแกรมการทดสอบตรวจรับและเกณฑ์ที่เกี่ยวข้อง ต้องจัดทาขึ้นสำหรับระบบสารสนเทศใหม่ ระบบที่ยกระดับขึ้น (Upgrade) และเวอร์ชันใหม่ของระบบ	ยังไม่มี

A.14.3 ข้อมูลทดสอบ (Test data)

วัตถุประสงค์ เพื่อให้มั่นใจว่าข้อมูลที่ใช้ในการทดสอบได้รับการปกป้อง

ตารางที่ 4.28 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.14.3

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.14.3.1	การปกป้องข้อมูลทดสอบ (Protection of test data)	มาตรการควบคุม ข้อมูลทดสอบต้องถูกคัดเลือกอย่างระมัดระวัง และได้รับการปกป้องและควบคุม	ยังไม่มี

A.15 ความสัมพันธ์กับผู้ขาย (Supplier relationships)

A.15.1 ความมั่นคงปลอดภัยสำหรับสารสนเทศในความสัมพันธ์กับผู้ขาย (Information security in supplier relationships)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วัตถุประสงค์ เพื่อให้มั่นใจว่าทรัพย์สินขององค์กรที่สำมารถเข้าถึงได้โดยหน่วยงานภายนอกได้รับการป้องกัน

ตารางที่ 4.29 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.15.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.15.1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศสำหรับความสัมพันธ์กับผู้ขาย (Information security	มาตรการควบคุม ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศเพื่อจัดการ	ยังไม่มี
	policy for supplier relationships)	ความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินองค์กรโดยหน่วยงานภายนอก ต้องได้รับการตกลงร่วมกันกับหน่วยงานภายนอก และจัดทำเป็นลายลักษณ์อักษร	
A.15.1.2	การระบุข้อกำหนดในข้อตกลงกับผู้ขาย (Addressing security within supplier agreements)	มาตรการควบคุม ข้อกำหนดทั้งหมดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องจัดทำขึ้น และตกลงร่วมกันกับผู้ขายแต่ละราย ที่อาจทำการเข้าถึง ประมวลผล จัดเก็บ สื่อสารกับสารสนเทศขององค์กร หรือให้บริการส่วนประกอบของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure Components) สำหรับสารสนเทศขององค์กร	ยังไม่มี
A.15.1.3	ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and communication technology	มาตรการควบคุม ข้อตกลงกับผู้ขาย ต้องรวมถึงข้อกำหนดที่ระบุถึงความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.29 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.15.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
	supply chain)	สารสนเทศที่เกี่ยวข้องกับสารสนเทศและบริการเทคโนโลยีการสื่อสารที่ก่อให้เกิดห่วงโซ่อุปทาน (Supply Chain)	

A.15.2 การบริหารจัดการการส่งมอบบริการของผู้ขาย (Supplier service delivery management)

วัตถุประสงค์ เพื่อรักษาระดับของความมั่นคงปลอดภัยสำหรับสารสนเทศ และระดับของการส่งมอบบริการ ที่เห็นชอบร่วมกันให้คงไว้ตามข้อตกลงกับผู้ขาย

ตารางที่ 4.30 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.15.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.15.2.1	การติดตามและทบทวนบริการของผู้ขาย (Monitoring and review of supplier services)	มาตรการควบคุม องค์กรต้องติดตาม ทบทวน และตรวจประเมินการส่งมอบบริการของผู้ขายอย่างสม่ำเสมอ	ยังไม่มี
A.15.2.2	การบริหารจัดการความเปลี่ยนแปลงบริการของผู้ขาย (Managing changes to supplier services)	มาตรการควบคุมการเปลี่ยนแปลงการให้บริการของผู้ขาย รวมถึงการรักษาให้คงไว้และการปรับปรุงนโยบาย ขั้นตอนปฏิบัติงาน และมาตรการควบคุมด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่มีอยู่ ต้องได้รับการบริหารจัดการ โดยพิจารณาถึงความสำคัญของสารสนเทศ ระบบ และกระบวนการทางธุรกิจที่เกี่ยวข้อง และต้องประเมินความเสี่ยงซ้ำ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.16 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security incident management)

A.16.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและการปรับปรุงพัฒนา (Management of information security incident and improvements)

วัตถุประสงค์ เพื่อมั่นใจถึงวิธีการที่สม่ำเสมอและมีประสิทธิภาพในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ รวมถึงการสื่อสารเกี่ยวกับจุดอ่อนและสถานการณ์ด้านความมั่นคงปลอดภัย

ตารางที่ 4.31 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.16.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.16.1.1	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Responsibilities and procedures)	มาตรการควบคุม หน้าที่ความรับผิดชอบของผู้บริหารและขั้นตอนปฏิบัติงาน ต้องจัดทำขึ้นเพื่อให้มั่นใจถึงการตอบสนองได้อย่างรวดเร็ว (Quick) มีประสิทธิผล (Effective) และเป็นระเบียบแบบแผน (Orderly) ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	ยังไม่มี
A.16.1.2	การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Reporting information security events)	มาตรการควบคุมสถานการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศต้องถูกรายงานผ่านช่องทางการบริหารจัดการที่เหมาะสมอย่างรวดเร็วเท่าที่ทำได้	ยังไม่มี
A.16.1.3	การรายงานจุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Reporting information security weaknesses)	ระบบและบริการสารสนเทศขององค์กร ต้องทำการจดบันทึกและรายงานข้อสังเกตหรือจุดอ่อนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่น่าสงสัยใดๆ ในระบบหรือบริการต่างๆ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.31 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.16.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.16.1.4	การประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Assessment of and decision on information security events)	มาตรการควบคุม สถานการณ์ (Events) ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกประเมินและถูกตัดสินใจ ถ้าสถานการณ์ดังกล่าวถูกจัดหมวดหมู่เป็นเหตุการณ์ (Incidents) ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	ยังไม่มี
A.16.1.5	การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Response to information security incidents)	มาตรการควบคุม เหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องได้รับการตอบสนองตามขั้นตอนปฏิบัติงานที่จัดทำเป็นลายลักษณ์อักษร	ยังไม่มี
A.16.1.6	การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Learning from information security incidents)	มาตรการควบคุม ความรู้ที่ได้รับจากการวิเคราะห์และการแก้ปัญหาเหตุการณ์ความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกนำไปใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต	ยังไม่มี
A.16.1.7	การเก็บรวบรวมหลักฐาน (Collection of evidence)	มาตรการควบคุม องค์กรต้องกำหนดขั้นตอนปฏิบัติงานและนำมาใช้ในการระบุ (Identification), การเก็บรวบรวม (Collection) การจัดหา (Acquisition) การเก็บรักษา (Preservation) สารสนเทศที่สามารถนำมาเป็นหลักฐาน	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

A.17 ความมั่นคงปลอดภัยสำหรับสารสนเทศในแง่มุมของการบริหารจัดการความต่อเนื่องทางธุรกิจ (Information security aspect of business continuity management)

A.17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security continuity)

วัตถุประสงค์ ความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องถูกฝังลงไปในระบบบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร

ตารางที่ 4.32 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.17.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.17.1.1	การวางแผนความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ (Planning information security continuity)	มาตรการควบคุม องค์กรต้องระบุข้อกำหนดของตน สำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร และความต่อเนื่องของการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศภายใต้สถานการณ์ที่ไม่พึงประสงค์ เช่น ในช่วงวิกฤติ หรือภัยพิบัติ	ยังไม่มี
A.17.1.2	การนำไปปฏิบัติด้านความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศ (Implementing information security continuity)	มาตรการควบคุม องค์กรต้องจัดตั้งขึ้น จัดทำเป็นลายลักษณ์อักษร นำไปปฏิบัติ และรักษากระบวนการ ขั้นตอน ปฏิบัติงาน และมาตรการควบคุม เพื่อให้มั่นใจถึงระดับความต่อเนื่องของความมั่นคงปลอดภัยสำหรับสารสนเทศที่ต้องการในระหว่างสถานการณ์ที่ไม่พึงประสงค์	ยังไม่มี
A.17.1.3	ทวนสอบ ทบทวน และประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Verify, review and evaluate	มาตรการควบคุม องค์กรต้องทวนสอบมาตรการความต่อเนื่องด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.32 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.17.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
	information security continuity)	จัดทำขึ้นและนำไปปฏิบัติตามรอบระยะเวลาที่กำหนด เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังคงใช้ได้สมเหตุสมผล และมีประสิทธิผลในระหว่างสถานการณ์ที่ไม่พึงประสงค์	

A.17.2 การสำรองซ้ำซ้อน (Redundancies)

