การวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กร : กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

สุพรรณี ชาติสุข

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร คณะวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2556

Analysis and Risk Assessment by ISO/IEC 27001 Standard for Information System Management in the Organization : A case Study to Information Tecnology Center,Office of the Consumers Protection Board

SUPUNNEE CHARTSUK

A Thematic Paper Submitted in Partial Fulfillment of theRequirements

for the Degree of Master of Science

Department of Computer and Communication Technology

Faculty of Engineering, Dhurakkij Pundit University

2013

ใบรับรองงานค้นคว้าอิสระ

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิทยาศาสตรมหาบัณฑิต

หัวข้องานค้นคว้าอิสระ การวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 เพื่อการบริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กร : กรณีศึกษา ศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

เสนอโดย สุพรรณี ชาติสุข

สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร

อาจารย์ที่ปรึกษางานค้นคว้าอิสระ รองศาสตราจารย์ ดร.ไพบูลย์ พฤกษ์สุนันท์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบงานค้นคว้าอิสระแล้ว

.....ประธานกรรมการ

(อาจารย์ ดร.ประศาสน์ จันทราทิพย์)

.....กรรมการและอาจารย์ที่ปรึกษางานค้นคว้าอิสระ

(รองศาสตราจารย์ ดร.ไพบูลย์ พฤกษ์สุนันท์)

.....กรรมการ

(อาจารย์ ดร.ชนัด เผ่าพันธ์ดี)

คณะวิศวกรรมศาสตร์รับรองแล้ว

..... คณบดีคณะวิศวกรรมศาสตร์

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

วันที่ 26 เดือน กันยายน พ.ศ. 2556

หัวข้อสารนิพนธ์	การวิเคราะห์และประเมินความเสี่ยง ด้วยมาตรฐาน ISO/IEC 27001 เพื่อการบริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กร : กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
ชื่อผู้เขียน	สุพรรณี ชาติสุข
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร.ไพบูลย์ พฤกษ์สุนันท์
สาขาวิชา	เทคโนโลยีคอมพิวเตอร์และการสื่อสาร
ปีการศึกษา	2556

บทคัดย่อ

สารนิพนธ์ฉบับนี้ได้จัดทำเป็นโครงงานการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 เพื่อบริหารจัดการศูนย์เทคโนโลยีสารสนเทศภายในองค์กร โดยมีวัตถุประสงค์ เพื่อต้องการตรวจสอบช่องโหว่/จุดอ่อนของระบบเทคโนโลยีสารสนเทศและต้องการให้ทราบถึงระดับความเสี่ยง/ภัยคุกคาม เพื่อนำมาพัฒนาปรับปรุงร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

โดยนำผลการวิเคราะห์และประเมินความเสี่ยงในครั้งนี้ ซึ่งมีทั้งก่อนดำเนินโครงการและหลังดำเนินโครงการ มาใช้กำหนดกลยุทธ์และแนวทางในการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศขององค์กรด้านต่างๆ เช่น กรณีผลการวิเคราะห์และประเมินความเสี่ยงก่อนการดำเนินโครงการ ได้นำมาพัฒนาปรับปรุงร่างนโยบายความมั่นคงปลอดภัยและปรับปรุงระบบเครือข่ายให้มีความปลอดภัยมากยิ่งขึ้น ส่วนกรณีผลการวิเคราะห์และประเมินความเสี่ยงหลังการดำเนินโครงการ นำมาประยุกต์ใช้ เพื่อหาแนวทางบริหารความเสี่ยงที่เหมาะสม จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เป็นต้น

การจัดทำโครงการดังกล่าว ในครั้งนี้เป็นจุดเริ่มต้นของการตรวจสอบความปลอดภัยของระบบสารสนเทศ เพื่อนำจุดอ่อน มาวางแผน พัฒนาและปรับปรุงระบบให้มีประสิทธิภาพ ให้รองรับการเข้าสู่การให้บริการในระดับสากลด้วยมาตรฐาน ISO/IEC 27001 และสามารถให้องค์กรนำมาใช้เป็นเครื่องมือและกลไกสนับสนุนการดำเนินงานให้สอดคล้องกับภารกิจหลักขององค์กร เพื่อมุ่งสู่ความเป็นเลิศในการบริการประชาชน ทั้งเป็นการเตรียมความพร้อมในด้าน ICT รองรับการเข้าสู่ประชาคมอาเซียน ซึ่งมีเป้าหมายในการพัฒนาและปรับปรุงระบบมีโครงการต่างๆ ดังนี้ คือ โครงการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารฉบับที่ 2 ปี 2557-2560

โครงการจัดทำแผนปฏิบัติราชการ 4 ปี (ด้านเทคโนโลยีสารสนเทศ) โครงการพัฒนาปรับปรุงการจัดทำนโยบายเพื่อความมั่นคงปลอดภัยสารสนเทศและโครงการจัดทำแผนบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

Thematic Paper Title	Risk Assessment and Analysis System for Information Assets with ISO /IEC 27001 Standard Case Study: Office Consumer Protection Board for Information Center
Author	Supunnee Chartsuk
Thematic Paper Advisor	Associate Professor Dr.Paibool Prueksunand.
Department	Computer and Communication Technology
Academic Year	2013

ABSTRACT

"The Project: Risk Analysis and Assessment on Information Technology Systems based ISO/IEC 27001 Standard for the Management of Information Technology Center in Organization". This project has objective to audit vulnerability of information technology system. We also want to acquire weaknesses and risk level of information system in order to improve information system security policies and practical ICT master plan of Information Technology Security.

The results, both before and after launched project, were utilized to determine strategies with Information System management Center in Organization aspects, for example: to develop and improve the Information system security policies and network security system. According to policies on networked systems to be more secure (in case study, before project was launched) and to apply for finding a suitable model of risk management for creating the ICT Master Plan (in case study, after the project was launched).

This project is preparing to begin and check vulnerability to Information Technology System with service and support an international level based ISO/IEC 27001 Standard and also to raise the efficiency of implementation of Information Technology. An organization can use this project as a model to improve efficiency of the Information Technology System. It can be implemented in harmonized working with core mission: we want to be the organization which is

"to be excellent in people service". Moreover the project also was created to support Information Technology to go the ASEAN Community so as to develop and improve various projects as follows; to bring apply to planning IT Master Plan II 2014-2017 or Operational Plan for 4 years of Information Technology. In the future, an organization can apply this project into development and improvement of IT Security Plan and Risk Management that going to change the management of Information Technology Systems.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จได้ด้วยดีและมีคุณค่า ด้วยความอนุเคราะห์และเสียสละเวลาอันมีค่าของอาจารย์ที่ปรึกษางานค้นคว้าอิสระ รองศาสตราจารย์ ดร.ไพบูลย์ พฤกษ์สุนันท์ และ ดร.บรรจง หะรังษี ได้ให้คำแนะนำและช่วยเหลือปรับปรุงงานค้นคว้าอิสระฉบับนี้ให้สมบูรณ์และให้ความรู้ ให้คำแนะนำและการจัดอบรมเกี่ยวกับมาตรฐาน ISO/IEC 27001 อีกทั้งช่วยตรวจสอบผลการวิเคราะห์และประเมินความเสี่ยงด้านความสมบูรณ์ครบถ้วนของเนื้อหา ที่เป็นประโยชน์ต่อการนำมาใช้งานภายในองค์กร ในการดำเนินงานโครงการนี้ ขอบพระคุณกรรมการผู้ทรงคุณวุฒิที่ได้สละเวลามาเป็นคณะกรรมการสอบงานค้นคว้าอิสระ ตลอดจนให้ข้อคิดเห็นอันเป็นประโยชน์เพื่อทำให้งานค้นคว้าอิสระฉบับนี้มีคุณค่ามากยิ่งขึ้น

ขอขอบพระคุณท่านอาจารย์ทุกท่านที่ได้ให้คำแนะนำและสั่งสอนวิชาความรู้ทุกวิชาเพื่อนำมาประยุกต์ใช้ให้เกิดประโยชน์ในการทำงานแก่ข้าพเจ้า

ขอกราบขอบพระคุณบิดามารดา กัลยาณมิตรและน้องมระลึกถึงผู้มีพระคุณทุกคนที่ให้กำลังใจช่วยเหลือทำให้ข้าพเจ้ามีวันนี้ และขออุทิศความดีทั้งหลายของงานค้นคว้าอิสระฉบับนี้แก่ผู้มีพระคุณทุกท่าน

ผู้เขียนหวังเป็นอย่างยิ่งว่างานค้นคว้าอิสระฉบับนี้ จะเป็นประโยชน์และมีคุณค่ากับผู้ที่ต้องการศึกษาการวิเคราะห์และบริหารความเสี่ยงระบบสารสนเทศภายในองค์กรและนำไปประยุกต์ใช้ให้เกิดประโยชน์ในหน่วยงานและสร้างมาตรฐานความปลอดภัยเข้าสู่สากลในอนาคตและเกิดประโยชน์แก่ชาติบ้านเมืองแผ่นดินเกิด หากมีข้อผิดพลาดประการใดในงานค้นคว้าอิสระฉบับนี้ ผู้เขียนต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

สุพรรณี ชาติสุข

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ฆ
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ช
สารบัญตาราง	ฎ
สารบัญภาพ	ฏ
บทที่	
1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการศึกษา	2
1.3 ขอบเขตของการศึกษาวิจัย	2
1.4 ปัญหาและอุปสรรค	3
1.5 กรณีศึกษา	3
1.6 แนวทางในการแก้ปัญหา	5
1.7 ประโยชน์ที่คาดว่าจะได้รับ	6
2 แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง	7
2.1 สถานะด้านเทคโนโลยีสารสนเทศ	7
2.2 ความมั่นคงปลอดภัยของระบบสารสนเทศ	8
2.3 ความเสี่ยงและการบริหารความเสี่ยง	9
2.4 นโยบายความมั่นคงปลอดภัย	12
2.5 มาตรฐานด้านความมั่นคงปลอดภัย	16
2.6 มาตรฐานที่เลือกใช้	24
2.7 เครื่องมือที่ใช้ในการวิเคราะห์	29
2.8 ผลงานวิจัยที่เกี่ยวข้อง	29
3 วิธีการและขั้นตอนการดำเนินการ	31
3.1 ศึกษาภาพรวมการดำเนินงานโครงการ	32
3.2 แหล่งที่มาและวิธีการเก็บรวบรวมข้อมูล	43

สารบัญ (ต่อ)

บทที่	หน้า
3 วิธีการและขั้นตอนการดำเนินการ	31
3.3 ศึกษา วิเคราะห์ จุดแข็ง จุดอ่อน โอกาสและภัยคุกคาม	43
3.4 อุปกรณ์และเครื่องมือที่ใช้ในการศึกษาวิจัย	44
3.5 วิธีการวิเคราะห์และประเมินความเสี่ยง	45
3.6 ระยะเวลาในการศึกษาวิจัย	46
3.7 ขั้นตอนวิธีการดำเนินการศึกษาและวิเคราะห์ความเสี่ยง	47
4 การวิเคราะห์และประเมินความเสี่ยง	48
4.1 การวางแผนเตรียมความพร้อม	49
4.2 การวิเคราะห์ความเสี่ยง	52
4.3 การประเมินความเสี่ยงก่อนดำเนินโครงการ	62
4.4 การวิเคราะห์และประเมินความเสี่ยงตรวจสอบและปิดช่องโหว่ของระบบ	64
4.5 การวิเคราะห์และประเมินความเสี่ยงหลังดำเนินโครงการ	65
4.6 การจัดการความเสี่ยง (Risk Management)	66
4.7 สรุปผลการวิเคราะห์และประเมินความเสี่ยง	67
4.8 การนำมาประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ	67
5 ผลการดำเนินงาน	68
5.1 ผลการวิเคราะห์และประเมินความเสี่ยงก่อนดำเนินโครงการ	68
5.2 การบริหารจัดการด้าน ICT ด้วยผลการวิเคราะห์และประเมินความเสี่ยง	72
5.3 ผลการวิเคราะห์และประเมินความเสี่ยงหลังดำเนินโครงการ	78
6 บทสรุปและข้อเสนอแนะ	81
6.1 ผลการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ	81
6.2 แนวทางการนำไปประยุกต์ใช้ในการบริหารจัดการระบบสารสนเทศ	81
6.3 ปัจจัยความสำเร็จ	83
6.4 ปัญหาอุปสรรค	83
6.5 ข้อเสนอแนะ	84

สารบัญ (ต่อ)

หน้า

บรรณานุกรม..... 86

ภาคผนวก

ก ระบุขอบเขตมาตรฐาน ISO/IEC 27001..... 91

ข ตารางประเมินความเสี่ยง..... 95

ค ผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนดำเนินโครงการ)..... 123

ง ผลการวิเคราะห์และประเมินความเสี่ยง (หลังดำเนินโครงการ)..... 149

จ ร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ..... 176

ประวัติผู้เขียน..... 210

สารบัญตาราง

หน้า

ตารางที่

2.1 คุณลักษณะความสามารถของระบบสารสนเทศ..... 9
3.1 ระยะเวลาในการดำเนินงานศึกษาวิจัย..... 41
4.1 ตารางบ่งชี้ความไม่มั่นคงปลอดภัยของระบบสารสนเทศ..... 53
4.2 ตารางบ่งชี้ประเภทภัยคุกคามของระบบสารสนเทศ..... 55
4.3 ชื่อทรัพย์สิน กลุ่มแม่ข่าย..... 56
4.4 กลุ่มอุปกรณ์เครือข่าย..... 57
4.5 กลุ่มอุปกรณ์สื่อสารโทรคมนาคม..... 57
4.6 รายชื่อทรัพย์สินประเภทโปรแกรม..... 58
4.7 รายชื่อทรัพย์สินด้านบุคลากร..... 59
4.8 รายชื่อทรัพย์สินประเภทข้อมูล..... 59
4.9 รายชื่อทรัพย์สินประเภทด้านงานบริการ..... 60
4.10 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ..... 61
4.11 เกณฑ์การประเมินผลกระทบต่อความปลอดภัยของระบบสารสนเทศ..... 61
4.12 การคำนวณประเมินความเสี่ยง..... 63
5.1 สรุปผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนดำเนินโครงการ)..... 69
5.2 ตารางการวิเคราะห์และประเมินความเสี่ยง ข้อ 1 (ก่อนดำเนินโครงการ)..... 70
5.3 ตารางวิเคราะห์และประเมินความสี่ยง ข้อ 2 (ก่อนดำเนินโครงการ)..... 71
5.4 สรุปผลการจัดทำนโยบายความปลอดภัย..... 73
5.5 ผลการตรวจสอบช่องโหว่..... 77
5.6 สรุปผลการวิเคราะห์และประเมินความสี่ยง(หลังดำเนินโครงการ)..... 79
6.1 ตารางวิเคราะห์และประเมินความสี่ยง ข้อ 2 (ก่อนดำเนินโครงการ)..... 82

สารบัญภาพ

ภาพที่		หน้า
2.1	ประวัติความเป็นมามาตรฐาน ISO/IEC 27001	17
2.2	โครงสร้างกรอบมาตฐานของ COBIT	19
2.3	COBIT As a Meta framework	19
2.4	COBIT 5 New Design	19
2.5	มาตฐาน ITIL	19
2.6	การพัฒนาปรับปรุงต่อเนื่องมาตรฐาน ISO ตาม Control Objective	19
2.7	บทความ Plan-Do-Check-Act	19
3.1	วิธีการดำเนินงาน	32
3.2	ระบบเครือข่าย์(Network System)	34
3.3	บทความ Plan-Do-Check-Act	40
4.1	กระบวนการวิเคราะห์และประเมินความเสี่ยง	48
4.2	ระบบเครือข่าย (Network System)	50
4.3	โครงสร้างระบบสารสนเทศ	51
5.1	ระบบเครือข่ายภายในองค์กรก่อนที่มีการปรับปรุง	75
5.2	เครือข่ายองค์กรที่มีการปรับปรุงแล้วในปัจจุบัน	76

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ความเจริญก้าวหน้าด้านเทคโนโลยีและการสื่อสารอย่างไร้พรหมแดนยุคโลกาภิวัตน์ทำให้มีนวัตกรรมใหม่ๆ เกิดขึ้น เพื่อนำมาใช้สนับสนุนการทำงานตามภารกิจหลักของหน่วยงานต่างๆ หรือตอบสนองธุรกิจทั้งภาครัฐและเอกชน ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่หน่วยงานต้องตระหนักถึงความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ทั้งภาครัฐและเอกชน จึงมีแนวคิดในการบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน ความเจริญก้าวหน้าทางเทคโนโลยีใหม่ๆ ก็จะมีความเสี่ยงในการถูกบุกรุกจากผู้ไม่ประสงค์ดีด้วยวิธีการใหม่ ๆ มากยิ่งขึ้น

จากปัญหาที่เกิดขึ้น คือระบบเว็บไซต์ของหน่วยงาน ถูกโจมตีและบุกรุกจากบุคคลภายนอกโดยไม่ได้รับอนุญาตแสดงให้เห็นว่าระบบเทคโนโลยีสารสนเทศของหน่วยงานยังมีจุดอ่อนอยู่ ซึ่งเป็นสาเหตุของปัญหาอย่างหนึ่ง ในหลายๆข้อจำกัด ทำให้ผู้จัดทำโครงการเกิดแนวคิดเพื่อที่จะศึกษา วิเคราะห์ ปัญหาดังกล่าวที่เกิดขึ้น จึงเป็นความตั้งใจของผู้วิจัยที่จะศึกษาวิเคราะห์และประเมินความเสี่ยงระบบสารสนเทศขององค์กร เพื่อค้นหาจุดอ่อนและช่องโหว่ของระบบสารสนเทศภายในองค์กร โดยใช้มาตรฐานสากล ISO/IEC 27001 เพื่อนำไปใช้ในองค์กรและนำไปสู่การวางแผนดำเนินงาน แผนรับมือกับความเสี่ยงที่เกิดขึ้นและแผนการกรณีฉุกเฉิน นำไปสู่การดำเนินงานและการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อตรวจสอบภัยคุกคามและช่องโหว่ของระบบสารสนเทศที่อาจเกิดความเสี่ยงต่อองค์กรได้ด้วยมาตรฐานสากล ISO/IEC 27001

2. เพื่อทบทวนและกำหนดแนวทางแก้ไขเบื้องต้นด้านความปลอดภัยของระบบสารสนเทศและหาแนวทางป้องกันได้อย่างมีระบบและมีประสิทธิภาพ

3. เพื่อนำไปพัฒนาปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

4. นำผลการวิเคราะห์และประเมินความเสี่ยงมาประยุกต์ใช้งานด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนภารกิจหลักขององค์กร

1.3 ขอบเขตของการศึกษาวิจัย

ขอบเขตของการศึกษาวิจัย มีดังต่อไปนี้

1. ศึกษา วิเคราะห์และการจัดการความเสี่ยงสำหรับระบบสารสนเทศในองค์กรด้วยมาตรฐานสากล ISO/IEC 270001 โดยใช้มาตรการป้องกันตามแนวทางของมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2)ประจำปี 2550 เป็นแนวทางเปรียบเทียบ เพื่อหาถึงภัยคุกคามหรือปัญหาและจุดอ่อน ที่เกิดขึ้นและจัดทำการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. จัดทำกระบวนการจัดการประเมินความเสี่ยงตามมาตรฐานสากล

3. วิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในด้านต่างๆ เช่น

1) ด้านระบบโปรแกรมประยุกต์(Application)

2) ด้านระบบเครือข่าย (Network)

3) ด้านสถาปัตยกรรมของระบบ

4. นำผลการวิเคราะห์และประเมินความเสี่ยงไปพัฒนาและปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัย เพื่อใช้เป็นแนวทางของเจ้าหน้าที่ใช้งานในระบบงานเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย โดยจะมีนโยบายที่มีไว้ให้ปฏิบัติตามดังต่อไปนี้

1) ด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

2) ด้านระบบการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์

3) ด้านระบบการรักษาความมั่นคงปลอดภัยระบบปฏิบัติการคอมพิวเตอร์

4) ด้านระบบการรักษาความมั่นคงปลอดภัยของข้อมูลระบบเครือข่าย

5) ด้านการเข้าถึงระบบงาน สิทธิการเข้าถึงข้อมูลต่างๆ

5. นำเสนอแผนการประเมินความเสี่ยงต่อผู้บริหารขององค์กร เพื่อให้เห็นความสำคัญของความปลอดภัยของระบบสารสนเทศพื้นฐานที่จำเป็น ดังนี้

1) ประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่ใช้ในปัจจุบันโดยอ้างอิงเกณฑ์จาก ISO27001/17799 (Risk Assessment)

2) ทบทวนนโยบายโดยยึดเป้าหมายและจุดประสงค์ ตามแนวทางของหน่วยงานโดยนำข้อกำหนดในมาตรฐาน ISO27001/17799 ซึ่งเป็นมาตรฐานมาปรับใช้เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลระบบสารสนเทศ

1.4 ปัญหาและอุปสรรค

จากปัญหาที่เกิดขึ้นและมีผลกระทบต่อหน่วยงานคือระบบเว็บไซต์ของหน่วยงานถูกโจมตีและถูกบุกรุกจากบุคคลภายนอกโดยไม่ได้รับอนุญาตมีการเข้าถึงข้อมูลของระบบโดยผู้ไม่มีสิทธิ์ แสดงให้เห็นว่าระบบสารสนเทศของหน่วยงานยังมีจุดอ่อน/ช่องโหว่ จึงจำเป็นต้องศึกษาวิเคราะห์ถึงปัญหาดังกล่าวและกำหนดแนวทางในการแก้ไขปัญหา ทั้งนี้หน่วยงานไม่มีงบประมาณในด้านการบริหารจัดการระบบความปลอดภัยระบบเทคโนโลยีสารสนเทศสนับสนุน

1.5 กรณีศึกษา

งานค้นคว้าอิสระเล่มนี้ กรณีศึกษาศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค ซึ่งปัจจุบันได้นำระบบเทคโนโลยีสารสนเทศมาใช้งานเพื่อสนับสนุนภารกิจหลัก ผู้ศึกษาวิจัย เป็นผู้กำกับ ดูแลและบริหารงานด้านเทคโนโลยีสารสนเทศ โดยตรงในตำแหน่งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ซึ่งมีความต้องการเผยแพร่แนวคิด และวิธีการนำไปประยุกต์ใช้งานในหน่วยงานภาครัฐอื่นๆ เพื่อให้มีการนำเทคนิคการวิเคราะห์และประเมินความเสี่ยงไปใช้การวางแผนด้านเทคโนโลยีสารสนเทศ ให้เกิดประสิทธิภาพสูงในเรื่องความเชื่อถือได้ (Reliability) ความมั่นคงปลอดภัย (Security) และคุณภาพ (Quality) รวมทั้งสนับสนุนระบบเพิ่มเติมในอนาคต

สำหรับการวิเคราะห์ SWOT ขององค์กรในจุดแข็ง (Strength) จุดอ่อน (Weakness) โอกาส (Opportunity) และภัยคุกคาม(Threat) จากปัจจัยต่างๆ ซึ่งไม่เป็นเพียงแต่ในด้านความมั่นคงปลอดภัยด้านสารสนเทศเท่านั้นแต่เป็นในภาพรวมขององค์กร ซึ่งมีผลต่อความมั่นคงปลอดภัยสารสนเทศของทั้งระบบ ดังรายละเอียดต่อไปนี้

1. จุดแข็งขององค์กร

1.1 เป็นองค์กรภาครัฐที่ให้การบริการประชาชนทั่วประเทศในการคุ้มครองผู้บริโภค

1.2 กำลังมีการขยายตัวขององค์กร เพื่อรองรับการก้าวสู่ประชาคมอาเซียน

2. จุดอ่อนขององค์กร

2.1 วัฒนธรรมองค์กรแบบเฉพาะที่เปลี่ยนแปลงได้ยาก การประสานงานในแต่ละฝ่ายจึงไม่ง่ายนัก

2.2 บุคลากรและเจ้าหน้าที่ยังขาดความเข้าใจด้าน ICT ในการถ่ายทอดความรู้และประสบการณ์

2.3 ระบบเทคโนโลยีสารสนเทศ ถือเป็นโครงสร้างพื้นฐานรองรับที่สำคัญแต่ขาดการพัฒนาอย่างต่อเนื่องยังมีช่องโหว่ของระบบเทคโนโลยีสารสนเทศ และมีความเสี่ยงต่อการล้มเหลวของระบบทำให้การปฏิบัติงานเกิดความขัดข้อง เช่น ความมั่นคงปลอดภัยของระบบต้องได้มาตรฐานเป็นที่เชื่อถือได้

3. โอกาสขององค์กร

3.1 รัฐบาลมีนโยบายชัดเจนด้านการคุ้มครองผู้บริโภคในประเทศไทยและประเทศในกลุ่มอาเซียนและสากล

3.2 มีโอกาสพัฒนาระบบสารสนเทศให้สามารถรองรับความต้องการใช้บริการได้อย่างพอเพียงและมีประสิทธิภาพ

3.3 องค์กรมีบทบาทในด้านความก้าวหน้าทางเทคโนโลยีสารสนเทศ

3.4 การวิจัยพัฒนาเกี่ยวกับการคุ้มครองผู้บริโภคด้วยประสบการณ์ที่ยาวนาน

4. ภัยคุกคามขององค์กร

4.1 ภัยคุกคามต่อระบบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศในระบบเครือข่ายสื่อสารคอมพิวเตอร์และระบบปัจจุบันอาจทำให้ระบบชะงัก หรืออาจถูกขโมยข้อมูลได้

4.2 การเปลี่ยนแปลงทางการเมืองบ่อยๆ ทำให้ขาดความต่อเนื่องในการทำงาน ต้องมาเริ่มต้นใหม่จึงทำให้พัฒนาได้ช้า

1.6 แนวทางการแก้ปัญหา

แนวทางการแก้ปัญหา เพื่อการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ เป็นการเตรียมพร้อมรับมือกับความเสี่ยง หรือความเสียหายให้แก่ ระบบสารสนเทศขององค์กรโดยไม่คาดคิด เพื่อลดความเสียหายให้ลดน้อยลงที่สุด โดยการวางแผนดำเนินงานมีขั้นตอนดังต่อไปนี้

1. วิเคราะห์มาตรฐานด้านความมั่นคงปลอดภัยและนโยบายที่เหมาะสมกับองค์กร การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อเป็นกรอบการรักษาความมั่นคงปลอดภัยและเป็นแนวทางปฏิบัติสาหรับบุคลากรทุกภาคส่วนในองค์กร โดยครอบคลุมทุกกระบวนงานที่เกี่ยวเนื่องกับระบบเทคโนโลยีสารสนเทศ

2. ศึกษาโครงสร้างขององค์กร ศึกษาการดำเนินงานและประสานงานของฝ่ายเทคโนโลยีสารสนเทศ โดยศึกษาในแต่ละเรื่องเพื่อการวางแผนรองรับเหตุการณ์ฉุกเฉินในปัจจุบัน หากเกิดปัญหาขึ้นจะกระทบกับฝ่ายอื่นหรือไม่

3. วางแผนรองรับสถานการณ์ฉุกเฉินที่เหมาะสม หากมีปัญหาที่อาจเกิดขึ้นและมีผลกระทบทางด้านธุรกิจ ถ้าระบบล้มเหลว ควรนำแผนรองรับสถานการณ์ฉุกเฉินมาใช้ทันที เช่น Incident Response Planning,Disaster Recovery Planning Business Continuity Planning ให้เหมาะสมกับสถานะการณ์ฉุกเฉินนั้นๆ ได้อย่างทันท่วงที

4. ทดสอบ และวิเคราะห์ปัญหา รวมถึงการปรับปรุงการฝึกอบรม การทดสอบแผนงานจะช่วยให้ทราบถึงข้อบกพร่องของการวางแผน ส่วนการฝึกอบรมก็เป็นการเตรียมความพร้อมให้พนักงานดำเนินงานได้อย่างคล่องตัว ส่งผลให้การนำแผนงานไปใช้อย่างมีประสิทธิผล

5. บำรุงรักษาแผนงานทบทวนและปรับปรุงข้อมูลแผนงานให้เป็นปัจจุบัน โดยประสานงานกับหน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อควบคุมการเผยแพร่เอกสารแผนงานและควบคุมการเปลี่ยนแปลงแผนงาน ซึ่งในแต่ละหัวข้อมีรายละเอียดที่มีความเกี่ยวเนื่องกันเพื่อผลสัมฤทธิในการจัดทำแผนเพื่อให้เกิดประสิทธิภาพและประสิทธิผล

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้บริหารสามารถใช้เป็นข้อมูลในการวิเคราะห์และตัดสินใจและประเมินความเสี่ยงขององค์กรเพื่อบริหารจัดการและการวางแผนรับมือกับความเสี่ยงที่เกิดขึ้น

2. ลดความเสี่ยงที่อาจเกิดขึ้นและมีผลต่อระบบเทคโนโลยีสารสนเทศที่ใช้งานภายในองค์กร สร้างความคล่องตัวในการให้บริการแก่ประชาชน

3. นำผลการวิเคราะห์และประเมินความเสี่ยงมาประยุกต์ใช้งานด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนภารกิจหลักขององค์กรในอนาคต

4. สร้างความเชื่อมั่นให้แก่ประชาชนผู้ใช้บริการและเพิ่มประสิทธิภาพในการใช้บริการให้แก่ประชาชนในภาพรวมมากยิ่งขึ้น

5. สร้างความน่าเชื่อถือให้องค์กรที่มีการป้องกันความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่อาจก่อให้เกิดผลกระทบกับการดำเนินงานในองค์กร

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 สถานะด้านเทคโนโลยีสารสนเทศ(Information Status)

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค มีหน้าที่กำกับดูแลการบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กรทั้งหมด เพื่อสนับสนุนงานตามภารกิจหลักขององค์กร ด้วยวิสัยทัศน์ของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค คือ " เป็นองค์กรกลางในการคุ้มครองผู้บริโภคของชาติในระดับสากล " โดยใช้ยุทธศาสตร์ ในด้านการกำกับดูแลนโยบายและการบริหารจัดการองค์กรสู่ความเป็นเลิศ ซึ่งมีเป้าประสงค์ เน้นการดำเนินการด้านเทคโนโลยีสารสนเทศให้ทันสมัย ใช้เป็นกลไกและเครื่องมือเพื่อตอบสนองการดำเนินงานด้านคุ้มครองผู้บริโภค ได้แก่ ระบบฐานข้อมูลอิเล็กทรอนิกส์ ระบบเรื่องราวร้องทุกข์ (1166) ระบบงานสารบรรณอิเล็กทรอนิกส์ ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จและระบบเครือข่าย รวมทั้งการใช้งานเครื่องแม่ข่ายในการบันทึกจัดเก็บและให้บริการข้อมูลต่างๆ ช่วยในการเข้าถึงและสืบค้นข้อมูลและการเผยแพร่ประชาสัมพันธ์ข่าวสารของหน่วยงาน

ในปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้นด้วย องค์กรต่างๆ ทั้งภาครัฐและภาคเอกชนต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่างๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรง และท้าทายต่อผู้บริหารองค์กรที่รับผิดชอบในการดูแลระบบเป็นอย่างมาก ดังนั้นการจัดการด้านความปลอดภัยระบบสารสนเทศของหน่วยงานจึงมีความสำคัญ

2.2 ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security) มุ่งเน้นการสร้างความมั่นคงปลอดภัยระบบสารสนเทศของของแต่ละองค์กรเพื่อรักษาคุณค่า 3 ด้านที่สำคัญคือ C I A ได้แก่ การรักษาความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) มีรายละเอียด ดังนี้

2.2.1 การรักษาความลับ (Confidentiality) หมายถึง การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาตผู้ใช้งานเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด (Authorization) เท่านั้น

2.2.2 ความคงสภาพ (Integrity) หมายถึง ในกรณีความมั่นคงปลอดภัยระบบสารสนเทศ เน้นความถูกต้องและความครบถ้วน โดยความสมบูรณ์มี 2 องค์ประกอบคือ ความสมบูรณ์ของข้อมูล (Data Integrity) และความสมบูรณ์ของระบบ (System Integrity) ได้แก่ ความสมบูรณ์ของข้อมูล หมายถึง ระบบสารสนเทศและโปรแกรมการใช้งานไม่มีการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ความสมบูรณ์ของระบบ หมายถึง ระบบต้องไม่มีการเปลี่ยนแปลงใดๆ โดยไม่ได้รับอนุญาต เช่น ไม่สามารถเข้าถึงระบบเครือข่ายได้ถ้าไม่ได้รับอนุญาต การแก้ไขเปลี่ยนแปลงหรือลบข้อมูลไม่สามารถทำได้ ถ้าไม่ได้กำหนดสิทธิการใช้งานจากผู้ดูแลระบบ (Admin)

2.2.3 ความพร้อมใช้งาน (Availability) หมายถึงระบบอยู่ในสภาพพร้อมที่ให้บริการตลอดเวลา แม้ระบบจะมีช่วงการหยุดให้บริการตามกำหนดการ (Planned Downtime) ก็สามารถยอมรับได้ เช่น การหยุดให้บริการเพื่อปรับปรุงหรือเปลี่ยนแปลงระบบ ระบบเครือข่ายทำงานช้าเพราะการคับคั่งในทำงานของข้อมูล

การรักษาคุณค่าพื้นฐาน C.I.A ของระบบสารสนเทศ ต้องคำนึงถึงการระบุตัวตนของผู้ใช้งานในระบบสารสนเทศ (Identification) ซึ่งมีองค์ประกอบ 3 ประการ เรียกสั้นๆว่า AAA ได้แก่ การพิสูจน์ตัวตน (Authentication) การพิสูจน์สิทธิ์ (Authorization) และการตรวจสอบการใช้ระบบ (Accountability) อธิบายได้ดังนี้

การพิสูจน์ตัวตน (Authentication) หมายถึง การตรวจสอบและการพิสูจน์สิทธิของการขอเข้าใช้ระบบของผู้ใช้บริการ จากรายชื่อผู้มีสิทธิสำหรับอุปกรณ์ไอทีรวมถึงแอพพลิเคชันทั้งหลาย

การพิสูจน์สิทธิ์ (Authorization) หมายถึง การตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพพลิเคชันนั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดหรือใช้ทรัพยากรของระบบสารสนเทศได้มากน้อยเพียงใด

การตรวจสอบได้ (Accountability) หมายถึงการบันทึกข้อมูลการใช้งานของผู้ที่เข้ามาใช้งานในระบบสารสนเทศ เช่น ชื่อผู้ใช้ เวลาเข้าระบบ การเข้าถึงระบบฐานข้อมูล เป็นต้น

2.3 ความเสี่ยงและการบริหารความเสี่ยง

2.3.1 การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและการจัดลำดับความเสี่ยง โดยประเมินจากโอกาสที่จะเกิดความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริหาร ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การประเมินความเสี่ยงมีจุดประสงค์ เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศใดๆ และมีระดับความเสี่ยงมากน้อยเพียงใด เพื่อจะได้เตรียมการป้องกันไว้ก่อนที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นจริงและทำให้องค์กรเกิดความเสียหายและสูญเสียโอกาส

2.3.2 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหนเมื่อใดและเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

2.3.3 ความเสี่ยง (Risks) หมายถึง เหตุการณ์ต่างๆ หรือการกระทำใดๆที่อาจจะเกิดขึ้นซึ่งเป็นภัยคุกคามและความเสียหายเกิดขึ้น โดยใช้ประโยชน์จากจุดอ่อนด้านใดด้านหนึ่งที่มีอยู่ เมื่อเกิดขึ้นจะส่งผลให้เกิดความเสียหายต่อองค์กร โดยจะส่งผลกระทบด้านความมั่นคงปลอดภัยอาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหายทั้งที่เป็นตัวเงินและ

ไม่เป็นตัวเงิน หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายองค์กร จุดอ่อน (Vulnerability) คือ ช่องโหว่ที่มีโดยจุดอ่อนอาจอยู่ในระบบ ได้แก่

โครงสร้างขององค์กร ในเรื่องของขั้นตอนการปฏิบัติงานรวมทั้งงานด้านบุคลากร ขาดความสามารถ การบริหารจัดการโดยไม่มีการดำเนินการด้านการรักษาความปลอดภัยของระบบสารสนเทศ

จุดอ่อนเรื่องฮาร์ดแวร์ซึ่งอาจจะรุ่นเสียบ่อยๆ และการให้บริการหลังการขายมีช่องว่างในการใช้งาน หรือมีข้อบกพร่องมาจากโรงงาน

จุดอ่อนเรื่องซอฟท์แวร์ ซึ่งอาจมีข้อบกพร่องมาจากโรงงาน ซึ่งจุดอ่อนในตัวมันเองมักไม่ก่อให้เกิดอันตราย ถ้าไม่มีภัยคุกคาม (Threat) นำมา เช่น ถ้าไม่ล็อคประตู แล้วแถวนั้นไม่มีโจรของก็ไม่หาย

2.3.4 เหตุการณ์ความเสี่ยง (Risk event) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศขององค์กร เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกขโมยซึ่งอาจทำให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสีย

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

2.3.6 แผนการลดความเสี่ยง (Risk treatment plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานเพื่อพิจารณาอนุมัติก่อนดำเนินการหรือดำเนินการเร่งด่วน

2.3.7 ภัยคุกคาม (Threat) คือเรื่องในทางลบต่อองค์กร ที่ยังไม่ได้เกิดขึ้นจะเกิดขึ้นก็ต่อเมื่อมีจุดอ่อนเป็นตัวนำ ในที่นี้ภัยคุกคามต่อระบบสารสนเทศ เช่น ไวรัส ข้อมูลถูกแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต DoS (Denial of Service) ข้อมูลไม่สามารถดึงขึ้นมาใช้งานได้ เป็นต้น

2.3.8 การจัดการความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้การบริหารจัดการด้านความเสี่ยงต่างๆ ในด้านการวางแผนจัดการองค์กร การบังคับบัญชา และการควบคุมการปฏิบัติงานขององค์กร เพื่อลดผลเสียหายของความเสี่ยงที่เกิดขึ้นกับองค์กร ทั้งนี้เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ตามที่กำหนดในการบริหารความเสี่ยง จะต้องมีต้นทุนทรัพยากรและบุคคล ดังนั้นจะต้องคำนึงถึงผลประโยชน์ที่จะได้รับด้วยว่าคุ้มค่าหรือไม่ ในการลดความเสี่ยงเหล่านั้นเพราะเหตุว่าความเสี่ยงนั้นมีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งการบริหารจัดการความเสี่ยงแบ่งได้เป็น 4 แนวทางหลัก คือ การยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การยกเลิกความเสี่ยงและการถ่ายโอนความเสี่ยง

การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) หมายถึง การบริหารปัจจัยภายในได้แก่ กระบวนการดำเนินงานและการควบคุมกิจกรรมต่างๆ เพื่อลดความเสี่ยงที่จะเกิดความเสียหายให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมาย ทั้งในด้านกลยุทธ์การปฏิบัติตามกฎระเบียบ การเงินและชื่อเสียงขององค์กรเป็นสำคัญ โดยได้รับการสนับสนุนและการมีส่วนร่วมในการบริหารความเสี่ยงจากหน่วยงานทุกระดับทั่วทั้งองค์กร

การควบคุม (Control) หมายถึง นโยบายแนวทางหรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อป้องกันการควบคุมเพื่อตรวจพบ การควบคุมเพื่อการแก้ไขและการควบคุมเพื่อการชี้แนะ

2.3.9 การวิเคราะห์ความเสี่ยง (Risk Analysis) หมายถึง การบริหารปัจจัยและกิจกรรมต่างๆ ที่อาจควบคุมได้ รวมทั้งกระบวนการดำเนินการต่าง ๆ เพื่อลดมูลเหตุของโอกาสที่ทำให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยงและผลกระทบที่เกิดขึ้นอยู่ในระดับที่ สามารถรับได้ประเมินได้ควบคุมได้และตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายขององค์กร

ประเมินความเสี่ยง (Risk Assessment) เป็นการประเมินความเสี่ยงขององค์กรว่ามีวัตถุประสงค์อะไร และมีความเสี่ยงอะไรบ้าง ที่ทำให้ไม่บรรลุวัตถุประสงค์และความเสี่ยงนั้นมีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยงและหาแนวทางการควบคุม (กิจกรรมที่ปฏิบัติ)เพื่อป้องกันหรือลดความเสี่ยงนั้นๆ

การระบุปัจจัยเสี่ยง (Risk Identification) ทั้งนี้จะต้องศึกษาวัตถุประสงค์และเป้าหมายขององค์กร ซึ่งจะสอดคล้องกับภารกิจ (Mission) ซึ่งแบ่งเป็น 2 ระดับ คือ

1) วัตถุประสงค์ระดับองค์กร (Entity – Level Objectives) เป็นวัตถุประสงค์ตามแผนกลยุทธ์ขององค์กร หรือแผนปฏิบัติราชการ 4 ปี (พ.ศ. 2548 – 2551)

2) วัตถุประสงค์ระดับกิจกรรม (Activity–Ievel Objectives) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจง สำหรับแต่ละกิจกรรมในแต่ละหน่วยงาน ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การวัดและประเมินความเสี่ยง (Risk Measurement) ทั้งนี้ต้องศึกษาว่าอะไรเป็นปัจจัยเสี่ยงและมีความเสี่ยงอย่างไร ด้านการดำเนินงาน งบประมาณ กลยุทธ์ในการวิเคราะห์จะดูถึงสาเหตุ (Cause) ของการเกิดนั้นมีโอกาส (Opportunity) มากน้อยเพียงใดและเมื่อเกิดแล้วมีผลกระทบ (Effect) มากน้อยเพียงใด ซึ่งในผลกระทบจะดูในด้านการเงินผู้รับบริการบุคลากร เวลา ความสำเร็จ

การจัดลำดับความเสี่ยง (Risk Prioritization) เมื่อเทียบความเสี่ยง และโอกาสและผลกระทบแล้วจะต้องมาจัดลำดับว่าความเสี่ยงนั้น มีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยงจากมากไปหาน้อย มีขั้นตอนการวิเคราะห์ ดังนี้

1) ประเมินระดับความสำคัญของปัจจัยเสี่ยง คือปัจจัยเสี่ยงแต่ละปัจจัยหากเกิดขึ้นแล้วมีผลกระทบต่อองค์กรมากน้อยเพียงใด

2) ประเมินความเสี่ยงที่ปัจจัยเสี่ยงจะเกิดขึ้น คือ พิจารณาว่าปัจจัยเสี่ยงที่ไว้เรียงลำดับความสำคัญไว้แล้วมีโอกาสที่จะเกิดขึ้น มากน้อยเพียงใด

3) เลือกเทคนิคการวิเคราะห์ความเสี่ยงที่เหมาะสมอาจจะวิเคราะห์ในรูปตัวเลข

4) พิจารณาหาวิธีหรือกำหนดกิจกรรมการควบคุมต่างๆ เพื่อป้องกันความเสี่ยงนั้นๆ วิธีการมีหลายวิธี เช่น หลีกเลี่ยง ยอมรับ ควบคุม หรือถ่ายโอน

2.4 นโยบายความมั่นคงปลอดภัย (Security Policy)

การจัดทำมาตรฐานนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรนั้นเป็นความสำคัญอย่างยิ่งที่ต้องให้ความสำคัญ ต้องจัดทำให้สอดคล้องกับภารกิจหลัก ข้อกำหนดทางธุรกิจ ข้อกฎหมายและระเบียบปฏิบัติขององค์กร โดยต้องจัดทำเป็นนโยบายลายลักษณ์อักษร

ที่ได้รับอนุมัติจากผู้บริหารขององค์กร เพื่อเผยแพร่ให้เจ้าหน้าที่ในหน่วยงานทุกคนปฏิบัติตาม รวมทั้งให้หน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

2.4.1 โครงสร้างด้านความมั่นคงปลอดภัยในองค์กร (Organization of Information Security) โครงสร้างด้านความมั่นคงปลอดภัยในองค์กร (Internal organization) การบริหารและจัดการด้านความมั่นคงปลอดภัยสารสนเทศในองค์กร มีดังนี้

2.4.1.1 การให้ความสำคัญสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัย (Management Commitment to Information Security) ที่มีข้อกำหนดที่ชัดเจน และการปฏิบัติที่สอดคล้องกับการมอบหมายงานที่เหมาะสมกับบุคลากร ที่เป็นหน้าที่ความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ

2.4.1.2 การประสานงานร่วมมือกันในการสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยการกำหนดตัวแทนบุคลากรขององค์กรในการสร้างความมั่นคงปลอดภัยสารสนเทศ

2.4.1.3 การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการดำเนินงานด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร

2.4.1.4 การกำหนดกระบวนการในการอนุมัติ การใช้งานอุปกรณ์ประมวลผลในระบบสารสนเทศ

2.4.1.5 การจัดให้มีการลงนามข้อตกลงระหว่างบุคลากรกับองค์กรมิให้เปิดเผยความลับขององค์กร

2.4.1.6 การกำหนดรายชื่อและข้อมูลสำหรับการติดต่อประสานงานกับหน่วยงานอื่นด้านความมั่นคงปลอดภัยในกรณีที่จำเป็น

2.4.1.7 การกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในกลุ่มด้านความมั่นคงปลอดภัยระบบสารสนเทศ

2.4.1.8 การกำหนดให้มีการตรวจสอบการบริหารจัดการดำเนินงาน การปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบอิสระเป็นผู้ตรวจสอบตามรอบระยะเวลาที่มีกำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกับองค์กร โครงสร้างด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties) การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่ถูกเข้าถึงถูกประมวลผลหรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

2.4.1.9 การกำหนดให้มีการประเมินความเสี่ยงที่เกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก

2.4.1.10 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร

2.4.1.11 การระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่มีความจำเป็นสำหรับความมั่นคงปลอดภัยขององค์กร ระหว่างองค์กรและหน่วยงานภายนอก

2.4.2 การบริหารจัดการทรัพย์สิน (Assess management) ต้องมีการกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) การจัดทำบัญชีทรัพย์สิน (Inventory of assets) การจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ การระบุผู้เป็นเจ้าของทรัพย์สินที่เป็นส่วนสารสนเทศ (Ownership of assets) ตามที่กำหนดไว้ในบัญชีทรัพย์สิน การจัดทำกฎ ระเบียบหรือหลักเกณฑ์ที่เป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศ และทรัพย์สินที่เกี่ยวกับการประมวลผลสารสนเทศอย่างเหมาะสม

2.4.3 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical andenvironmental security) มีการป้องกันการเข้าถึงทางกายภาพโดยกำหนดบริเวณที่ไม่ได้รับอนุญาตเป็นการก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร การจัดทำบริเวณความมั่นคงปลอดภัย มีดังนี้

2.4.3.1 การจัดทำบริเวณล้อมรอบ เป็นการจัดสรรพื้นที่ กั้นบริเวณการเข้า – ออก ของสำนักงานองค์กร โดยมี รปภ.ควบคุมการผ่านเข้าออก เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

2.4.3.2 การควบคุมการเข้า – ออก ในบริเวณพื้นที่ที่ต้องการรักษาความปลอดภัยต้องอนุญาตให้ผ่าน เข้า - ออกได้เฉพาะผู้ได้รับอนุญาตเท่านั้นเพื่อเป็นการรักษาความมั่นคงปลอดภัยสำหรับสำนักงานขององค์กรและทรัพย์สิน

2.4.3.3 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และภัยธรรมชาติ

2.4.1.9 การกำหนดให้มีการประเมินความเสี่ยงที่เกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก

2.4.1.10 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร

2.4.1.11 การระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่มีความจำเป็นสำหรับความมั่นคงปลอดภัยขององค์กร ระหว่างองค์กรและหน่วยงานภายนอก

2.4.2 การบริหารจัดการทรัพย์สิน (Assess management) ต้องมีการกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) การจัดทำบัญชีทรัพย์สิน (Inventory of assets) การจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ การระบุผู้เป็นเจ้าของทรัพย์สินที่เป็นส่วนสารสนเทศ (Ownership of assets) ตามที่กำหนดไว้ในบัญชีทรัพย์สิน การจัดทำกฎ ระเบียบหรือหลักเกณฑ์ที่เป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศ และทรัพย์สินที่เกี่ยวกับการประมวลผลสารสนเทศอย่างเหมาะสม

2.4.3 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical andenvironmental security) มีการป้องกันการเข้าถึงทางกายภาพโดยกำหนดบริเวณที่ไม่ได้รับอนุญาตเป็นการก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร การจัดทำบริเวณความมั่นคงปลอดภัย มีดังนี้

2.4.3.1 การจัดทำบริเวณล้อมรอบ เป็นการจัดสรรพื้นที่ กั้นบริเวณการเข้า – ออก ของสำนักงานองค์กร โดยมี รปภ.ควบคุมการผ่านเข้าออก เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

2.4.3.2 การควบคุมการเข้า – ออก ในบริเวณพื้นที่ที่ต้องการรักษาความปลอดภัยต้องอนุญาตให้ผ่าน เข้า - ออกได้เฉพาะผู้ได้รับอนุญาตเท่านั้นเพื่อเป็นการรักษาความมั่นคงปลอดภัยสำหรับสำนักงานขององค์กรและทรัพย์สิน

2.4.3.3 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และภัยธรรมชาติ

2.4.3.4 การจัดให้มีการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคง ปลอดภัย

2.4.3.5 การจัดบริเวณสำหรับการเข้าถึงเทคโนโลยีสารสนเทศ หรือการส่งมอบผลิตภัณฑ์โดย บุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กร โดยไม่ได้รับอนุญาต การจัดบริเวณควรจัดแยกออกมาต่างหากตามความจำเป็น

2.4.4 การบริหารจัดการ ด้านการสื่อสาร และด้านการดำเนินงานของเครือข่ายสารสนเทศ (Communication and operations management) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงานเพื่อการดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศ ที่เป็นไปอย่างถูกต้องและปลอดภัยตามการปฏิบัติงาน มีดังนี้

2.4.4.1 การจัดทำคู่มือขั้นตอนปฏิบัติงาน โดยมีการปรับปรุงตามระยะเวลาและแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

2.4.4.2 กำหนดให้มีการควบคุมเปลี่ยนแปลงปรับปรุงหรือแก้ไขระบบอุปกรณ์ประมวลผลสารสนเทศ

2.4.4.3 กำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบในด้านระบบเครือข่าย

2.4.4.4 จัดให้มีการคัดแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน การบริหารจัดการการให้บริการของหน่วยงานภายนอก ซึ่งมีข้อตกลงในการรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

2.4.4.5 ข้อตกลงในการเป็นผู้ให้บริการโดยหน่วยงานภายนอกที่จัดทำขึ้นระหว่างองค์กรนั้น ข้อตกลง ต้องมีการระบุเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย ลักษณะการ ให้บริการและระดับของการให้บริการ

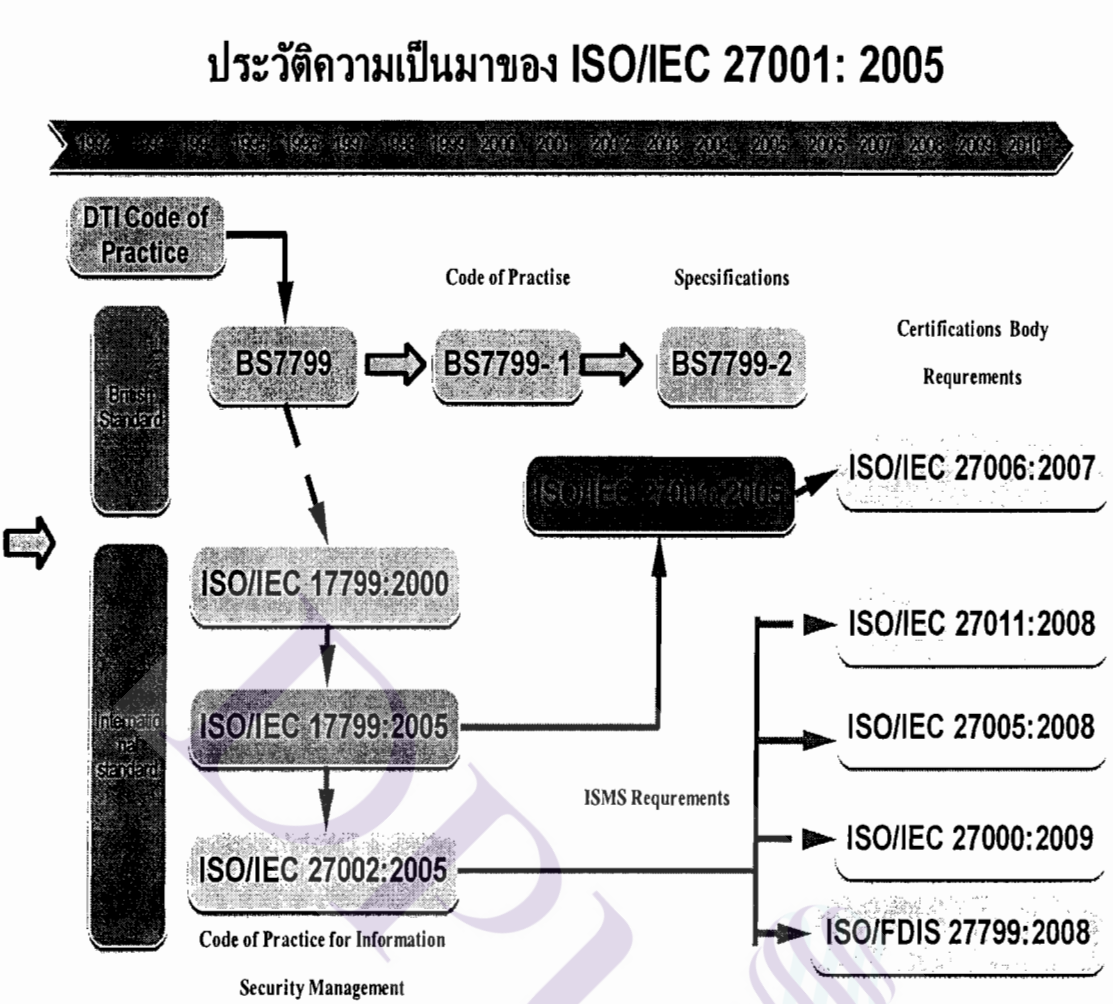
2.4.4.6 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ โดยกำหนดเงื่อนไขการให้บริการของ หน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก ได้แก่ การพัฒนาปรับปรุงระบบสารสนเทศใหม่ ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก การป้องกันโปรแกรมที่ไม่ประสงค์ดี เป็นการรักษาซอฟต์แวร์และระบบสารสนเทศให้ปลอดภัย จากการถูกทำลายโดยโปรแกรมที่ไม่ประสงค์ดี มีดังนี้ การป้องกันโปรแกรมที่ไม่ประสงค์ดีโดยการมีมาตรการสำหรับการตรวจจับ

การป้องกันและการกู้คืนในการป้องกันทรัพย์สินสารสนเทศจากโปรแกรมและที่ไม่ประสงค์ดี การป้องกันโปรแกรมชนิดเคลื่อนที่ คือโปรแกรมที่เคลื่อนที่จากหน่วยความจำหนึ่งไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง เพื่อป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

2.5 มาตรฐานด้านความมั่นคงปลอดภัย

ด้วยปัจจุบันนี้ความก้าวหน้าด้านเทคโนโลยีสารสนเทศและมีนวัตกรรมใหม่เพิ่มมากขึ้น ทำให้ทั้งภาครัฐและภาคเอกชน มีความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้นด้วยและ มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่างๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งเป็นหัวใจที่ความสำคัญของกลยุทธ์ทางธุรกิจ และท้าทายต่อความสามารถของผู้บริหารองค์กรที่รับผิดชอบในการดูแลระบบเป็นอย่างมาก ซึ่งมาตรฐานในด้านความปลอดภัยมีหลายมาตรฐาน ดังตามตัวอย่างต่อไปนี้

2.5.1 มาตรฐาน ISO/IEC 27001 : 2005 เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization) โดยเป็นมาตรฐานสากลที่มุ่งเน้นด้านการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System, ISMS) เพื่อสร้างความมั่นใจในความมีประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศขององค์กรซึ่งสามารถศึกษาได้จากประวัติความเป็นมา ดังภาพที่ 2.1



ภาพที่ 2.1 ประวัติความเป็นมามาตรฐาน ISO/IEC 27001

ที่มา : http:// www.isaca.org

ด้วยมาตรฐาน ISO/IEC 27001: 2005 มีการดำเนินการให้สอดคล้องตามข้อกำหนด ข้อกฎหมาย และระเบียบข้อบังคับต่างๆที่เกี่ยวข้องประกอบด้วย 2 ส่วน คือ

(1) ส่วนของการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งในระบบบริหารจัดการขององค์กร ซึ่งมีพื้นฐานมาจากแนวทางการจัดการความเสี่ยงของธุรกิจ (Business Risk Approach) มีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ (Information) รวมทั้งทรัพย์สินอื่นๆ ที่มีความสำคัญขององค์กร ที่นำมาใช้ ตรวจสอบ วัดผล ทบทวน บำรุงรักษา

และปรับปรุงระบบบริหารความมั่นคงปลอดภัย เพื่อให้องค์กรรอดพ้นจากภัยคุกคามต่างๆ โดยใช้หลัก Plan-Do-Check-Act

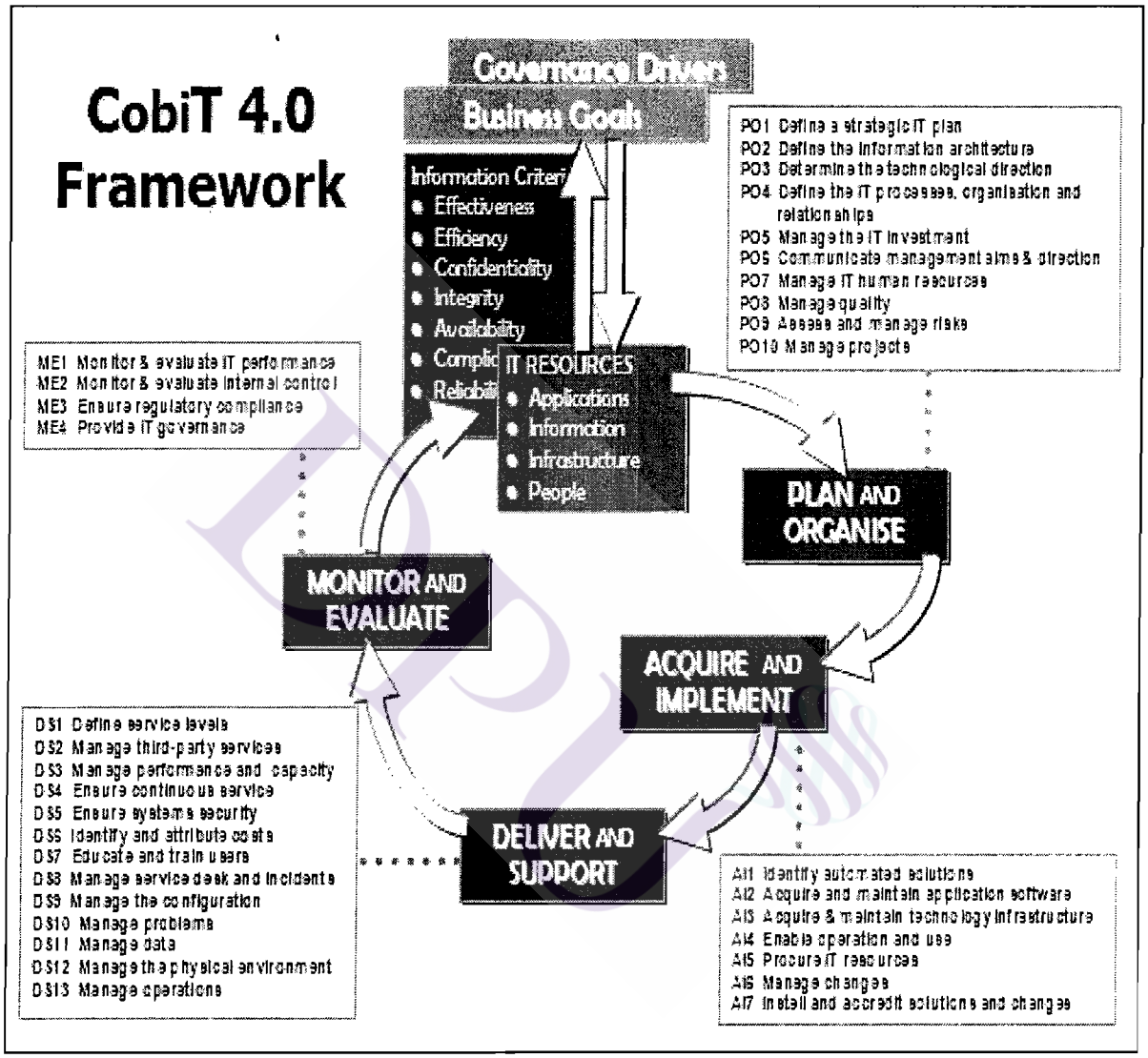
(2) ส่วนของรายการควบคุม และวัตถุประสงค์ของการควบคุม ซึ่งจะต้องกำหนดความต้องการ (Set of Requirements) ที่เกี่ยวข้องกับการจัดทำระบบให้มีความมั่นคงปลอดภัยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศได้อย่างมีประสิทธิภาพ

ทั้งนี้มาตรฐานดังกล่าว สามารถนำมาใช้ได้กับทุกๆ ประเภทขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไม่ว่าจะเป็นองค์กรขนาดใหญ่หรือขนาดย่อมก็ตามระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ เป็นส่วนหนึ่งในระบบบริหารจัดการขององค์กร เพื่อให้องค์กรรอดพ้นจากภัยคุกคามต่างๆ โดยใช้หลัก Plan-Do-Check-Act (PDCA Model) หากองค์กรใดได้จัดทำระบบตามมาตรฐานนี้ครบถ้วนตามความต้องการที่กำหนดไว้แล้ว องค์กรดังกล่าวสามารถยื่นคำขอไปยังหน่วยงานรับตรวจประเมินระบบ(Certification Body) เพื่อให้เข้ามาดำเนินการตรวจประเมินและรับรองระบบที่จัดทำขึ้นได้ ทั้งนี้ความต้องการที่องค์กรจำเป็นต้องดำเนินการเพื่อให้ได้รับการตรวจประเมินจะถูกระบุตามเงื่อนไขของมาตรฐานดังกล่าว อย่างไรก็ตามความซับซ้อนของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศที่แต่ละองค์กรพัฒนาขึ้นจะมีความแตกต่างกันไปขึ้นอยู่กับขนาดโครงสร้าง วัตถุประสงค์ความต้องการเกี่ยวกับความมั่นคงปลอดภัย รวมถึงกระบวนการทางธุรกิจ (Business Processes) ขององค์กรในส่วน Annex A ภายในมาตรฐานดังกล่าวจะระบุเกี่ยวกับมาตรการความมั่นคงปลอดภัย (Control Objective) และ Controls โดยนำมาจากมาตรฐาน ISO/IEC 17799:2005 ซึ่งเป็นอีกมาตรฐานหนึ่งที่ระบุเกี่ยวกับแนวทางในการพัฒนาระบบ (Implementation Guidance) เพื่อให้การจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศมีความมั่นคงปลอดภัยและมีประสิทธิภาพ ทั้งนี้องค์กรสามารถเลือกใช้ Control Objective และ Controls ได้ตามความเหมาะสมกับสภาพการดำเนินงานขององค์กร

2.5.2 มาตรฐาน COBIT

มาตรฐาน Cobit เป็นกระบวนการบริหารและการควบคุมระบบสารสนเทศที่ดีเพื่อบรรลุวัตถุประสงค์ขององค์กร (Business Ojective) กับ COBIT ภายใต้ IT Governance หรือกระบวนการ

บริหารและการควบคุมสารสนเทศที่ดี ที่เกี่ยวข้องกับ Data และ Integrity of the Information โดยมี KPI ที่วัดจาก Performance Measurement ที่ได้มาตรฐานที่เกี่ยวเนื่องกัน ดังภาพที่ 2.2



ภาพที่ 2.2 โครงสร้างกรอบมาตรฐาน COBIT

ที่มา : http :// www.isaca.org , http:// www.itgi.org

Cobit จะให้ความสำคัญของข้อมูลและระบบสารสนเทศที่ดีมีผลต่อการบริหารและการตรวจสอบเป็นอย่างยิ่ง และได้ให้ความสำคัญในกรอบการบริหารความเสี่ยงที่เกี่ยวข้องกับ

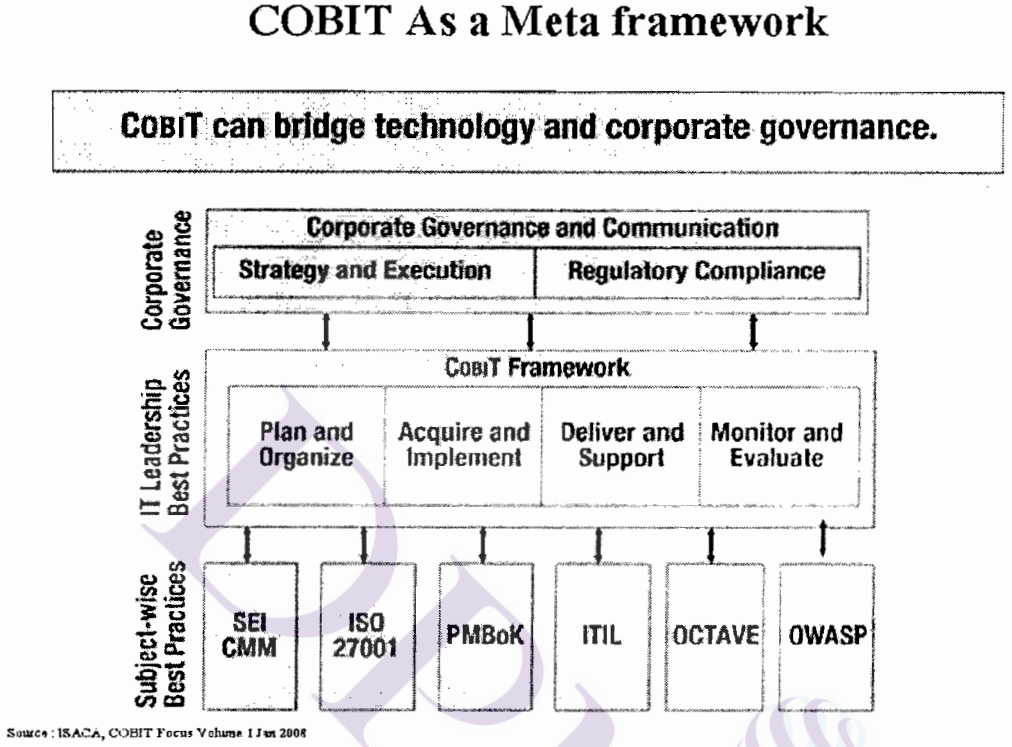
ความสำคัญที่เกี่ยวข้องกับ Data และ Integrity of the Information จำเป็นอย่างยิ่งที่เราควรจะมีจุดยืนร่วมกันนั่นคือ การใช้ Best Practice (ถ้ามี) หรือใช้ Standard โดยเฉพาะอย่างยิ่งที่เป็น International Standard โดยมี KPI ที่วัดจาก Performance Measurement ที่ได้มาตรฐานที่เกี่ยวเนื่องกัน รายละเอียดตามภาพที่ 2.3

ภาพที่ 2.3 COBIT As a Meta framework

ที่มา : http :// www.isaca.org

รายละเอียดของ Cobit 5 มีการปรับปรุงในส่วนของ "Process Model" โดยให้สอดคล้องกับมาตรฐานISO 38500:2008 "Corporate Governance of Information Technology โดยยึดหลัก 3 กระบวนการ ได้แก่ ประเมิน (Evaluate) กำกับ (Direct) และเฝ้าระวัง (Monitor) ซึ่ง

ครอบคลุมใน 3 กระบวนการโดยมีการปรับปรุงจาก CobiT 4.1 ซึ่งประกอบด้วย 4 โดเมน รายละเอียด ตามภาพที่ 2.4



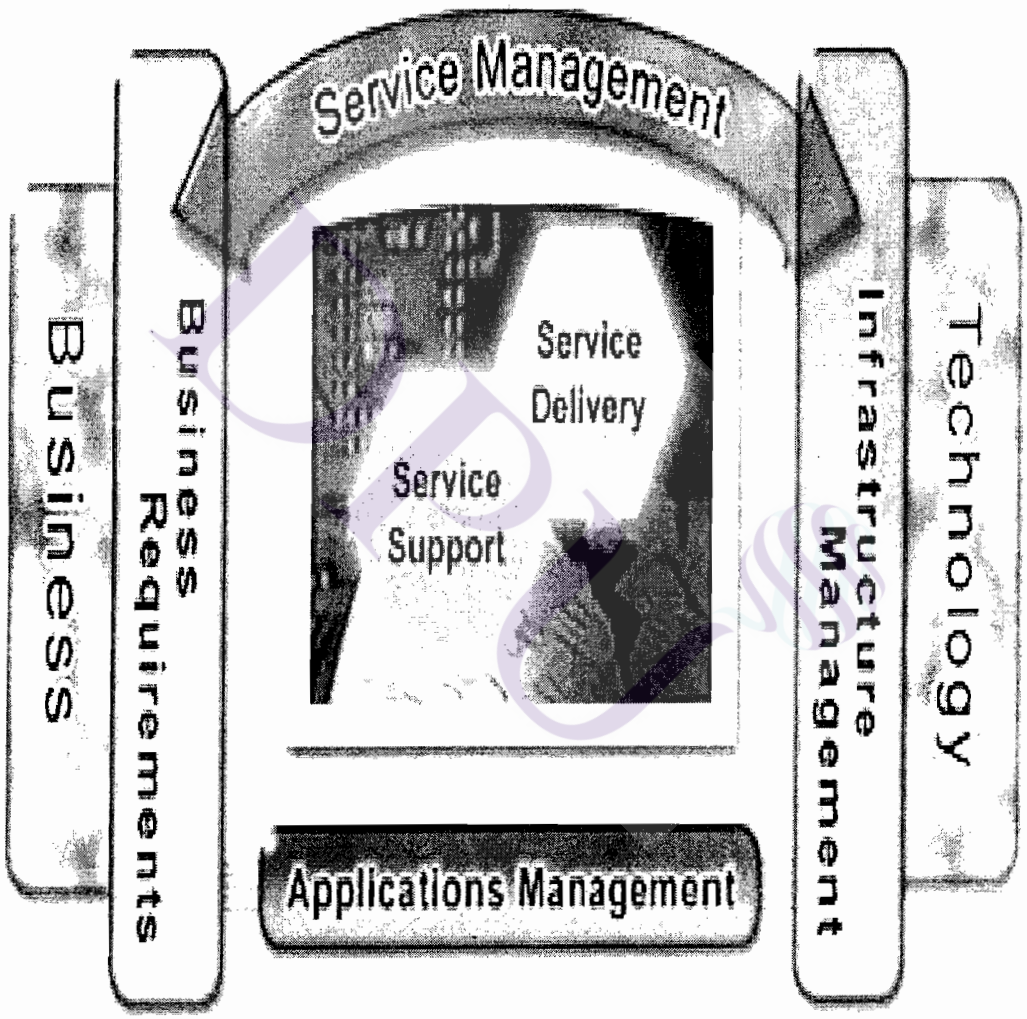
ภาพที่ 2.4 CobiT 5 New Design

ที่มา : http :// www.isaca.org

Cobit 5 มีการปรับปรุงจาก CobiT 4.1 ซึ่งประกอบด้วย 4 โดเมน ได้แก่ "Plan and Organize", "Acquire and Implement", "Deliver and Support" และ "Monitor and Evaluate" มาเป็น "Align, Plan and Organize", "Build, Acquire & Implement", "Deliver and Support" และ "Monitor & Assess" อีกทั้งใน CobiT 5 ยังมีการนำ Standard และ Best Practice มาใช้อ้างอิง เช่น ITIL V3, ISO 27000 Series, ISO 20000, ISO 38500:2008, TOGAF V9 และ ISO 9000:2008 การนำ CobiT 5 มาใช้ได้ผลดี ต้องคำนึงถึงวัฒนธรรมขององค์กรด้วย เพราะจะต้องเกิดการเปลี่ยน เรื่องคือ "Risk Governance"; "Value Governance" และ "Resource Governance" เป็นต้น

2.5.3 มาตรฐาน ITIL

มาตรฐาน ITIL นั้นเป็นมาตรฐานด้านความปลอดภัยระบบสารสนเทศจากประเทศอังกฤษมีวัตถุประสงค์ ในการสร้าง Best Practices สำหรับกระบวนการของ IT Service Delivery และSupport แต่ไม่ได้เป็นการกำหนด Framework การควบคุมของระบบ ITIL จะมุ่งเน้นแนวทางและวิธีการในการปฏิบัติ มีขอบเขตงานเพียงแค่ IT service Management ดังภาพที่ 2.5