วัตถุประสงค์ เพื่อให้มั่นใจว่าอุปกรณ์ประมวลผลข้อมูลมีความพร้อมใช้งาน

ตารางที่ 4.33 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.17.2

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.17.2.1	ความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Availability of information processing facilities)	มาตรการควบคุม อุปกรณ์ประมวลผลข้อมูล ต้องมีการสำรองซ้ำซ้อนไว้อย่างเพียงพอ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน	ยังไม่มี

A.18 การปฏิบัติตามข้อกำหนด (Compliance)

A.18.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและสัญญา (Compliance with legal and contractual requirements)

วัตถุประสงค์ เพื่อหลีกเลี่ยงการละเมิดกฎหมาย ระเบียบข้อบังคับ ข้อกำหนด หรือข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ และข้อกำหนดด้านความมั่นคงปลอดภัยใดๆ ก็ตาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.34 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.18.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.18.1.1	การระบุข้อกำหนดด้านกฎหมายและสัญญาที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)	มาตรการควบคุม กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องทั้งหมด และวิธีการขององค์กรเพื่อให้เป็นไปตามข้อกำหนดดังกล่าว ต้องถูกระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัยสำหรับแต่ละระบบสารสนเทศและสำหรับองค์กร	ยังไม่มี
A.18.1.2	สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)	มาตรการควบคุม ขั้นตอนปฏิบัติที่เหมาะสมต้องนำไปปฏิบัติ เพื่อให้มั่นใจว่าสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญาที่เกี่ยวข้องกับสิทธิในทรัพย์สินทางปัญญาและการใช้ซอฟต์แวร์ที่มีกรรมสิทธิ์ (Proprietary Software)	ยังไม่มี
A.18.1.3	การป้องกันบันทึก (Protection of records)	มาตรการควบคุม บันทึกต้องได้รับการป้องกันจากการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพรออกไปโดยไม่ได้รับอนุญาตตามที่กฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญา และข้อกำหนดทางธุรกิจที่ได้กำหนดไว้	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.34 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.18.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.18.1.4	ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)	มาตรการควบคุม การรักษาความเป็นส่วนตัว และการปกป้องข้อมูลส่วนบุคคล ต้องมั่นใจว่าเป็นไปตามที่ระบุไว้ในกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง ถ้าเหมาะสม	ยังไม่มี
A.18.1.5	ข้อบังคับของมาตรการควบคุมของการเข้ารหัสข้อมูล (Regulation of cryptographic controls)	มาตรการควบคุม มาตรการควบคุมการเข้ารหัส ต้องนำไปใช้เพื่อให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด	ยังไม่มี

A.18.2 การทบทวนความมั่นคงปลอดภัยด้านสารสนเทศ (Information security reviews)

วัตถุประสงค์ เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสำหรับสารสนเทศมีการนำไปปฏิบัติและมีการดำเนินงานตามนโยบายและขั้นตอนปฏิบัติงานขององค์กร

ตารางที่ 4.35 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.18.1

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
A.18.2.1	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นอิสระ (Independent review of information security)	มาตรการควบคุม วิธีการขององค์กรที่ใช้เพื่อบริการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ และการนำไปปฏิบัติ เช่น วัตถุประสงค์ของมาตรการ (Control objectives) มาตรการควบคุม (Controls) นโยบาย กระบวนการ และขั้นตอนปฏิบัติงานสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ	ยังไม่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.35 แสดงการสำรวจนโยบายด้านความปลอดภัยก่อนการดำเนินโครงการหัวข้อ A.18.1 (ต่อ)

ข้อ	ชื่อหัวข้อ	รายละเอียด	สถานะ
		ต้องได้รับการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนด หรือเมื่อมีความเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น	
A.18.2.2	การปฏิบัติตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)	มาตรการควบคุม ผู้จัดการต้องทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลข้อมูล และขั้นตอนปฏิบัติงานที่อยู่ภายใต้ความรับผิดชอบของตน กับนโยบายและมาตรฐานความมั่นคงปลอดภัย และข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ ที่เหมาะสม	ยังไม่มี
A.18.2.3	การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)	มาตรการควบคุม ระบบสารสนเทศต้องได้รับการทบทวนความสอดคล้องอย่างสม่ำเสมอกับนโยบายและมาตรฐานความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร	ยังไม่มี

จากที่กล่าวมาข้างต้นสามารถนำมาสร้างเป็นตารางสรุปหัวข้อที่ผู้จัดทำได้นำมาจัดทำทั้งหมดดังนี้

ตารางที่ 4.36 แสดงจำนวนหัวข้อที่นำมาจัดทำทั้งหมด

สถานะ	จำนวนทั้งหมด	จำนวนที่นำมาจัดทำ
มีแล้ว	4 หัวข้อ	3 หัวข้อ (A.8.1.4, A.8.2.2, A.9.4.2, A.11.2.5)
ยังไม่มี	10 หัวข้อ	5 หัวข้อ (A.8.1.3, A.9.1.1, A.9.2.5, A.9.2.6, A.9.4.1, A.11.1.1, A.11.1.2,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

		A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6,

ตารางที่ 4.36 แสดงจำนวนหัวข้อที่นำมาจัดทำทั้งหมด (ต่อ)

สถานะ	จำนวนทั้งหมด	จำนวนที่นำมาจัดทำ
		A.11.2.1, A.11.2.2, A.11.2.4, A.11.2.5, A.11.2.7, A.11.2.9, A.13.1.1, A.13.1.2, A.18.1.1, A.18.1.2)

4.2 ผลการดำเนินงาน

ในส่วนนี้เป็นการสัมภาษณ์ผู้บริหารเกี่ยวกับข้อเสนอแนะนโยบายที่ได้จัดทำก่อนและทำการสรุปผลการสัมภาษณ์

4.2.1 การสัมภาษณ์ผู้บริหารเกี่ยวกับข้อเสนอแนะการจัดทำนโยบาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.37 แสดงผลการสัมภาษณ์ผู้บริหาร

Phase 1				
Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะเพื่อการจัดทำ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.5.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสำหรับสารสนเทศ		- ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร - เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน - ต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ	✓	- ในการจัดทำจะต้องมีการทำความเข้าใจร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียทั้งหมด - มีการหาข้อมูลเกี่ยวกับระบบเดิมที่มีอยู่แล้ว - มีการหาปัญหาที่เกิดขึ้นในปัจจุบัน
A.5.1.2 การทบทวนนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ		- ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร	✓	
A.8.1.1 การจัดทำบัญชีทรัพย์สิน	- มีบัญชีทรัพย์สินของอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศเป็นลายลักษณ์อักษรแล้ว	- เมื่อมีการเปลี่ยนแปลงอุปกรณ์ในระบบสารสนเทศต้องทำการปรับปรุงบัญชีสารสนเทศทันที	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.8.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน		- ต้องจัดให้มีการระบุชื่อผู้ที่เป็นเจ้าของอุปกรณ์ในระบบสารสนเทศเป็นลายลักษณ์อักษร - เมื่อมีการเพิ่มอุปกรณ์ใหม่เข้ามาในระบบสารสนเทศต้องทำการระบุชื่อเจ้าของอุปกรณ์เพิ่มเข้าไปด้วย	✓	- โดยปกติทรัพย์สินทั้งหมดจะเป็นของภาควิชา แต่หากว่าทรัพย์สินนั้นได้จากการซื้อโดยเงินทุนวิจัยของอาจารย์ ทรัยพ์สินนั้นจะมีอาจารย์ผู้ขอสั่งซื้อเป็นเจ้าของ
A.8.1.3 การใช้งานทรัพย์สินที่เหมาะสม		- เครื่องคอมพิวเตอร์ในห้องปฏิบัติการใช้สำหรับทำงานและสืบค้นข้อมูลที่เกี่ยวข้องกับการเรียนการสอนเท่านั้น ห้ามนักศึกษาเล่นเกมในห้องปฏิบัติการ - เครื่องพิมพ์เอกสารทำการจำกัดจำนวนการพิมพ์เอกสารของผู้ใช้งาน	✓	- จะต้องมีมาตรการในการเตือนหรือป้องปราม เมื่อมีการใช้งานอย่างไม่เหมาะสม - การใช้งานเครื่องพิมพ์เอกสาร จะมีการกำหนดช่วงระยะเวลาการใช้งาน เช่น การใช้เครื่องพิมพ์เอกสารสี จะอนุญาตให้ใช้เฉพาะนักศึกษาชั้นปีที่ 4 ในภาคเรียนที่ 2 เท่านั้น
A.8.1.4 การคืนทรัพย์สินขององค์กร	- มีข้อกำหนดในการคืนทรัพย์สินอยู่แล้ว	- ต้องคืนทรัพย์สินเมื่อสิ้นสุดการศึกษา - หากยังคืนทรัพย์สินไม่ครบ จะไม่สามารถจบการศึกษาได้	✓	- ต้องมีการพยายามติดจามเพื่อให้นำทรัพย์สินมาคืนให้ได้