ภาพที่ 2.5 มาตรฐาน ITIL

ที่มา : http:// www.isaca.org/Itil

มาตรฐาน ITIL เน้นการสร้าง Best Practices สำหรับกระบวนการ IT Servive Delivery และ Support เพื่อเสนอแนวทางการและวิธีการในการปฏิบัติ มีขอบเขตงานเพียงแค่ IT Service Management และมีวัตถุประสงค์ ในรายละเอียดของกระบวนการทำงานให้ฝ่ายสารสนเทศ และ Service Management เป็นผู้นำไปใช้ซึ่งได้จัดแบ่งกระบวนการเทคโนโลยีสารสนเทศ ดังนี้

1) Security Management เป็นการบริหาร IT โดยการสร้างข้อกำหนด ตรวจสอบผล และควบคุมรักษาความปลอดภัยของระบบด้านข้อมูลและบริการขององค์กร เมื่อมีผู้เกี่ยวข้องเข้าสู่ระบบเทคโนโลยีสารสนเทศ

2) Change Management คือ การบริหารการเปลี่ยนแปลง เพื่อกำหนดวิธีการและแนวปฏิบัติและกระบวนการที่มีมาตรฐาน เพื่อจัดการด้าน IT ให้ลดผลกระทบ จากปัญหาเนื่องจากการเปลี่ยนแปลงเพื่อพัฒนาคุณภาพของบริการ

3) Release Management คือการบริหารกระบวนการนำระบบผู้ใช้สามารถใช้ระบบงานต่างๆ ได้โดยเริ่มต้น จากการวางแผน การเตรียมเอกสารของระบบเผยแพร่และการจัดอบรมให้แก่ลูกค้า เพื่อให้เกิดความมั่นใจในระบบเทคโนโลยีสารสนเทศที่ได้พัฒนาขึ้น

4) Incident Management หรือเรียกว่า Help Desk หรือ Service Desk เป็นกระบวนการแก้ไขระบบ ให้สามารถกลับมาใช้งานได้ปกติ ซึ่งจะแก้ไขก็ต่อเมื่อมีการแจ้งปัญหาจากลูกค้าหรือผู้ใช้งานโดย IT จะต้องจัดการแก้ไขปัญหาให้เสร็จสิ้นเร็วที่สุด เพื่อให้กระทบกับผู้มีส่วนเกี่ยวข้องน้อยที่สุด

5) Problem Management คือการบริหาร IT โดยการคิดเชิงรุก (Proactive) เพื่อลดปัญหาของระบบที่เกิดจาก การแจ้งของผู้ใช้งาน มุ่งเน้นการวิเคราะห์ไปที่ต้นเหตุของปัญหา เทคนิคในการจัดการปัญหา การควบคุมความผิดพลาดที่อาจเกิดขึ้นในอนาคต

6) Service-Level Management คือการบริหารการให้บริการระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและเป็นไปตามความต้องการของลูกค้า หรือผู้ที่มีส่วนเกี่ยวข้องในระบบด้านต่างๆ โดย IT สามารถให้คำมั่นในการดำเนินงาน เพื่อการบริการที่มีศักยภาพแก่ลูกค้าได้

7) Availability Management เป็นการบริหารระบบเทคโนโลยีสารสนเทศ เพื่อแสดงเปอร์เซ็นต์ความถูกต้องของข้อมูล จากระบบต่างๆ ที่องค์กรบริการแก่ลูกค้า โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศ มีหน้าที่ในการกำหนดลักษณะการใช้งาน ตรวจสอบ การเข้าสู่ระบบของลูกค้าและควบคุมการบริการให้เกิดประสิทธิภาพสูงสุดแก่ลูกค้า

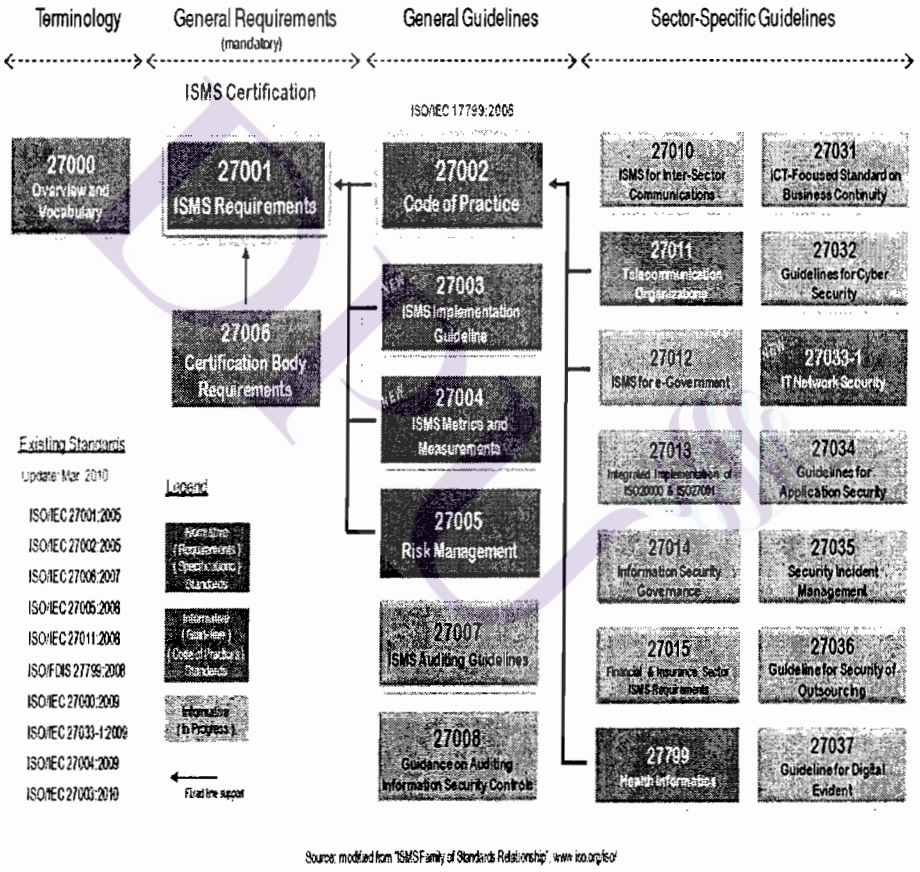
8) Configuration Management เป็นกระบวนการของการวางแผน เพื่อรองรับการบริหารการเปลี่ยนแปลงซึ่งจะเป็น การกำหนด ควบคุม และตรวจสอบความถูกต้องของ Configuration Item หรือ CI ให้มี ความทันสมัย และถูกต้องอยู่เสมอ เพื่อการบริหารงานบริการเทคโนโลยีสารสนเทศ (IT) ที่มีความซับซ้อนและยุ่งยากให้สำเร็จทำให้องค์กรมีประสิทธิภาพสูงสุด รองรับการเปลี่ยนแปลงทางกลยุทธ์และขับเคลื่อนธุรกิจ ด้วย "'งานบริการไอทีที่มีคุณภาพ" คือ การทำให้ไอทีสอดคล้องกับเป้าหมายธุรกิจ โดยให้ส่วนไอทีสามารถทำงานแบบ "หน่วยงานที่พร้อมปรับเปลี่ยนตลอดเวลา" ซึ่งเป็นปัจจัยกลยุทธ์เชิงรุกที่สำคัญที่ ส่งผลต่อความสำเร็จขององค์กรให้มีความพร้อมที่จะมุ่งสู่ความเป็นเลิศในการดำเนินงานด้านไอทีได้ โดยมี ITIL เป็นเครื่องมือการพัฒนาที่สำคัญ ในการรวบรวมกระบวนการพื้นฐานและต้นแบบที่เหมาะสมรวมถึงการเชื่อมต่อระบบรวมเข้ากัน เ พื่อการพัฒนาอย่างต่อเนื่อง แ ละการสร้างคุณค่าโดยการปรับปรุงประสิทธิภาพการดำเนินงานที่ยังสามารถลดค่าใช้จ่ายในการดำเนินงานไอทีพร้อมกัน ในการดำเนินงานบริการ (Service Operations)

2.6 มาตรฐานที่เลือกใช้

2.6.1 มาตรฐาน ISO/IEC 27001 : 2005

เป็นมาตรฐานเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งจะกำหนดความต้องการ (Set of Requirements) เกี่ยวกับการจัดทำระบบให้มีความมั่นคงปลอดภัย ซึ่งมีวัตถุประสงค์ เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างมีประสิทธิภาพ โดยสามารถนำมาประยุกต์ได้กับทุกๆ ประเภทขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัย ในการบริหารจัดการขององค์กรซึ่งมีพื้นฐานมาจากแนวทางการจัดการความเสี่ยงของธุรกิจ (Business RiskApproach) ที่มีความสำคัญขององค์กร เพื่อนำมาใช้ตรวจสอบ วัดผล ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารความมั่นคงปลอดภัยให้องค์กรรอดพ้นจากภัยคุกคามต่างๆ โดยใช้มาตรฐาน ISO/IEC27001:2005 ในการดำเนินงานตามมาตรฐานนี้ จะมีผลต่อการปรับโครงสร้างและขนาด หน่วยงานต่างๆในองค์กรที่เกี่ยวข้องต้องเข้าร่วมดำเนินการ มีการสำรวจความเสี่ยงด้านความปลอดภัยสารสนเทศ และดำเนินการสร้างตัวควบคุมการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศที่ต้องการโดยมีทิศทางและคำแนะนำที่

เกี่ยวข้องในการปรับเปลี่ยนด้านความปลอดภัย มีการปรับเปลี่ยนตลอดซึ่งแนวคิด ISMS ต้องดำเนินการปรับปรุงและให้ข้อมูลอย่างต่อเนื่อง โดยใช้แนวคิดของ Deming เรียกว่า Plan-Do-Check-Act เพื่อกำาหนดการปรับเปลี่ยนต่อภัยคุกคามที่เกิด ช่องโหว่ และผลกระทบต่อเหตุการณ์ผิดปกติ มาตรฐานนี้ได้ดำเนินการโดยความร่วมมือระหว่าง ISO กับ IEC หรือเรียกว่า ISO/IEC JTC1 (Joint Technical Committee 1) โดยได้มีการพัฒนาและปรับปรุงมาตรฐานมาอย่างต่อเนื่องจนถึงปัจจุบันมีการนำเสนอการพัฒนาปรับปรุงอย่างต่อเนื่อง ได้ตาม Control Objective และ Controls ได้ตามความเหมาะสมกับสภาพการดำเนินงานขององค์กร ดังภาพที่ 2.6

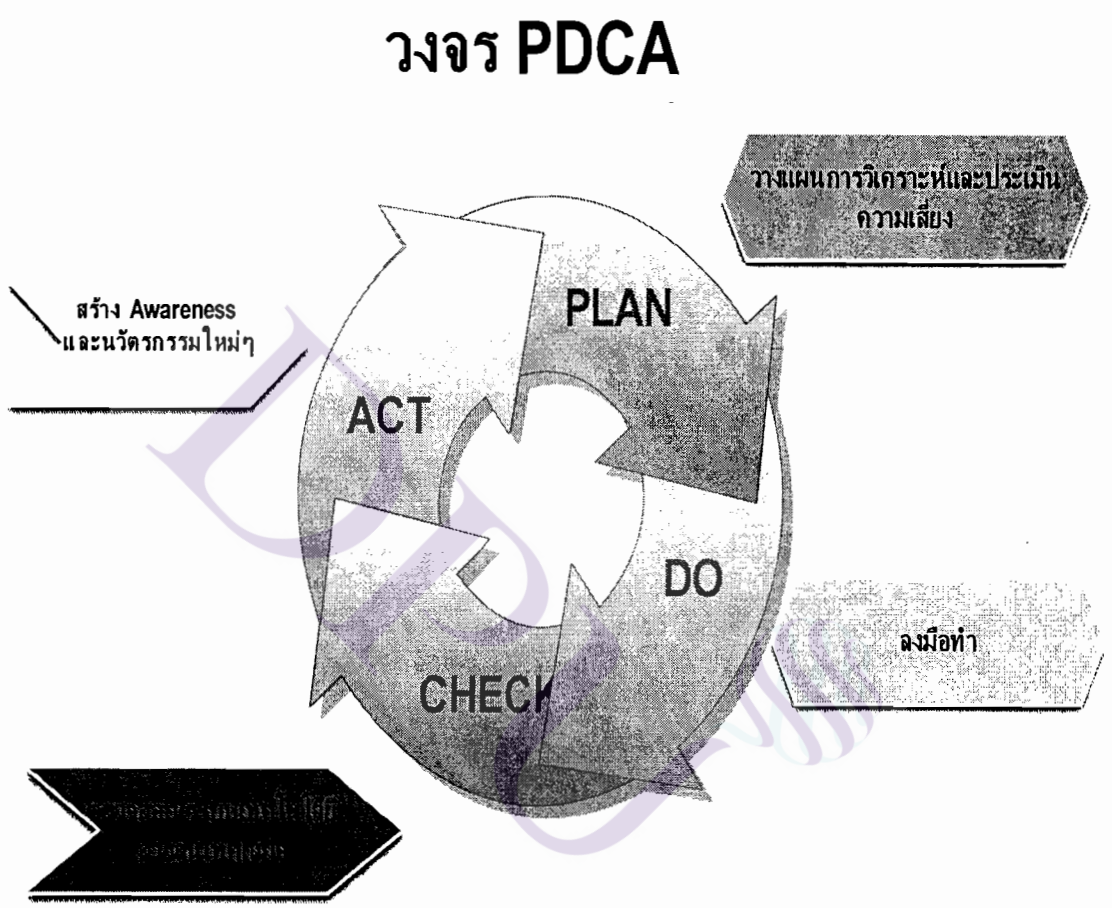


ภาพที่ 2.6 การพัฒนาปรับปรุงต่อเนื่องมาตรฐาน ISO ตาม Control Objective

ที่มา : http:// www.iso27001certificate.com

2.6.2 วงจร PDCA (Plan –Do- Check-Act)

PDCA เป็นกิจกรรมพื้นฐานในการพัฒนาประสิทธิภาพและคุณภาพของการดำเนินงานด้านบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 โดยหัวใจหลักสำคัญของกระบวนการประกอบด้วย 4 ขั้นตอนหลักรายละเอียด ดังภาพที่ 2.7



ภาพที่ 2. 7 หัวใจหลักกระบวนการ PDCA

ที่มา : บทความ Plan-Do-Check-Act [2]

หัวใจหลักของกระบวนการ PDCA ประกอบด้วย การวางแผน (Plan) การดำเนินการตามแผน (Do) การเฝ้าระวังและติดตามการดำเนินการตามแผน (Check) การดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act) แม้ในข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001 ซึ่งคือข้อ 4.2.1

Establish the ISMS (เทียบเท่ากับ Plan) 4.2.2 Implement and operate the ISMS (เทียบเท่ากับ Do) 4.2.3 Monitor and review the ISMS (เทียบเท่ากับ Check) และข้อ 4.2.4 Maintain and Improve the ISMS (เทียบเท่ากับ Act)

ตามลำดับจะมีรายละเอียดมากมาย แต่เมื่อพิจารณาแล้วหัวใจหลักของทั้ง 4 ข้อนั้นคือ การประเมินความเสี่ยงและการจัดทำแผนการลดความเสี่ยง (หรือก็คือขั้นตอนการวางแผน--Plan) การดำเนินการตามแผนการลดความเสี่ยง (หรือก็คือขั้นตอนการดำเนินการตามแผน -- Do) การเฝ้าระวังและติดตามการดำเนินการตามแผน (หรือก็คือขั้นตอนการเฝ้าระวังและติดตามการดำเนินการตามแผน--Check) และการดำเนินการเพิ่มเติมตามที่เห็นสมควร (หรือก็คือขั้นตอนการดำเนินการเพิ่มเติมตามสมควร--Act) เช่น กรณีที่พบว่ายังมีความเสี่ยงที่ต้องบริหารจัดการอยู่ขออธิบายคำจำกัดความที่สำคัญๆ ที่เกี่ยวข้องกับความเสี่ยงที่ใช้ในบทความ ดังนี้

การวางแผน (Plan)

เป็นขั้นตอนแรก ที่มองถึงการกำหนดเป้าหมายหรือวัตถุประสงค์ในการดำเนินงาน วิธีการ และขั้นตอนที่จำเป็นเพื่อให้การดำเนินงาน บรรลุเป้าหมายในการวางแผนจะต้องทำความเข้าใจกับ เป้าหมาย วัตถุประสงค์ให้ชัดเจน เป้าหมายที่กำหนดต้องเป็นไปตามนโยบาย วิสัยทัศน์ และพันธกิจ ขององค์กร การวางแผน ต้องกำหนดมาตรฐา วิธีการทำงานหรือ นำไปใช้เป็นเกณฑ์ในการตรวจสอบได้ว่า การปฏิบัติงานเป็นไปตามมาตรฐานที่ได้ระบุไว้ในแผนหรือไม่ ตัวอย่างเช่น ขั้นตอนที่หนึ่งคือการวางแผนหรือ Plan ซึ่งเป็นการประเมินความเสี่ยงที่มีต่อทรัพย์สินสารสนเทศ ซึ่งส่วนใหญ่จะหมายถึงทรัพย์สินสารสนเทศใหม่ที่กำลังนำเข้ามาสู่การใช้งาน ที่จะต้องมีการประเมินความเสี่ยงเพื่อเตรียมการป้องกันก่อนเริ่มต้นใช้งานทรัพย์สินใหม่เหล่านั้น เช่น กรณีมีโครงการจัดทำระบบงาน E-mail ที่ต้องดำเนินการให้แล้วเสร็จในปีงบประมาณนี้ ทรัพย์สินสารสนเทศใหม่ของโครงการนี้อาจประกอบด้วย ระบบงาน E-mail ฮาร์ดแวร์ของระบบงาน E-mail และซอฟต์แวร์ต่างๆ ของระบบงาน E-mail เช่น ระบบปฏิบัติการ Windows 2008 เป็นต้น

DO (ปฏิบัติ)

เป็นการปฏิบัติให้เป็นไปตามแผนที่ได้กำหนดไว้ ซึ่งต้องศึกษาแผนงาน ข้อมูลและเงื่อนไขต่างๆ ของแต่ละบริบท ที่ได้กำหนดไว้และจะต้องเก็บรวบรวมและบันทึกข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานไว้ด้วยเพื่อใช้เป็นข้อมูลในการดำเนินงานในขั้นตอนต่อไป

Check (ตรวจสอบ)

เป็นกิจกรรมที่มีดี มีการทบทวนเพื่อประเมินผลว่ามีการปฏิบัติงานตามแผน หรือไม่มีปัญหาเกิดขึ้นในระหว่างการปฏิบัติงานหรือไม่ ขั้นตอนนี้มีความสำคัญ เนื่องจากในการดำเนินงานใดๆ มักจะเกิดปัญหาแทรกซ้อนที่ทำให้การดำเนินงานไม่เป็นไปตามแผนอยู่เสมอ ซึ่งเป็นอุปสรรคต่อประสิทธิภาพและคุณภาพของการทำงาน การติดตามการตรวจสอบ และการประเมินปัญหาจึงเป็นสิ่งสำคัญที่ต้องกระทำควบคู่ไปกับการดำเนินงาน เพื่อจะได้ทราบข้อมูลที่เป็นประโยชน์ในการปรับปรุงการดำเนินงานต่อไป และการประเมินการปฏิบัติงานจะต้องตรวจสอบด้วย ว่าการปฏิบัตินั้น เป็นไปตามมาตรฐานที่กำหนดไว้หรือไม่ทั้งนี้เพื่อเป็นประโยชน์ต่อการพัฒนาคุณภาพของงาน

Act (การปรับปรุง)

กิจกรรมที่มีขึ้นเพื่อแก้ไขปัญหาที่เกิดขึ้นหลังจากได้ทำการตรวจสอบแล้ว การปรับปรุงคุณภาพของงาน เพื่อนำไปสู่การกำหนดมาตรฐานของวิธีการทำงานที่ต่างจากเดิมเมื่อมีการดำเนินงานตามวงจร PDCA ในรอบใหม่ข้อมูลที่ได้จากการ ปรับปรุงจะช่วยให้การวางแผนมีความสมบูรณ์และมีคุณภาพ การบริหารงานในระดับต่างๆ ทุกระดับ จนถึงการบริหารโครงการต่างๆย่อมมีกิจกรรม PDCA เกิดขึ้นเสมอ ในแต่ละองค์กรจะมีวงจร PDCA อยู่เสมอ หลายๆกระบวนการทำงานก็ได้เป็นแผนงาน (P) แผนงานวงใหญ่สุดนี้ อาจครอบคลุมระยะเวลาต่อเนื่องกันหลายปีจึงจะบรรลุผลการจะผลักดันให้วิสัยทัศน์และแผนยุทธศาสตร์ ขององค์กรปรากฏเป็นจริงได้จะต้องปฏิบัติ (P)โดยนำแผนยุทธศาสตร์มากำหนดเป็นแผนการปฏิบัติงาน ปฏิบัติงานประจำปีจะก่อให้เกิดวงจร PDCA ของหน่วยงานขึ้นใหม่ ทั้งหมดจะรวมกันเป็น (D) ขององค์กร นั้น ซึ่งองค์กรจะต้องทำการติดตามตรวจสอบ (C) และแก้ไขปรับปรุงจุดที่เป็นปัญหาหรืออาจต้องปรับแผนใหม่ในแต่ละปี (A) เพื่อให้วิสัยทัศน์และแผนยุทธศาสตร์ระยะยาวนั้นปรากฏเป็นจริงและ ทำให้การดำเนินงานบรรลุเป้าหมายและวัตถุประสงค์รวมขององค์กร ได้อย่างมีประสิทธิภาพและมีคุณภาพ

2.6.3 ผลประโยชน์หลักจากการใช้มาตรฐาน ISO27001:2005

2.6.3.1 เนื่องจาก การมีข้อมูลและระบบการจัดเก็บข้อมูล ที่มีความปลอดภัยเที่ยงตรงและพร้อมใช้งานเสมอนั้นย่อมช่วยสร้างความได้เปรียบทางการแข่งขัน สร้างผลกำไร และสร้างโอกาสทางการธุรกิจ

2.6.3.2 สอดคล้องกับกฎหมาย ตามพระราชบัญญัติ

2.6.3.3 สร้างความมั่นใจให้กับผู้รับบริการและผู้มีส่วนได้เสียซึ่งสามารถรับประกันความต่อเนื่องในการทำธุรกิจระหว่างคู่ค้าและผู้รับบริการ

2.6.3.4 จากการวิเคราะห์และประเมินความเสี่ยง มีการแยกแยะภัยคุกคามของข้อมูล การรับรู้จุดอ่อนและความเป็นไปได้ของความเสี่ยง และ จากการพิจารณาอย่างละเอียดของผลกระทบที่จะเกิด ย่อมทำให้เป็นผลดีกับการให้บริการแก่ประชาน และเลือกทำโครงการที่มีความจำเป็นต่อการลงทุนที่จะก่อประโยชน์และคุ้มค่าที่สุดประหยัดงบประมาณ

2.7 เครื่องมือที่ใช้ในการวิเคราะห์

มาตรฐาน ISO/IEC 27001 :2005 โดยการนำมาใช้ในการวิเคราะห์และประเมินความเสี่ยงเพื่อการบริหารจัดการระบบสารสนเทศ เป็นการแยกแยะภัยคุกคาม การจัดกลุ่มของข้อมูลและการตรวบสอบจุดอ่อนของระบบและความเป็นไปได้ของความเสี่ยง อีกทั้งมีการบริหารจัดการความเสี่ยงที่เหมาะสมให้กับองค์กรได้

2.8 ผลงานวิจัยที่เกี่ยวข้อง

ธีรวัฒน์ ขวาทอง (2553) วิทยาศาสตร์มหาบัณฑิต มหาวิทยาลัยมหานครศึกษาเรื่องนโยบายความมั่นคงปลอดภัยและการประเมินความเสี่ยงให้กับองค์กร งานวิจัยนี้ได้รวบรวมข้อมูลด้านสารสนเทศขององค์กรและวิธีการดำเนินงานด้านความมั่นคงปลอดภัยและการประเมินความเสี่ยงให้กับองค์กร มีการกำหนดการประเมินความเสี่ยงที่เกิดขึ้นและการวางแผนแก้ไขปัญหาที่เป็นจุดอ่อนและความเป็นไปได้ของความเสี่ยง เพื่อจัดทำมาตรฐานและขั้นตอนและนโยบายความมั่นคงปลอดภัยให้สอดคล้องกับมาตรฐาน ISO/IEC 27001 ซึ่งเป็นงานวิจัยที่ดี โดยได้นำมาตรฐาน ISO/IEC 27001 โดยมาใช้ในการดำเนินงาน

กำธน สุทธิรักษ์ศิริ (2553) วิทยาศาสตร์มหาบัณฑิต มหาวิทยาลัยมหานครได้ศึกษาเรื่อง การวางแผนรองรับสถานการณ์ฉุกเฉินและเหตการณ์ที่ไม่คาดคิด โดยการผสมผสานระหว่างมาตรฐาน ISO/IEC 27001 และแนวทางการดำเนินงานของ NIST กรณีศึกษาฝ่ายเทคโนโลยีสารสนเทศ งานวิจัยเรื่องนี้ได้ศึกษา แนวทางในการรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับหน่วยงานใดๆและก่อให้เกิดความเสียหายต่อองค์กร และรวบรวมแนวทาง การดำเนินงานต่างๆ

หน่วยงานใดๆและก่อให้เกิดความเสียหายต่อองค์กร และรวบรวมแนวทาง การดำเนินงานต่างๆ เพื่อให้นำมาประยุกต์ใช้ให้เกิดประโยชน์โดยวางแผนป้องกัน เตรียมการทั้งด้านเทคนิคและด้านปฏิบัติการเพื่อลดผลกระทบต่อองค์กรหากเกิดขึ้น

ไพฑูรย์ อ๊อสวงศ์ (2553) วิทยาศาสตร์มหาบัณฑิต มหาวิทยาลัยมหานคร ศึกษาเรื่อง โครงการประยุกต์กระบวนการ ITIL กับการบริการด้านเทคโนโลยีสารสนเทศ งานวิจัยเรื่องนี้ได้ศึกษาเทคนิคในการบริหารงานและนำมาปรับปรุงแนวทางในการพัฒนากระบวนการในการให้บริการโดยมีเป้าหมายเพื่อสร้าง Best Practise ให้แก่หน่วยงาน ซึ่งนำไปสู่การเพิ่มประสิทธิภาพในการให้บริการและสร้างมาตรฐานที่ดีในการดำเนินงานต่างๆ เช่น การกำหนดกรอบของปัญหา การกำหนดบทบาทหน้าที่ความรับผิดชอบ การติดตามงาน เพื่อให้นำมาประยุกต์ใช้ให้เกิดประโยชน์ มากที่สุดทั้งในด้านเทคนิคและด้านปฏิบัติการเพื่อสร้างความพึงพอใจแก่ผู้รับบริการ

กฤษฎา แก้วผุดผ่อง (2551) วิทยาศาสตร์มหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์ได้ศึกษาเรื่อง ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินในองค์กรตามมาตรฐานสากล BS 7799 กรณีศึกษา สำนักหอสมุด มหาวิทยาลัยมหิดล งานค้นคว้าอิสระเรื่องนี้ได้ศึกษา เทคนิคในการบริหารงานและนำมาปรับปรุงแนวทางในการพัฒนากระบวนการในการให้บริการโดยมีเป้าหมายเพื่อสร้าง Best Practise ให้แก่หน่วยงานให้นำไปสู่การเพิ่มประสิทธิภาพในการให้บริการและสร้างมาตรฐานที่ดีในการดำเนินงานต่างๆ เช่น การกำหนดกรอบของปัญหา การกำหนดบทบาทหน้าที่ความรับผิดชอบ การติดตามงาน เพื่อให้นำมาประยุกต์ใช้ให้เกิดประโยชน์มากที่สุด ทั้งในด้านเทคนิคและด้านปฏิบัติการเพื่อสร้างความพึงพอใจแก่ผู้รับบริการ

บทที่ 3
วิธีการและขั้นตอนการดำเนินงาน

ในการจัดทำโครงงานสารนิพนธ์จะกล่าวถึง วิธีการและขั้นตอนการดำเนินงานในการศึกษาวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค เพื่อให้สอดคล้องกับวัตถุประสงค์ของโครงงาน ที่ได้กำหนดไว้ ซึ่งรายละเอียดขั้นตอนในการดำเนินงาน(Process) มีความสำคัญอย่างมาก ซึ่งเป็นการศึกษาวิเคราะห์ถึงปัญหาและสาเหตุความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร เพื่อต้องการทราบจุดอ่อนหรือช่องโหว่ของระบบเทคโนโลยีสารสนเทศ เพื่อจะได้หาวิธีการ จัดการแก้ปัญหาและพัฒนาปรับปรุงระบบให้ดีขึ้น ทั้งนี้ในการจัดทำและนำเสนอขั้นตอนต่างๆ ให้ชัดเจนทำให้หน่วยงานภาครัฐที่เป็นองค์กรเล็ก ๆ ด้าน ICT สามารถวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรด้วยตัวเอง โดยเลือกใช้มาตรฐานสากล ISO/IEC 27001 ที่เน้นในด้านความปลอดภัยของระบบสารสนเทศที่ยอมรับทั่วไป โดยศึกษาและกำหนดขั้นตอนการดำเนินงานให้ชัดเจน วิธีการศึกษาวิเคราะห์ให้เหมาะสมกับลักษณะงานขององค์กรนั้นๆ เพื่อนำมาปรับปรุงช่องโหว่หรือจุดอ่อนด้าน ICT โดยไม่ต้องเสียงบประมาณ ในการบริหารจัดการหรือสามารถใช้เป็นกรณีศึกษาในการบริหารจัดการด้านความปลอดภัยของระบบสารสนเทศและนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีวิธีการและขั้นตอนในการดำเนินงานและรายละเอียด ดังนี้

3.1 ศึกษาภาพรวมการดำเนินงานโครงการ

3.2 แหล่งที่มาและวิธีการเก็บรวบรวมข้อมูล

3.3 ศึกษาวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและภัยคุกคาม

3.4 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

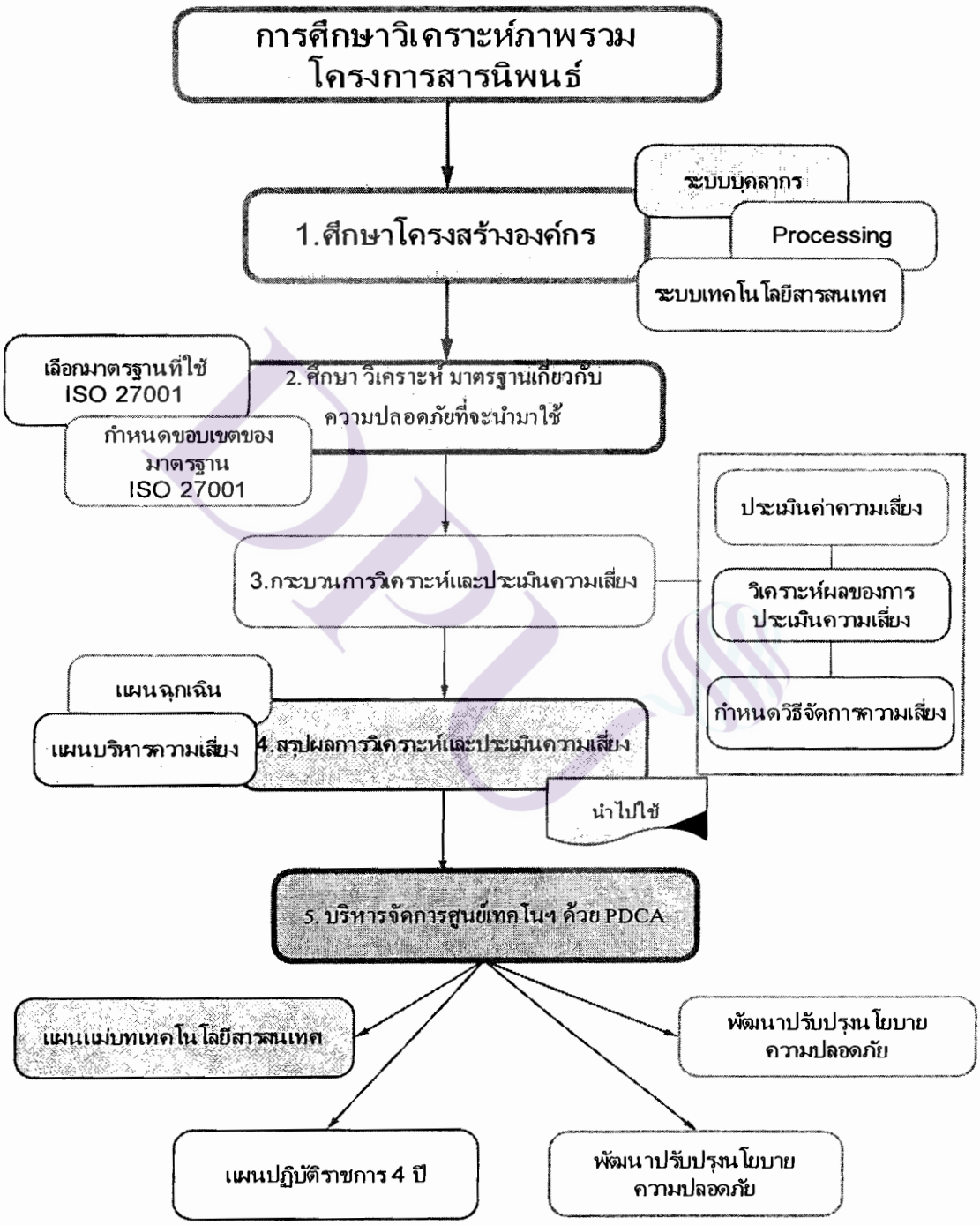
3.5 วิธีการวิเคราะห์และประเมินความเสี่ยง

3.6 ระยะเวลาในการดำเนินการวิจัย

3.7 ขั้นตอนวิธีการดำเนินการศึกษาและวิเคราะห์ความเสี่ยง

3.1 ศึกษาภาพรวมการดำเนินงานโครงการ

การศึกษาภาพรวมวิธีการและขั้นตอนในการดำเนินงานการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ ขั้นตอนตามภาพที่ 3.1



ภาพที่ 3.1 วิธีการดำเนินงาน

การศึกษาวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศเพื่อนำผลการวิเคราะห์และประเมินความเสี่ยงมาบริหารจัดการระบบสารสนเทศของหน่วยงานให้สอดคล้องกับวัตถุประสงค์ของโครงงานที่ได้กำหนดไว้ เพื่อให้การดำเนินงานโครงการมีประสิทธิภาพสะท้อนปัญหาหรือจุดอ่อนที่แท้จริงของการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศโดยได้กำหนดกรอบแนวคิดในการศึกษา 4 หัวข้อ ดังนี้

3.1.1 ศึกษา วิเคราะห์ สถานะของระบบเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อรับทราบปัญหาและความเสี่ยงด้าน ICT ในปัจจุบันขององค์กร โดยศึกษาผลกระทบความเสี่ยงด้านต่างๆ วิธีการแก้ปัญหา จากผู้มีส่วนเกี่ยวข้องโดยศึกษาวิเคราะห์ สังเกต สัมภาษณ์ จากระบบทั้งหมดที่เป็น Work Flow ต่างๆ ได้แก่

3.1.1.1 สัมภาษณ์บุคคลที่เกี่ยวข้อง ได้แก่

ผู้บริหาร (CIO) เพื่อทราบถึง พันธกิจ วิสัยทัศน์และกลยุทธ์ในการดำเนินงานด้าน ICT เพื่อหาโอกาสในการแก้ปัญหา

บุคลากรด้าน ICT เพื่อรับทราบปัญหา ในการปฏิบัติงาน สถานปัจจุบันของระบบสารสนเทศของหน่วยงาน