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.8.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ		- อุปกรณ์ทั่วไปนักศึกษาสาขาวิทยาการคอมพิวเตอร์ทุกคนสามารถเข้าถึงได้ เช่น PC, Printer เป็นต้น - อุปกรณ์ที่มีความสำคัญมากสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบและผู้ที่ได้รับอนุญาตเท่านั้น เช่น server เป็นต้น	✓	- จำแนกสิทธิตามชั้นปี ได้แก่ ปี 1 และ ปี 2 จะสามารถเข้าใช้และยืมอุปกรณ์ทั่วๆไปได้ ปี 3 จะสามารถเข้าใช้และยืมอุปกรณ์ที่เกี่ยวข้องกับวิชาที่ตนลงเรียนได้ ส่วนปี 4 จะสามารถเข้าใช้และยืมอุปกรณ์เฉพาะทาง ที่เกี่ยวข้องกับโปรเจคของตนได้
A.9.1.1 นโยบายควบคุมการเข้าถึงระบบ	- ตอนนี้ใช้ของสถาบันอยู่ ซึ่งไม่สามารถระบุได้ว่าเป็นนักศึกษาของภาคเราหรือไม่	- ต้องกำหนดกฎการเข้าห้องปฏิบัติการและการใช้งานเครื่องคอมพิวเตอร์ออกมาเป็นลายลักษณ์อักษร - สามารถเข้าถึงได้เฉพาะนักศึกษาภาควิทยาการคอมพิวเตอร์เท่านั้น - ต้องมีการทบทวนให้เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างน้อยปีละ 1 ครั้ง	✓	-ให้เข้าถึงโดยการพิสูจน์ตัวตน ใส่ username และ password

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.9.2.1 การลงทะเบียน และการถอนทะเบียนผู้ใช้งาน	- มีอยู่แล้ว แต่ใช้ของสถาบัน	- ต้องกำหนดกระบวนการลงทะเบียนและถอนทะเบียนผู้ใช้งาน เพื่อให้เกิดการมอบสิทธิในการเข้าถึง	✓	
A.9.2.4 การบริหารจัดการข้อมูลลับที่ใช้พิสูจน์ตัวตนของผู้ใช้งาน	- มีอยู่แล้ว แต่ใช้ของสถาบัน	- ต้องมีกระบวนการในการควบคุมการบริหารจัดการข้อมูลลับที่ใช้ในการพิสูจน์ตัวตน	✓	
A.9.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน	- มีอยู่แล้ว แต่ใช้ของสถาบัน	- ต้องมีการทบทวนสิทธิ์ทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลง	✓	- ในอนาคตใช้ username และ password ในการ log in และมีการเก็บ log การเข้าใช้งาน
A.9.2.6 การลบหรือปรับเปลี่ยนสิทธิการเข้าถึง	- นโยบายการลบหรือปรับเปลี่ยนสิทธิการเข้าถึง จะดำเนินการตามรอบระยะเวลาที่ขออนุญาตที่ขอไว้	- นักศึกษาที่จบการศึกษาไปแล้ว จะถูกถอดถอนสิทธิ์ในการเข้าถึงสารสนเทศภายในเวลา 6 เดือน - บุคคลากรที่องค์กรสิ้นสุดการจ้างงาน จะถูกถอดถอนสิทธิ์ในการเข้าถึงสารสนเทศทันที - ผู้ใช้งานจากหน่วยงานภายนอก จะถูกถอดถอนสิทธิ์ในการเข้าถึงสารสนเทศ	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
		ทันทีเมื่อสิ้นสุดการใช้งาน		
A.9.3.1 การใช้ข้อมูลลับของการพิสูจน์ตัวตน	- มีอยู่แล้วเฉพาะห้องที่ต้องทำการอนุญาตเป็นพิเศษ	- ต้องมีการกำหนดให้นักศึกษาใช้ข้อมูลลับในการพิสูจน์ตัวตนเพื่อเข้าใช้งานห้องปฏิบัติการ	✓	- อนาคตจะทำทุกห้อง โดยใช้ technology RFID
A.9.4.1 การจำกัดการเข้าถึงสารสนเทศ		- นักศึกษา อาจารย์ และบุคลากรสามารถเข้าใช้งานสารสนเทศได้ ตามสิทธิที่ได้รับ - เฉพาะผู้ดูแลระบบเท่านั้น ที่จะสามารถจัดการเกี่ยวกับระบบได้ ตามสิทธิ์ที่กำหนดไว้ในนโยบายควบคุมการเข้าถึงระบบ	✓	- อนาคตจะมีการพัฒนา web portal ของภาควิชา ผู้ใช้งานจะใช้ username และ password ในการระบุตัวตน
A.9.4.2 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย	- การเข้าใช้งานเครื่อง server จะมี admin เป็นผู้ทำการสร้าง username และ password ที่ใช้ในการเข้าใช้งานให้กับผู้ขอเข้าใช้งานแต่ละคน	- ต้องมีการลงทะเบียนลายนิ้วมือ และมีการลงทะเบียนกำหนดสิทธิ์ในการเข้าใช้งานเครื่องคอมพิวเตอร์ในห้องปฏิบัติการ - ก่อนเข้าใช้งานห้องปฏิบัติการต้องทำการสแกนลายนิ้วมือ - ก่อนเข้าใช้งานระบบคอมพิวเตอร์ต้อง	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
		ทำการลงชื่อเข้าใช้งาน		
A.9.4.3 ระบบบริหารจัดการรหัสผ่าน		- รหัสผ่านของผู้ใช้งานควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร - รหัสผ่านของผู้ใช้งานควรประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ - ผู้ใช้งานจะควรทำการเปลี่ยนรหัสผ่านใหม่ทุกๆ 3 เดือน	✓	- แนบ password security level มาด้วย (ภาคผนวก)
A.11.1.2 การควบคุมการเข้า – ออก พื้นที่		- ต้องมีเครื่องสแกนลายนิ้วมือควบคุมการเข้า-ออกห้องปฏิบัติการ - ต้องมีกล้องวงจรปิดบันทึกภาพการเข้า-ออกห้องปฏิบัติการ - อนุญาตให้เข้าใช้งานห้องปฏิบัติการเฉพาะนักศึกษาระดับปริญญาตรี และบุคคลากรของภาควิชาวิทยาการคอมพิวเตอร์เท่านั้น	✓	- ต้องเปลี่ยนประตู เพื่อเตรียมพร้อมสำหรับการติดตั้งเครื่องสแกนลายนิ้วมือ
A.11.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน	- มีขั้นตอนการยืม-คืนทรัพยสินของภาควิชาอยู่แล้ว	- ใช้ขั้นตอนในการยืมทรัพย์สินของภาควิชาวิทยาการคอมพิวเตอร์ตามเดิม	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.11.1.1 การจัดทำบริเวณล้อมรอบ	- อุปกรณ์สารสนเทศอยู่ใน ห้องที่มีประตูปิดมิดชิด มีกำแพงล้อมรอบทุกด้าน	- มีการติดตั้งอุปกรณ์ควบคุมการเข้าออก	✓	
A.11.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ		- จำแนกออกตามห้อง - ห้องปฏิบัติการทั่วไป: มีกล้องวงจรปิดและอุปกรณ์ควบคุมการเข้าออก (fingerscan) - ห้องปฏิบัติการมัลติมีเดีย: มีกล้องวงจรปิด และอุปกรณ์ควบคุมการเข้าออก (fingerscan) - ห้องโปรเจค: มีกล้องวงจรปิด และอุปกรณ์ควบคุมการเข้าออก (ใช้ fingerscan) - ห้องเซิฟเวอร์: มีกล้องวงจรปิด และอุปกรณ์ควบคุมการเข้าออก (ใช้คีย์การ์ดและต้องขออนุญาติก่อน) - ห้องพนักงานดูแล: มีพื้นที่สำหรับผู้มาติดต่อ กล้องวงจรปิด	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
A.11.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม	- มีการติดตั้งเครื่องสำรองไฟ เพื่อป้องกันภัยจากเหตุไฟดับ - มีการติดตั้งสายดิน เพื่อป้องกันไฟฟ้ารั่วไหล	- มีการติดตั้งอุปกรณ์ควบคุมการเข้าออก - มีการติดตั้งสารเคมีที่สำหรับดับเพลิง - มีการซ้อมหนีไฟสำหรับบุคลากรที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง	✓	
A.11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย		- ต้องทำการขออนุญาตก่อนเข้าไปปฏิบัติงาน - เมื่อได้รับอนุญาตแล้ว ต้องปฏิบัติตามกฎของห้องนั้นๆ ที่ได้กำหนดไว้แล้วอย่างเคร่งครัด	✓	
A.11.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก		- ต้องมีห้องสำหรับการส่งมอบผลิตภัณฑ์โดยเฉพาะ และต้องมีเจ้าหน้าที่คอยควบคุมดูแล	✓	** ข้อเสนอแนะจากผู้ดูแล - สถานที่ที่มีอยู่ไม่เพียงพอ และแคบเกินไป
A.11.2.1 การจัดวางและการป้องกันอุปกรณ์		- ต้องมีการจัดวางอุปกรณ์ในห้องที่มีการติดตั้งอุปกรณ์ควบคุมการเข้า-ออก - ต้องจัดวางอุปกรณ์ในตำแหน่งที่เหมาะสมที่จะไม่เกิดอันตรายต่ออุปกรณ์ - ต้องมีการตรวจสอบผังเน็ตเวิร์ค เพื่อการตรวจสอบการจัดวางอุปกรณ์	✓	** ข้อเสนอแนะจากผู้ดูแล - โต๊ะที่ใช้วางเครื่องคอมพิวเตอร์ในห้องปฏิบัติการแคบเกินไป

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
		เน็ตเวิร์ค		
A.11.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน	- มีการติดตั้งเครื่องสำรองไฟฟ้าเพื่อสำรองไฟฟ้าในกรณีไฟดับ - มีการติดตั้งเครื่องปรับอากาศเพื่อควบคุมอุณหภูมิในห้องให้เหมาะสมกับอุปกรณ์สารสนเทศ	- มีการสำรองข้อมูลที่สำคัญเพื่อเก็บรักษาไว้ในกรณีที่ระบบเกิดความล้มเหลวในการทำงาน	✓	- back up ข้อมูลไว้บน cloud
A.11.2.4 การบำรุงรักษาอุปกรณ์	- printer: ตรวจเช็คจากการใช้งาน - หมึกพิมพ์: ปรับตามสถานการณ์ - เครื่องคอมพิวเตอร์: Ghost ก่อนเปิดเทอมทุกครั้ง / ตรวจเช็คตามอาการที่เสีย - UPS เปลี่ยนแบต 2 ปี ต่อ 1 ครั้ง / 1 เครื่อง ใช้งานได้ 5 ปี / 2 ปี จะส่งซ่อม 2 ครั้ง / ตรวจเช็คทุกปิดภาคเรียน	- มีการกำหนดให้มีการบำรุงรักษาอุปกรณ์ทุกๆ 4 เดือน - กรณีมีเหตุการณ์ฉุกเฉินเกิดขึ้นกับอุปกรณ์ต้องมีการเรียกเจ้าหน้าที่ที่เกี่ยวข้องเข้ามาจัดการแก้ไขทันที - ต้องมีการตรวจเช็คอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ	✓	- ทำวิธีการแก้ไขปัญหาเบื้องต้น ติดประกาศไว้ที่ห้องปฏิบัติการ
A.11.2.7 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง	- ถ้าเป็นวัสดุ จะทำการทิ้ง - ถ้าเป็นครุภัณฑ์ จะทำการจำหน่ายหรือบริจาค	- ก่อนการจำหน่ายอุปกรณ์ ต้องทำการลบซอฟต์แวร์ลิขสิทธิ์ออก เพื่อป้องกันการละเมิดลิขสิทธิ์	✓	

Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
	- Harddisk เปลี่ยนทุกๆ 3 ปี	- ต้องทำการลบข้อมูลสำคัญเกี่ยวกับองค์กรออกก่อนการจำหน่ายอุปกรณ์ เพื่อป้องกันความลับขององค์กรรั่วไหล		
A.11.2.9 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย		- ต้องแนะนำบุคลากร ไม่ให้วางคอมพิวเตอร์พกพาที่มีข้อมูลสำคัญไว้ในที่สาธารณะ - ต้องแนะนำบุคลากรให้ไม่ทิ้งสื่อบันทึกข้อมูลที่สำคัญ และเอกสารสำคัญไว้ในที่สาธารณะ เพื่อป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาต	✓	- ทางภาควิชาทำการอบรมให้นักศึกษาและบุคลากรคำนึงถึงความผิดตาม พรบ. คอมพิวเตอร์
A.11.2.3 การเดินสายไฟ สายสื่อสารและสายเคเบิลอื่นๆ	- ขึ้นอยู่กับทางคณะ	- ส่วนของสายไฟฟ้าและสายสื่อสารในห้องปฏิบัติการต้องจัดเก็บให้อยู่ในรางที่มีการปิดมิดชิด เพื่อป้องกันการเดินเกี่ยวสายหรือทำให้สายขาด - ต้องมีการทำเต้ารับเพื่อใช้ต่อพ่วงกับปลั๊กไฟหรือสายสื่อสารที่เชื่อมต่อกับคอมพิวเตอร์	✓	- รางเก็บสายไฟ ต้องเปลี่ยนเป็นเหล็กไม่มีเหลี่ยม และข้างในเป็นท่อพลาสติกเพื่อป้องกันไฟรั่ว

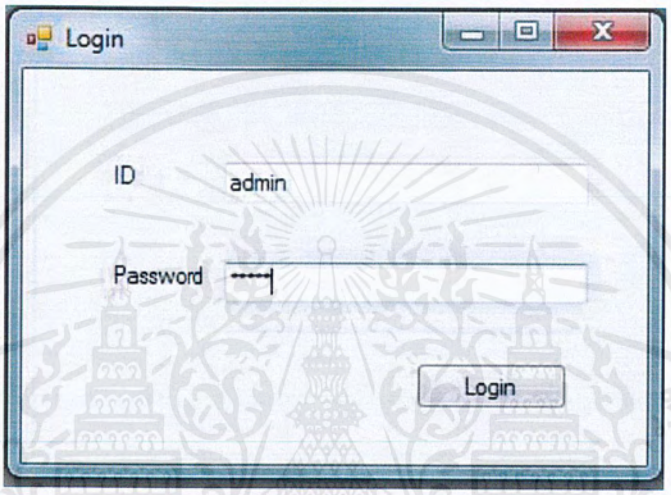
Annex	สิ่งที่ภาควิชาได้มีการจัดทำแล้ว	ข้อเสนอแนะ	ยอมรับ	ความคิดเห็นของผู้บริหาร
		- ในส่วนของสายไฟฟ้าและสายสื่อสารภายนอกที่เชื่อมต่อระหว่างอาคารต้องจัดเก็บให้อยู่ในท่อที่มีการปิดมิดชิดเพื่อป้องกันสายไฟฟ้าโดนแดดเผาและเปียกฝน และต้องมีการจัดทำฝาที่สามารถเปิดปิดได้ เพื่อความสะดวกในการบำรุงรักษาและการเปลี่ยนแปลงสาย		
A.18.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย	- Traffic Log ทางสำนักคอมพิวเตอร์เป็นผู้เก็บ	- ต้องมีการจัดทำข้อกำหนดของภาควิชาวิทยาการคอมพิวเตอร์ในการเข้าใช้งานอุปกรณ์สารสนเทศเป็นลายลักษณ์อักษรและต้องมีการประกาศให้ทราบโดยทั่วถึง - ต้องมีการจัดทำการบันทึกข้อมูลการใช้งานตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐	✓	
A.18.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา	- มีการ recovery ภาคการศึกษาละ 1 ครั้ง เพราะภาควิชาเป็น Lab เฉพาะทางจำเป็นต้องลงโปรแกรมอื่นเพิ่มเติม	- ต้องมีการกำหนดไม่อนุญาตให้นักศึกษาติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์	✓	

4.2.2 โปรแกรมจำกัดจำนวนการพิมพ์เอกสาร

ในส่วนของโปรแกรมจำกัดจำนวนการพิมพ์เอกสาร เป็นการนำนโยบายในข้อการจัดการสารสนเทศมาประยุกต์ใช้ เพื่อใช้ในการจัดการทรัพยากรในการพิมพ์เอกสาร

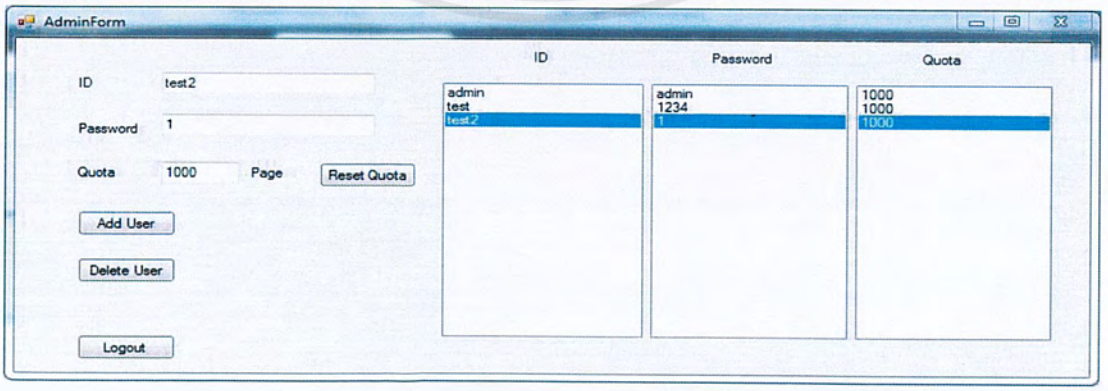
4.2.2.1 ส่วนการใช้งานสำหรับผู้ดูแลระบบ

ผู้ดูแลระบบจำเป็นต้องลงชื่อเข้าใช้งานก่อน โดยจะมีหน้าลงชื่อเข้าใช้งาน ดังรูป 4.1



รูปที่ 4.1 หน้าลงชื่อเข้าใช้งานโปรแกรม

เมื่อลงชื่อเข้าใช้โปรแกรมแล้ว จะปรากฏหน้าการจัดการสำหรับผู้ดูแลระบบใช้งาน ดังรูป 4.2 ซึ่งจะสามารถทำการเพิ่ม/ลบชื่อผู้ใช้งาน และเพิ่ม/ลดจำนวนหน้าในการพิมพ์เอกสาร