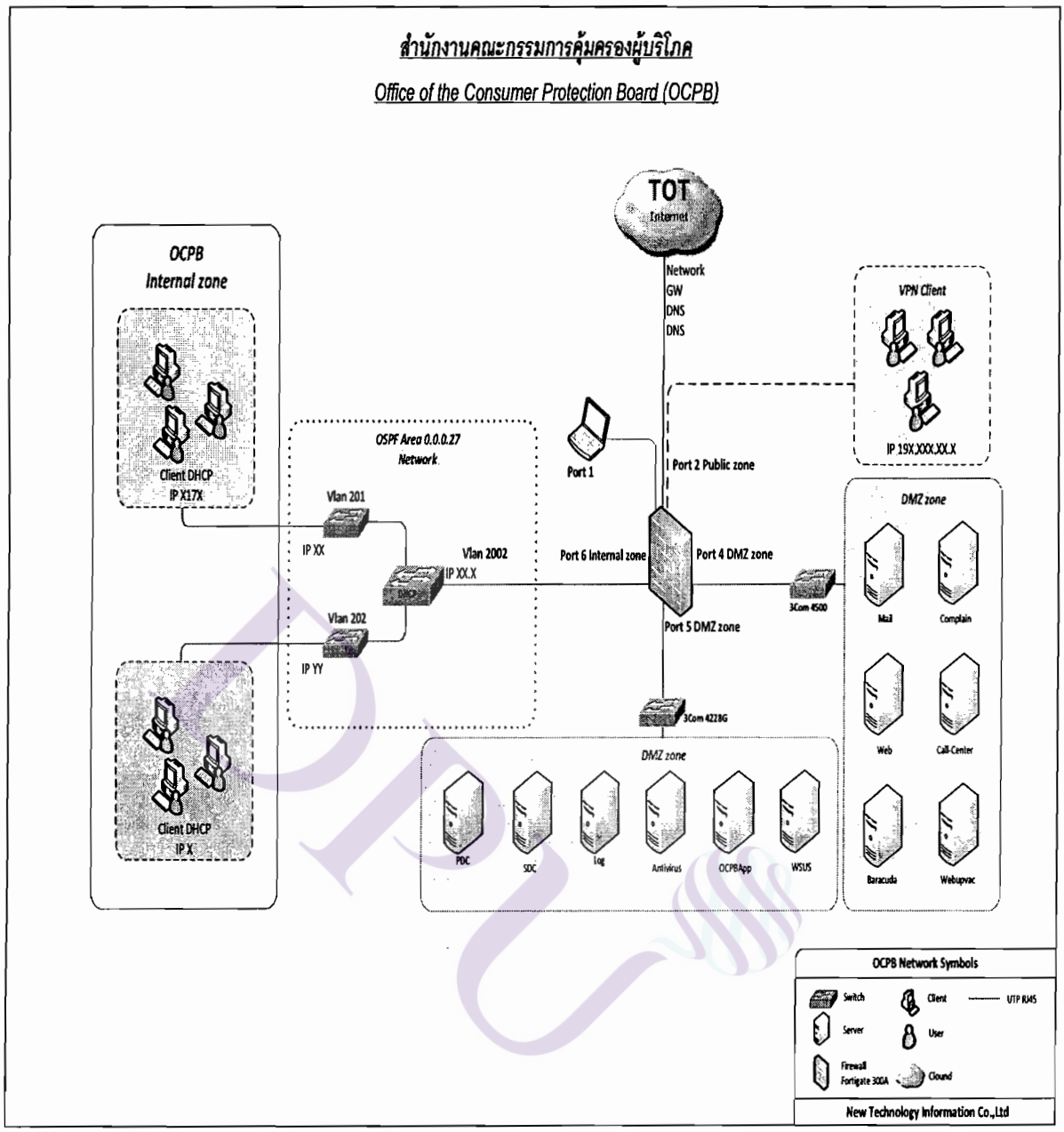
ผู้ใช้ระบบ (User) ทำให้ทราบปัญหาต่างๆ ในการใช้งาน เช่น ระบบช้า หน้าจอผู้ใช้งานซับซ้อนเกินไป ระบบเครือข่ายหลุดบ่อยๆ

3.1.1.2 ศึกษาจากเอกสารคู่มือต่างๆ

เอกสารผู้ดูแลระบบ เพื่อให้ทราบถึงขั้นตอนในการทำงานของระบบด้าน ICT เพื่อหาวิเคราะห์ปัญหาที่กระทบต่อระบบ

เอกสารคู่มือผู้ใช้ระบบด้าน ICT เพื่อรับทราบปัญหา ในการปฏิบัติงานสถานะปัจจุบันขอบระบบสารสนเทศของหน่วยงาน

3.1.2 ศึกษาโครงสร้างของระบบเครือข่าย เพื่อวิเคราะห์สถานะการณ์ในการดำเนินงานด้าน ICT ในปัจจุบัน การวางแผนด้านระบบเครือข่าย วางแผนในด้านการจัดหาเครื่องแม่ข่ายเพื่อรองรับการขยายงานที่เพิ่มขึ้น การดูแลความปลอดภัยด้านกายภาพของ โครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วง เพื่อนำมาวิเคราะห์ ความปลอดภัยและการควบคุมการเข้าถึงข้อมูลมีไดอะแกรมรายละเอียด ตามภาพที่ 3.2



ภาพที่ 3.2 ระบบเครือข่าย (Network System)

ที่มา : ศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

3.1.3 ศึกษาเรื่องของความเสี่ยงและการประเมินความเสี่ยง เพื่อนำมาการวิเคราะห์ปัญหาที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศ ซึ่งแต่ละองค์กรจะมีความเสี่ยงไม่เหมือนกันแล้วแต่ภารกิจหลักและบริบทต่างๆ เพื่อให้รู้ปัญหาต่างๆ มีดังนี้

3.1.3.1 เหตุการณ์ความเสี่ยง (Risks) หมายถึง เหตุการณ์ต่างๆ ที่มีโอกาสเกิดขึ้นได้ซึ่งเป็นภัยคุกคามและความเสียหายเกิดขึ้นจะเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กรและส่งผลเสียหายทั้งเป็นเงินและไม่เป็นตัวเงิน หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายองค์กร จุดอ่อน (Vulnerability) คือ ช่องโหว่ที่มี โดยจุดอ่อนต่างๆ อาจอยู่ในโครงสร้างขององค์กร ในเรื่องของขั้นตอนการปฏิบัติงาน บุคลากรขาดความสามารถ ไม่มีการบริหารจัดการด้านการรักษาความปลอดภัยของสารสนเทศที่ดีพอ จุดอ่อนเรื่องฮาร์ดแวร์ซึ่งอาจจะรุ่น เสียบ่อยๆ และการให้บริการหลังการขายมีช่องว่างในการใช้งาน หรือมีข้อบกพร่องมาจากโรงงาน จุดอ่อนเรื่องซอฟท์แวร์ ซึ่งอาจมีข้อบกพร่องมาจากโรงงาน ซึ่งจุดอ่อนในตัวมันเองมักไม่ก่อให้เกิดอันตรายถ้าไม่มีภัยคุกคาม (Threat) เช่น ถ้าไม่ล็อคประตูบริเวณแถวนั้นไม่มีโจรของก็ไม่หาย ไวรัสทำให้ข้อมูลเสียหายข้อมูลสำคัญถูกขโมยซึ่งอาจทำให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน หรือหน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง

3.1.3.2 การประเมินความเสี่ยง (Risk assessment) หมายถึง การกำหนดเหตุการณ์ความเสี่ยงที่มีโอกาสเกิดขึ้นได้ กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การประเมินความเสี่ยงมีจุดประสงค์เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศหนึ่ง และมีระดับความเสี่ยงมากน้อยเพียงใด ทั้งนี้เพื่อจะได้เตรียมการป้องกันไว้ก่อน ก่อนที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นจริงและทำให้องค์กรเกิดความเสียหาย

การประเมินความเสี่ยง (Risk Assessment) เป็นการประเมินความเสี่ยงขององค์กรว่ามีวัตถุประสงค์อะไร และมีความเสี่ยงอะไรบ้าง ที่ทำให้ไม่บรรลุวัตถุประสงค์และความเสี่ยงนั้นมีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยง และหาแนวทางการควบคุม (กิจกรรมที่ปฏิบัติ) เพื่อป้องกัน หรือลดความเสี่ยงนั้นๆ มีขั้นตอนดังนี้

การระบุปัจจัยเสี่ยง (Risk Identification) ทั้งนี้จะต้องศึกษาวัตถุประสงค์และเป้าหมายขององค์กรซึ่งจะสอดคล้องกับภารกิจ (Mission) ซึ่งแบ่งเป็น 2 ระดับ คือ

1. วัตถุประสงค์ระดับองค์กร (Entity – Ievel Objectives) เป็นวัตถุประสงค์ตามแผนกลยุทธ์ขององค์กร หรือแผนปฏิบัติราชการ 4 ปี (พ.ศ. 2555 – 2558)

2. วัตถุประสงค์ระดับกิจกรรม (Activity–Ievel Objectives) เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจง สำหรับแต่ละกิจกรรมในแต่ละหน่วยงาน ซึ่งต้องสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การวัดและประเมินความเสี่ยง (Risk Measurement) ทั้งนี้ต้องศึกษาก่อน ว่าอะไรเป็นปัจจัยเสี่ยงและมีความเสี่ยงอย่างไร ด้านการดำเนินงาน งบประมาณ กลยุทธ์ในการวิเคราะห์จะดูถึง

สาเหตุ (Cause) ของการเกิดนั้นมีโอกาส (Opportunity) มากน้อยเพียงใดและเมื่อเกิดแล้วจะมีผลกระทบ (Effect) มากน้อยเพียงใด

การจัดลำดับความเสี่ยง (Risk Prioritization) เมื่อเทียบความเสี่ยง โอกาสและผลกระทบแล้วจะต้องมาจัดลำดับว่าความเสี่ยงนนั้ มีนัยสำคัญเพียงใด โดยการจัดลำดับความเสี่ยง จากมากไปหาน้อย หรือเลือกเทคนิคการวิเคราะห์ความเสี่ยงที่เหมาะสม โดยอาจจะวิเคราะห์ในรูปตัวเลขก็ได้ มีขั้นตอนการในการวิเคราะห์ ดังนี้

1. ประเมินระดับความสำคัญของปัจจัยเสี่ยง คือปัจจัยเสี่ยงแต่ละปัจจัย หากเกิดขึ้นแล้วมีผลกระทบต่อองค์กรมากน้อยเพียงใด

2. ประเมินความเสี่ยงที่ปัจจัยเสี่ยงจะเกิดขึ้นคือพิจารณาว่าปัจจัยเสี่ยงที่เรียงลำดับความสำคัญแล้วมีโอกาสที่จะเกิดขึ้น มากน้อยเพียงใด

3.1.3.3 ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าค่าที่ยอมรับได้นี้ จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม)

3.1.3.4 แผนการลดความเสี่ยง (Risk treatment plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานเพื่อพิจารณาอนุมัติก่อน

3.1.3.5 ภัยคุกคาม (Threat) คือเรื่องในทางลบต่อองค์กร ซึ่งยังไม่ได้เกิดขึ้น หรือหากเกิดขึ้นอาจเกิดจากจุดอ่อนหรือช่องโหว่ของระบบสารสนเทศ เช่น ไวรัสโจมตี ข้อมูลเปลี่ยนแปลงโดยไม่ได้รับอนุญาต DoS (Denial of Service) ข้อมูลไม่สามารถดึงมาใช้งานได้ เป็นต้น

3.1.3.6 การจัดการความเสี่ยง (Risk Management) หมายถึง การบริหารจัดการด้านต่างๆ ในด้านการวางแผนจัดองค์กร การบังคับบัญชา และการควบคุมการปฏิบัติงานขององค์กร เพื่อลดผลเสียหายของความไม่แน่นอนที่จะเกิดขึ้นกับองค์กร เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ตามที่กำหนดในการบริหารความเสี่ยง จะต้องมีต้นทุนทรัพยากรและบุคคล ดังนั้นจะต้องคำนึงถึงผลประโยชน์ที่จะได้รับด้วยว่าคุ้มค่าหรือไม่ ในการลดความเสี่ยงเหล่านั้น เพราะเหตุว่าความเสี่ยงนั้นมีการเปลี่ยนแปลงอยู่ตลอดเวลา แล้วแต่บริบทของเหตุการณ์นั้นๆ เมื่อวิเคราะห์และจัดลำดับความเสี่ยงตามโอกาสที่เกิดความเสี่ยงและวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยงรวมทั้งพิจารณาหาวิธีหรือกำหนดกิจกรรมการต่างๆ เพื่อควบคุมความเสี่ยงนั้นๆ วิธีการมีหลายวิธี เช่น หลีกเลี่ยง

ยอมรับ ควบคุม หรือถ่ายโอนความเสี่ยง ในการบริหารความเสี่ยงต้องพิจารณาด้านงบประมาณในการใช้จ่าย รวมทั้งความคุ้มค่าและความเหมาะสม

3.1.4 ศึกษาทำความเข้าใจมาตรฐาน ISO/IEC 27001 โดยศึกษา วิเคราะห์กระบวนการและจัดเตรียมความพร้อม จัดทำขอบเขตของการบริหารความเสี่ยงตามแนวทางมาตรฐาน ISO/IEC 270001 เพื่อการบริหารจัดการความเสี่ยงของระบบสารสนเทศซึ่งประกอบด้วย ขั้นตอนต่างๆ ผู้เขียนได้จัดทำโครงการศึกษาได้จัดทำในรูปแบบมีขั้นตอนที่ชัดเจน(Process) เพื่อง่ายต่อการทำความเข้าใจ มี 11 โดเมน 133 Control Objective มีรายละเอียด ดังนี้

3.1.4.1 Security Policy-A5 (นโยบายการรักษาความปลอดภัย) เป็นสิ่งแรกที่สำคัญและจำเป็นสำหรับองค์กรที่ต้องมีเพื่อเป็นแนวทาง และสนับสนุนการรักษาความปลอดภัยของระบบสารสนเทศ

3.1.4.2 Organizing Information Security-A6 (การจัดโครงสร้างระบบการรักษาด้านความปลอดภัยขององค์กร) มีจุดประสงค์เพื่อการบริหารความปลอดภัยของข้อมูลภายในองค์กร และดูแลควบคุมระบบการรักษาความปลอดภัยของข้อมูลและระบบที่ต้องมีการเข้าถึงจากภายนอกองค์กร

3.1.4.3 Asset Management-A7 (การจัดการทรัพย์สิน) เป็นสิ่งที่มีความจำเป็นสำหรับการดูแล และควบคุมการเข้าถึงข้อมูลที่มีชั้นความลับ

3.1.4.4 Human Resource Security-A8 (การรักษาความปลอดภัยในระดับบุคลากร) โดยมีจุดมุ่งหมายดังนี้

(1) เพื่อลดความเสี่ยงที่อาจเกิดเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกง หรือหลอกลวง และการใช้งานระบบในทางที่ผิด

(2) เพื่อทำให้มั่นใจว่า ผู้ใช้มีความระมัดระวังเกี่ยวกับภัยคุกคามต่อการรักษาความปลอดภัยของข้อมูลและมีระบบป้องกัน และรองรับนโยบายทางด้านการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน

(3) ลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์ การทำงานที่ผิดพลาดของระบบ และเรียนรู้จากบทเรียนต่างๆ

3.1.4.5 Physical and Environmental Security–A9 (การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม) มีจุดมุ่งหมายเพื่อ

(1) ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อจะทำลายหรือขัดขวางการดำเนินธุรกิจขององค์กร

(2) ป้องกันการสูญเสีย และการขัดขวางการดำเนินธุรกิจขององค์กร

(3) ป้องกันการขโมยข้อมูล และการใช้ทรัพยากรขององค์กร

3.1.4.6 Communications and Operations Management-A10 (การสื่อสารและการบริหารการปฏิบัติงาน) มีจุดมุ่งหมายดังนี้

(1) เพื่อทำให้แน่ใจว่าระบบจัดการข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย

(2) ลดความเสี่ยงในการที่ระบบล่ม

(3) รักษาความคงสภาพ และมั่นคงของซอฟต์แวร์และข้อมูล

(4) เพื่อรักษาความคงสภาพ และความพร้อมใช้งานของระบบสื่อสารข้อมูล และระบบจัดการข้อมูล

(5) เพื่อป้องกันและรักษาความปลอดภัยข้อมูลบนเครือข่าย และการป้องกันโครงสร้างของระบบ

(6) ป้องกันการสูญเสียต่อทรัพย์สิน และการขัดขวางต่อการดำเนินธุรกิจ

(7) ป้องกันการสูญเสีย การดัดแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดเมื่อต้องมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร

3.1.4.7 Access Cotrol-A11 (การควบคุมการเข้าถึงระบบ) มีจุดมุ่งหมายเพื่อการควบคุมการเข้าถึงข้อมูล

(1) ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

(2) ป้องกันการให้บริการทางเครือข่าย

(3) ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(4) ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาตมีระบบรักษาความปลอดภัยเมื่อมีการใช้งานอุปกรณ์เคลื่อนที่ และการใช้งานการสื่อสารทางด้านโทรคมนาคม

3.1.4.8 Information systems acquisition, development and maintenance-A12 (การดูแลและพัฒนาระบบ) มีวัตถุประสงค์ดังนี้

(1) เพื่อให้แน่ใจว่าระบบที่พัฒนาหรือสร้างนั้นมีความปลอดภัยเพียงพอสำหรับการใช้งานจริง

(2) ป้องกันการสูญเสีย หรือมีการเปลี่ยนแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดในแอพพลิเคชัน

(3) ป้องกันความลับ การพิสูจน์ทราบตัวตน และความคงสภาพของข้อมูล

(4) ทำให้แน่ใจว่าโครงการต่างๆนั้นให้ความสำคัญกับการรักษาความปลอดภัย

(5) ดูแลรักษาความปลอดภัยของแอพพลิเคชันและข้อมูล

3.1.4.9 Information security incident management - A13 (การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย) ซึ่งมีมาตรการ 2 ส่วนคือ

(1) การรายงานเหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัย

(2) การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย เพื่อให้มีความรวดเร็วและมีประสิทธิภาพ

3.1.4.10 Business Continuity Management-A14 (การบริหารความต่อเนื่องของธุรกิจ) เพื่อป้องกันเหตุการณ์ที่จะขัดขวางการดำเนินธุรกิจจากเหตุการณ์ล้มเหลวขนาดใหญ่หรือภัยธรรมชาติ

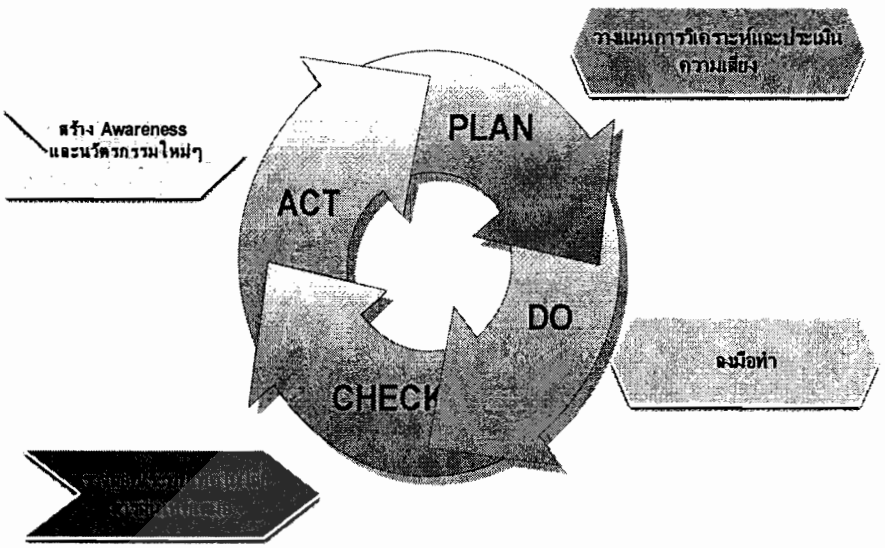
3.1.4.11 Compliance-A15 (ไม่ขัดต่อกฎหมาย) มีวัตถุประสงค์เพื่อ

(1) ป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่างๆ

(2) เพื่อทำให้แน่ใจว่าระบบไม่ขัดต่อนโยบายการรักษาความปลอดภัยขององค์กรหรือมาตรฐานที่เลือกใช้

3.1.5 ศึกษา รูปแบบการดำเนินการแบบ Plan-Do-Check-Act (PDCA) เพิ่มเติมมาตรฐาน ISO/IEC 27001 ซึ่งศึกษามองเห็นว่าเป็นรูปแบบการดำเนินงานที่สำคัญ เพื่อนำมาพัฒนาระบบการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ จึงเป็นแนวทางพื้นฐานเพื่อที่จะสร้างระบบควบคุมเพื่อให้องค์กรให้สามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้และเพื่อให้ระบบต่างๆได้รับการพัฒนาปรับปรุงอย่างต่อเนื่องหรือทบทวน อย่างน้อยปีละ 1 ครั้ง เมื่อถึงเวลา มีรายละเอียดของวงจร PDCA ตามระบบบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 หัวใจหลักของกระบวนการ ซึ่งประกอบด้วย 4 ขั้นตอนหลัก รายละเอียด ดังภาพที่ 3.3

วงจร PDCA



ภาพที่ 3.3 หัวใจหลักกระบวนการ PDCA

ที่มา : บทความ Plan-Do-Check-Act (12)

เมื่อวิเคราะห์และพิจารณาแล้ว หัวใจหลักของ การเพิ่มประสิทธิภาพในการดำเนินงานกิจกรรมใดๆ ต้องมีกระบวนการ PDCA แทรกอยู่เสมอ ได้แก่

1) การวางแผน (Establish the ISMS (เทียบเท่ากับ Plan)) ถ้าหากหน่วยงานยังไม่มีการวางแผนงานสำหรับกิจกรรมใดๆ ที่อาจเกิดขึ้น

2) การดำเนินการตามแผน (Do) Implement and operate the ISMS (เทียบเท่ากับ Do) หมายถึงการดำเนินงานตามแผนที่ได้วางไว้

3) การเฝ้าระวังและติดตามการดำเนินการตามแผน (Monitor and Review the ISMS (เทียบเท่ากับ Check)) มีการตรวจสอบการทำงาน ตรวจสอบแผนงาน

4) การดำเนินการเพิ่มเติมตามสมควร (Maintain and Improve the ISMS (เทียบเท่ากับ Act)) ทบทวน ปรับปรุงงานให้ดีขึ้น แก้ไขให้ตรงตามความต้องการ

อธิบายรายละเอียด แนวทางในการดำเนินการตาม PDCA ได้ ดังนี้

3.1.5.1 การวางแผน (Plan) คือการวางแผนหรือ Plan เป็นการประเมินความเสี่ยงที่มีต่อทรัพย์สินสารสนเทศซึ่งส่วนใหญ่จะหมายถึงทรัพย์สินสารสนเทศใหม่ที่กำลังนำเข้ามาสู่การใช้งานที่จะต้องมีแผนในการประเมินความเสี่ยง เพื่อเตรียมการป้องกันก่อนเริ่มต้นใช้งานทรัพย์สินใหม่

เหล่านั้น เช่น กรณีมีโครงการจัดทำระบบงาน E-Meeting ที่ต้องดำเนินการให้แล้วเสร็จในปีงบประมาณนี้ ทรัพย์สินสารสนเทศใหม่ของโครงการนี้อาจประกอบด้วย

(1) วางแผนในการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศระบบงาน E-Meeting ฮาร์ดแวร์ของระบบงาน E-Meeting ซอฟต์แวร์ต่างๆ ของระบบงาน E-mail เช่น ระบบปฏิบัติการ Windows ระบบฐานข้อมูล

(2) การกำหนดแนวทางในการประเมินความเสี่ยงสำหรับองค์กรที่เหมาะสมต้องสอดคล้องกับการบริหารความเสี่ยงเชิงกลยุทธ์ขององค์กร กำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยงและได้รับการอนุมัติโดยฝ่ายบริหาร

(3) วางแผนงานเพื่อวิเคราะห์ความเสี่ยง ซึ่งประกอบด้วย การระบุทรัพย์สิน ระบุภัยคุกคามที่มีต่อทรัพย์สิน ระบุผลกระทบ การค้นหาจุดอ่อนการประเมินถึงโอกาสในการเกิดขึ้นของความล้มเหลวที่มีต่อความมั่นคงปลอดภัยระบบสารสนเทศ

(4) วางแผนกำหนดแนวทางมาตรการควบคุมสำหรับองค์กรที่เหมาะสม เช่น กำหนดมาตรการควบคุมที่เหมาะสม การยอมรับความเสี่ยงที่เกิดขึ้น การหลีกเลี่ยงความเสี่ยง การโอนย้ายความเสี่ยง

(5) วางแผน การจัดเตรียมเอกสาร มีเอกสารแสดงการประยุกต์ใช้งาน หรือ Statement of Applicability (SOA) โดยเป็นเอกสารที่อธิบายถึงรายการของหัวข้อควบคุม (Control) วัตถุประสงค์การควบคุม (Control objectives) ที่ได้เลือกไว้ และเหตุผลของการเลือก รวมถึงหัวข้อควบคุมและวัตถุประสงค์ควบคุมที่มีอยู่ วางแผน Base line control ในกรณีที่หัวข้อการควบคุมอะไร

3.1.5.2 การลงมือทำ (DO) คือการดำเนินการตามแผนที่วางไว้ DO ในขั้นตอนของการลงมือทำจะประกอบด้วย

(1) จัดทำแผนเกี่ยวกับความมั่นคงปลอดภัยระบบสารสนเทศ เช่น วางแผนกำหนดผู้รับผิดชอบทรัพยากร

(2) จัดลำดับความสำคัญในการดำเนินงาน สำหรับการจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศการจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กร

(3) ดำเนินการตามมาตรการควบคุมที่กำหนดไว้เพื่อให้ได้ตามวัตถุประสงค์ของการควบคุมการบริหารงาน ISMSการจัดการทรัพยากรสำหรับ ISMS(4)การดำเนินงานตามวิธีการปฏิบัติงาน และการควบคุมอื่นๆ เพื่อให้สามารถตรวจสอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยและการตอบสนองต่อเหตุการณ์นั้นๆ

3.1.5.3 การตรวจสอบ (Check) องค์กรจะต้องมีการดำเนินการต่างๆ ประกอบด้วย

(1) การดำเนินการเฝ้าติดตาม และทบทวนวิธีการปฏิบัติงาน และการควบคุมต่างๆ ระบุถึงการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ต่างๆ ที่เกิดขึ้น ช่วยให้ฝ่ายบริหารสามารถระบุถึงการดำเนินการความมั่นคงที่ได้มอบหมายให้บุคลากรต่างๆ เป็นไปตามที่คาดหมายไว้ ช่วยในการตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยโดยการใช้ดัชนีวัดที่เหมาะสม โดยพิจารณาถึงความมีประสิทธิผลในการดาเนินการเพื่อแก้ไขการละเมิดความมั่นคงปลอดภัย

(2) การดำเนินการทบทวนความมีประสิทธิผลของ ISMS อย่างสม่าเสมอ โดยพิจารณาถึงของการตรวจประเมินความมั่นคงปลอดภัย (Audit) เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ และข้อมูลแจ้งกลับจากหน่วยงานต่างๆ ที่เกี่ยวข้อง การวัดความมีประสิทธิผลของการควบคุมเพื่อทวนสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย และทบทวนการประเมินความเสี่ยงตามแผนที่ได้กาหนดไว้ รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงการเปลี่ยนแปลงในองค์กรด้านเทคโนโลยี

(3) การปรับปรุงงานกิจกรรมต่างๆ เกี่ยวกับระบบสารสนเทศและการควบคุมต่าง การดำเนินการทบทวนโดยฝ่ายบริหาร เพื่อดูแลความเพียงพอของขอบเขต และการดำเนินการปรับปรุงกระบวนการ ISMS การปรับปรุงแผนความมั่นคงปลอดภัย โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตามการทบทวน การบันทึกผลการดำเนินการ และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผลหรือผลการดำเนินงานของ ISMS

(4) การตรวจสอบ ดูแลว่าการปรับปรุงเป็นไปตาม วัตถุประสงค์ที่วางไว้ คู่มือการปฏิบัติงานเป็นปัจจุบัน มีการทบทวนตรวจสอบความครบถ้วนสมบูรณ์ของกระบวนการที่อาจส่งผลต่อความมีประสิทธิผล หรือผลการดำเนินงานของ ISMS

3.1.5.4 การปรับปรุงแก้ไข (Act) ในขั้นตอนการของการปรับปรุงและแก้ไขระบบต่างๆ อาจจะประกอบด้วย

(1) การดำเนินการปรับปรุง ISMS ตามที่กำหนดไว้ ปรับปรุงเอกสารให้ถูกต้องการปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคงปลอดภัยขององค์กรอื่นๆ ขององค์กรมาปรับใช้ให้เหมาะสม

(2) การสื่อสารการปรับปรุง ISMS ตามที่กำหนดไว้ การสื่อสารแนวปฏิบัติการที่แก้ไขและการปรับปรุงไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งหมด การสื่อสารแผนบริหารความเสี่ยงให้เข้าใจทั่วทั้งองค์กรรวมทั้งการจัดทำรายงานต่างๆ นำเสนอผู้บริหาร

3.2 แหล่งที่มาและวิธีการเก็บรวบรวมข้อมูล

3.2.1 ศึกษาจากเอกสาร (Document) ต้องศึกษา จากเอกสารต่างๆที่เกี่ยวข้องทั้งแนวคิดและทฤษฎีที่เกี่ยวข้อง ได้แก่ ศึกษามาตรฐาน ISO/IEC 27001 ศึกษาสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศขององค์กรพร้อมทำความเข้าใจเพื่อใช้เป็นข้อเพื่อประกอบการวิเคราะห์ เช่น ศึกษาจากขั้นตอนการทำงานและกระบวนการทำงาน ศึกษาขั้นตอนการปฏิบัติงานเป็นหลัก ศึกษาจากเอกสารจากงานวิจัยที่เกี่ยวข้อง บทความด้านความปลอดภัยสารสนเทศจากแหล่งข้อมูลต่างๆ เพื่อนำมาใช้เป็นแนวทางในการวิเคราะห์ผลการจัดทำโครงงาน

3.2.2 สังเกต (Observation) ทำให้เกิดความเข้าใจในการศึกษา วิเคราะห์ระบบสารสนเทศของหน่วยงาน สังเกตการปฏิบัตงานเชิงนโยบาย ลักษณะการบริหารงาน เทคนิคกลยุทธ์เพื่อสร้างให้เกิดจินตนาการในการวิเคราะห์ระบบและนำข้อมูลพื้นฐานไปประเมินและวิเคราะห์ความเสี่ยงต่อไป

3.2.3 การประชุม/สัมมนา เพื่อเก็บรวบรวม รายละเอียดของข้อมูลที่จะศึกษา การบริหารความเสี่ยงของโครงการเพื่อรวบรวมข้อมูลพื้นฐานในการจัดทำโครงการด้าน ICT นำมาศึกษาแนวคิดของเจ้าหน้าที่ทั้งระดับบริหาร และระดับปฏิบัติงานของหน่วยงาน

3.2.4 การสัมภาษณ์ (Interview) ผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ระดับผู้บริหารของหน่วยงานเจ้าหน้าที่ที่ปฏิบัติงาน ตลอดจนถึงผู้รับบริการ เพื่อค้นหาทิศทาง วิสัยทัศน์ พันธกิจในการตอบสนองวัตถุประสงค์ขององค์กร นำมาเลือกใช้เทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือสนับสนุนการทำงานให้เหมาะสมและสอดคล้องกับภารกิจหลักขององค์กร รวมทั้งกำหนดขอบเขตในการดำเนินงานด้าน ICT การแก้ปัญหาในปัจจุบันและวางแผนในอนาคต

3.3 ศึกษาวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและภัยคุกคาม

3.3.1 จุดแข็งขององค์กร

1. เป็นองค์กรภาครัฐที่ให้การบริการประชาชนทั่วประเทศในการคุ้มครองผู้บริโภค
2. การให้บริการอย่างทั่วถึงของพื้นที่ที่รับผิดชอบ มีประสิทธิภาพและคุณภาพ
3. มีการขยายตัวขององค์กรเพื่อรองรับการก้าวสู่ประชาคมอาเซียน

3.3.2 จุดอ่อนขององค์กร

1. วัฒนธรรมองค์กรแบบเฉพาะที่เปลี่ยนแปลงได้ยากในการประสานงาน
2. บุคลากรและเจ้าหน้าที่ยังขาดความรู้ความเข้าใจด้าน ICT ในการถ่ายทอดความรู้และประสบการณ์หรือไม่ได้รับการฝึกอบรม
3. ระบบเทคโนโลยีสารสนเทศ ถือเป็นโครงสร้างพื้นฐานรองรับที่สาคัญ แต่ยังไม่ได้รับการสนับสนุนและขาดการพัฒนาอย่างต่อเนื่องยังมีช่องโหว่ของระบบเทคโนโลยีสารสนเทศและ

มีความเสี่ยงต่อการล้มเหลวของระบบทาให้การปฏิบัติงานเกิดความขัดข้อง เช่น ระบบรักษาความมั่นคงปลอดภัยที่ต้องได้มาตรฐานเป็นที่เชื่อถือได้

3.3.3 โอกาสขององค์กร

1. รัฐบาลมีนโยบายชัดเจน ด้านการคุ้มครองผู้บริโภคในประเทศไทยและอาเซียน โดยเฉพาะด้านเทคโนโลยีสารสนเทศ

2. มีโอกาสพัฒนาระบบสารสนเทศให้สามารถรองรับความต้องการใช้บริการได้อย่างพอเพียงและมีประสิทธิภาพ

3. องค์กรมีบทบาทในด้านความก้าวหน้าทางเทคโนโลยีเพื่อรองรับการคุ้มครองผู้บริโภคก้าวสู่อาเซียน

4. การวิจัยพัฒนาเกี่ยวกับการคุ้มครองผู้บริโภคด้วยประสบการณ์ที่ยาวนาน

3.3.4 ภัยคุกคามขององค์กร

1. ภัยคุกคามต่อระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในระบบเครือข่ายสื่อสารคอมพิวเตอร์ และระบบปัจจุบันอาจทำให้ระบบชะงัก หรืออาจถูกขโมยข้อมูลได้

2. การเปลี่ยนแปลงทางการเมืองบ่อยๆ ทำให้ขาดความต่อเนื่องในการทำงานต้องมาเริ่มต้นใหม่จึงทำให้พัฒนาได้ช้า

3.4 อุปกรณ์และเครื่องมือที่ใช้ในการศึกษาวิจัย

3.4.1 เครื่องมือที่ใช้ในการศึกษาวิจัย ได้แก่ มาตรฐานสากล ISO/IEC 27001 PDCA Model การบริหารความเสี่ยง (Risk Management)

3.4.2 เครื่องมือที่ใช้ในการตรวจสอบ (Tools) การเก็บข้อมูลของปัญหา โดยเครื่องมือการตรวจสอบช่องโหว่ และเอกสาร Checklist เพื่อให้ทราบถึงสภาพโครงสร้างระบบเครือข่ายภายในองค์กรที่ใช้เป็นกรณีศึกษา และสามารถทราบถึงปัญหาที่ตรวจพบในระบบเทคโนโลยีสารสนเทศเพื่อหาแนวทางป้องกันมีดังนี้

3.4.2.1 Super Scan โปรแกรมสแกนพอร์ตแบบฟรีแวร์ (Freeware) เป็นโปรแกรม Super Sean ที่มีชื่อเสียงและจุดเด่นในด้านการสแกนพอร์ตได้อย่าง รวดเร็วและมีประสิทธิภาพ

3.4.2.2 Nmap (Network Mapping) เป็นโปรแกรม Open source ที่ใช้สแกนเครือข่ายและตรวจสอบความปลอดภัยซึ่ง Nmap สามารถทำการสแกนเครือข่ายขนาดใหญ่ได้อย่างรวดเร็วโดยการสแกนไอพีแอดเดรส เพื่อที่จะรายงาน Port Application OS และ Firewall ในปัจจุบัน Nmap มีการประมวลผลได้กับระบบปฏิบัติการ(OS) ทุกประเภท สามารถเลือกใช้งานได้ทั้งแบบผ่าน Command และแบบ Graphic GUI ซึ่งไม่จำเป็นต้องจำคำสั่งต่างๆ

3.4.2.3 เป็นเครื่องมือสำหรับการตรวจสอบการบุกรุกซึ่งใช้สำหรับการสแกนช่องโหว่ Nessus สามารถแสดงรายงานออกมาว่าแต่ละเครื่องมี ช่องโหว่อะไรบาง ระดับความเสี่ยงที่จะถูกโจมตีมี มาก-น้อย แค่ไหน วิธีป้องกันทำได้อย่างไรบ้าง

3.4.2.4 SQL Scan เป็นเครื่องมือสำหรับทำการตรวจสอบว่าเครื่องไหนบ้างภายในเครือข่ายได้ติดตั้ง โปรแกรม Microsoft Sql Server

3.4.2.5 SQL Dict เป็นเครื่องมือสำหรับถอดรหัส Microsoft Sql Server โดยเทียบจากคำศัพท์ จากไฟล์ดิกชั่นนารี

3.4.2.6 Pwdump3v2 เป็นเครื่องมือสำหรับดัมพ์เอารหัสผ่านจาก Registry ของเครื่องเหยื่อออกมาเป็นไฟล Text

3.5 วิธีการวิเคราะห์และประเมินความเสี่ยง

หลังจากผ่านกระบวนการศึกษา รวบรวมข้อมูล และมีการจัดเตรียมข้อมูล วางแผนงาน ทำความเข้าใจศึกษาข้อกำหนดในมาตรฐานที่เลือกใช้ทำการเปรียบเทียบข้อมูลพื้นฐานต่างๆ การระบุทรัพย์สิน การประเมินความเสี่ยงของทำการพัฒนานโยบายสารสนเทศแต่ละหัวข้อด้วยขั้นตอนดังต่อไปนี้

3.5.1 นำข้อมูลพื้นฐานมาจัดลำดับความสำคัญ เพื่อกำหนดลำดับในการจัดกลุ่มทรัพย์สินของระบบสารสนเทศ โดยจัดทำตารางการให้คะแนนอัตราความเสียหายที่จะเกิดขึ้นกับข้อมูล โดยแยกเป็นอัตราความเสี่ยงที่มีต่อการรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมให้บริการ (Availability) นำคะแนนต่างๆ ที่ได้จากการประเมินความเสี่ยงมารวมกันแล้วนำคะแนนมาวิเคราะห์และจัดลำดับความเสี่ยง

3.5.2 ศึกษาข้อกำหนดและวิธีการโดยละเอียด โดยใช้ข้อมูลจากเอกสาร ISO/IEC 27001 เพื่อระบุว่าจะต้องบรรจุ หัวข้ออะไรบ้างลงในการวิเคราะห์และประเมินความเสี่ยง

3.5.3 ระบุทรัพย์สิน นำข้อมูลที่ได้จาก การรวบรวม สัมภาษณ์ มาจัดกลุ่มแยกประเภทเพื่อวิเคราะห์ ตรวจสอบหาจุดอ่อน จุดแข็งและ ช่องโหว่

3.5.4 แยกการวิเคราะห์ออกเป็นหัวข้อย่อย ตามมาตรฐาน ISO ทั้ง 11 Domain ซึ่งในแต่ละกระบวนการอาจแยกได้มากกว่า 1 หัวข้อ ขึ้นอยู่กับความต้องการในการแบ่งแยกชนิดของการควบคุม เช่น กระบวนการสร้างความปลอดภัยให้กับระบบสารสนเทศ อาจแยกออกเป็นการควบคุมการเข้าถึงข้อมูล นโยบายด้านความปลอดภัยของเซิร์ฟเวอร์(server) เป็นต้น ข้อมูลในแต่ละตารางประกอบไปด้วย หมายเลขนโยบาย ชื่อนโยบาย วัตถุประสงค์ หลักการและเหตุผล หน้าที่รับผิดชอบ รายละเอียดของนโยบายความปลอดภัย

3.5.5 เพิ่มขั้นตอนของวิธีการของ PDCA เพื่อให้ครอบคลุมข้อกำหนดตามกระบวนการของมาตรฐาน ISO/IEC 27001

3.5.6 นำผลการวิเคราะห์และการประเมินความเสี่ยงที่พัฒนาเสร็จแล้วแต่ละกระบวนการปรึกษากับอาจารย์ที่ปรึกษา เพื่อทำการตรวจสอบและแก้ไขและปรับปรุงเพิ่มเติมความครบถ้วนให้มีความสมบูรณ์ยิ่งขึ้น

3.5.7 ทำตามขั้นตอนตั้งแต่ข้อ 3 จนถึงข้อ 7 เรียงตามลำดับจนครบทุกกระบวนการ

3.5.8 จัดทำผลสรุป เพื่อรวบรวม วางแผน จัดทำแผนงานพัฒนา ICT แผนแม่บทเทคโนโลยีสารสนเทศ ฉบับที่ 2 ปี 2557-2560 ส่งรายงานสรุปต่อให้ผู้บริหารองค์กรพิจารณา

3.6 ระยะเวลาในการดำเนินการศึกษาวิจัย

ระยะเวลาในการดำเนินการวิจัยตั้งแต่ ตุลาคม 2555 – มิถุนายน 2556 เพื่อการศึกษาวิเคราะห์วางแผนการดำเนินงานตามตารางข้างล่างนี้

ตารางที่ 3.1 ระยะเวลาในการดำเนินงานศึกษาวิจัย

ระยะเวลาดำเนินงาน (เม.ย.- กันยายน)	ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.
1. ศึกษา รวบรวมข้อมูลที่เกี่ยวข้องระบบสารสนเทศภายในองค์กร									
2. จัดหมวดหมู่ของทรัพย์สินสารสนเทศ									
3. วิเคราะห์ประเมินความเสี่ยงทางระบบสารสนเทศ									
4. กำหนดมาตรการป้องกันและวิเคราะห์									
5. สรุปผลการ วิจัยและข้อเสนอแนะ									
6. เรียบเรียงงานค้นคว้าอิสระให้สมบูรณ์/เสนอจบ									

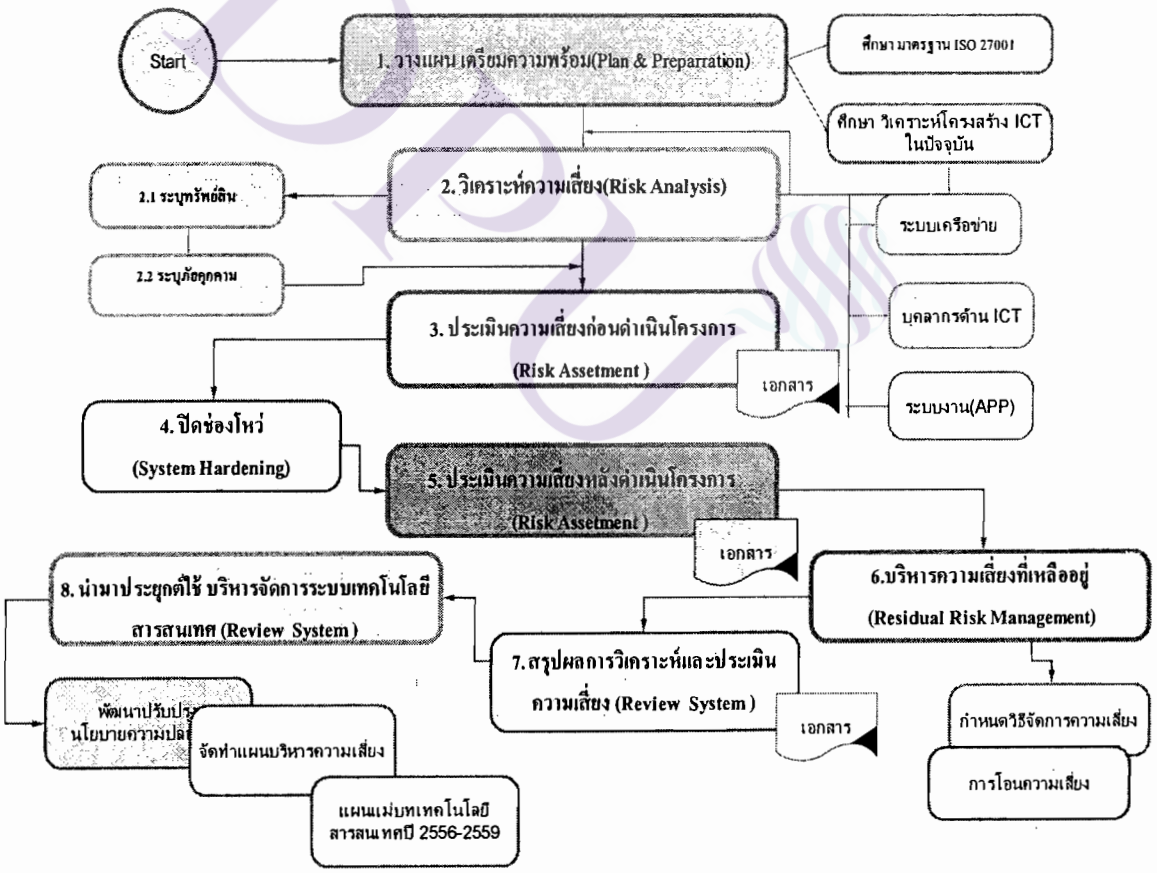
3.7 ขั้นตอนวิธีการดำเนินการศึกษาและวิเคราะห์ความเสี่ยง

จากวิธีการและการออกแบบขั้นตอนการทำงานในภาพรวม สามารถกำหนดข้อมูลที่ใช้ในการวิเคราะห์และประเมินความเสี่ยง ซึ่งมีขั้นตอนการดำเนินงาน(รายละเอียดในบทที่4) มีดังต่อไปนี้

1. รวบรวม ศึกษาข้อมูลและระบบสารสนเทศภายในองค์กรทั้งหมด
2. จัดหมวดหมู่ แยกประเภทสารสนเทศแยกตามประเภทระบบงาน
3. วิเคราะห์องค์กร จุดแข็ง จุดอ่อน โอกาสและภัยคุกคามขององค์กร
4. วิเคราะห์การใช้งานระบบสารสนเทศและอุปกรณ์ในปัจจุบัน
5. ประเมินความเสี่ยงและผลกระทบต่อองค์กร
6. กำหนดมาตรการป้องกันที่สามารถจัดการได้ ในด้านความปลอดภัยขององค์กร
7. สรุปผลการวิเคราะห์และประเมินความเสี่ยง
8. แนวทางในการนำไปใช้การวิจัยและข้อเสนอแนะ

บทที่ 4
การวิเคราะห์และประเมินความเสี่ยง

จากการวิเคราะห์ปัญหา และออกแบบขั้นตอนและวิธีการดำเนินงาน ในบทนี้จะกล่าวถึง การวิเคราะห์และประเมินความเสี่ยง โดยการนำมาตรฐานสากล ISO/IEC 27001 มาใช้เป็นกรอบในการกำหนดขอบเขต การวิเคราะห์และประเมินความเสี่ยงให้ตรงตามวัตถุประสงค์ของการดำเนินงานโครงการและนำผลการวิเคราะห์และประเมินความเสี่ยง ไปใช้บริหารจัดการระบบเทคโนโลยีสารสนเทศภายในองค์กรประกอบด้วยขั้นตอนต่างๆ ของกระบวนการวิเคราะห์และประเมินความเสี่ยง ดังภาพที่ 4.1



ภาพที่ 4.1 กระบวนการวิเคราะห์และประเมินความเสี่ยง

การวิเคราะห์และประเมินความเสี่ยงตามที่ได้มีการวิเคราะห์ออกแบบไว้ในบทที่ 3 มีรายละเอียดต่างๆ ดังนี้ การศึกษา วิเคราะห์ การบริหารจัดการความเสี่ยงภายใต้มาตรฐาน ISO/IEC 270001 เป็นขั้นตอนศึกษาวิเคราะห์ความเสี่ยงของทรัพย์สินสารสนเทศ ในแง่ของโอกาสที่จะเกิดหรือเหตุการณ์ (Event) ว่ามีโอกาสที่จะเกิดมากน้อยแค่ไหนและเมื่อเกิดขึ้นแล้วมีผลกระทบ (Impact) ความรุนแรงเสียหายอย่างไรบ้างมีขั้นตอนและรายละเอียด ตามข้อ 4.1-4.6 อธิบายรายละเอียดดังนี้

4.1 การวางแผนเตรียมความพร้อม

4.2 การวิเคราะห์ความเสี่ยงโดยการนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้

4.3 การประเมินความเสี่ยงก่อนดำเนินโครงการ

4.4 วิเคราะห์ ตามตารางประเมินความเสี่ยงที่ได้ตรวจสอบปิดช่องโหว่ของระบบ

4.5 วิเคราะห์และประเมินความเสี่ยงหลังดำเนินโครงการ

4.6 การจัดการความเสี่ยง (Risk Management) มีวิธีจัดการความเสี่ยงได้หลายวิธี ได้แก่ การลดความเสี่ยง การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง การยอมรับความเสี่ยงที่มีอยู่ (Accept Risk)

4.7 สรุปผลการวิเคราะห์และประเมินความเสี่ยง วิเคราะห์เปรียบเทียบตารางความเสี่ยงก่อนดำเนินโครงการและหลังดำเนินโครงการ นำผลการวิเคราะห์และประเมินความเสี่ยงไปใช้วางแผน เพื่อดำเนินงานต่างๆ ด้านเทคโนโลยีและการสื่อสาร(ICT) ขององค์กร

4.8 นำมาประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับที่ 2 ปี 2556-2559 การพัฒนาปรับปรุงนโยบายความปลอดภัยของหน่วยงานและการจัดทำแผนบริหารความเสี่ยง

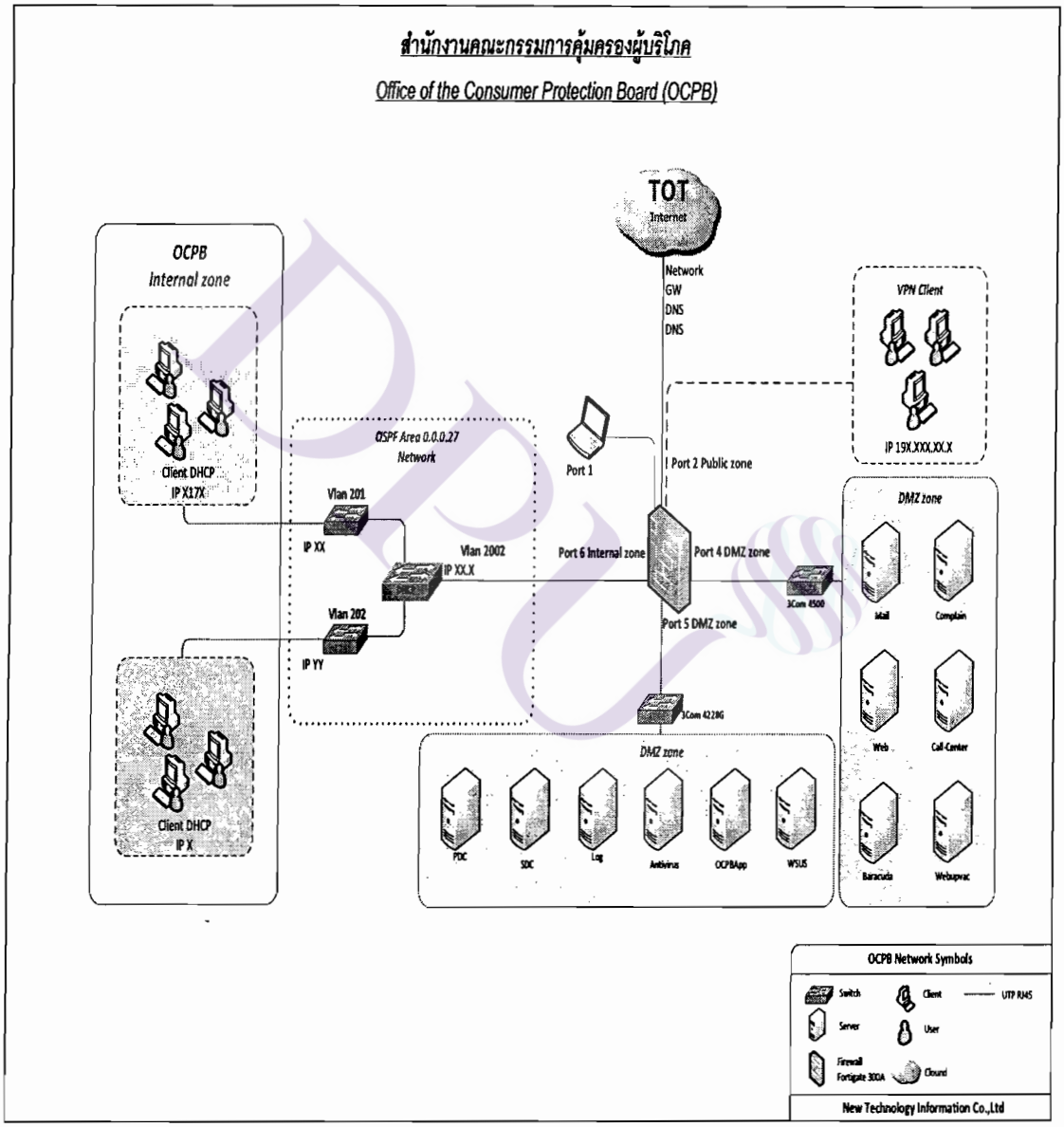
4.1 การวางแผนเตรียมความพร้อม ต้องมีการวางแผนเตรียมความพร้อมใน การศึกษา วิเคราะห์ข้อมูลด้านความปลอดภัยของระบบสารสนเทศ เพื่อมีการเตรียมพร้อมในการวิเคราะห์และประเมินความเสี่ยง

4.1.1 ศึกษาข้อมูลด้านความปลอดภัยตามมาตรฐาน ISO/IEC 27001 เพื่อเป็นแนวทางในการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ และกำหนดขอบเขต ระบุภัยคุกคาม/ความเสี่ยงที่อาจเกิดขึ้น ทำความเข้าใจขั้นตอนการวิเคราะห์ความเสี่ยง ศึกษาผลกระทบ เป็นต้น

4.1.2 ศึกษา การบริหารความเสี่ยง ภัยคุกคาม/ช่องโหว่ การศึกษาวิเคราะห์ด้านการจัดการความเสี่ยงการใช้งานระบบสารสนเทศและอุปกรณ์ในปัจจุบัน การวิเคราะห์และประเมินความเสี่ยงต้องมีการระบุปัจจัยเสี่ยงอะไรบ้าง ศึกษาการบริหารความเสี่ยง เพื่อบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นต้น

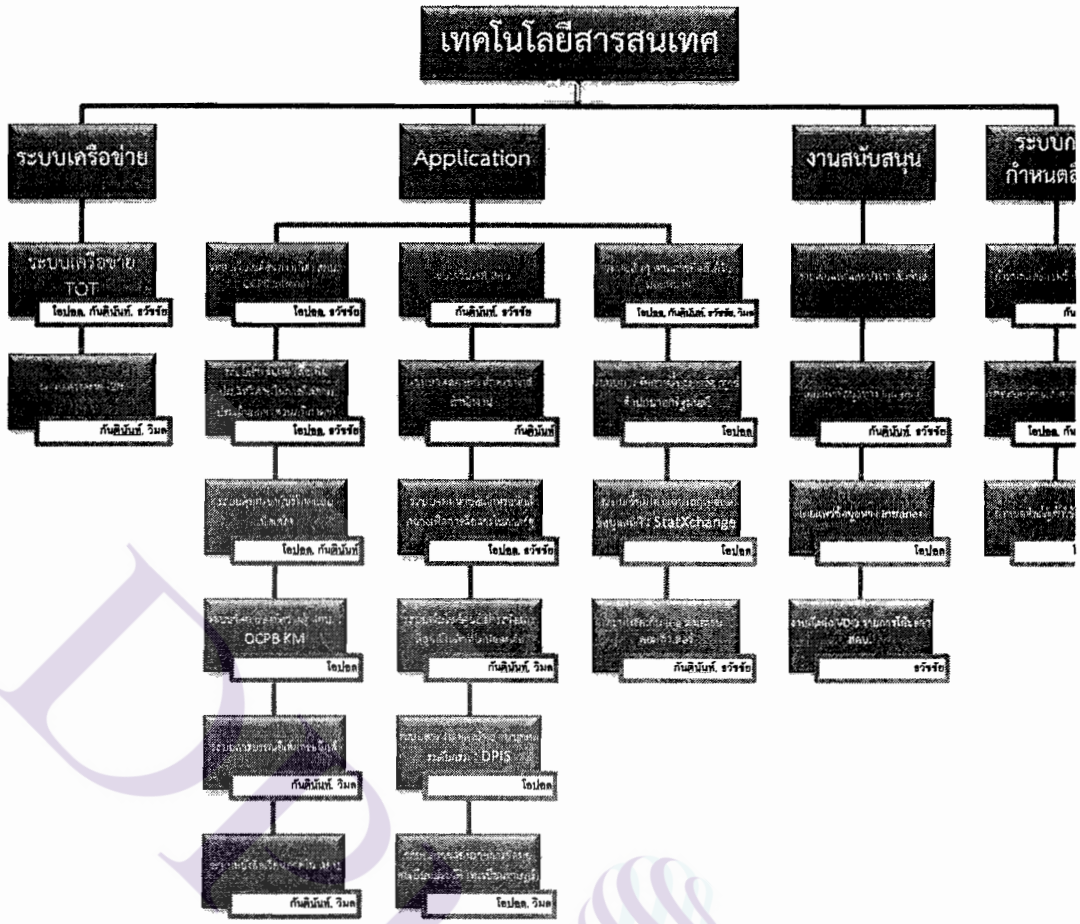
4.1.3 ศึกษาโครงสร้างขององค์กร ในการศึกษาโครงสร้างขององค์กรในด้านต่างๆ ทำให้ทราบขั้นตอนการทำงานและ กระบวนงานหลัก กระบวนงานสนับสนุน เพื่อข้อมูลนำมาวิเคราะห์และประเมินความเสี่ยงให้กับระบบ เช่น ระบุขอบเขตดำเนินงาน ระบุทรัพย์สิน มีการศึกษาระบบเครือข่าย กระบวนการ และโครงสร้างของระบบงานต่างๆ ได้แก่

4.1.3.1 ศึกษาโครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วง เพื่อนำมาวิเคราะห์ความปลอดภัยและการควบคุมการเข้าถึงข้อมูล รายละเอียดตามภาพที่ 4.2



ภาพที่ 4.2 ระบบเครือข่าย (Network System)

4.1.3.2 ศึกษาโครงสร้างระบบงานเทคโนโลยีสารสนเทศ



ภาพที่ 4.3 โครงสร้างระบบงานสารสนเทศ

4.1.3.2 ศึกษากระบวนการ (Process) ศึกษาถึงกระบวนการต่างๆ เช่น กระบวนการและขั้นตอนในการติดตั้ง เครื่องแม่ข่ายใหม่เพิ่มเติม วิเคราะห์โครงสร้างระบบเครือข่ายและอุปกรณ์ต่อพ่วงของระบบเทคโนโลยีสารสนเทศตามความเป็นจริง เพื่อนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยง เช่น การจัดการความเสี่ยงการใช้งานระบบสารสนเทศและอุปกรณ์ กรณีห้องเซิร์ฟเวอร์ เน้นหัวข้อสร้างความมั่นคงปลอดภัยทางกายภาพและควบคุมการเข้าถึง การระบุขอบเขตดำเนินงาน ระบุถึงทรัพย์สินความไม่มั่นคงของระบบและภัยคุกคามต่างๆ เป็นการรวบรวมข้อมูลหรือ สัมภาษณ์บุคคลที่เกี่ยวข้องและดูจากสถานที่จริงโดยผู้จัดทำได้แบ่งชนิดระบบสารสนเทศเฉพาะที่เกี่ยวข้องกับการดำเนินโครงงาน สามารถแบ่งได้หลายประเภท ได้แก่ กลุ่มเครื่องเซิร์ฟเวอร์

ที่ติดตั้งภายในห้องเซิร์ฟเวอร์ของหน่วยงานประกอบไปด้วย รายละเอียดและประเภทของเซิร์ฟเวอร์ตามลักษณะการใช้งานต่างๆ

4.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

จากการศึกษา รวบรวมข้อมูล ด้วยวิธีการต่างๆ นำมาวิเคราะห์และประเมินความเสี่ยง โดยมีการระบุขอบเขตการดำเนินงาน ระบุถึงทรัพย์สินความไม่มั่นคงปลอดภัยของระบบและภัยคุกคามต่างๆ จากการรวบรวมข้อมูล หรือ สัมภาษณ์บุคคลที่เกี่ยวข้อง และ ดูจากสถานที่จริงโดยผู้จัดทำได้แบ่งชนิดระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินโครงงาน เพื่อการวิเคราะห์ให้ใกล้เคียงความเป็นจริงมากที่สุด

การวิเคราะห์ความเสี่ยงในโครงงานนี้ เป็นการวิเคราะห์สถานะภาพของระบบเทคโนโลยีสารสนเทศ และศึกษากระบวนการจัดการความเสี่ยง เพื่อตรวจสอบและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศขององค์กรทำให้ทราบสาเหตุ ปัจจัย และเพื่อวัดผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นและนำไปใช้สร้างเกณฑ์กำหนดระดับในการประเมินความเสี่ยง (Risk Model) โดยจะต้องกำหนดเกณฑ์การประเมินผลกระทบต่อระดับของความปลอดภัย เกณฑ์การประเมินโอกาสในการเกิดภัยคุกคามความเสี่ยง และเกณฑ์ในการประเมินความเสี่ยง ซึ่งกระบวนวิเคราะห์ความเสี่ยงประกอบด้วย ขั้นตอนต่างๆ ประกอบด้วย การบ่งชี้ความไม่มั่นคงปลอดภัย (Vulnerability Identification) จัดกลุ่มทรัพย์สินกำหนดเกณฑ์ระดับการประเมินความเสี่ยงของระบบสารสนเทศที่จะประเมินความเสี่ยง การกำหนดประเภทภัยคุกคาม ซึ่งมีรายละเอียดดังนี้

4.2.1 การบ่งชี้ความไม่มั่นคงปลอดภัย (Vulnerability Identification) ของระบบสารสนเทศที่จะประเมินความเสี่ยง ซึ่งได้จากการรวบรวมจากการวิเคราะห์ ศึกษา สภาพ ICT ตามความเป็นจริงที่มี เช่น การระบุภัยคุมคาม/ช่องโหว่ระบบ ได้จาก

4.2.1.1 การสัมภาษณ์การใช้งานจาก ผู้ดูแลระบบ ผู้ใช้งานระบบ ผู้บริหาร

4.2.1.2 ติดตั้ง Software เพื่อตรวจสอบพฤติกรรมของผู้ใช้งานระบบ Internet Scanner เพื่อค้นหาช่องโหว่ ได้แก่ Nessus เพื่อค้นหาช่องโหว่ของระบบ Lancope เพื่อตรวจจับตรวจสอบช่องโหว่ของ Server ระบบงาน

4.2.1.3 ระบบเครือข่าย

4.2.14 ภัยคุกคามจากธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ไฟฟ้าดับ

การศึกษา วิเคราะห์ จากแหล่งข้อมูลต่างๆ ของสถานะภาพด้าน ICT ที่อาจบ่งชี้ถึงความไม่มั่นคงปลอดภัยของระบบสารสนเทศ สรุปรายละเอียดตามตารางที่ 4.1

ตารางที่ 4.1 ตารางบ่งชี้ความไม่มั่นคงปลอดภัยของระบบสารสนเทศ

ลำดับ	ความเสี่ยงไม่มั่นคงปลอดภัยของระบบสารสนเทศ
1.	ขาดการป้องกันทางกายภาพของประตูเข้า- ออก
2.	มีความรู้เกี่ยวกับความปลอดภัยระบบสารสนเทศไม่เพียงพอ
3.	ไม่มีนโยบายการใช้งานเครือข่ายบริการที่ชัดเจน
4.	ไม่มีการทบทวนสิทธิของผู้ใช้งานการเข้าถึงของผู้ใช้ระบบ
5.	ขาดการตรวจสอบระบบจากหน่วยงานภายนอก
6.	ไม่มีการลงทะเบียน ในการใช้ระบบอินเตอร์เนต ออกสู่ภายนอก
7.	ไม่มีนโยบายความปลอดภัยสารสนเทศที่ชัดเจนสำหรับภายในองค์กร
8.	ขาดบุคลากรทางด้าน IT
9.	การดูแลระบบงานขาดผู้รับผิดชอบที่ชัดเจน
10.	บุคลากรทางด้าน IT ขาดทักษะและความเชี่ยวชาญในการวิเคราะห์ระบบ
11.	ปริมาณแบนด์วิดที่ไม่เพียงพอ
12.	การโจมตีระบบจากภายในระบบเครือข่าย
13.	ระบบปฏิบัติการเครื่องไคลน์เอนด์ไม่ได้รับการปรับปรุง
14.	ระบบสำรองไฟฟ้าที่ไม่สามารถรองรับทำการเพื่ออุปกรณ์ในอนาคต
15.	การเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต เนื่องจากมีการป้องกันที่ไม่เหมาะสม
16.	การเข้าถึงระบบโดยใช้ User และ Password ของคนก่อน
17.	การปฏิเสธความรับผิดชอบ จากลักษณะงานหรือหน้าที่ความรับผิดชอบไม่ชัดเจน
18.	ไม่มีระบบเครือข่ายสำรองใช้งาน(Backup Line) เมื่อระบบเครือข่ายหลักล่ม
19.	ไม่มีคู่มือแสดงขั้นตอนการปฏิบัติงานของระบบเครือข่าย
20.	อุปกรณ์สำรองข้อมูล มีไม่เพียงพอ เช่น ขนาดความจุของ Hard Disk Storage
21.	เซิร์ฟเวอร์ Active Directory ที่ทำหน้าที่ตรวจสอบบัญชีของผู้ใช้กรุณาเข้าสู่ระบบบางเครื่องไม่ทำการ Join Domain
22.	ผู้ดูแลระบบงานต่างๆยังไม่สามารถทำงาน ในการวิเคราะห์ปัญหาจากการใช้งานระบบได้ ทำให้ขาดความต่อเนื่องในการปฏิบัติงานและไม่สามารถทำงานแทนกันได้อย่างต่อเนื่อง

ตารางที่ 4.1 (ต่อ)

ลำดับ	ความเสี่ยงไม่มั่นคงปลอดภัยของระบบสารสนเทศ
23.	การกำหนด ไฟร์วอลล์ ไม่รัดกุม เป็นแบบอนุญาตทั้งหมด ซึ่งมีความเสี่ยงที่จะทำให้ถูกโจมตีจากภายนอก และทำให้ระบบเซิร์ฟเวอร์ และเน็ตเวิร์กได้รับความเสียหายได้อาจส่งผลให้ระบบข้อมูลที่มีความสำคัญมีความเสียหายได้
24.	ความเสี่ยงเรื่องโครงสร้างระบบเครือข่ายเนื่องจากทางบริษัทไม่มีการแบ่งโซนแยกกันระหว่าง เซิร์ฟเวอร์ และไคลเอ็น
25.	สิทธิ์ในการรีโมทเข้าเครื่อง เซิร์ฟเวอร์ ไม่มีการควบคุม
26.	พบพนักงานสามารถการติดตั้งซอฟต์แวร์เองได้
27.	พบบัญชีรายชื่อ ของพนักงานที่ลาออกไปแล้วยังอยู่ในระบบ
28.	พบบัญชีรายชื่อที่มีการตั้งรหัส แบบไม่มีวันหมดอายุ (Password Never Expire)
29.	ไม่มีการกำหนดสิทธิ์การเข้าใช้งานระบบอินเตอร์เน็ตแล้วกำหนดสิทธิ์ ช่วงเวลาในการเข้าใช้งานของผู้ใช้
30.	ระบบฐานข้อมูลไม่มีการกำหนดสิทธิ์ในการเข้าใช้งาน
31.	เครื่องแม่ข่าย (Server) มีอายุการใช้งานเกิน 5 ปี

การระบุภัยประเภทภัยคุกคาม จากการวิเคราะห์สถานะด้านระบบเทคโนโลยีสารสนเทศ เช่น น้ำท่วม ไฟไหม้ ไฟฟ้าดับ ภัยคุกคามจากช่องโหว่ของอุปกรณ์ต่างๆ เป็นต้น สรุปได้ตามตารางที่ 4.2 ดังนี้

ตารางที่ 4.2 ตารางบ่งชี้ประเภทภัยคุกคามของระบบสารสนเทศ

ลำดับที่	ประเภทของภัยคุกคาม
1.	ภัยคุกคามที่เกิดจากการละเมิดทรัพย์สินทางปัญญา
2.	ภัยคุกคามจากการบุกรุก การเจาะระบบ
3.	ภัยคุกคามจากไม่มีนโยบายการใช้งานเครือข่ายบริการ
4.	ภัยคุกคามจากไม่มีการทบทวนสิทธิของผู้ใช้งาน การเข้าถึงของผู้ใช้
5.	ภัยคุกคามจากการขาดการตรวจสอบระบบบ่อยๆ
6.	ภัยคุกคามจากไม่มีการลงทะเบียน ในการออกสู่ระบบอินเตอร์เน็ตภายนอก
7.	ภัยคุกคามจากไม่มีนโยบายความปลอดภัยสารสนเทศที่ชัดเจน
8.	ภัยคุกคามจากขาดบุคลากรทางด้าน IT ที่มีประสิทธิภาพ
9.	ภัยคุกคามจากภัยธรรมชาติ
10.	ภัยคุกคามจากคุณภาพการให้บริการ
11.	ภัยคุกคามจากการโจรกรรมข้อมูล
12.	ภัยคุกคามจากการโจมตีซอฟต์แวร์
13.	ภัยคุกคามจากข้อผิดพลาดทางด้านฮาร์ดแวร์
14.	ภัยคุกคามจากการใช้เทคโนโลยีที่ทันสมัย
15.	ภัยคุกคามจากการขาดการกำกับ ดูแลระบบที่ดีในการควบคุมบริษัท Outsource ในการบำรุงรักษาระบบงานต่างๆ
16.	ภัยคุกคามจาก การไม่มีเอกสารในการจัดทำ Process เช่น ข้อกำหนดรายละเอียด เอกสารการออกแบบระบบ

4.2.2 ระบุทรัพย์สินด้าน ICT ที่จะประเมินความเสี่ยง /การกำหนดประเภทรายการทรัพย์สิน

การสำรวจและระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน ต้องมีการระบุทรัพย์สินสารสนเทศ เพื่อนำมาวิเคราะห์และประเมินความเสี่ยง ซึ่งมีการแบ่งหมวดหมู่และรายละเอียดของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Asset Inventory) ที่จำเป็นของทรัพย์สินตลอดจนแนวนโยบายด้านความมั่นคงปลอดภัยคงสารสนเทศขององค์กรที่อาจมีผลต่อองค์กรและระบุภัยคุกคามที่มีต่อแต่ละทรัพย์สิน แบ่งรายการทรัพย์สินต่างๆได้ 5 ประเภท โดยแยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ ได้แก่ ทรัพย์สินประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วง (Hardware Assets) ทรัพย์สินประเภทโปรแกรม (Software Assets) ทรัพย์สินประเภทบุคลากร

(People Assets) ทรัพย์สินด้านข้อมูล (Information Assets) และทรัพย์สินประเภทบริการ (Service Assets) มีรายละเอียด ดังนี้

4.2.2.1 ทรัพย์สินกลุ่มประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วงต่างๆ (Hardware Assets) จัดกลุ่มย่อย ๆ ได้แก่ กลุ่มเครื่องแม่ข่าย กลุ่มอุปกรณ์เครือข่าย รายละเอียดตามตารางข้างล่าง

(1) กลุ่มเครื่องแม่ข่าย

ตารางที่ 4.3 รายชื่อทรัพย์สิน กลุ่มเครื่องแม่ข่าย

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. Active Directory Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
2. Domain Name Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
3. File Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
4. Mail Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
5.Mail Gateway	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
6.Anti Virus Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
7. Proxy Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
8. Intranet Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
9. Log Server	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
10.เครื่องคอมพิวเตอร์แม่ข่ายระบบเบ็ดเสร็จ	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
11. เครื่องคอมพิวเตอร์แม่ข่ายระบบเรื่องราวร้องทุกข์ 1166	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
12.เครื่องคอมพิวเตอร์แม่ข่ายระบบงานสารบรรณ	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
13.เครื่องคอมพิวเตอร์ แม่ข่ายระบบรายงานผล ส่วนภูมิภาค	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
14.เครื่องคอมพิวเตอร์ แม่ข่ายระบบเว็บไซต์	กลุ่มเครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ