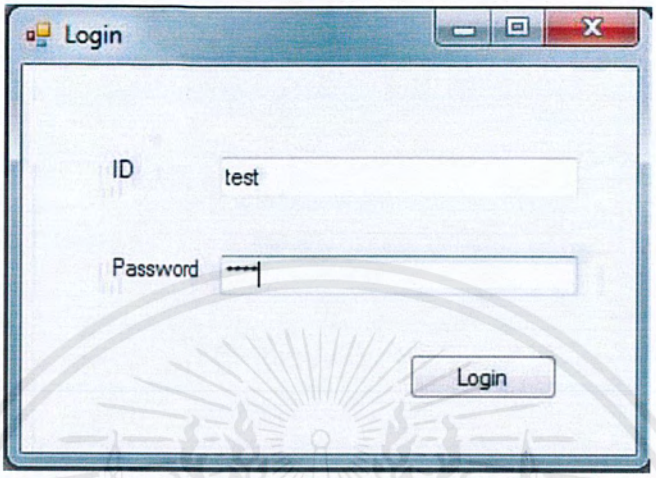


รูปที่ 4.2 หน้าการจัดการสำหรับผู้ดูแลระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

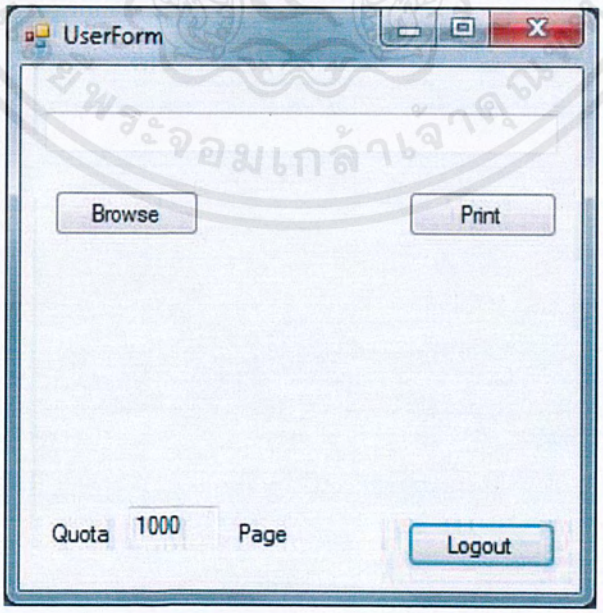
4.2.2.2 ส่วนการใช้งานสำหรับผู้ใช้

ผู้ใช้งานจำเป็นต้องลงชื่อเข้าใช้งานก่อน โดยจะมีหน้าลงชื่อเข้าใช้งาน ดังรูป 4.3



รูปที่ 4.3 หน้าลงชื่อเข้าใช้งานโปรแกรม

เมื่อลงชื่อเข้าใช้โปรแกรมแล้ว จะปรากฏหน้าการใช้งานสำหรับผู้ใช้งาน ดังรูป 4.4 โดยผู้ใช้งานจะทำการเลือกไฟล์ที่ต้องการพิมพ์จากหน้านี้ พร้อมทั้งบอกจำนวนหน้าเอกสารที่สามารถพิมพ์ได้ และเมื่อใช้งานเรียบร้อยแล้วผู้ใช้จำเป็นที่จะต้องลงชื่อออกจากโปรแกรมด้วย



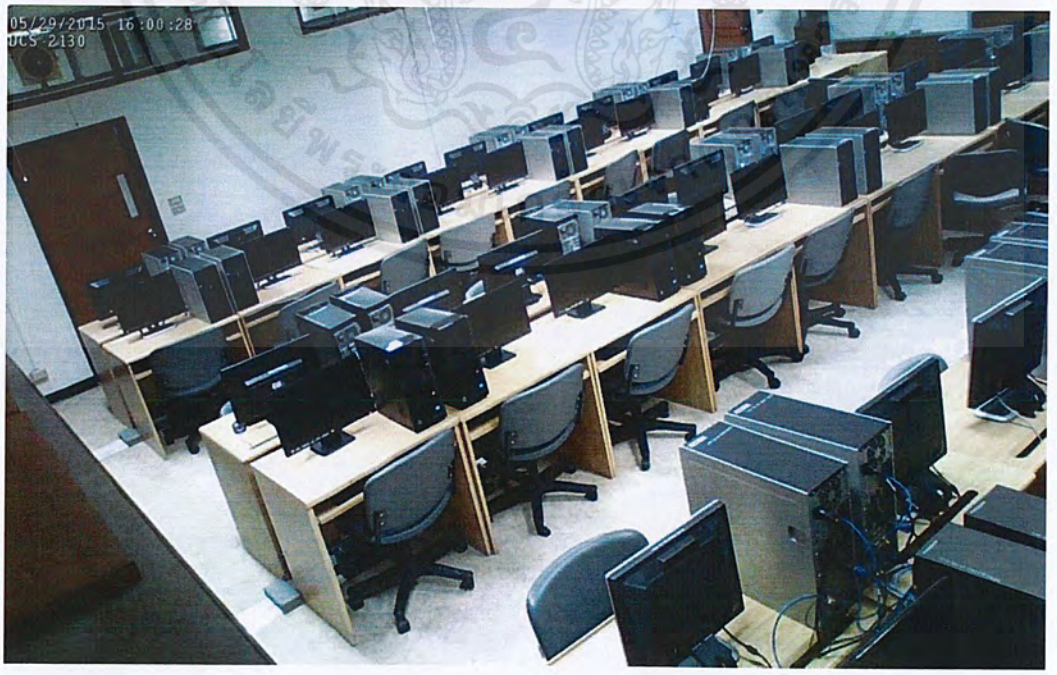
รูปที่ 4.4 หน้าการใช้งานสำหรับผู้ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.3 ตัวอย่างภาพจากกล้องวงจรปิดภายในห้องปฏิบัติการ

จากภาพจะพบว่ากล้องวงจรปิด ณ ห้อง 214 ตึกจุฬาภรณวลัยลักษณ์ 1 ไม่สามารถดูได้อย่างทั่วถึงทั้งห้อง พบจุดบอดของกล้องที่บริเวณแถวที่ 3 นับจากประตู ดังรูปที่ 4.5 และห้อง 224 ก็เช่นเดียวกัน คือพบจุดบอดที่บริเวณแถวที่ 3 นับจากประตู ดังรูป 4.6

รูปที่ 4.5 ตัวอย่างภาพจากกล้องวงจรปิด ณ ห้อง 214 ตึกจุฬาภรณวลัยลักษณ์ 1



รูปที่ 4.6 ตัวอย่างภาพจากกล้องวงจรปิด ณ ห้อง 224 ตึกจุฬาภรณวลัยลักษณ์ 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนห้องปฏิบัติการ 203 ตึกวิทยาศาสตร์ (เก่า) จะมีกล้องวงจรปิดติดตั้งอยู่ 2 ตัว แต่ก็ยังพบว่ามีจุดบอดอยู่ที่บริเวณหนึ่ง ดังรูปที่ 4.7

ก) ภาพจากกล้องวงจรปิดตัวที่ 1 ข) ภาพจากกล้องวงจรปิดตัวที่ 2

รูปที่ 4.7 ตัวอย่างภาพจากกล้องวงจรปิด ณ ห้อง 203 ตึกวิทยาศาสตร์ (เก่า)

4.2.4 บัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1

ทรัพย์สินภายในห้องปฏิบัติการนี้ จะประกอบด้วย คอมพิวเตอร์ตั้งโต๊ะ เครื่องพิมพ์ เครื่องฉายภาพ เครื่องสำรองไฟ และกล้องวงจรปิด โดยจะแสดงรายละเอียดดังตารางที่ 4.37