(2) กลุ่มอุปกรณ์เครือข่ายประกอบด้วยรายละเอียด ดังนี้

ตารางที่ 4.4 กลุ่มอุปกรณ์เครือข่าย

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. ตู้ Rack	กลุ่มอุปกรณ์เครือข่าย	สำนัก/กอง/ฝ่ายงานต่างๆ
2.Firewall	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
3 Core Switch	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน
4.Access Switch	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
5. Patch Panel	กลุ่มอุปกรณ์เครือข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
6. Core Switch	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน
7. Router ISP	กลุ่มอุปกรณ์เครือข่าย	บริษัท ทีโอที จำกัดมหาชน

(3) กลุ่มอุปกรณ์สื่อสารโทรคมนามและอื่นๆ รายละเอียด ดังนี้

ตารางที่ 4.5 กลุ่มอุปกรณ์สื่อสารโทรคมนาคมและอื่นๆ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
1. เครื่องคอมพิวเตอร์ (PC) จำนวน 228 เครื่อง	เครื่องลูกข่าย	สำนัก/กอง/ฝ่ายงานต่างๆ
2.เครื่องคอมพิวเตอร์ /Notebook	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
3. KVM Switch	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
4. UPS	อุปกรณ์	ฝ่ายเทคโนโลยีสารสนเทศ
5. ตู้ PBX	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
6. WiFi Access Control	อุปกรณ์สื่อสาร	บริษัท ทีโอที จำกัดมหาชน
7. สาย Fireber Optic E1	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
8. Central Copper wire	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ
9. Lease line link	อุปกรณ์สื่อสาร	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.2 ทรัพย์สินประเภทโปรแกรม (Software Assets) จัดแบ่งประเภทของโปรแกรมต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน ได้แก่ รายละเอียดตามตาราง 4.6 ข้างล่างนี้

ตารางที่ 4.6 รายชื่อทรัพย์สินประเภทโปรแกรม (Software)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบงานคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบ 1166	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบงานติดตามประเมินผลภูมิภาคและท้องถิ่น	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
Microsoft Office	โปรแกรมพื้นฐานทั่วไป	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบสารบรรณอิเล็กทรอนิกส์	โปรแกรมประยุกต์	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window XP Profession	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window 2005	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
OS Microsoft window 2008	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
Microsorft Exchange 2008	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ
KapeskyAnti Virus	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบฐานข้อมูล SQL Server 2008	ระบบฐานข้อมูล SQL	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบฐานข้อมูล SQL Server 2012	ระบบฐานข้อมูล SQL	ฝ่ายเทคโนโลยีสารสนเทศ
โปรแกรมป้องกันไวรัส	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.2.3 ทรัพย์สินประเภทบุคลากร (People Assets) จัดแบ่งประเภทโปรแกรมต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน รายละเอียดตามตารางที่ 4.7 ข้างล่างนี้

ตารางที่ 4.7 รายชื่อทรัพย์สินทางด้านบุคลากร (People Assets)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
บุคลากร	ผู้บริหารระดับสูง	ฝ่ายการเจ้าหน้าที่
บุคลากร	ผู้บริหารระดับกลาง	ฝ่ายการเจ้าหน้าที่
บุคลากร	อำนวยการระดับสูง	ฝ่ายการเจ้าหน้าที่
บุคลากร	อำนวยการระดับต้น	ฝ่ายการเจ้าหน้าที่
บุคลากร	ชำนาญการพิเศษ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ชำนาญการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ปฏิบัติการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	พนักงานทั่วไป	ฝ่ายการเจ้าหน้าที่
บุคลากร	พนักงานราชการ	ฝ่ายการเจ้าหน้าที่
บุคลากร	ลูกจ้างโครงการ	กอง/สำนัก

4.2.2.4 ทรัพย์สินข้อมูล (Information Assets) จัดแบ่งประเภทของข้อมูลต่างๆที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งาน รายละเอียดตามตารางที่ 4.8 ข้างล่างนี้

ตารางที่ 4.8 รายชื่อทรัพย์สินประเภทข้อมูล (Information Assets)

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบเว็บไซต์	ระบบฐานข้อมูล Access	ศูนย์เทคโน ฯ
ระบบ 1166	ระบบฐานข้อมูล SQL	ศูนย์เทคโน ฯ
ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	ระบบฐานข้อมูล SQL	ศูนย์เทคโน ฯ
ระบบสารบรรณอิเล็กทรอนิกส์	ระบบฐานข้อมูล Oracle	ศูนย์เทคโน ฯ
ระบบ Dpis (บุคลากร)	ข้อมูลบุคลากร	ศูนย์เทคโน ฯ
ระบบ e-Mail	ข้อมูลภายใน	ศูนย์เทคโน ฯ
ระบบหนังสือเวียน	ข้อมูลภายใน เฉพาะ	ศูนย์เทคโน ฯ

4.2.2.5 ทรัพย์สินประเภทบริการ (Service Assets) สามารถจัดแบ่งประเภทการบริการต่างๆ ที่เป็นทรัพย์สินโดยแยกตามลักษณะความจำเป็นในการใช้งานรายละเอียด ดังนี้

ตารางที่ 4.9 รายชื่อทรัพย์สินด้านงานบริการ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
งานบริการ Internet	ให้บริการเผยแพร่ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการ Intranet	ให้บริการเผยแพร่ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการ ตัดต่อภาพ แปลง File	ให้บริการ	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการติดตั้ง บำรุงรักษา อุปกรณ์เครื่อง PC	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการติดตั้ง บำรุงรักษา โปรแกรมคอมพิวเตอร์	บำรุงรักษา (Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริหารจัดการสิทธิ ในการเข้าถึงข้อมูล การเข้าใช้งานระบบต่างๆ	Computing (Admin)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบำรุงรักษาระบบเครื่องแม่ข่าย	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ
งานบำรุงรักษา ระบบเครือข่าย	บำรุงรักษา(Outsource)	ฝ่ายเทคโนโลยีสารสนเทศ

4.2.3 กำหนดเกณฑ์การประเมินระดับความเสี่ยงของระบบด้วย Risk Assessment Matrix ได้แก่ ระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) รายละเอียดแสดงได้ ดังนี้

4.2.3.1 ระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) ตามตารางที่ 4.10 ดังนี้

ตารางที่ 4.10 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสเกิดขึ้นสูงมาก
4	สูง	มีโอกาสเกิดขึ้นค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดขึ้นบางครั้ง
2	น้อย	อาจจะมีโอกาสเกิดขึ้นแต่นานๆครั้ง
1	น้อยมาก	อาจจะไม่มีโอกาสเกิดขึ้นเลย

4.2.3.2 ระดับความรุนแรงของผลกระทบ (Impact) ตามตารางที่ 4.11

ตารางที่ 4.11 เกณฑ์การประเมินผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (Impact)

	ระดับความรุนแรงของผลกระทบของความเสี่ยง(Impact)	
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	มีผลกระทบมาก ระบบเสียหายทั้งหมดไม่สามารถใช้งานอีกต่อไป/ข้อมูลที่สำคัญเสียหายทั้งหมด ทำให้องค์กรเสียหายมาก
4	สูง	มีผลกระทบต่อความปลอดภัยของระบบเสียหายบางส่วน ไม่สามารถใช้งานได้ตามปกติ/ข้อมูลที่เป็นความลับ ถูกเปิดเผยมีผลกระทบร้ายแรงต่อองค์กรมากต้องใช้ระยะเวลาในการกู้คืนระบบ
3	ปานกลาง	มีผลกระทบต่อความปลอดภัยของระบบเสียหายหายทั้งหมดบางส่วน ไม่สามารถใช้งานชั่วคราวได้ตามปกติ/ข้อมูลที่เป็นความลับ ถูกเปิดเผยมีผลกระทบร้ายแรงต่อองค์กรมาก
2	ต่ำ	มีผลกระทบต่อความปลอดภัยเล็กน้อย ระบบสามารถใช้งานได้ตามปกติ/ข้อมูลที่เปิดเผยไม่มีผลกระทบหรือไม่สำคัญต่อองค์กรมีไม่มากนัก
1	ต่ำมาก	มีผลกระทบต่อความปลอดภัยเล็กน้อย ระบบสามารถใช้งานได้ตามปกติ/ข้อมูลที่เปิดเผยไม่มีผลกระทบหรือไม่สำคัญต่อองค์กร

การวิเคราะห์ความเสี่ยง (Risk Analysis) และเกณฑ์ในการประเมินความเสี่ยง ในโครงงานนี้จะนำผลของการประเมินความเสี่ยงประยุกต์ใช้ในการบริหารจัดการด้านเทคโนโลยีสารสนเทศและวางแผนการบริหารจัดการความเสี่ยง พร้อมทั้งจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ฉบับที่ 2 ประจำปี 2556-2559 (ซึ่งอยู่ระหว่างดำเนินการจัดทำ) และแผนปฏิบัติราชการ 4 ปี โดยศึกษาวิเคราะห์ระบบเทคโนโลยีสารสนเทศขององค์กรทั้งหมดในปัจจุบัน เพื่อหาสาเหตุ ปัจจัย และวัดผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นและหาแนวทางแก้ไข พร้อมทั้งวางแผนจัดเตรียมการวิเคราะห์ เพื่อของบประมาณด้าน ICT ประจำปี ตามเหตุผลความจำเป็นที่หน่วยงานต้องการปิดช่องโหว่ของระบบและแก้ไข ป้องกันปัญหาที่อาจจะเกิดขึ้นได้จากการวิเคราะห์และประเมินความเสี่ยง

4.3 การประเมินความเสี่ยงก่อนการดำเนินโครงการ

การประเมินความเสี่ยง (Risk Assessment) หมายถึง การคาดคะเนหรือคำนวณโอกาสที่จะเกิดเหตุการณ์ที่นำไปสู่ความเสียหายและมีการสูญเสียเกิดขึ้น จากการที่มีกระบวนการ/ขั้นตอนจากการระบุ/สินทรัพย์ เรียบร้อยแล้วก็นำมาสู่หลักการของประเมินความเสี่ยง(Risk Assessment) และคำนวณค่าความเสี่ยงโดยรวมซึ่งประกอบด้วย ขั้นตอนการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยง เพื่อการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กร เช่น ต้องการทราบว่ามีอะไรบ้างที่จะเป็นจุดอ่อน หรือช่องโหว่ เป็นสาเหตุให้เกิดภัยคุกคามซึ่งนำมาให้เกิดความเสียหายและผลกระทบต่อองค์กร เมื่อถูกโจมตีจุดอ่อน หรือช่องโหว่ที่มีอยู่ หรือมูลค่าทรัพย์สินขององค์กรเสียหาย มีอะไรบ้างและจำนวนเท่าไร เราจะป้องกันหรือแก้ไขช่องโหว่ หรือจุดอ่อนได้อย่างไร

ในการพิจารณาจากระดับความสำคัญของทรัพย์สิน ซึ่งผลลัพธ์การประเมินจะทำให้ทราบระดับความเสี่ยงต่อทรัพย์สินแต่ละอย่าง ทั้งที่ยอมรับได้และยอมรับไม่ได้ ซึ่งจะทำให้ได้แผนงานในการดำเนินงาน การเตรียมรับมือ ป้องกันความเสี่ยงที่เกิดขึ้น โดยจะต้องผ่านการอนุมัติจากผู้บริหารขององค์กร โดยกำหนดมาตรการที่เหมาะสมอ้างอิงตามมาตรฐานความปลอดภัยสากล ISO/IEC 17799, BS7799 และ ISO/IEC 27001 ทำให้ทราบถึงความสำคัญของความเสี่ยงที่แตกต่างกันและใช้ในการพิจารณากำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ การประเมินความเสี่ยงเป็นกระบวนการ ที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กรก่อนที่จะทำการประเมินความเสี่ยง เพื่อให้เกิดความชัดเจนในการประเมิน ประกอบด้วยขั้นตอนและข้อมูลต่างๆ ซึ่งสามารถสรุปได้ดังต่อไปนี้

(1) ระบุปัจจัยในกระบวนการประเมินความเสี่ยงซึ่ง ได้แก่ ทรัพย์สิน (Assets) ช่องโหว่ (Vulnerabilities) ภัยคุกคาม (Treats) ผลกระทบต่อธุรกิจ (Business Impact) และการควบคุม (Controls) จากการวิเคราะห์ความเสี่ยงเพื่อการนำข้อมูลที่ได้มาประเมินความเสี่ยง ดังนี้

การประเมินความเสี่ยงก่อน การดำเนินโครงการ จะใช้ Risk Calculation

Risk Value = Likelihood (โอกาสที่จะเกิด) X Impact (ผลกระทบ)

Risk Value = ค่าความเสี่ยง

Likelihood = โอกาสที่จะเกิด

Impact = ผลกระทบ

(2) การประเมินโอกาสและผลกระทบของความเสี่ยง วิเคราะห์ระดับความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงที่ระบุไว้มาประเมินโอกาสที่จะเกิดความเสียหาย (Likelihood) และประเมินระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์การประเมินความเสี่ยงขององค์กร ตามระดับของความเสี่ยง (Degree of Risk) ที่แตกต่างกัน กำหนดเกณฑ์ระดับความเสี่ยงไว้ 3 ระดับ ได้แก่ ต่ำ ปานกลาง สูง ดังนี้

ระดับความเสี่ยง 1 – 8 ต่ำ (Low)

ระดับความเสี่ยง 9 – 16 กลาง (Medium)

ระดับความเสี่ยง 17 – 25 สูง (High)

รายละเอียด การคำนวณประเมินความเสี่ยง (Risk Value) ตามตารางข้างล่างนี้

ตารางที่ 4.12 การคำนวณประเมินความเสี่ยง (Risk Value)

Risk Value		Likelihood				
		Very Low	Low	Medium	High	Very High
	Very low	1	2	3	4	5
	Low	2	4	6	8	10
	Medium	3	6	9	12	15
	High	4	8	12	16	20
	Very High	5	10	15	20	25

(3) การวัดและประเมิน เพื่อให้ผู้บริหารเข้าใจและรับรู้ถึงความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศและมีการกำหนดแผนปฏิบัติในการลดความเสี่ยงดังกล่าว ให้อยู่ในระดับที่ยอมรับได้ (Risk Acceptance Level)

(4) ขั้นตอนในการวิเคราะห์ หาวิธีการในการควบคุมความเสี่ยง (Control Analysis) หลังจากได้ทำการรวบรวมข้อมูลและศึกษาข้อมูลเกี่ยวกับระบบ ตลอดจนสามารถระบุภัยคุกคามและช่องโหว่ต่างๆ ของระบบได้แล้ว ขั้นตอนต่อไปคือวิเคราะห์วิธีการหรือแนวทางใน การควบคุมความเสี่ยงที่หน่วยงาน มีการดำเนินการอยู่แล้วในปัจจุบันหรือมีแผนที่จะดำเนินการกิจกรรมโครงการใน อนาคตอันใกล้ โดยอาศัย การควบคุมความมั่นคงปลอดภัย (Control Checklist) ของ ISO/IEC 27001 ที่ได้จากการประเมินความเสี่ยง

4.3.1 การประเมินความเสี่ยง (Risk Assessment) ก่อนการดำเนินโครงการ มีการจัดทำตารางวิเคราะห์และประเมินความเสี่ยงก่อนดำเนินโครงการ รายละเอียดดังนี้

4.3.1.1 ตารางระบุขอบเขตประเมินความเสี่ยงตามกลุ่มทั้ง 11 โดเมน ด้วยมาตรฐาน ISO/IEC 27001 วิเคราะห์ตามวัตถุประสงค์ที่จำเป็น ตามรายละเอียด (ภาคผนวก ก)

4.3.1.2 ตารางประเมินความเสี่ยงแยกตามกลุ่มสินทรัพย์ ในการประเมินทรัพย์สินและบริหารความเสี่ยงโดยแบ่งระบุสินทรัพย์ได้ 5 ประเภท โดยแยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ ได้แก่ (1) ทรัพย์สินประเภทฮาร์ดแวร์และอุปกรณ์ต่อพ่วง (Hardware Assets) (2) ทรัพย์สินประเภทซอร์ฟแวร์ (Software Assets) (3) ทรัพย์สินข้อมูล (Information Assets)

(4) ทรัพย์สินประเภทบริการ (Service Assets) (5) ทรัพย์สินประเภทบุคคลากร(People Assets) ตามรายละเอียด (ภาคผนวก ข)

4.3.2 การตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยตรวจสอบช่องโหว่ หรือจุดอ่อนด้วยโปรแกรมต่างๆ ที่มีการโจมตีทั้งจากภายในและภายนอก ได้แก่ (1) ด้วยโปรแกรม Nessus (2)โปรแกรม Lancope (3) การจัดลำดับความสำคัญของความเสี่ยง

4.4 ปิดช่องโหว่ของระบบ(Hardening) และดำเนินการปรับปรุงให้ระบบมีความปลอดภัยมากขึ้น

จากการวิเคราะห์และประเมินความเสี่ยง ก่อนการดำเนินโครงการ แล้วนำผลวิเคราะห์มาทบทวนพิจารณาและมีการตรวจสอบ ช่องโหว่/ จุดอ่อนของระบบ เพื่อควบคุม แก้ไขปัญหาความเสี่ยงเบื้องต้นที่สามารถจัดการได้โดย ยังไม่มีการใช้งบประมาณ เมื่อองค์กรได้ดำเนินการและทราบผลการประเมินความเสี่ยงก่อนและนำมาปรับปรุง ก็จะทำการประเมินความเสี่ยงอีกครั้ง เพื่อนำผลที่ได้มาวิเคราะห์เปรียบเทียบ และปิดช่องโหว่ ของระบบเทคโนโลยีสารสนเทศ ที่สามารถดำเนินการได้ในแบบพื้นฐานสำคัญ ดังนี้

4.4.1 การควบคุมการเข้าถึงระบบ ทบทวนแนวปฏิบัติพื้นฐาน เพื่อให้เกิดความปลอดภัยของระบบในเบื้องต้น ได้แก่

4.4.1.1 การตรวจสอบระบบต่างๆ ได้แก่ ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ป้องกันการให้บริการทางเครือข่าย ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาต

4.4.1.2 ควบคุมการเข้าถึงข้อมูล

4.4.1.3 มีการควบคุมการเข้าออก (Physical entry Control)

4.4.2 มีการระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets) มีการจัดทำฉลากให้ทราบผู้รับผิดชอบทรัพย์สินต่างๆ

4.4.2.1 เพื่อกำหนดผู้รับผิดชอบให้ชัดเจน ได้แก่ การลดความเสี่ยงที่อาจเกิดเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกงหรือหลอกลวง การใช้งานระบบในทางที่ผิด

4.4.2.2 เพื่อให้มั่นใจว่าผู้ใช้มีความระมัดระวังเกี่ยวการรักษาความปลอดภัยของข้อมูลและมีระบบป้องกัน เช่น รองรับนโยบายทางด้านการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน การวางแผนความเสี่ยงเพื่อลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์การทำงานที่ผิดพลาดของระบบ

4.4.3 จัดทำเอกสารแสดงนโยบาย ISMS

4.4.3.1 เอกสารข้อกำหนดรายละเอียดของระบบงาน

4.4.3.2 จัดทำคู่มือวิธีการปฏิบัติงาน และการควบคุมเพื่อสนับสนุนต่อ ISMS

4.4.3.3 รายงานต่างๆ ที่จำเป็น

4.4.3.4 เอกสารวิธีการปฏิบัติงานที่จำเป็นสำหรับองค์กร เพื่อให้มั่นใจได้ถึงความมีประสิทธิผลในการวางแผนการดำเนินงาน

4.5 การประเมินความเสี่ยงหลังดำเนินโครงการ

มีการตรวจสอบ ช่องโหว่/ จุดอ่อนของระบบ เพื่อควบคุม แก้ไข ปัญหาความเสี่ยงเบื้องต้นที่สามารถจัดการได้โดย ยังไม่มีการใช้งบประมาณ เมื่อองค์กร ได้ดำเนินการและทราบผลการประเมินความเสี่ยงก่อนและนำมาปรับปรุง ก็จะทำการประเมินความเสี่ยงอีกครั้ง เพื่อนำผลที่ได้มาวิเคราะห์เปรียบเทียบ ระหว่างการวิเคราะห์และประเมินความเสี่ยง ทั้งก่อน-หลังการดำเนินโครงการ

4.6 การจัดการความเสี่ยง(Risk Management)

โดยควบคุม แก้ไข ปัญหาการจัดการความเสี่ยง เมื่อองค์กร ได้ดำเนินการและทราบผลการประเมินความเสี่ยงก็จะได้รับทราบประกอบด้วยขั้นตอนและข้อมูลต่างๆ ซึ่งมีการบริหารความเสี่ยงได้หลายวิธี ได้แก่ การลดความเสี่ยง การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง การยอมรับความเสี่ยงที่เหลืออยู่มีรายละเอียด ดังนี้

4.6.1 การลดความเสี่ยง

4.6.1.1 จัดทำ Check List ตามมาตรฐาน ISO 27001 เพื่อตรวจสอบและเก็บข้อมูลจากผู้มีส่วนได้เสียและผู้ที่เกี่ยวข้องในการใช้งานและมีผลกระทบระบบ ICT

4.6.1.2 นำผลการวิเคราะห์ นำเสนอที่ประชุมผู้บริหาร หรือคณะกรรมการ ICT ของสำนักงาน เพื่อรับข้อเสนอแนะ จากผู้เชี่ยวชาญด้าน ICT มาวิเคราะห์และจัดหมวดหมู่ จัดกลุ่มแยกประเภท เพื่อการบริหารจัดการความเสี่ยงในด้าน ICT ภายใต้การควบคุม

การควบคุม หมายถึง ความเสี่ยงที่ยอมรับได้แต่ต้องมีการแก้ไขเกี่ยวกับการควบคุมที่มีอยู่ในปัจจุบัน เพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น จัดทำแผนการดำเนินงาน จัดทำแผนงานบริหารความเสี่ยง จัดทำแผนฉุกเฉิน เป็นต้น

4.6.1.3 นำข้อมูลเบื้องต้นด้านอื่นๆ ที่เกี่ยวข้อง รวมทั้ง Check List มาวิเคราะห์ เพื่อหาแนวทาง จัดทำข้อเสนอในการบริหารจัดการความเสี่ยงด้าน ICT เพื่อให้มีการทบทวน ปรับปรุง จัดทำนโยบายความปลอดภัยระบบสารสนเทศ (Policy) และนำมาจัดทำแผนฉุกเฉิน

4.6.2 หลีกเลี่ยง หรือ ยกเลิกความเสี่ยง หมายถึง ความเสี่ยงที่ไม่สามารถยอมรับได้และต้องจัดการให้ความเสี่ยงนั้นอยู่นอกเหนือเงื่อนไขการดำเนินงาน โดยต้องมีวิธีการจัดการความเสี่ยงในกลุ่มนี้ให้เหมาะสม อาจจะเกี่ยวข้องกับงบประมาณในการดำเนินการ

4.6.3 ถ่ายโอนความเสี่ยง คือการถ่ายโอนความเสี่ยงให้กับบุคคลภายนอกรับผิดชอบแทน แต่ในกรณีของหน่วยงานภาครัฐ จะมีปัจจัยหลายอย่างที่เกี่ยวข้อง เช่น ข้อจำกัดด้านงบประมาณ ความเหมาะสมตามภารกิจ ข้อจำกัดด้านบุคลากร

4.6.4 ยอมรับความเสี่ยงที่มีอยู่ (Accept Risk) คือความเสี่ยงที่เกิดขึ้นสามารถยอมรับได้ ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องมีการดำเนินการใดๆ

4.6.5 วางแผนฉุกเฉิน ต้องมีแผนการในการจัดทำแผนฉุกเฉินเพื่อรองรับความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งมีผลกระทบต่อการให้การบริการประชาชน

4.7 สรุปผลการวิเคราะห์และประเมินความเสี่ยง

จากการวิเคราะห์ความเสี่ยงระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค โดยพิจารณาจาก การให้ความสำคัญของระดับของผลกระทบ และโอกาสในการเกิดภัยคุกคาม รวมทั้งชนิดของภัยคุกคามที่อาจเกิดขึ้น ซึ่งได้แยกการพิจารณาตามประเภทของทรัพย์สินสารสนเทศขององค์กร

4.8 นำมาประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

ผลที่ได้จากการวิเคราะห์ความเสี่ยงระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค นำมาพัฒนาปรับปรุงนโยบายความปลอดภัยระบบสารสนเทศ ใช้ในการวางแผนการจัดการดำเนินงานต่างๆ จัดทำแผนงานบริหารความเสี่ยงของหน่วยงาน รวมทั้งการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) ปี 2556-2559

บทที่ 5
ผลการดำเนินงาน

จากการศึกษาวิจัย ตามขั้นตอนในบทที่ 4 ได้นำผลการวิเคราะห์และประเมินความเสี่ยงมาจัดหมวดหมู่แยกประเภทตามมาตรฐาน ISO/IEC 27001 ทั้ง 11 โดเมน โดยสรุปตามระดับของความเสี่ยงที่ประเมินได้ 3 ระดับ ได้แก่ ต่ำ ปานกลาง สูง ดังนี้

ระดับความเสี่ยง 1 – 8 คือ ระดับความเสี่ยงต่ำ (Low) ยังไม่จำเป็นต้องมีการจัดการในขณะนี้ก็ได้ไม่มีผลกระทบต่อการทำงานขององค์กรมากนัก แต่ควรมีแผนการดำเนินงานหรือพัฒนาปรับปรุงงานให้มีประสิทธิภาพยิ่งขึ้น

ระดับความเสี่ยง 9 – 16 คือ ระดับความเสี่ยงกลาง (Medium) องค์กรเริ่มมองว่าเป็นระดับความเสี่ยงที่มีความสำคัญ ควรมีการปรับปรุงแต่ยังไม่เร่งด่วน แต่ควรอยู่ในแผนการดำเนินงานขององค์กรในระยะยาว ซึ่งต้องมีการวางแผนการดำเนินงานไว้ล่วงหน้า

ระดับความเสี่ยง 17 – 25 คือ ระดับความเสี่ยงสูง (High) องค์กรต้องมองว่าเป็นระดับความเสี่ยงที่มีสำคัญมาก มีโอกาสเกิดความเสียหายที่เกิดขึ้นสูง ต้องมีการจัดการอย่างเร่งด่วน ควรกำหนดอยู่ให้อยู่ในแผนการดำเนินงานระยะสั้น แผนการดำเนินงานทั้งระยะกลางและระยะยาว ซึ่งแสดงให้เห็นถึงความจำเป็นอย่างยิ่งและต้องมีการบริหารจัดการโดยเร็ว เพื่อป้องกันความเสียหายที่จะเกิดขึ้น

มีผลการดำเนินงานสรุปได้ 3 ระยะ ได้แก่ ผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนการดำเนินโครงการ) นำผลการวิเคราะห์มาดำเนินการปรับปรุงระบบสารสนเทศ และ มีการวิเคราะห์และประเมินความเสี่ยง(หลังดำเนินโครงการ) โดยมีผลการดำเนินงาน ดังนี้

5.1 ผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนการดำเนินโครงการ)

วัตถุประสงค์

1. เพื่อให้ทราบถึงความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กรที่อาจจะเกิดขึ้น
2. เพื่อทราบถึงช่องโห่ว/จุดอ่อน ด้านเทคโนโลยีสารสนเทศในปัจจุบัน
3. เพื่อนำผลการวิเคราะห์และประเมินความเสี่ยงไปประยุกต์ใช้งานต่างๆ

จากการวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 ก่อนการดำเนินโครงการทำให้ศูนย์เทคโน ฯ ทราบถึงความเสี่ยง จุดอ่อน/ช่องโหว่ ของระบบและเครือข่ายที่มีอยู่ในปัจจุบัน ซึ่งสรุปผลการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ 11 หัวข้อ (Domain) รายละเอียด ภาคผนวก ค ตารางผลการวิเคราะห์และประเมินความเสี่ยง(ก่อนดำเนินโครงการ) ได้ผลสรุปตามตารางที่ 5.1 ดังนี้

ตารางที่ 5.1 สรุปผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนดำเนินโครงการ)

11 หัวข้อ(ก่อนดำเนินโครงการ)	ระดับความเสี่ยง		
	สูง	กลาง	ต่ำ
1.นโยบายความมั่นคงปลอดภัย (Security policy) –A5	3	-	-
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) –A6	3	2	-
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)-A7	1	4	-
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources ecurity) – A8	1	6	2
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) – A9	2	5	2
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management) – A10	5	2	1
7.การควบคุมการเข้าถึง (Access control) – A11	4	1	1
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) – A12	4	2	1

ตารางที่ 5.1 (ต่อ)

11 หัวข้อ(ก่อนดำเนินโครงการ)	ระดับความเสี่ยง		
	สูง	กลาง	ต่ำ
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) – A13	-	2	-
10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity) – A14	4	-	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	-	1	2
รวม	27	25	9

การสรุปข้อมูลจากรายละเอียดใน (ภาคผนวก ค) ขออธิบายเพิ่มเติมถึงวิธีการผลสรุปผลที่ได้ตามตารางที่ 5.1 ดังตามตัวอย่างที่ 1 ข้างล่างนี้เพื่อความเข้าใจที่ชัดเจน

ตัวอย่างที่ 1. ผลการวิเคราะห์จากรายละเอียดในภาคผนวก ค สรุปได้ตาราง 5.1 ข้อ 1 นโยบายความมั่นคงปลอดภัยสำหรับองค์กร(Security Policy) – A5 และตามมาตรฐาน ISO/IEC 27001 ดังนี้

ตารางที่ 5.2 ตารางการวิเคราะห์และประเมินความเสี่ยงข้อ 1 (ก่อนดำเนินโครงการ) ตามภาคผนวก ค

ข้อ 1	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
1.1	ยังไม่มีการประกาศใช้นโยบายด้านความปลอดภัยเป็นทางการ	ยังไม่ได้จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบ	5	5	25	สูง
1.2	ไม่มีการกำหนดหน้าที่และความรับผิดชอบในการจัดทำนโยบายความปลอดภัยและแนวปฏิบัติ	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบดูแลระบบสารสนเทศอย่างชัดเจน	5	5	25	สูง

ตารางที่ 5.2 (ต่อ)

ข้อ 1	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
1.3	ไม่มีการทบทวนปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัย	มีการละเมิดด้านความมั่นคงปลอดภัยขององค์กร	4	5	20	สูง

ผลสรุปได้ ตามหัวข้อที่ 1 ตารางที่ 5.1 ระดับความเสี่ยงสูง = 3 หัวข้อย่อย ได้แก่ 1.1-1.3 ตัวอย่างที่ 2. นำผลการวิเคราะห์จากรายละเอียดในภาคผนวก ค สรุปได้ในตาราง 5.1 ในข้อ 2 ของโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security) – A6 ตามมาตรฐาน ISO/IEC 27001 ได้ตามตารางที่ 5.3 รายละเอียดดังนี้

ตารางที่ 5.3 ตารางการวิเคราะห์และประเมินความเสี่ยง ข้อ2 (ก่อนดำเนินโครงการ) ในภาคผนวก ค

ข้อ 2	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
2.1	ไม่สามารถผลักดันนโยบายด้านความปลอดภัยให้ชัดเจน	ขาดการกำหนดประสานงานด้านความมั่นคงปลอดภัยระบบจากสำนัก/กอง	5	4	20	สูง
2.2	ระบบสารสนเทศไม่มีความมั่นคงปลอดภัยเนื่องจากขาดผู้รับผิดชอบและดูแลอย่างจริงจัง	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบดูแลระบบสารสนเทศอย่างชัดเจน	5	4	20	สูง

ตารางที่ 5.3 (ต่อ)

ข้อ 2	ประเด็นความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส	ผลการวิเคราะห์	ระดับความเสี่ยง
2.3	การเข้าถึงระบบและข้อมูลสำคัญโดยไม่ได้รับอนุญาต	มีการระบุข้อกำหนดหรือเงื่อนไขในการเข้าถึงระบบงานหรือสารสนเทศขององค์กร	5	2	10	กลาง
2.4	ข้อมูลสำคัญรั่วไหลหรือถูกเปิดเผยโดยบุคคลผู้ไม่มีสิทธิ์ทั้งภายในและนอกองค์กร	ไม่มีการจัดทำข้อตกลงการไม่เปิดเผยความลับด้านข้อมูลและเอกสารขององค์กร	5	4	20	สูง
2.5	ไม่มีการจัดทำแผนฉุกเฉิน กรณีระบบมีปัญหา	ไม่สามารถกู้ระบบได้ตามเวลาที่เหมาะสมอาจส่งผลกระทบต่อการทำงาน	4	4	16	กลาง

ผลสรุป ตามหัวข้อที่ 2 ตารางที่ 5.1 ข้างบน ระดับความเสี่ยงสูง = 3 ได้แก่ หัวข้อ 2.1, 2.2 และ 2.4 ระดับความเสี่ยงกลาง = 2 ได้แก่หัวข้อ 2.3 และ 2.5

5.2 นำผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนดำเนินโครงการ) เพื่อการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ โดยดำเนินการ ดังนี้

5.2.1 นำมาพัฒนาและปรับปรุงแนวคิดในการจัดทำนโยบายด้านความปลอดภัย (Security Policy Development) ตามมาตรฐานและแนวปฏิบัติของมาตรฐาน ISO/IEC 27001 โดยนำผลการวิเคราะห์และประเมินความเสี่ยง เข้าประชุมคณะกรรมการด้านระบบสารสนเทศเพื่อคัดเลือกหัวข้อ

ที่จะใช้ กำหนดนโยบายด้านความปลอดภัย ซึ่งประกอบด้วย 11 หัวข้อ (Domain) สรุปได้ตามตารางที่ 5.4 ดังนี้

ตารางที่ 5.4 สรุปผลการจัดทำนโยบายความปลอดภัย

หัวข้อ(Domain)	จัดทำนโยบายความปลอดภัย	
	ทำ	ไม่ทำ
1. A5-นโยบายความมั่นคงปลอดภัย (Security policy)	/	
2. A6 -โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)		/
3. A7 -การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)		/
4.A8-ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources ecurity)	/	
5.A-9 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	/	
6. A-10 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management)	/	
7.A-11 การควบคุมการเข้าถึง (Access control)	/	
8.A-12 การจัดหา การพัฒนา และการบำรุงรักษาระบบ การจัดหาการพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)	/	
9.A-13 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ขององค์กร (Information security incident management)		/
10.A-14 บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity)	/	
11.A-15 การปฏิบัติตามข้อกำหนด (Compliance)		/
รวม	7	4

สามารถนำมาจัดหมวดหมู่แยกตามประเด็นความเสี่ยงสิ่งที่ต้องจัดทำก่อนได้ หลังจากนั้นนำผลการวิเคราะห์และการเลือกหัวข้อ สิ่งที่ต้องปรับปรุงนโยบายความปลอดภัยระบบสารสนเทศและแนวปฏิบัติตามมาตรฐาน ISO/IEC 27001 ปี 2556 สรุปได้ 7 หัวข้อประกอบด้วย

1. A5 - นโยบายความมั่นคงปลอดภัย (Security Policy)

2. A8 - ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resource security)

3. A9 - การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

4. A10 - การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายสารสนเทศขององค์กร(Communications and operations management)

5. A11- การควบคุมการเข้าถึง (Access control)

6. A12- การจัดหา การพัฒนา และการบำรุงรักษาระบบ การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ(Information systems acquisition, development and maintenance)

7. A14 - การบริหาร ความต่อเนื่องในการดำเนินงานขององค์กร(Business continuity)

จากหัวข้อดังกล่าวข้างต้นคณะกรรมการ ICT ได้เลือก มีความสอดคล้องตามข้อกำหนดในการจัดทำนโยบายของกระทรวง ICT (สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,กันยายน 2556, น 4) มีรายละเอียดเกี่ยวกับความเสี่ยงที่ต้องบริหารจัดการอย่างเร่งด่วนและมีความจำปีน ซึ่งผู้ศึกษาวิจัยได้ร่วมจัดทำและตรวจสอบนโยบายที่ได้ปรับปรุงเรียบร้อยแล้วรายละเอียดตาม (ภาคผนวก จ)

ส่วนหัวข้อที่ไม่ๆได้เลือกในการพัฒนาปรับปรุงและจัดทำนโยบาย ความปลอดภัยระบบสารสนเทศและแนวปฏิบัติตามมาตรฐาน ISO/IEC 27001 ในครั้งนี้ก็มีความสำคัญแต่จะพิจารณาจากความเร่งด่วน โดยอาจจะพัฒนาในปี 2557-2558 สรุปได้ 4 หัวข้อประกอบด้วย

1. A6 – โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร(Organization of information security)

2. A7 - การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

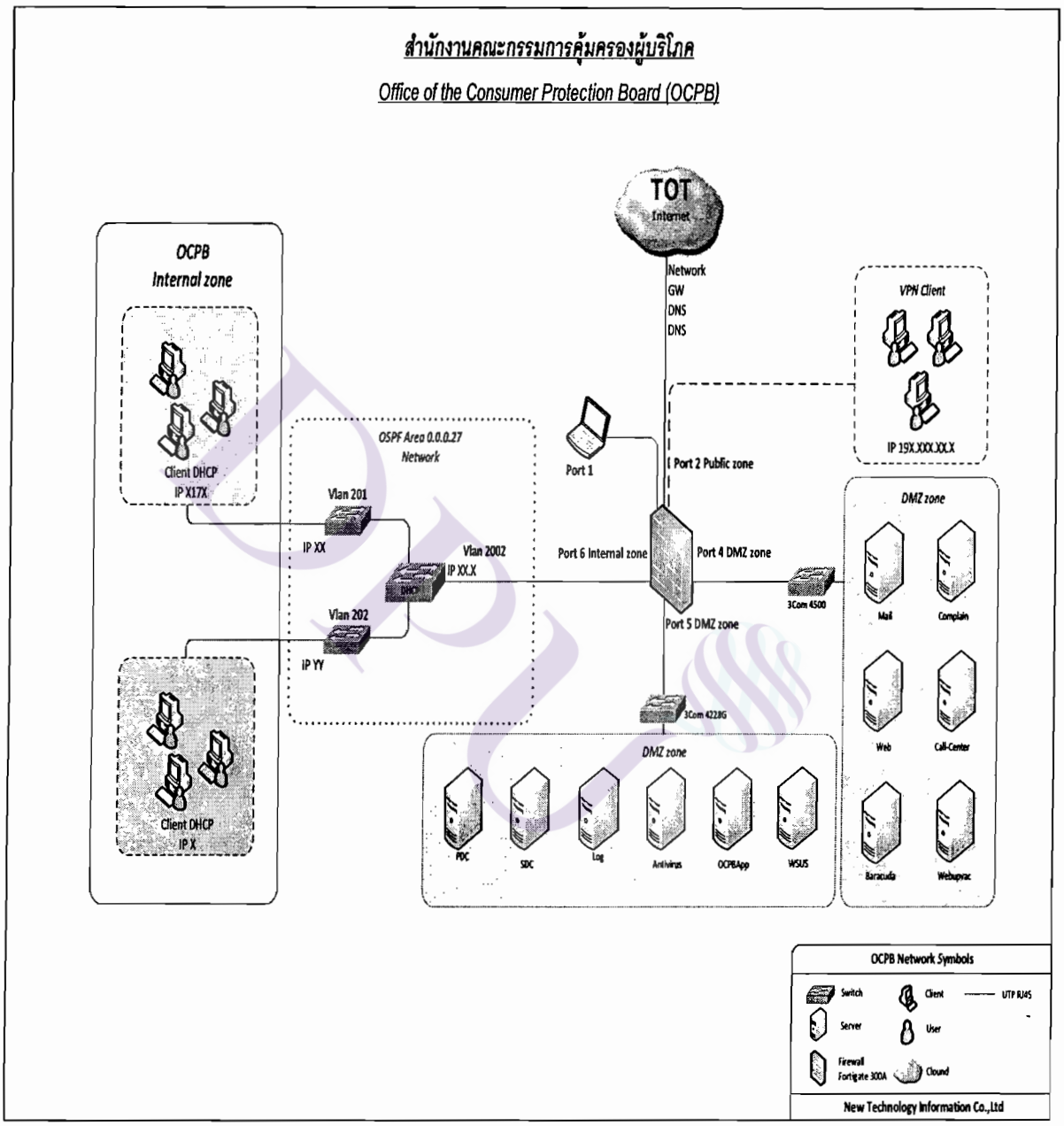
3. A13 -การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

4. A15- การปฏิบัติตามข้อกำหนด (Compliance)

5.2.2 นำมาพัฒนาและปรับปรุงด้านความปลอดภัยระบบสารสนเทศของหน่วยงานเพื่อจัดทำโครงการจัดซื้ออุปกรณ์ป้องกันการบุกรุกระบบเครือข่าย และสามารถดำเนินการเพิ่ม

ปลอดภัยให้กับระบบเครือข่ายได้ สามารถดำเนินการปรับปรุงระบบเครือข่ายเพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น ดังนี้

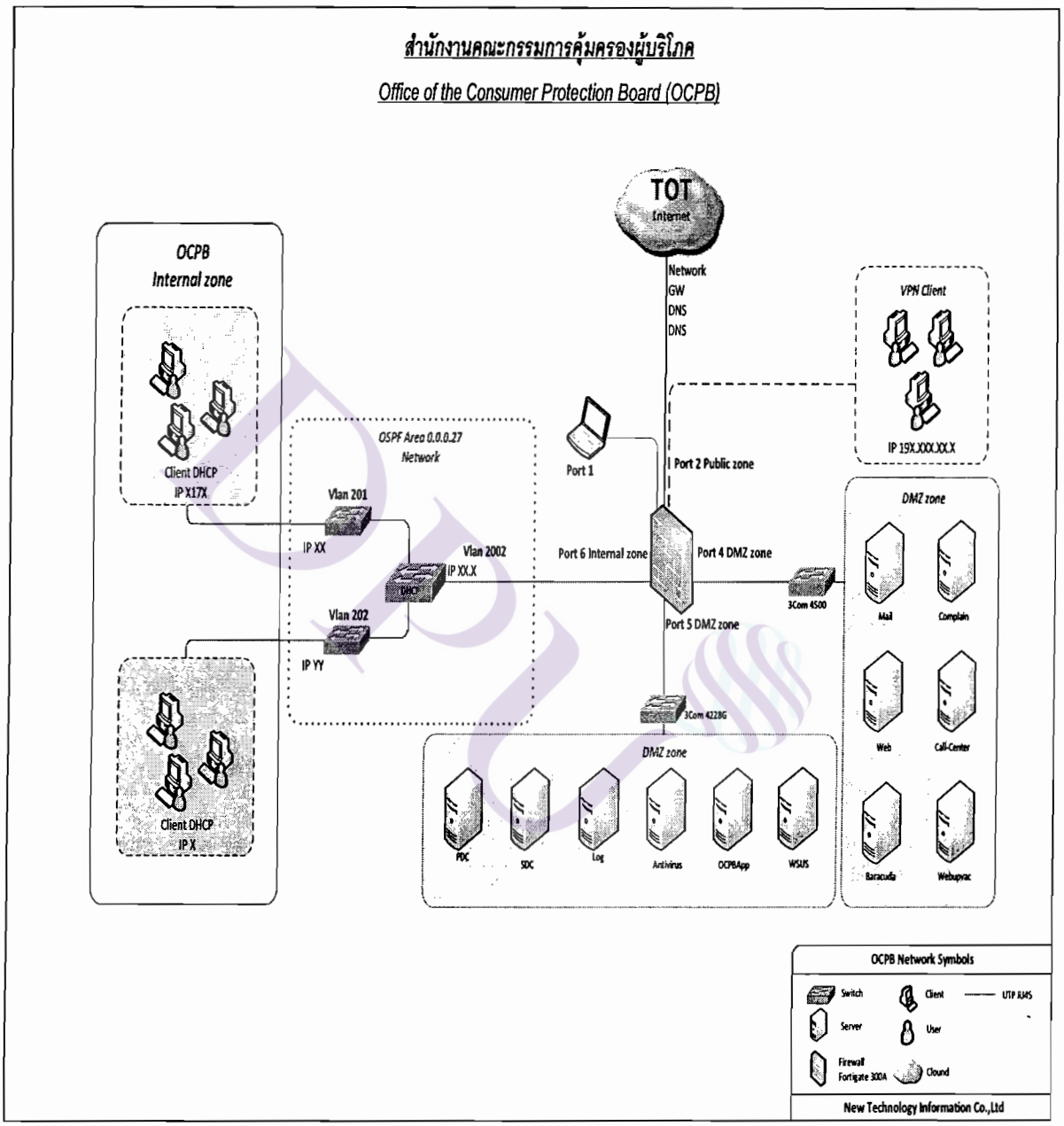
5.2.2.1 โครงสร้างของระบบเครือข่ายเดิม ขณะที่ดำเนินการวิเคราะห์และประเมินความเสี่ยง ก่อนการดำเนินการโครงการรายละเอียด ดังภาพที่ 5.1



ภาพที่ 5.1 ระบบเครือข่ายภายในองค์กรก่อนที่มีการปรับปรุง

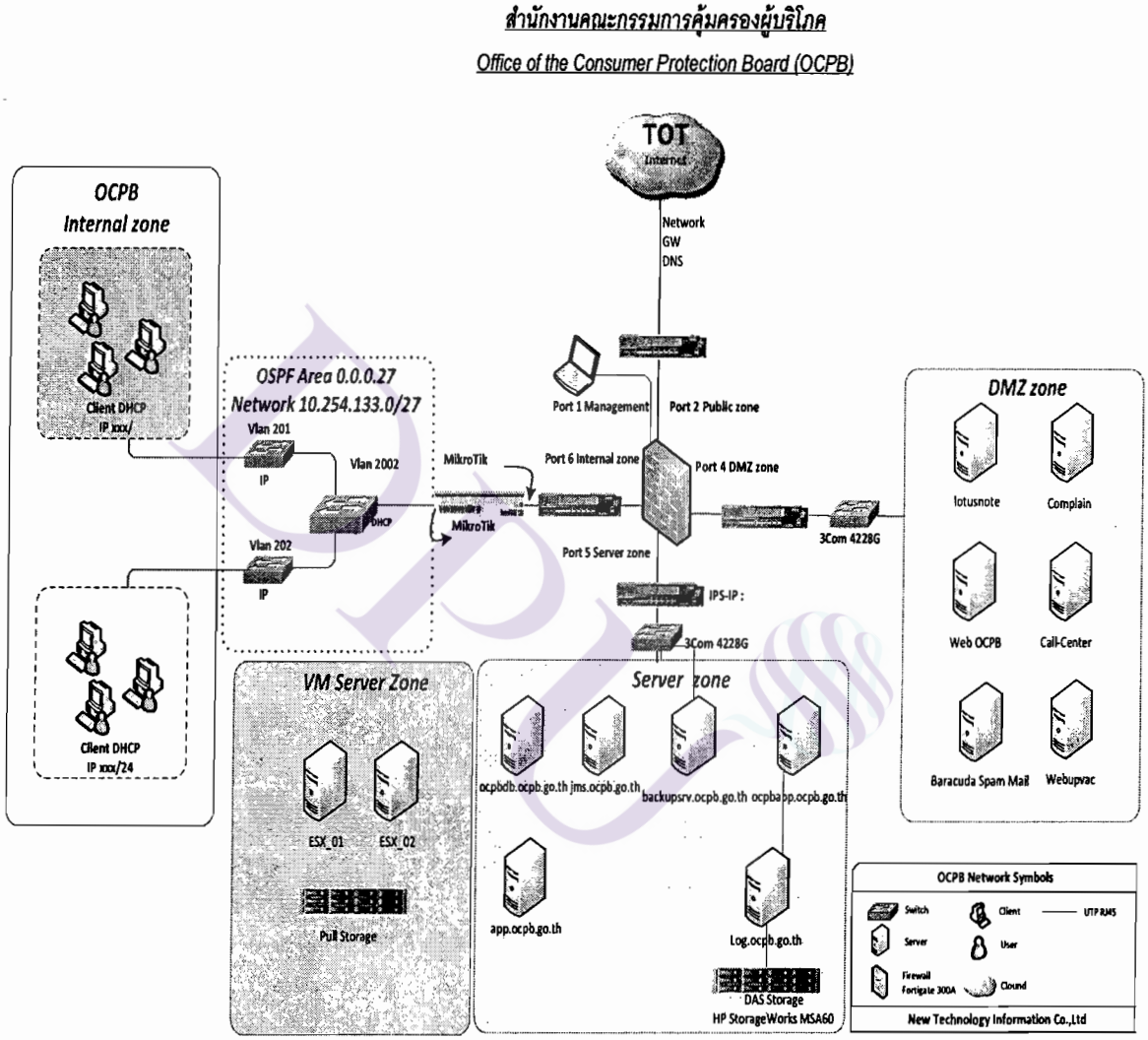
ปลอดภัยให้กับระบบเครือข่ายได้ สามารถดำเนินการปรับปรุงระบบเครือข่ายเพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น ดังนี้

5.2.2.1 โครงสร้างของระบบเครือข่ายเดิม ขณะที่ดำเนินการวิเคราะห์และประเมินความเสี่ยง ก่อนการดำเนินการโครงการรายละเอียด ดังภาพที่ 5.1



ภาพที่ 5.1 ระบบเครือข่ายภายในองค์กรก่อนที่มีการปรับปรุง

5.2.2.2 ได้มีการปรับปรุงระบบเครือข่าย จากผลการวิเคราะห์และประเมินความเสี่ยง (ภาคผนวก ค) ในข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operating Management- A10) หัวข้อย่อย 6.2 ผลการวิเคราะห์และประเมินความเสี่ยง = 25/ ระดับสูง และได้ดำเนินการปรับปรุงระบบเครือข่ายใหม่รายละเอียด ดังภาพที่ 5.2



ภาพที่ 5.2 ระบบเครือข่ายภายในองค์กรที่มีการปรับปรุงแล้วในปัจจุบัน

จากการวิเคราะห์และปรับปรุงระบบเครือข่าย โดยปกติมีการแบ่งโซนของระบบเครือข่ายให้เหมาะสมตามอุปกรณ์ต่างๆ เพื่อไม่ให้เกิดความเสี่ยงในการโจมตีระบบ ทั้งภายนอกและภายใน จากการนำเสนอผลการวิเคราะห์และประเมินความเสี่ยงก่อนการดำเนินการโครงการ

เข้าสู่ที่ประชุมผู้บริหาร ได้รับการจัดสรรงบประมาณเพื่อจัดซื้ออุปกรณ์ป้องกันการบุกรุก (IPS) เพื่อสร้างความปลอดภัยของระบบเพิ่มขึ้น ในการเข้าถึงระบบเครือข่ายและการเข้าถึงข้อมูล โดยให้มีการแบ่งโซน ดังนี้

1. DMZ Zone (DMZ) ใช้สำหรับเชื่อมต่อกับอุปกรณ์ Server และ Log เพื่อให้เกิดการควบคุมและป้องกันการเข้าถึงเครื่อง Server และการแก้ไข Log

2. Server Zone ใช้สำหรับเชื่อมต่อกับอุปกรณ์ไปยัง Server เพื่อให้การทำงานของระบบเครือข่ายสามารถควบคุมการเข้าถึงข้อมูลได้

3. Internal Zone ใช้สำหรับเชื่อมต่อกับเครือข่ายภายใน Office ของผู้ใช้งานเพื่อให้เกิดความปลอดภัยและป้องกันการเข้าออกของข้อมูล

4. IPS-IP : ใช้สำหรับเชื่อมต่อกับ Server Zone และ DMZ Zone ใช้สำหรับการตรวจสอบความปลอดภัยในของระบบเครือข่าย ที่ได้จัดซื้อเพิ่มเติมตามโครงการนี้

5.2.3 การตรวจสอบความปลอดภัยของระบบเครือข่ายสารสนเทศโดยตรวจสอบช่องโหว่หรือจุดอ่อนด้วยโปรแกรม Nessus

การดำเนินการตามข้อนี้ได้ดำเนินการทดสอบจาก เครื่องแม่ข่ายที่สำคัญหลายเครื่อง แต่นำเสนอเพียงบางตัวเท่านั้นเพื่อสร้างความเข้าใจในการตรวจสอบระบบเครือข่าย ตามตัวอย่างที่ 5.3 ตัวอย่างที่ 5.3 รายงานการตรวจสอบช่องโหว่เครื่องคอมพิวเตอร์แม่ข่ายปีงบประมาณ 2555 มีดังนี้ รายละเอียดเครื่องคอมพิวเตอร์แม่ข่าย ดังรูปหน้าถัดไป

ตารางที่ 5.5 ผลการตรวจสอบช่องโหว่ (Vulnerabilities)

Hostname : www.ocpb.go.th Private IP Address : 172.16.106.3

Public IP Address : 180.180.240.36 Date Scan : 30 Aug 2012

WWW.OCPB.GO.TH	
Scan Time	
Start time:	Tue Aug 30 18:18:17 2012
End time:	Tue Aug 30 18:24:12 2012
Number of vulnerabilities	
High	8
Medium	5
Low	123
Remote Host Information	
Operating System:	Microsoft Windows Server 2008 R2 Standard
NetBIOS name:	WEB
DNS name:	www.ocpb.go.th
IP address:	172.16.106.3
MAC address:	e4:1f:13:1c:19:08

จะเห็นได้ว่า Number of Vulnerabilities รายละเอียดในการตรวจสอบช่องโหว่ของระบบของ Plugin ID ในระดับต่างๆ

5.3 ผลการวิเคราะห์และประเมินความเสี่ยง (หลังการดำเนินโครงการ)

วัตถุประสงค์

1. เพื่อให้รู้ว่าความเสี่ยงของระบบเทคโนโลยีสารสนเทศขององค์กรมีอะไรบ้าง ที่ต้องปรับปรุง และต้องจัดการความเสี่ยงทรัพย์สินสารสนเทศ

2. นำผลการวิเคราะห์และการประเมินความเสี่ยงมาวางแผนการบริหารความเสี่ยงที่ยังเหลืออยู่

สรุปผลการวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ จากรายละเอียดใน (ภาคผนวก ง) ตารางผลการวิเคราะห์และประเมินความเสี่ยง(หลังดำเนินโครงการ) ผลสรุปตามตารางที่ 5.6 มีรายละเอียด ดังนี้

ตารางที่ 5.6 สรุปผลการวิเคราะห์และประเมินความเสี่ยง (หลังการดำเนินโครงการ)

11 หัวข้อ (หลังดำเนินโครงการ)	ระดับความเสี่ยง		
	สูง	กลาง	ต่ำ
1.นโยบายความมั่นคงปลอดภัย (Security policy) –A5	1	-	1
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) –A6	1	3	1
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) - A7	-	4	2
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resource security) – A8	-	4	5
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) – A9	-	3	7
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and operations management) – A10	3	3	2
7.การควบคุมการเข้าถึง (Access control) – A11	-	5	2
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) – A12	1	5	1
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) – A13	-	2	-
10.บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity) – A14	3	1	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	1	2	-
รวม	26	27	10

จากการวิเคราะห์และประเมินความเสี่ยงด้วยมาตรฐาน ISO/IEC 27001 อีกครั้งหลังการดำเนินโครงการทำให้องค์กรทราบถึงความเสี่ยงของระบบที่ยังมีอยู่ในปัจจุบันและนำผลที่ได้ประยุกต์ใช้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศต่อไป

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 ผลการวิเคราะห์และประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศ

ตามที่ผู้จัดทำโครงงานได้ดำเนินการศึกษาวิเคราะห์และประเมินความเสี่ยงการจัดการด้านความปลอดภัยของระบบสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นการเพิ่มประสิทธิภาพในการบริหารจัดการศูนย์คอมพิวเตอร์และข้อมูลภายในองค์กร เพื่อสร้างมาตรฐานความปลอดภัยของระบบสารสนเทศและแก้ไขช่องโหว่/จุดอ่อนที่มีอยู่ พร้อมทั้งปรับปรุงระบบเดิมให้ดียิ่งขึ้น โดยสรุปผลการดำเนินงานได้ดังนี้

6.1.1 ทำให้ได้รับทราบ จุดอ่อนหรือช่องโหว่ ที่อาจทำให้เกิดความเสี่ยงต่อองค์กร และสามารถหาวิธีการแก้ปัญหาได้อย่างเหมาะสม

6.1.2 นำมาพัฒนาปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งในขณะนี้ได้ดำเนินการจัดทำร่างนโยบายเรียบร้อยแล้ว (ภาคผนวก จ)

6.1.3 นำผลวิเคราะห์และประเมินความเสี่ยง มาประกอบการจัดทำโครงการ จัดซื้อจัดจ้างอุปกรณ์ป้องกันการบุกรุกความปลอดภัย เพื่อปรับปรุงระบบเครือข่ายขององค์กร

6.1.4 จากผลการวิเคราะห์ สามารถปิดช่องโหว่ของระบบต่างๆ เช่น การทดสอบการโจมตีทำให้รู้ถึงโครงสร้างหลักการและวิธีการทำงานของการทดสอบโจมตี รวมถึงวิธีการเลือกเป้าหมายและเครื่องมือต่างๆ ที่ใช้ในการทดสอบการโจมตีรวมถึงขั้นตอนการดำเนินงานการปิดช่องโหว่รวมถึงแนวทางในการป้องกัน

6.2 แนวทางการนำไปประยุกต์ใช้ ในการบริหารจัดการศูนย์เทคโนโลยีสารสนเทศ

เมื่อได้นำผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลัง การดำเนินงานโครงการมาเปรียบเทียบจะผ่านขั้นตอนการวิเคราะห์และการปิดช่องโหว่ของระบบและทบทวนจุดอ่อนด้านความปลอดภัยสารสนเทศที่องค์กรมีอยู่และสามารถดำเนินการปรับปรุงได้ทันทีโดยไม่ต้องใช้งบประมาณ เช่น การปรับค่าการติดตั้งสำหรับค่าของ Operating System ต่างๆ การจัดทำคู่มือเอกสารต่างๆ เพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น ซึ่งมีการเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลังดำเนินโครงการรายละเอียดตามตารางที่ 6.1 ดังนี้

ตารางที่ 6.1 การเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อน-หลังดำเนินโครงการ

Domain	ระดับความเสี่ยงสูง		ระดับความเสี่ยงกลาง		ระดับความเสี่ยงต่ำ	
	ก่อน	หลัง	ก่อน	หลัง	ก่อน	หลัง
1.นโยบายความมั่นคงปลอดภัย (Secur Policy) – A5	2	1	-	-	-	1
2.โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) – A6	3	1	2	3	-	1
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) – A7	2	-	4	4	-	2
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) – A8	1	-	7	-	2	-
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental) – A9	1	-	5	3	5	7
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communicate and Operations Management) – A10	5	3	2	3	1	2
7.การควบคุมการเข้าถึง (Access Control) –A11	2	-	4	5	-	2
8.การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ(Information systems acquisition, development and maintenance) – A12	3	1	3	5	1	1
9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ขององค์กร (Information security incident management) – A13	-	-	2	2	-	-
10.บริหาร การความต่อเนื่องในการดำเนินงานขององค์กร(Business continuity) – A14	4	3	-	1	-	-
11.การปฏิบัติตามข้อกำหนด (Compliance) – A15	3	1	-	2	-	-
รวมทั้งหมด	24	10	31	27	9	21

จากการเปรียบเทียบผลการวิเคราะห์และประเมินความเสี่ยงก่อนและหลังดำเนินโครงการ ที่ผ่าน มาสามารถนำไปประยุกต์ใช้โดยรู้ถึงความเสี่ยงที่อาจจะเกิดขึ้น เพื่อนำมากำหนดแนวทางแก้ไขพร้อมรับมือกับความเสี่ยงที่อาจจะเกิดขึ้นหรือกำหนดแนวทางป้องกัน ดังนี้

6.2.1 ทำให้ได้รับทราบจุดอ่อนหรือช่องโหว่ ที่อาจทำให้เกิดความเสี่ยงต่อองค์กรและสามารถหาวิธีการแก้ปัญหาได้อย่างเหมาะสม

6.2.2 นำผลที่ได้ใช้กำหนดทิศทาง (Roadmap) สำหรับการพัฒนาปรับปรุงนโยบายความปลอดภัยภายในองค์กรด้วยมาตรฐาน ISO/IEC 27001

6.2.3 นำผลการวิเคราะห์ที่ได้มาจัดทำแผนการดำเนินงานประจำปี แผนปฏิบัติราชการ 4 ปี รวมทั้งการจัดทำแผนแม่บทด้านเทคโนโลยีสารสนเทศ

6.2.4 วางแผนพัฒนาระบบสารสนเทศ เพื่อรองรับการขยายงานขององค์กรก้าวสู่ประชาคมอาเซียนในการคุ้มครองผู้บริโภคสู่สากล พร้อมทั้งสร้างมาตรฐานข้อมูลในการติดต่อแลกเปลี่ยนข้อมูลระหว่างองค์กร ดังนั้นการรักษาความปลอดภัยข้อมูล การประเมินและการบริหารความเสี่ยงที่เกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ

6.3 ปัจจัยความสำเร็จ ที่สำคัญในการประยุกต์ใช้มาตรฐาน ISO/IEC 27001 ในองค์กรมีดังนี้

6.3.1 การสนับสนุนจากฝ่ายบริหาร (Management Support) เนื่องจากการบริหารจัดการด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศให้สำเร็จต้องได้รับความร่วมมือร่วมใจ จากบุคลากรในหน่วยงานที่เกี่ยวข้องทุกส่วนงาน ได้แก่ ด้านงบประมาณ ด้านผู้ใช้ระบบ

6.3.2 ความร่วมมือของบุคลากรภายในองค์กร (Internal Approach)

6.3.3 การสื่อสารภายในองค์กร(Document Control) การประสานงานและการติดต่อสื่อสารภายในองค์กร ต้องชัดเจนและก้าวไปในทิศทางเดียวกัน

6.3.4 ขอบเขตการดำเนินงาน (Scope of Work) ต้องมีความชัดเจน

6.4 ปัญหาอุปสรรค

ต้องมีการวางแผนการดำเนินงานที่ดี ทำงานซ้ำซ้อนในช่วงแรกที่มีการเริ่มดำเนินการโครงการทำให้ไม่ได้รับความร่วมมือจากเจ้าหน้าที่ปฏิบัติเท่าที่ควร ต้องมีการสื่อสารให้เจ้าหน้าที่/หรือบุคลากรในองค์เข้าใจถึง การจัดการดำเนินงานด้านความปลอดภัยของระบบเทคโนโลยี และมีความตระหนักในการการจัดทำ

6.5 ข้อเสนอแนะ

6.5.1 การปฏิบัติตามมาตรฐาน ISO/IEC 27001:2005 ซึ่งเป็นที่ยอมรับตามมารตฐานสากล หากหน่วยงานของรัฐหรือภาคเอกชน นำมาประยุกต์ใช้ให้เหมาะสมกับสภาพแวดล้อมหรือบริบทของลักษณะงานและวัฒนธรรมขององค์กร จะสามารถทำให้องค์กรพัฒนาและสร้างความศรัทธาและเชื่อมั่นจากผู้ใช้บริการได้และสามารถใช้เป็นเครื่องมือในการพัฒนาองค์กรให้ก้าวสู่ความเป็นเลิศได้อย่างมีประสิทธภาพ

6.5.2 การฝึกอบรมสำหรับนักพัฒนาโปรแกรมหรือนักพัฒนาแอพพลิเคชันนั้น ควรเป็นส่วนหนึ่งที่เพิ่มจากการฝึกอบรมพนักงานทั่วไป โดยส่วนที่เพิ่มขึ้นมานั้นควรเป็นเรื่องเกี่ยวกับเทคนิคการเขียนโปรแกรมอย่างไรเพื่อให้มีความปลอดภัย นอกจากนี้ก็ควรจะอธิบายถึงเหตุผลและหน้าที่ของฝ่ายรักษาความปลอดภัย ในระหว่างที่ได้มีการพัฒนา กระบวนการรักษาความปลอดภัยสำหรับโครงการใหม่ฝ่ายรักษาความปลอดภัยนั้น ควรที่จะมีส่วนร่วมในระหว่างการออกแบบด้วย ซึ่งเป็นการเปิดโอกาส ให้ฝ่ายการรักษาความปลอดภัยได้มีการพิจารณาเกี่ยวกับ เรื่องความปลอดภัย ก่อนที่จะผลิตในระหว่างการอบรมนั้น ควรจะอธิบายให้นักพัฒนาโปรแกรมทราบถึงคุณค่าของความปลอดภัยในช่วงต้นของการผลิตซอฟต์แวร์

6.5.3 การตรวจสอบการปฏิบัติตามนโยบายนั้น ไม่ควรที่จะเน้นในเฉพาะระบบคอมพิวเตอร์เท่านั้น ควรให้ความสำคัญกับข้อมูลที่มีอยู่ในรูปแบบอื่นด้วย ควรตรวจสอบด้วยว่านโยบายข้อมูลนั้นมีการปฏิบัติตามเคร่งครัดแค่ไหน หรือเอกสารที่มีข้อมูลที่สำคัญมีการจัดเก็บหรือรับส่งอย่างไร

การตรวจสอบควรกระทำปีละครั้ง อาจทำโดยเจ้าหน้าที่จากฝ่ายรักษาความปลอดภัย หรืออาจจะเป็นฝ่ายตรวจสอบต่างหาก หรืออาจจ้างบริษัทข้างนอก ซึ่งมีความชำนาญทางด้านนี้โดยเฉพาะมาทำงานให้ การรักษาความปลอดภัยนั้นเกี่ยวกับการบริหารจัดการความเสี่ยง ถ้าระบบไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีระบบการรักษาความปลอดภัย แต่ถ้าระบบมีความเสี่ยงก็จำเป็นต้องรู้ว่าเสี่ยงมากน้อยแค่ไหน และต้องออกแบบและติดตั้งระบบอะไร เพื่อที่จะช่วยลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และงบประมาณเพียงพอ

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

หนังสือ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2550). *พระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์*. กรุงเทพฯ : ผู้แต่ง.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2551). *คู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์* (พิมพ์ครั้งที่ 1). กรุงเทพฯ :

ขจร สินอภิรมย์สราญ. (2550). *การสร้างเครื่องมือตรวจสอบความปลอดภัยมั่นคงสารสนเทศด้วยมาตรฐาน ISO 27001:2006.*

คณะอนุกรรมการด้านความมั่นคงปลอดภัย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (2552, 27 เมษายน) *ร่างแนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย ISO27001*

จตุชัย แพงจันทร์ . (2550). *การบริหารความเสี่ยงทางด้านการรักษาความปลอดภัยข้อมูล และเป็นแนวทางในการจัดทำมาตรฐาน BS 7799-2.*

ศรีสมรัก อินทุจันทร์ยง. (2550). *ระบบสารสนเทศเพื่อการจัดการ*. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์

สารสนเทศจากสื่ออิเล็กทรอนิกส์

บรรจง หะรังษี (2554,11 สิงหาคม). *บทความ "Plan-Do-Check-Act ตามมาตรฐาน ISO/IEC 27001* สืบค้นเมื่อ 15 มีนาคม 2556 จาก http://www.thaicert.nectec.or./paper/Dos.php

ปริญญา หอมอเนก. (2555,24 ตุลาคม) . *มาตรฐาน ISO 27001 :2005*. สืบค้นเมื่อ 1 มีนาคม 2556, จาก http://www.acisonline.net./article_prinya_eEnterprise_jun_08.htm

ระบบมาตรฐานด้านความมั่นคงปลอดภัยของข้อมูล ISO27001. สืบค้นเมื่อ 10 กุมภาพันธ์ 2556, จาก http://www.ryt9.com/s/prg/1086086

สารสนเทศจากสื่ออิเล็กทรอนิกส์

บรรจง หะรังษี (2555,17 มกราคม) . *บทความ "Cobit5 กับการนำไปใช้งาน* "" สืบค้นเมื่อ 15 มีนาคม 2556 .จาก http://www.tnetsecurity.com/content_audit/cobit5_implementation_step.php

มาตรฐาน ISO/27001. สืบค้นเมื่อ 18 เมษายน 2556 , จาก *http://www.*iso27001certificates.com

ไอเอสโอ คือ อะไร. สืบค้นเมื่อ 1 มีนาคม 2556, จาก http://www.mimdphp.com

มาตรฐานด้านความมั่นคงปลอดภัยของข้อมูล. สืบค้นเมื่อ 10 มิถุนายน 2556, จาก http://www.iso.org

ภาษาต่างประเทศ

ARTICLE

Suyash Mishra, Rishi Kant. (2012). "Effectiveness of Management Information System in Improving the Performance of Punjab National Bank (PNB),"

ELECTRONIC SOURCE

How to Design Questionnaires for Usability Evaluation. *"How to Design Questionnaires"* Retrieved March 3 ,2013, form http://www.shengdongzhao.com/research_tips/how-to-design-aquestionnaire for usability-evaluation/.