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
1	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
2	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
3	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
4	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
5	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
6	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
7	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
8	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
9	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
10	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
11	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
12	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
13	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
14	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
15	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
16	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
17	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
18	Computer PC	DELL - optiplex 3020	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
19	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
20	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
21	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
22	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
23	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
24	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
25	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
26	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
27	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
28	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
29	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
30	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
31	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
32	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
33	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
34	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
35	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
36	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
37	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
38	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
39	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
40	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
41	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
42	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
43	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
44	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
45	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
59	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
60	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
61	Computer PC	HP - compaq pro 6300	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
62	Scanner	HP - Scanjet G4010	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
63	Printer	HP - LaserJet P3015	161.254.58.172	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
64	Printer	HP - Officejet 7000 Wide Format	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
65	Printer	HP - LaserJet 2430dtn	161.246.58.231	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
66	Printer	HP - LaserJet 600 M601	161.246.58.233	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
67	Printer	HP - Officejet Pro 8100	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
68	LCD	Infocus	DHCP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
69	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
70	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
71	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
72	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
73	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
74	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
75	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
76	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
77	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
78	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
79	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
80	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
81	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
82	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
83	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
84	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
85	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
86	Monitor	DELL - E2214hb	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
87	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
88	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
89	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
90	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
91	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
92	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
93	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
94	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
95	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
96	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
97	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
98	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
99	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
100	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
101	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
102	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
103	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
104	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
105	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
106	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
107	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
108	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
109	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
110	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
111	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
112	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
113	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
114	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
115	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
116	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
117	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
118	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
119	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
120	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
121	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
122	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
123	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
124	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
125	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
126	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
127	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
128	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
129	Monitor	Acer - T231H	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
130	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
131	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
132	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
133	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
134	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
135	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
136	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
137	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
138	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
139	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
140	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
141	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
142	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
143	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
144	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
145	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
146	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
147	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
148	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
149	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
150	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
151	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
152	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
153	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
154	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
155	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
156	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
157	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
158	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
159	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
160	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
161	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
162	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
163	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
164	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
165	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
166	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
167	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
168	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
169	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
170	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
171	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
172	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
173	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
174	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
175	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
176	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
177	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
178	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
179	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
180	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
181	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
182	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
183	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
184	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
185	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
186	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
187	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
188	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.38 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 214 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
189	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
190	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
191	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
192	CCTV	D-Link - DCS-2130	161.246.58.244	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
193	Switch	D-Link - DGS 1210-48	defualt IP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
194	Switch	D-Link - DGS 1210-48	defualt IP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
195	Switch	SMC - EZ1024dt	defualt IP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
196	Switch	SMC - EZ1024dt	defualt IP	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
197	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
198	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ
199	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	214	พชิรา แก้วเจริญ

4.2.5 บัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1

ทรัพย์สินภายในห้องปฏิบัติการนี้ จะประกอบด้วย คอมพิวเตอร์ตั้งโต๊ะ เครื่องพิมพ์ เครื่องฉายภาพ เครื่องสำรองไฟ และกล้องวงจรปิด โดยจะแสดงรายละเอียดดังตารางที่ 4.38

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
1	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
2	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
3	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
4	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
5	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
6	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
7	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
8	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
9	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
10	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
11	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
12	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
13	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
14	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
15	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
16	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
17	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
18	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
19	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
20	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
21	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
22	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
23	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
24	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
25	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
26	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
27	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
28	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
29	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
30	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
31	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
32	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
33	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
34	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
35	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
36	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
37	Computer PC	HP - compaq dc 5800	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
38	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
39	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
40	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
41	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
42	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
43	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
44	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
45	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
46	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
47	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
48	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
49	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
50	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
51	Computer PC	HP - compaq dc 7900	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
52	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
53	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
54	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
55	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
56	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
57	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
58	Computer PC	HP - Pravilion HPE	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
59	Computer PC	HP - compaq pro 6300	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
60	Computer PC	Lenovo - thinkcenter	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
61	Computer PC	Lenovo - thinkcenter	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
62	Printer	Samsung - ML-4510ND	161.246.58 .236	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
63	LCD	Infocus	DHCP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
64	Monitor	Philips - 196v3l	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
65	Monitor	HP - x20led	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
66	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
67	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
68	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
69	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
70	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
71	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
72	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
73	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
74	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
75	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
76	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
77	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
78	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
79	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
80	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
81	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
82	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
83	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
84	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
85	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
86	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
87	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
88	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
89	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
90	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
91	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
92	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
93	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
94	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
95	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
96	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
97	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
98	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
99	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
100	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
101	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
102	Monitor	HP - L1908 wm	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
103	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
104	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
105	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
106	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
107	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
108	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
109	Monitor	HP - w2072b	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
110	Monitor	HP - L1910	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
111	Monitor	HP - L1911	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
112	Monitor	HP - L1912	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
113	Monitor	HP - L1913	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
114	Monitor	HP - L1914	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
115	Monitor	HP - L1915	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
116	Monitor	HP - L1916	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
117	Monitor	HP - L1917	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
118	Monitor	HP - L1918	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
119	Monitor	HP - L1919	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
120	Monitor	HP - L1920	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
121	Monitor	HP - L1921	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
122	Monitor	HP - L1922	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
123	Monitor	HP - L1923	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
124	Monitor	EliteDisplay - E231	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
125	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
126	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
127	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
128	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
129	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
130	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
131	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
132	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
133	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
134	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
135	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
136	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
137	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
138	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
139	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
140	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
141	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
142	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
143	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
144	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
145	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
146	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
147	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
148	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
149	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
150	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
151	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
152	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
153	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
154	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
155	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
156	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
157	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
158	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
159	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
160	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
161	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
162	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
163	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
164	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
165	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
166	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
167	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
168	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
169	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
170	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
171	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
172	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
173	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
174	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
175	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
176	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
177	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
178	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
179	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
180	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
181	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
182	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.39 แสดงรายละเอียดของบัญชีทรัพย์สินภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 (ต่อ)

ลำดับ	อุปกรณ์	ชื่อรุ่น	IP Address	ตึก	ชั้น	ห้อง	ผู้ดูแล
183	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
184	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
185	UPS	Cleanline	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
186	CCTV	D-Link - DCS-2130	161.246.58 .245	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
187	Switch	D-Link - DGS 1210-48	defualt IP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
188	Switch	D-Link - DGS 1210-48	defualt IP	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
189	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
190	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ
191	Patch Panel	Bellcomms - CAT6 24port	None	ตึกจุฬาภรณฯ1	2	224	พชิรา แก้วเจริญ

4.2.6 การสำรวจการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1

อุปกรณ์ต่างๆภายในห้องปฏิบัติการจะถูกเชื่อมต่อผ่านสวิตช์และแผงกระจายสาย ซึ่งจะมีสวิตช์ทั้งหมด 2 ตัว และแผงกระจายสาย 3 ตัว ดังตารางที่ 4.39 และ 4.40

ตารางที่ 4.40 แสดงการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 ผ่านสวิตช์ตัวที่ 1

Switch (SW1) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
1	1:C1	-	-	ไม่มีการเชื่อมต่อ	-
2	2:C2	-	-	com อาจารย์	56วท.7440-0-02-1022
3	3:C3	-	-	com 49	52วท.7440-01-02-049
4	4:C4	-	-	com 59	52วท.7440-01-02-054
5	5:C5	-	-	com 48	52วท.7440-01-02-047

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.40 แสดงการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 ผ่านสวิตช์ตัวที่ 1 (ต่อ)

Switch (SW1) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
6	6:C6	-	-	com 58	52วท.7440-01-02-059
7	7:C7	-	-	com 47	52วท.7440-01-02-052
8	8:C8	-	-	com 57	52วท.7440-01-02-064
9	9:C9	-	-	com 61	51วท.7440-01-02-126
10	10:C10	-	-	com 62	51วท.7440-01-02-115
11	11:C11	-	-	com 51	52วท.7440-01-02-051
12	12:C12	-	-	com 52	52วท.7440-01-02-046
13	13:C13	-	-	com 50	52วม.7440-01-02-055
14	14:C14	-	-	com 60	51วท.7440-01-02-102
15	15:C15	-	-	com 55	52วท.7440-01-02-050
16	16:C16	-	-	com 65	54วท.ค.7440-01-07-002
17	17:C17	-	-	com 54	52วท.7440-01-02-056
18	18:C18	-	-	com 64	54วท.ค.7440-01-07-001
19	19:C19	-	-	com 53	52วท.7440-01-02-058
20	20:C20	-	-	com 63	51วท.7440-01-02-096
21	21:C21	-	-	ไม่มีการเชื่อมต่อ	-
22	22:C22	-	-	ไม่มีการเชื่อมต่อ	-
23	23:C23	-	-	com 27	51วท.7440-01-02-113
24	24:C24	-	-	com 39	51วท.7440-01-02-122
25	-	1:C25	-	com 26	51วท.7440-01-02-108
26	-	2:C26	-	com 38	51วท.7440-01-02-132
27	-	3:C27	-	com 24	51วท.7440-01-02-094
28	-	4:C28	-	com 37	51วท.7440-01-02-109
29	-	5:C29	-	com 31	51วท.7440-01-02-131
30	-	6:C30	-	com 42	55วท.7440-01-07-040
31	-	7:C31	-	com 29	51วท.7440-01-02-112
32	-	8:C32	-	com 41	51วท.7440-01-02-101
33	-	9:C33	-	com 28	51วท.7440-01-02-110

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.40 แสดงการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 ผ่านสวิตช์ตัวที่ 1 (ต่อ)

Switch (SW1) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
34	-	10:C34	-	com 40	51วท.7440-01-02-130
35	-	11:C35	-	com 34	55วท.7440-01-07-057
36	-	12:C36	-	com 45	55วท.7440-01-07-048
37	-	13:C37	-	com 33	55วท.7440-01-07-064
38	-	14:C38	-	com 44	55วท.7440-01-07-069
39	-	15:C39	-	com 32	55วท.7440-01-07-070
40	-	16:C40	-	com 43	55วท.7440-01-07-058
41	-	17:C41	-	com 01	51วท.7440-01-02-111
42	-	18:C42	-	ไม่มีการเชื่อมต่อ	-
43	-	19:C43	-	com 04	51วท.7440-01-02-118
44	-	20:C44	-	com 14	51วท.7440-01-02-103
45	-	21:C45	-	com 03	51วท.7440-01-02-134
46	-	22:C46	-	com 15	51วท.7440-01-02-095
47	-	23:213-1	-	สวิตช์ห้อง 213	-
48	-	24:SW2		SW2	ไม่สามารถระบุได้

ตารางที่ 4.41 แสดงการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 ผ่านสวิตช์ตัวที่ 2

Switch (SW2) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
1	-	23:C47	-	com 02	51วท.7440-01-02-133
2	-	24:C48	-	com 13	51วท.7440-01-02-104
3	-	-	1:C49	com 08	51วท.7440-01-02-121
4	-	-	2:C50	com 09	51วท.7440-01-02-093
5	-	-	3:C51	com 07	51วท.7440-01-02-107
6	-	-	4:C52	com 17	51วท.7440-01-02-124
7	-	-	5:C53	com 05	51วท.7440-01-02-106

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.41 แสดงการเชื่อมต่ออุปกรณ์ภายในห้องปฏิบัติการ 224 ตึกจุฬาภรณวลัยลักษณ์ 1 ผ่านสวิตช์ตัวที่ 2 (ต่อ)

Switch (SW2) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
8	-	-	6:C54	com 16	51วท.7440-01-02-125
9	-	-	7:C55	com 11	51วท.7440-01-02-099
10	-	-	8:C56	com 12	51วท.7440-01-02-107
11	-	-	9:C57	com 10	51วท.7440-01-02-097
12	-	-	10:C58	com 20	51วท.7440-01-02-135
13	-	-	11:C59	com 19	51วท.7440-01-02-127
14	-	-	12:C60	com 18	51วท.7440-01-02-116
15	-	-	13:C61	-	-
16	-	-	14:C62	-	-
17	-	-	15:C63	-	-
18	-	-	16:C64	-	-
19	-	-	17:C65	com 46	52วท.7440-01-02-053
20	-	-	18:C66	com 56	52วท.7440-01-02-061
21	-	-	19:C67	com 22	51วท.7440-01-02-100
22	-	-	20:C68	com 35	51วท.7440-01-02-128
23	-	-	21:C69	-	-
24	-	-	22:C70	com 12	51วท.7440-01-02-119
25	-	-	-	Projector	-
26	-	-	-	CCTV	-
27	-	-	-	-	-
28	-	-	-	-	-
29	-	-	-	-	-
30	-	-	-	-	-
31	-	-	-	-	-
32	-	-	-	-	-
33	-	-	-	-	-
34	-	-	-	-	-
35	-	-	-	-	-

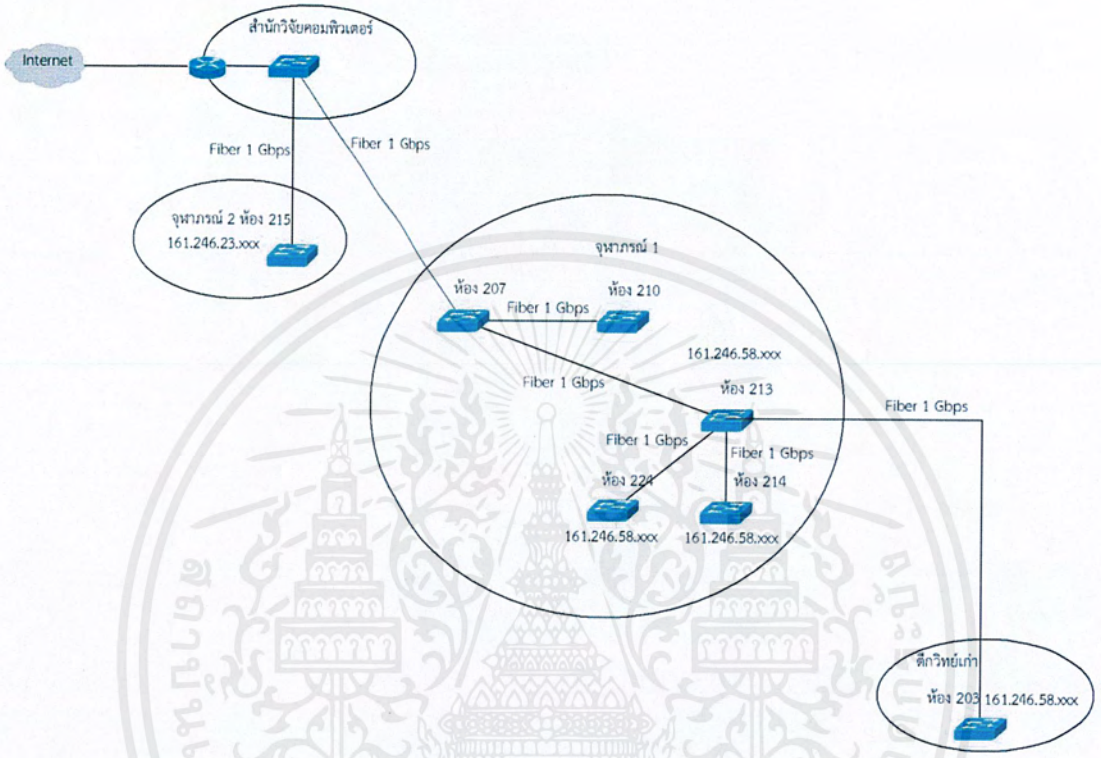
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Switch (SW2) Port NO.	Patch Panel (B1) Port NO.	Patch Panel (B2) Port NO.	Patch Panel (B3) Port NO.	อุปกรณ์	หมายเลขครุภัณฑ์
36	-	-	-	-	-
37	-	-	-	-	-
38	-	-	-	-	-
39	-	-	-	-	-
40	-	-	-	-	-
41	-	-	-	-	-
42	-	-	-	-	-
43	-	-	-	-	-
44	-	-	-	-	-
45	-	-	-	-	-
46	-	-	23:UP-Link 213-1	-	-
47	-	-	24:UP-Link 213-2	-	-
48	-	-	25:SW1	SW1	-

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.7 แผนผังเครือข่ายของภาควิชาวิทยาการคอมพิวเตอร์

แสดงการเชื่อมต่อเครือข่ายของภาควิชาวิทยาการคอมพิวเตอร์กับสำนักวิจัยคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ดังรูปที่ 4.8



รูปที่ 4.8 แผนผังเครือข่ายภาควิชาวิทยาการคอมพิวเตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

กรณีศึกษาการจัดทำ ISO 27001:2013 ให้กับภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เป็นการจัดทำนโยบายเพื่อเพิ่มความปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศของสาขาวิทยาการคอมพิวเตอร์ โดยทางผู้จัดทำได้แบ่งงานออกเป็นสองส่วน ส่วนแรกจะเป็นการเสนอแนะการจัดทำนโยบายเพื่อเพิ่มความปลอดภัยในการเข้าถึงอุปกรณ์ที่ใช้ในระบบสารสนเทศ ส่วนที่สองเป็นการจัดทำโปรแกรมจำกัดจำนวนการพิมพ์เอกสารของผู้ใช้งานตามโควตาที่ผู้ดูแลระบบได้จัดการไว้ให้

การเสนอแนะการจัดทำนโยบายเพื่อเพิ่มความปลอดภัยในการเข้าถึงสารสนเทศ แบ่งออกเป็น 2 ส่วนย่อย คือ การจัดทำนโยบายตามหัวข้อ (annex) ของมาตรฐาน ISO 27001:2013 โดยจัดทำเป็นเอกสารเพื่อใช้ประกอบการดำเนินงานเพื่อความปลอดภัยต่างๆ และการลงมือปฏิบัติเพื่อให้สารสนเทศมีความปลอดภัยมากยิ่งขึ้น โดยทางผู้จัดทำได้เลือกมาทำเพียงบางหัวข้อ (annex) ที่สามารถทำได้ เพราะมาตรฐาน ISO 27001:2013 นั้นมีหัวข้อ (annex) มากถึง 14 หัวข้อ (annex) ดังตารางที่ 4.1

โปรแกรมจำกัดจำนวนการพิมพ์เอกสารเป็นโปรแกรมที่จะช่วยจำกัดจำนวนการพิมพ์เอกสารของผู้ใช้งานแต่ละคน โดยจะมีผู้ดูแลระบบเป็นคนจัดการกำหนดโควตาว่าแต่ละคนจะได้โควตาการพิมพ์เอกสารคนละกี่หน้า รวมทั้งสามารถจัดการเกี่ยวกับรายชื่อผู้ใช้งานแต่ละคนได้ด้วย

5.2 ข้อจำกัดและปัญหาที่พบ

- มาตรฐาน ISO 27001:2013 มีจำนวนหัวข้อ (annex) มาก จึงทำให้ทางผู้จัดทำไม่สามารถจัดทำนโยบายได้ครบทุกหัวข้อ (annex)

- ทางผู้จัดทำไม่มีความรู้พื้นฐานทางด้านมาตรฐาน ISO 27001:2013 ทำให้ทางผู้จัดทำต้องสืบค้นและทำความเข้าใจมาตรฐาน ISO 27001:2013 เป็นเวลานาน

- การจัดทำระบบสารสนเทศให้มีความปลอดภัยเป็นไปตามมาตรฐาน ISO 27001:2013 เป็นการทำโดยผู้เชี่ยวชาญจากทางบริษัท จึงมีข้อมูลตัวอย่างให้น้อย ส่วนใหญ่มีแต่หลักการกว้างๆ ทำให้ทางผู้จัดทำมีข้อมูลประกอบในการทำปัญหาพิเศษจำนวนน้อย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- มาตรฐาน ISO 27001:2013 เป็นมาตรฐานที่เกี่ยวกับความปลอดภัยขององค์กร ซึ่งข้อมูลต่างๆเป็นความลับ ทำให้ทางผู้จัดทำมีข้อมูลในการอ้างอิงจำนวนน้อย

- การทำโครงงานปัญหาพิเศษในเรื่องการจัดทำระบบสารสนเทศให้มีความปลอดภัยเป็นไปตามมาตรฐาน ISO 27001:2013 เป็นเรื่องที่เกี่ยวกัยนโยบายค่อนข้างมาก จึงทำให้ใช้เวลานานในการเขียนเล่ม

- โปรแกรมจำกัดจำนวนการพิมพ์เอกสารเป็นรุ่นทดลอง ทางผู้จัดทำจึงยังไม่ได้ทำการเชื่อมโปรแกรมกับเซิร์ฟเวอร์ฐานข้อมูล

5.3 ข้อเสนอแนะ

- ควรมีการจัดการอบรมเรื่องความสำคัญของมาตรฐาน ISO 27001:2013 โดยผู้เชี่ยวชาญเพื่อเพิ่มความรู้ให้กับบุคลากรและนักศึกษาภายในสาขาวิชาวิทยาการคอมพิวเตอร์

- ควรมีการพูดคุยและตกลงกับผู้ใช้งานให้แน่ชัดในเรื่องจำนวนโควตาในการพิมพ์เอกสารของผู้ใช้งาน เพื่อป้องกันปัญหาจำนวนโควตาไม่พอและให้ผู้ใช้งานสามารถบริหารจำนวนโควตาได้อย่างดี

- ควรมีการเปลี่ยนมุมกล้องวงจรปิดให้มองเห็นครอบคลุมพื้นที่ห้องทั้งหมด หรือเปลี่ยนอุปกรณ์เป็นรุ่นที่สามารถควบคุมการเปลี่ยนทิศทางมุมกล้องได้

- ควรเพิ่มอุปกรณ์ที่ใช้ในการเก็บข้อมูลภาพจากกล้องวงจรปิด

5.4 แนวทางในการพัฒนาต่อ

- เอกสารการจัดทำระบบสารสนเทศให้มีความปลอดภัยเป็นไปตามมาตรฐาน ISO 27001:2013 นั้นเมื่อทำได้ครบทุกหัวข้อแล้ว สามารถนำไปขอให้องค์กรกลางที่ได้รับการรับรองจาก ISO ให้สามารถประเมินองค์กรอื่นได้ มาทำการประเมินเพื่อของใบรับรองการผ่านการประเมินมาตรฐาน ISO 27001:2013 ได้

- โปรแกรมจำกัดจำนวนการพิมพ์เอกสารสามารถต่อยอดนำไปใช้กับคณะได้ ในกรณีที่ทางคณะต้องการจำกัดจำนวนการพิมพ์เอกสารของผู้ใช้บริการการพิมพ์เอกสารฟรีของคณะ

- พัฒนาโปรแกรมในการลงชื่อเข้าใช้งานก่อนการเข้าใช้งานเครื่องคอมพิวเตอร์

- พัฒนาโปรแกรมในการตรวจสอบว่ารหัสผ่านมีความปลอดภัยหรือไม่

- พัฒนาต่อใน phase2 และ phase3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารอ้างอิง

[1] Pryn Sereepong. 2557. **โครงสร้างของมาตรฐาน ISO 27001.** [Online].

Available : http://www.club27001.com/2013/08/isoiec-27001_21.html.

[2] Pryn Sereepong. 2557. **รีวิว ISO 27001 : 2013 - ตอนที่1 พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ.** [Online].

Available : http://www.club27001.com/2014/01/review-iso27001-2013-part1.html.

[3] Pryn Sereepong. 2557. **รู้จัก ISO/IEC 27001 มาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ.** [Online].

Available : http://www.club27001.com/2013/08/isoiec-27001.html.

[4] Pryn Sereepong. 2557. **บันได 4 ขั้นสู่มาตรฐาน ISO 27001 Information Security Management.** [Online].

Available : http://www.club27001.com/2013/08/4-isoiec-27001.html.

[5] Pryn Sereepong. 2557. **องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ.** [Online].

Available : http://www.club27001.com/2013/08/normal-0-false-false-false-en-us-x-none.html.

[6] Pryn Sereepong. 2557. **มาตรการ (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001 :2013.** [Online].

Available : http://www.club27001.com/2014/02/ISO-27001-2013-Controls-requirement.html.

[7] ณัฐวุฒิ วิศยทักษิณ. 2554. "การพัฒนานโยบายด้านความปลอดภัยภายใต้มาตรฐาน ISO27001 และการบริหารความเสี่ยง มหาวิทยาลัยกรุงเทพ." สารนิพนธ์วิทยาศาสตร์มหาบัณฑิต สาขาวิชาวิศวกรรมเครือข่าย บัณฑิตวิทยาลัย, มหาวิทยาลัยเทคโนโลยีมหานคร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[8] วีระชัย. 2552. **หมายเลข port คืออะไร.** [Online].
Available : http://www.suchinko.com/index.php?lay=boardshow&ac=webboard_show&WBntype=1&No=1222404.

[9] Charles Nadeau. 2556. **Setting the password security level for your Zendesk (Plus and Enterprise).** [Online].
Available : https://support.zendesk.com/hc/en-us/articles/203663736-Setting-the-password-security-level-for-your-Zendesk-Plus-and-Enterprise-.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก. Password Security Level [9]

ก.1 Low Level

- พาสเวิร์ดจะต้องประกอบด้วยอักขระอย่างน้อย 5 ตัวอักษร

ก.2 Medium Level

- พาสเวิร์ดจะต้องประกอบด้วยอักขระอย่างน้อย 6 ตัวอักษร และต้องตรงตามข้อกำหนดต่อไปนี้

- ประกอบด้วยตัวเลข และตัวอักษรพิมพ์เล็กพิมพ์ใหญ่
- ประกอบด้วยอักขระพิเศษที่ไม่ใช่ตัวอักษรหรือตัวเลข

ก.3 High Level

- พาสเวิร์ดจะต้องประกอบด้วยอักขระอย่างน้อย 6 ตัวอักษร และต้องตรงตามข้อกำหนดต่อไปนี้

- ประกอบด้วยตัวเลข และตัวอักษรพิมพ์เล็กพิมพ์ใหญ่
- ประกอบด้วยอักขระพิเศษที่ไม่ใช่ตัวอักษรหรือตัวเลข
- รหัสผ่านต้องหมดอายุหลังจากใช้งานไปแล้ว 90 วัน และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่านเก่า 5 รหัสผ่านที่เคยใช้ก่อนหน้านี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้