COBIT 5: A Business Framework for the Governance and Management of Enterprise . *"Cobit 5 "* Retrieved March 18 ,2013, form http://www.isaca.org/

International Organization for Standardization ISO Central Secretariat *"Risk management"* form http://iso.org

ภาคผนวก

ภาคผนวก ก

ระบุขอบเขตตามมาตรฐาน ISO/IEC 27001

ตารางที่ 1 การระบุขอบเขตตามมาตรฐาน ISO/IEC 2700 11 หัวข้อ

ISO/IEC 27001 : ขอบเขตของการระบุความเสี่ยง
1.Security Policy-A5 (นโยบายการรักษาความปลอดภัย)
วัตถุประสงค์
1.1 A 5.1 สนับสนุนการรักษาความปลอดภัยข้อมูล
1.2 A 5.2 ทบทวนการรักษาความปลอดภัยข้อมูลอย่างน้อยปีละ 1 ครั้ง
2.Organizing Information Security-A6 (การจัดโครงสร้างระบบการรักษาด้านความปลอดภัยขององค์กร)
วัตถุประสงค์ เพื่อการบริหารความปลอดภัยของข้อมูลภายในองค์กร
2.1 A.6.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements
2.2 A 6.1.6 ควบคุมการเข้าถึงข้อมูลที่มีชั้นความลับ
3. Asset Management – A7 (การจัดการทรัพย์สิน)
วัตถุประสงค์ เพื่อบริหารจัดการทรัพย์สินให้เกิดความปลอดภัย
3.1 A 7.1.1 การควบคุมการเข้า – ออก (Physical entry Control)
3.2 A 7.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of Assets)
3.3 A 7.1.5 การมีข้อตกลงในการรักษาความลับ
3.4 A 7.3.2 กำหนดเกณฑ์ในการแยกหมวดหมู่ให้ชัดเจน (Classification)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001 : ขอบเขตของการระบุความเสี่ยง
4. Human Resource Security- A8 (การรักษาความปลอดภัยในระดับบุคลากร)
วัตถุประสงค์ การบริหารจัดการสิทธิในการเข้าถึง/การใช้บ
4.1 A.8.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)
4.2 A.8.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)
4.3 A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)
4.4 A.8.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)
4.5 A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)
5. Physical and Environmental Security- A9 (การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม)
วัตถุประสงค์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
5.1 A 9.1.2 การควบคุมการเข้า – ออก (Physical entry Control)
5.2 A 9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment Security)
5.3 A 9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)
5.4 A 9.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal of re-use of equipment)
5.5 A 9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001 : ขอบเขตของการระบุความเสี่ยง
6.Communication and Operations Management- A10 (การสื่อสารและการบริหารการปฏิบัติงาน)
วัตถุประสงค์ ป้องกันการให้บริการทางเครือข่าย
6.1 A 10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating Procedures)
6.2 A 10.1.2 การควบคุมการเปลี่ยนแปลง
6.3 A 10.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)
6.4 A 10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)
6.5 A 10.5.1 การสำรองข้อมูล (Information Back-up)
6.6 A 10.6.1 มาตรการทางเครือข่าย (Network controls)
6.7 A 10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system us
7. Access Control – A11 (การควบคุมการเข้าถึงระบบ)
มีจุดมุ่งหมายเพื่อ ควบคุมการเข้าถึงข้อมูล ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
7.1 A 11.2.1 การลงทะเบียนพนักงาน (User registration)
7.2 A 11.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
7.2 A 11.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้(Use of System Utilities)
7.3 A 11.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

ตารางที่ 1 (ต่อ)

ISO/IEC 27001 : ขอบเขตของการระบุความเสี่ยง
8. Information systems acquisition, development and maintenance-A12 (การดูแลและพัฒนาระบบ) มีวัตถุประสงค์ดังนี้
8.1 A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)
8.2 A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)
8.3 A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)
ต 8.4 A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)
19. Information security incident management-A13 (การบริหารและจัดการเหตุการณ์ฉะเมิดความปลอดภัย) ซึ่งมีมาตรการ 2 ส่วนคือ
ร 9.1 A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)
า 9.2 A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)
ง10. ความต่อเนื่องทางธุรกิจ- A14
ที่ 10.1 A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)
11. Compliance-A15 (ไม่ขัดต่อกฎหมาย)
1 11.1 A15.1.2 ป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่างๆ
11.2 A15.2 เพื่อทำให้แน่ใจว่าระบบนั้น ไม่ขัดต่อนโยบายการรักษาความปลอดภัย ขององค์กรหรือมาตรฐาน

(

ภาคผนวก ข

ตารางประเมินความเสี่ยงแยกตามกลุ่มสินทรัพย์

กลุ่มที่ 1 ฮาร์ดแวร์และอุปกรณ์คอมพิวเตอร์(Hardware) รายละเอียด ดังนี้

ตารางที่ 2 ตารางประเมินความเสี่ยงเครื่องคอมพิวเตอร์แม่ข่ายจำนวน 22 เครื่อง

1.ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Server ทุกตัว						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 1.1 (A9.)	(S) มีการอนุญาตให้ผ่านเข้า-ออก ในห้อง Server เฉพาะผู้มีบัตรเท่านั้น	สามารถเข้าถึง ระบบเครื่องคอมพิวเตอร์แม่ข่ายได้ง่าย	4	1	4	อนุญาตให้สำหรับผู้ที่มีบัตรเข้าออกเท่านั้นหรือลงทะเบียนเข้า - ออก ห้อง Server
ข้อ 1.2 (A 9.2.1)	(W) การจัดวางอุปกรณ์อยู่ในที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อาจจะทำให้อุปกรณ์มีการทำงานผิดพลาด	3	1	3	ข้อจำกัดสำหรับสถานที่ /ใช้งบประมาณสูง
ข้อ 1.3 (A 9.2.4)	(S) มีการวางแผนในการบำรุงรักษาอุปกรณ์อย่างต่อเนื่องและสม่ำเสมอ	อุปกรณ์อาจจะเสีย หรือไม่สามารถทำงานได้	5	2	10	มีการวางแผนงานการบำรุงรักษาระบบ
ข้อ 1.4	(W) เมื่อไฟดับ เครื่อง UPS ทำให้ Server ดับ เมื่อไฟติด ไฟเข้าสู่ Server แล้วทำให้ ไม่สามารถเข้าสู่ระบบได้ HW เสีย	การ Restart ตัวเองของ Server ทำให้ค่าต่างๆของอุปกรณ์ที่กำหนดไว้ผิดพลาดและไม่สามารถทำงานต่อได้	4	2	8	มีระบบสำรองไฟได้ ไม่เกิน 3 ชั่วโมง

ตารางที่ 2 (ต่อ)

1.ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Server ทุกตัว						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 1.5 (A10.1.1)	(W) ไม่มีคู่มือการปฏิบัติงานที่เป็นลายลักษณ์อักษร	เกิดการทำงานผิดพลาด	5	4	20	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง Server
ข้อ 1.6 (A10.4.1)	(W) การใช้เครื่อง Server เข้าถึงหน้าเว็บไซต์บางแห่งและดาวน์โหลดข้อมูลจากแหล่งที่ไม่เหมาะสม	เครื่อง Server ติดไวรัส	5	5	25	ติดตั้งโปรแกรมป้องกันไวรัส -ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล

ตารางที่ 3 ตารางประเมินความเสี่ยงเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) จำนวน 228 เครื่อง

2.ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ส่วนบุคคล(PC) จำนวน 228 เครื่อง						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 2.1 (A 7.1.1)	(W) ไม่มีการจัดทำ/จัดเก็บและแก้ไขทะเบียนครุภัณฑ์คอมพิวเตอร์ให้ถูกต้องอยู่เสมอ	เกิดการสูญหายเกิดขึ้น/ทำให้ไม่มีอุปกรณ์ในการใช้งาน	3	4	12	ยังไม่มีการจัดเก็บทะเบียนครุภัณฑ์คอมพิวเตอร์ให้ถูกต้อง
ข้อ 2.2 (A 7.1.2)	(S) จัดให้มีการระบุผู้เป็นเจ้าของในเครื่องคอมพิวเตอร์แต่ละเครื่อง	มีการเลื่อนย้ายเครื่อง PC ทำให้ยากในการติดตามการใช้งาน	3	3	9	ยังไม่มีเอกสารที่ระบุชัดเจน
ข้อ 2.3 (A 9.2.1)	(W) การจัดวางอุปกรณ์อยู่ในที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อาจจะทำให้อุปกรณ์มีการทำงานผิดพลาด	5	1	5	จัดวางให้ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้า ท่อน้ำของอาคาร
ข้อ 2.4 (A 9.2.4)	(S) มีการบำรุงรักษาอุปกรณ์อย่างต่อเนื่องและสม่ำเสมอ	อุปกรณ์ทำงานผิดพลาดหรือไม่สามารถทำงานได้	5	1	5	มีแผนงานการบำรุงรักษาเครื่องคอมพิวเตอร์
ข้อ 2.5	(S) มีเครื่อง UPS สำรองให้ใช้เมื่อไฟดับทำให้ไม่สามารถเข้าสู่ระบบได้ HW เสีย	มีการเสียหายข้อมูลเกิดขึ้น/ค่าต่างๆของอุปกรณ์ที่กำหนดไว้ผิดพลาดและทำงานไม่ได้	3	1	3	มี UPS สำรองไฟให้ใช้ทุกเครื่อง

ตารางที่ 3 (ต่อ)

2.ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ส่วนบุคคล(PC) จำนวน 228 เครื่อง						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 2.6 (A 9.2.6)	(W) ขาดการตรวจสอบการลบทิ้งของข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว	ข้อมูลที่เป็นความลับถูกเปิดเผย	4	5	20	มีการกำหนดแนวปฏิบัติที่ชัดเจนในการลบทิ้งของข้อมูลภายในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว
ข้อ 2.7 (A 9.2.7)	(S) ห้ามนำทรัพย์สินในองค์กรออกไปภายนอก นอกจากได้รับอนุญาตเท่านั้น	เกิดการสูญหาย	3	5	15	ยังไม่ได้กำหนดแนวปฏิบัติให้ชัดเจน
ข้อ 2.8 (A10.4.1)	(W) ขาดการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี อย่างทั่วถึง	เครื่อง PC ติดไวรัส เครื่องคอมพิวเตอร์ใช้งานไม่ได้	4	1	4	ติดตั้งโปรแกรมป้องกันไวรัสให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล
ข้อ 2.9 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานเฉพาะทางอย่างสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	5	5	25	วางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

ตารางที่ 3 (ต่อ)

2.ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ส่วนบุคคล(PC) จำนวน 228 เครื่อง						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 2.6 (A 9.2.6)	(W) ขาดการตรวจสอบการลบทิ้งของข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว	ข้อมูลที่เป็นความลับถูกเปิดเผย	4	5	20	มีการกำหนดแนวปฏิบัติที่ชัดเจนในการลบทิ้งของข้อมูลภายในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว
ข้อ 2.7 (A 9.2.7)	(S) ห้ามนำทรัพย์สินในองค์กรออกไปภายนอก นอกจากได้รับอนุญาตเท่านั้น	เกิดการสูญหาย	3	5	15	ยังไม่ได้กำหนดแนวปฏิบัติให้ชัดเจน
ข้อ 2.8 (A10.4.1)	(W) ขาดการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี อย่างทั่วถึง	เครื่อง PC ติดไวรัส เครื่องคอมพิวเตอร์ใช้งานไม่ได้	4	1	4	ติดตั้งโปรแกรมป้องกันไวรัสให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล
ข้อ 2.9 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานเฉพาะทางอย่างสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	5	5	25	วางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

กลุ่มที่ 2 โปรแกรม(Software)

การประเมินความเสี่ยงทางด้านโปรแกรม จะรวบรวมทั้ง ระบบฐานข้อมูล ระบบปฏิบัติการต่างๆ ที่ใช้ในหน่วยงาน รายละเอียด ดังนี้

ตารางที่ 4 ตารางประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Window

3.ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Window						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 3.1 (A10.4.1)	(S) ผู้ใช้งานขาดความตระหนักในการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี อย่างทั่วถึง	ระบบทำงานไม่ได้ หรืออาจทำงานผิดพลาด	4	1	4	มีการสร้างแนวปฏิบัติให้ชัดเจน และสร้างความตระหนักถึงระดับจิตสำนึก
ข้อ 3.2 (A11.4.2)	(W) ขาดการควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ควรมีการกำหนดขั้นตอนการปฏิบัติที่ชัดเจนเพื่อควบคุมการติดตั้งโปรแกรมต่างๆ ในระบบปฏิบัติการที่ใช้

ตารางที่ 4 (ต่อ)

3.ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Window						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 3.3 (A11.4.3)	(W) ไม่มีจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด/เข้าถึงระบบได้ง่าย	4	5	20	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 3.4 (A12.5.1)	(W) การกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบ ยังไม่ครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	4	5	20	ยังไม่มีการจัดการระบบควบคุมที่ดี
ข้อ 3.5 (A12.6.1)	(S) มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่และทำการปรับปรุงในระบบที่ใช้งานอย่างสม่ำเสมอ	ไม่ทราบข้อมูลใหม่ๆ	5	2	10	ฝึกอบรมให้เจ้าหน้าที่มีความตระหนักในเรื่องการติดตามข้อมูลข่าวสาร
ข้อ 3.6 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานเฉพาะทางอย่างสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	4	3	12	วางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

ตารางที่ 5 ตารางประเมินความเสี่ยงของระบบฐานข้อมูล SQL for Server

4.ชื่อทรัพย์สิน : ระบบฐานข้อมูล SQL Server						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 4.1 (A10.4.1)	(S) ผู้ใช้งานขาดความตระหนักในการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี และขาดการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่	ระบบทำงานไม่ได้ หรืออาจทำงานผิดพลาด	4	1	4	มีการสร้างแนวปฏิบัติให้ชัดเจน และสร้างความตระหนัก
ข้อ 4.2 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ด(Source Code)สำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 4.3 (A12.5.1)	(W) ยังไม่มีการกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบยังไม่มีรายละเอียดครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	4	5	20	ยังไม่มีการกำหนดให้มีการควบคุมที่ดี
ข้อ 4.4 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	4	3	12	ยังขาดการวางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

ตารางที่ 6 ตารางประเมินความเสี่ยงสำหรับโปรแกรมประยุกต์และระบบงานต่างๆ

5.ชื่อทรัพย์สิน : ระบบโปรแกรมต่างๆ (มาตรการที่ 12)						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 5.1 (A10.4.1)	(W) ผู้ใช้งานขาดความตระหนักในการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี อย่างทั่วถึง	ระบบทำงานไม่ได้ หรืออาจทำงานผิดพลาด	4	1	4	มีการสร้างแนวปฏิบัติให้ชัดเจน และต้องช่วยสร้างความตระหนักแก่ผู้ใช้
ข้อ 5.2 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 5.3 (A12.5.1)	(W) การกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบ ยังไม่ครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	4	5	20	ยังไม่มีการกำหนดให้มีการควบคุมที่ดี
ข้อ 5.4 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานเฉพาะทางอย่างสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	3	5	15	ยังไม่มีการวางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

กลุ่มที่ 3 ด้านบุคลากร(People)

การประเมินความเสี่ยงทางด้านบุคลากรจะรวมทั้งองค์กร ซึ่งพิจารณาได้หลายมิติหลายมุมที่มีผลกระทบกับหน่วยงาน

ตารางที่ 7 ตารางประเมินความเสี่ยงด้านบุคลากร

6.ชื่อทรัพย์สิน : บุคลากร (เน้นมาตรการที่ A8)						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 6.1 (A8.1.1)	(W) กำหนดความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศให้แก่พนักงาน	มีการละเมิดสิทธิ	3	5	15	ยังไม่มีการจัดทำนโยบายด้านความปลอดภัยระบบสารสนเทศและประกาศใช้
ข้อ 6.2 (A8.1.2	(W) มีการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียดเพื่อความปลอดภัยสำหรับสารสนเทศขององค์กร	ป้องกันการเข้าถึงข้อมูลและอุปกรณ์เครือข่าย	3	2	6	ยังไม่มีการควบคุมและการตรวจสอบเรื่องนี้
ข้อ 6.3 (A8.2.2)	(W) ขาดการให้ความรู้ด้านความมั่นคงปลอดภัย ให้แก่เจ้าหน้าที่ ผู้ใช้ระบบ	ทำให้เกิดการสร้างความตระหนักการทำงานผิดพลาด	5	3	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 7 (ต่อ)

6.ชื่อทรัพย์สิน : บุคลากร (เน้น มาตรการที่ A8)						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 6.4 (A 8.3.2)	(W) ไม่มีการกำหนดให้ผู้ที่สิ้นสุดการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน	ทรัพย์สินสูญหาย	3	5	15	ต้องมีข้อกำหนดในการคืนอุปกรณ์และการถอดถอนสิทธิเมื่อสิ้นสุดการจ้างงาน
ข้อ 6.5 (A8.3.3)	(W) ไม่มีการถอดถอนสิทธิในการเข้าถึงสารสนเทศของผู้ที่สิ้นสุดการจ้างงาน	ระบบสารสนเทศถูกใช้โดยไม่ได้รับอนุญาต	5	5	25	ไม่มีเคยมีการทบทวนสิทธิในการเข้าถึงสารสนเทศของพนักงานอย่างสม่ำเสมอ

กลุ่มที่ 4 ด้านข้อมูล(Information)

การประเมินความเสี่ยงทางด้านข้อมูลในแต่ละ Server พิจารณาได้หลายมิติ หลายมุม ที่มีผลกระทบกับการจัดการข้อมูลของหน่วยงานมี ดังนี้

ตารางที่ 8 ตารางประเมินความเสี่ยงด้านข้อมูลของระบบ Web /Server

7.ชื่อทรัพย์สิน : ระบบ Web Server						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 7.1 (A 6.1.5)	(W) ยังไม่มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร	ข้อมูลอาจถูกเปิดเผยได้	5	4	20	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 7.2 (A7.1.3)	(W)ไม่มีการจัดทำกฎ ระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน	ถูกละเมิด ความปลอดภัย	4	3	12	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 7.3 (A8.3.3)	(W) ขาดการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างเป็นขั้นตอน	สามารถเข้าถึงข้อมูลได้ง่าย	5	3	15	ควรมีแผนการกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 8 (ต่อ)

7.ชื่อทรัพย์สิน : ระบบ Web Server						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 7.4 (A8.3.3)	((W) ไม่มีการถอดถอนสิทธิในการเข้าถึงสารสนเทศของผู้ที่สิ้นสุดการจ้างงาน	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	3	5	15	ไม่มีการทบทวนสิทธิในการเข้าถึงสารสนเทศของพนักงานอย่างสม่ำเสมอ
ข้อ 7.5 (A10.5.1)	(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ	ระบบสารสนเทศถูกใช้โดยไม่ได้รับอนุญาต	3	3	9	การสำรองข้อมูล ยังไม่ได้กำหนดเป็นระบบชัดเจน
ข้อ 7.6 (A10.10.2)	(S) มีการตรวจสอบการใช้งานระบบประจำเพื่อป้องกันข้อผิดพลาดที่เกิดขึ้น	ระบบไม่สามารถใช้งานได้	1	5	5	มีการตรวจสอบสม่ำเสมอ
ข้อ 7.7 (A 11.2.1)	(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบอย่างถูกต้อง	สิทธิ์การเข้าถึงข้อมูลมีความปลอดภัย	1	5	5	มีการกำหนดสิทธิ์การเข้าถึงได้ชัดเจน

ตารางที่ 8 (ต่อ)

7.ชื่อทรัพย์สิน : ระบบ Web Server						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 7.8 (A12.4.1)	(S) มีการป้องกันการติดตั้งโปรแกรมต่างๆ ลงไปยังระบบที่ให้บริการ	การทำงานของระบบผิดพลาดเกิดขึ้นได้	2	3	6	ไม่มีข้อกำหนด
ข้อ 7.9 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 9 ตารางประเมินความเสี่ยงสำหรับระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ

8.ชื่อทรัพย์สิน : ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 8.1 (A 6.1.5)	(W) ยังไม่มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร	ข้อมูลอาจถูกเปิดเผยได้	5	4	20	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 8.2 (A7.1.3)	(W)ไม่มีการจัดทำกฎ ระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน	ถูกละเมิด ความปลอดภัย	4	3	12	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 8.3 (A8.3.3)	(W) ขาดการทบทวนและไม่มีการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	ทำให้เกิดการทำงานผิดพลาด การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	5	3	15	ไม่มีการทบทวนสิทธิในการเข้าถึงสารสนเทศของพนักงานอย่างสม่ำเสมอ
ข้อ 8.4 (A10.5.1)	(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ	ระบบสารสนเทศถูกใช้โดยไม่ได้รับอนุญาต	3	3	9	การสำรองข้อมูล ยังไม่ได้กำหนดเป็นระบบชัดเจน

ตารางที่ 9 (ต่อ)

8.ชื่อทรัพย์สิน : ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 8.5 (A10.10.2)	(S) มีการตรวจสอบการใช้งานระบบสม่ำเสมอเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้น	ระบบไม่สามารถใช้งานได้	1	5	5	มีการตรวจสอบสม่ำเสมอ
ข้อ 8.6 (A11.2.1)	(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ	สิทธิ์การเข้าถึงข้อมูลมีความปลอดภัย	1	5	5	มีการกำหนดสิทธิ์การเข้าถึงได้ชัดเจน
ข้อ 8.7 (A 12.4.1)	(S) มีการป้องกันการติดตั้งโปรแกรมต่างๆ ลงไปยังระบบที่ให้บริการ	การทำงานของระบบผิดพลาดเกิดขึ้นได้	2	3	6	ไม่มีข้อกำหนด
ข้อ 8.8 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 10 ตารางประเมินความเสี่ยงสำหรับระบบฐานข้อมูลคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ

9.ชื่อทรัพย์สิน : ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 9.1 (A 6.1.5)	(W) ยังไม่มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร	ข้อมูลอาจถูกเปิดเผยได้	5	4	20	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 9.2 (A 7.1.3)	(W)ไม่มีการจัดทำกฎ ระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน	ถูกละเมิด ความปลอดภัย	4	3	12	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 9.3 (A 8.3.3)	(W) ขาดความสม่ำเสมอในการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	ทำให้เกิดการทำงานผิดพลาด	5	3	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 9.4 (A10.5.1)	(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ	ระบบสารสนเทศถูกใช้โดยไม่ได้รับอนุญาต	3	3	9	การสำรองข้อมูล ยังไม่ได้กำหนดเป็นระบบชัดเจน

ตารางที่ 10 (ต่อ)

9.ชื่อทรัพย์สิน : ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 9.5 (A10.10.2)	(S) มีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้น	ระบบไม่สามารถใช้งานได้	1	5	5	มีการตรวจสอบสม่ำเสมอ
ข้อ 9.6 (A11.2.1)	S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ	สิทธิ์การเข้าถึงข้อมูลมีความปลอดภัย	1	5	5	มีการกำหนดสิทธิ์การเข้าถึงได้ชัดเจน
ข้อ 9.7 (A12.4.1)	(S) มีการป้องกันการติดตั้งโปรแกรมต่างๆ ลงไปยังระบบที่ให้บริการ	การทำงานของระบบผิดพลาดเกิดขึ้นได้	2	3	6	ไม่มีข้อกำหนด
ข้อ 9.8 (A12.4.3)	(W)ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

กลุ่มที่ 5 งานบริการ(Service)

ตารางที่ 11 ตารางประเมินความเสี่ยงสำหรับระบบงานบริการ Internet

10. ชื่อทรัพย์สิน : ระบบงานบริการ Internet						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 10.1 (A6.1.5)	(W) ยังไม่มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร	ข้อมูลอาจถูกเปิดเผยได้	5	4	20	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 10.2 (A7.1.3)	(W)ไม่มีการจัดทำกฎ ระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน	ถูกละเมิด ความปลอดภัย	4	3	12	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 10.3 (A8.2.2)	(W) ขาดการให้ความรู้ด้านความมั่นคงปลอดภัย ให้แก่เจ้าหน้าที่ ผู้ใช้ระบบ	ทำให้เกิดการสร้างความตระหนักการทำงานผิดพลาด	5	3	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 10.4 (A10.6.1)	(S) ขาดความสม่ำเสมอในการดูแลระบบและสารสนเทศต่าง ๆ ที่ส่งผ่านเครือข่าย	ระบบไม่สามารถใช้งานได้	5	2	10	มีการวางแผนบำรุงรักษาระบบและกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 11 (ต่อ)

10. ชื่อทรัพย์สิน : ระบบงานบริการ Internet						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 10.5 (A11.5.2)	(S) ผู้ใช้งานต้องมีการระบุตัวตนก่อนเข้าใช้งานระบบ	มีการกำหนดสิทธิในการเข้าใช้ระบบ	5	2	10	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 10.6 (A11.5.5)	(W) ไม่มีการกำหนดให้ระบบตัดการใช้งานผู้ใช้ เมื่อไม่ได้ใช้งานตามระยะเวลาที่กำหนดไว้	การเข้าถึงระบบงานทั้งที่ไม่มีสิทธิ์แล้ว เช่น ของคนเก่า	4	5	20	ยังไม่มีการกำหนดเป็นนโยบายความปลอดภัยระบบสารสนเทศ
ข้อ 10.7 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 12 ตารางประเมินความเสี่ยงสำหรับระบบงานบริการคุ้มครองบริโภคแบบเบ็ดเสร็จ

11. ชื่อทรัพย์สิน : ระบบงานบริการ การคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 11.1 (A6.1.5)	(W) ยังไม่มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร	ข้อมูลอาจถูกเปิดเผยได้	5	4	20	ยังไม่มีการกำหนดนโยบายการรักษาความปลอดภัยและประกาศใช้
ข้อ 11.2 (A8.2.2)	(W) ขาดการให้ความรู้ด้านความมั่นคงปลอดภัย ให้แก่เจ้าหน้าที่ ผู้ใช้ระบบ	ทำให้เกิดการสร้างความตระหนักการทำงานผิดพลาด	5	3	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 11.3 (A10.6.1)	(S) ขาดความสม่ำเสมอในการดูแลระบบและสารสนเทศต่าง ๆ ที่ส่งผ่านเครือข่าย	ระบบไม่สามารถใช้งานได้	5	2	10	มีการวางแผนการบำรุงรักษาระบบและกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 11.4 (A11.5.2)	(S) ผู้ใช้งานต้องมีการระบุตัวตนก่อนเข้าใช้งานระบบ	มีการกำหนดสิทธิในการเข้าใช้ระบบ	5	2	10	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 11.6 (A11.5.5)	(S) มีการกำหนดให้ระบบตัดการใช้งานผู้ใช้ เมื่อไม่ได้ใช้งานตามระยะเวลาที่กำหนดไว้	การเข้าถึงระบบงานทั้งที่ไม่มีสิทธิ์แล้ว เช่น ของคนเก่า	4	5	20	ยังไม่มีการกำหนด เป็นนโยบาย

ตารางที่ 12 (ต่อ)

11. ชื่อทรัพย์สิน : ระบบงานบริการ การคุ้มครองผู้บริโภคแบบเบ็ดเสร็จt						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 11.7 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 11.8 (A13.1.2)	(W) ขาดการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ	เกิดความเสียหายต่อระบบงาน	5	5	25	ไม่มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ
ข้อ 11.9 (A14.1.2)	(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของระบบติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการทำงานและให้บริการของระบบงาน	5	5	25	ประเมินปัญหาของเหตุการณ์ต่างๆและกำหนดแนวทางป้องกัน

ตารางที่ 13 ตารางประเมินความเสี่ยงสำหรับระบบปรับอากาศห้อง Server

12. ชื่อทรัพย์สิน : ระบบปรับอากาศห้อง Server						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 12.1 (A9.2.4)	(S) มีการบำรุงรักษาอุปกรณ์สม่ำเสมอให้มีความสมบูรณ์ในการใช้งาน	อุปกรณ์ทำงานผิดพลาดและเกิดความชำรุดเสียหาย	1	2	2	- มีการวางแผนบำรุงรักษาอุปกรณ์ตามระยะเวลาที่กำหนด - ควรมีการวางแผนต่อเนื่องในการจัดเตรียมงบประมาณสำหรับการบำรุงรักษาระบบปีต่อไป

ตารางที่ 14 ตารางประเมินความเสี่ยงสำหรับงานบริหารจัดการสิทธิในการใช้งานระบบต่างๆ

13. ชื่อทรัพย์สิน : การบริหารจัดการสิทธิ์ในการเข้าใช้งานระบบต่างๆของผู้ใช้ (User)						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 13.1 (A8.3.3)	(W) ขาดความสม่ำเสมอในการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	ทำให้มีการเข้าใช้งานระบบโดยไม่ได้รับอนุญาต	3	5	15	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น/ควรมีทบทวนถอดถอนสิทธิ์ของผู้ใช้ระบบทุกๆเดือน
ข้อ 13.2 (A11.2.1)	(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ	การเข้าถึงข้อมูล	1	5	5	ยังไม่มีการกำหนดนโยบายชัดเจน
ข้อ 13.3 (A11.2.2)	(S) กำหนดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นและต้องได้รับความเห็นชอบจากผู้อำนวยการสำนัก/กอง/หัวหน้าฝ่าย	ไม่อนุญาตให้เข้าถึงข้อมูล	2	2	4	มีการกำหนดสิทธิชัดเจน

ตารางที่ 14 (ต่อ)

13. ชื่อทรัพย์สิน : การบริหารจัดการสิทธิ์ในการเข้าใช้งานระบบต่างๆของผู้ใช้ (User)						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 13.4 (A11.2.4)	(W) ขาดความสม่ำเสมอในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเหมาะสม	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	4	5	20	กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างสม่ำเสมอ
ข้อ 13.5 (A11.5.1)	(W) ยังไม่มีขั้นตอนปฏิบัติที่มีความปลอดภัยสำหรับการเข้าใช้งานระบบอย่างเหมาะสม	อาจใช้งานผิดพลาด	3	4	12	ยังไม่มีนโยบายความปลอดภัยระบบสารสนเทศ
ข้อ 13.6 (A11.5.2)	(S) ผู้ใช้งานต้องมีกวรระบุตัวตนก่อนเข้าใช้งานระบบ	มีการกำหนดสิทธิในการเข้าใช้ระบบ	5	2	10	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
ข้อ 13 .7 (A12.4.3)	(W) ไม่มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด	3	5	15	ต้องกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 15 ตารางประเมินความเสี่ยงสำหรับการติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์

14.ชื่อทรัพย์สิน :งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
ข้อ 14.1 (A9.2.1)	(W) การจัดวางอุปกรณ์อยู่ในที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อาจจะทำให้อุปกรณ์มีการทำงานผิดพลาด	4	4	16	ให้มีการจัดวางอุปกรณ์ตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้า รบกวน
ข้อ 14.2 (A9.2.4)	(W) ขาดการวางแผนในการบำรุงรักษาอุปกรณ์อย่างต่อเนื่องและสม่ำเสมอ	อุปกรณ์ขาดสภาพความพร้อมใช้งานหรือไม่สามารถทำงานได้หรืออาจมีปัญหา	4	5	20	ขาดวางแผนการบำรุงรักษาอุปกรณ์ให้ทำงานได้อย่างต่อเนื่องและสม่ำเสมอ
ข้อ 14.3 (A9.2.7)	(S) ไม่อนุญาตให้นำทรัพย์สินขององค์กรออกนอกองค์กร นอกจากได้รับอนุญาตแล้วเท่านั้น	เกิดการสูญหาย	3	5	15	ยังไม่ได้กำหนดแนวปฏิบัติให้ชัดเจน
ข้อ 14.4 (A10.3.1)	(W) ขาดการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต	อุปกรณ์ที่มีสภาพความพร้อมใช้ในการทำงานมีจำนวนไม่พอเพียง	5	5	25	มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรด้าน ICTเพิ่มเติมในอนาคต

ตารางที่ 15 (ต่อ)

14.ชื่อทรัพย์สิน :งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์						
ข้อ	ประเด็นความเสี่ยง/ ช่องโหว่ /จุดแข็ง(S)/จุดอ่อน (W)	ปัจจัยเสี่ยง/ภัยคุกคาม	ระดับผลกระทบ	ระดับของโอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
ข้อ 14.5 (A10.3.2)	(W) มีการทดสอบก่อนที่จะใช้งานจริง และนำระบบนั้นมาใช้งาน แต่ไม่มีกระบวนการที่ชัดเจน	ระบบอาจจะทำงานผิดพลาด	5	4	20	กำหนดขั้นตอนก่อนการตรวจรับและการตรวจสอบด้านเทคนิค รวมทั้งให้ความรู้แก่เจ้าหน้าที่ด้านเทคนิค
ข้อ 14.5 (A10.4.1)	(S) มีการตรวจจับและป้องกันโปรแกรมที่ไม่ประสงค์ดี	ข้อมูลอาจถูกทำลายได้	3	2	6	มีโปรแกรมตรวจสอบไวรัส
ข้อ 14.6 (A10.5.1)	(W) ขาดการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ	ข้อมูลที่ใช้งานขาดความครบถ้วน	3	7	21	วางแผนการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ
ข้อ 14.7 (A11.5.4)	(W) ขาดการดูแลควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้	ระบบทำงานผิดพลาด	4	3	12	กำหนดแนวทางในการควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ให้ชัดเจน
ข้อ 14.8 (A14.1.2)	(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของอุปกรณ์ต่าง ๆติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการดำเนินงาน	4	5	20	ควรประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน

ภาคผนวก ค

ตารางผลการวิเคราะห์และประเมินความเสี่ยง

(ก่อนการดำเนินโครงการ)

ตารางที่ 16 ผลการวิเคราะห์และประเมินความเสี่ยง (ก่อนการดำเนินโครงการ)

1.นโยบายความมั่นคงปลอดภัย (Security policy)-A5						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
1.1	ยังไม่มีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัยในองค์กรอย่างเป็นทางการ	ยังไม่ได้จัดทำ/กำลังอยู่ระหว่างการดำเนินการ	5	5	25 /สูง	ควรจัดทำร่างนโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ
1.2	ยังไม่มีการกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการจัดทำนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ไม่มีแนวปฏิบัติในการจัดทำนโยบาย มีโอกาสโดนเจาะระบบได้ง่าย	5	5	25/สูง	ยังไม่ได้กำหนดผู้รับผิดชอบในการจัดทำนโยบายความมั่นคงปลอดภัย
1.3	ยังไม่มีการทบทวน ปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	มีการละเมิดความปลอดภัยสูง	4	5	20/สูง	ยังไม่มีการพัฒนาและปรับปรุงจัดทำร่างนโยบายมั่นคงปลอดภัยของระบบสารสนเทศ

ตารางที่ 16 (ต่อ)

2. โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) – A6						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
2.1	ไม่สามารถผลักดันนโยบายด้านความมั่นคงปลอดภัยให้มีผลชัดเจนและสำเร็จอย่างเป็นรูปธรรม	ขาดการกำหนดให้มีตัวแทนพนักงานจากสำนัก/กองต่างๆเพื่อประสานงานในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ	5	4	20/สูง	ข้อเสนอแนะ : ผู้บริหารสารสนเทศต้องกำหนดให้มีตัวแทนจากสำนัก/กองต่างๆ เพื่อประสานงานงานด้านความมั่นคงปลอดภัย
2.2	ระบบสารสนเทศไม่มีความมั่นคงปลอดภัยเนื่องจากขาดผู้รับผิดชอบและดูแลอย่างจริงจังและชัดเจน	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบในการดูแลระบบสารสนเทศอย่างชัดเจนและไม่มีการกำหนดทิศทางที่ชัดเจน	5	4	20/สูง	สถานะปัจจุบัน : ผู้รับผิดชอบด้านระบบสารสนเทศ มีจำนวนน้อย ไม่สามารถแบ่งแยกความรับผิดชอบที่ชัดเจนได้

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
2.3	การเข้าถึงระบบและข้อมูลสำคัญโดยไม่ได้รับอนุญาต	มีการระบุข้อกำหนดหรือเงื่อนไขด้านความมั่นคงปลอดภัยในการเข้าถึงระบบ ระบบ งานหรือสารสน- เทศขององค์กร	5	2	10/กลาง	สถานะปัจจุบัน : มีการกำหนดความปลอดภัยในการเข้าถึงและใช้งานระบบสารสนเทศขององค์กร
2.4	ข้อมูลสำคัญรั่วไหลหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต แก่บุคลคลผู้ไม่มีสิทธิ์ทั้งภายในและนอกองค์กร	ไม่มีการจัดทำข้อตกลงการไม่เปิดเผยความลับ	5	4	20/สูง	สถานะปัจจุบัน : ยังไม่มีนโยบายเรื่องการรักษาความลับและให้พนักงานลงชื่อรับทราบ
2.5	ไม่มีการจัดทำแผนฉุกเฉิน กรณีระบบมีปัญหา	ไม่สามารถกู้ระบบ ได้ตามเวลาที่เหมาะสม อาจส่งผลกระทบต่อการทำงาน	4	4	16/กลาง	สถานะปัจจุบัน : ควรจัดทำแผนฉุกเฉินรองรับ กรณีระบบมีปัญหาและไม่สามารถใช้งานได้จากระบบหลัก

ตารางที่ 16 (ต่อ)

3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) – A7						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
3.1	ขาดการบริหารจัดการด้านทรัพย์สินต่างๆ ให้ชัดเจน เช่น การใช้งานผิดพลาด	- มีการจัดทำป้ายชื่อและบัญชีทรัพย์สินสารสนเทศขององค์กร -มีการควบคุมการใช้ทรัพย์สินขององค์กรอย่างเหมาะสม	3	4	12/กลาง	สถานะปัจจุบัน : ยังไม่มีการทำและปรับปรุงบัญชีสินทรัพย์ที่มีความสำคัญ ให้ถูกต้องอยู่เสมอ
3.2	การปฏิเสธความรับผิดชอบเมื่อเกิดการสูญหายของทรัพย์สิน/ขาดการดูแลอย่างเหมาะสม	มีการกำหนดผู้ดูแลหรือผู้ถือครองทรัพย์สินในบัญชีทรัพย์สิน	4	3	12/กลาง	สถานะปัจจุบัน : มีการกำหนดผู้ดูแลในบัญชีทรัพย์สิน
3.3	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตเนื่องจากมีการป้องกันที่ไม่เหมาะสม	ยังไม่มีแนวทางการจัดหมวดหมู่ความสำคัญข้อมูลสารสนเทศ (classification guidelines)	4	5	20/สูง	สถานะปัจจุบัน : ยังไม่มีแนวทางการจัดหมวดหมู่ข้อมูลและไม่มีเอกสารระบุชัดเจน

ตารางที่ 16 (ต่อ)

3.การบริหารจัดการทรัพย์สินของงค์กร (Asset Management) – A7						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
3.4	การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)	ยังไม่มีการจัดหมวดหมู่ความสำคัญของข้อมูลสารสนเทศและระบุความเป็นเจ้าของระบบ	4	4	16/สูง	สถานะปัจจุบัน : ยังไม่มีแนวทางการจัดหมวดหมู่ข้อมูลและไม่มีเอกสารระบุชัดเจนและระบบความเป็นเจ้าของระบบ
3.5	ไม่มีการจัดเก็บทะเบียนครุภัณฑ์คอมพิวเตอร์ให้ถูกต้อง	ไม่มีการบำรุงรักษาอย่างเหมาะสม	4	3	12/กลาง	ไม่มีการจัดเก็บทะเบียนครุภัณฑ์

ตารางที่ 16 (ต่อ)

4 ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร (Human Resources Security) –A8						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.1	การเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยใช้ User ID ของพนักงานคนก่อน	ขาดการติดตาม เรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือย้ายแผนก/ขาดการปรับปรุงข้อมูลในการจัดการสิทธิของระบบงานต่างๆ	4	4	16/กลาง	สถานะปัจจุบัน:ขาดการจัดการที่ดีในการถอดถอนสิทธิของเจ้าหน้าที่ที่ลาออก หรือย้ายแผนก เจ้าหน้าที่ไม่ได้แจ้งแผนก ICT ทราบ ข้อเสนอแนะ:ควรมีการกำหนดหน้าที่และขั้นตอนปฏิบัติให้ชัดเจน
4.2	ทรัพย์สินขององค์กรเกิดการสูญหายไป/หรือไม่มีการเก็บข้อมูลการยืมคืนทรัพย์สินอย่างเป็นระบบ	มีขั้นตอนปฏิบัติสำหรับการยืม-คืนทรัพย์สินขององค์กรเมื่อพนักงานมีการลาออกหรือเข้าใหม่	3	4	12/กลาง	สถานะปัจจุบัน : มีขั้นตอนปฏิบัติสำหรับการคืนทรัพย์สินขององค์กรโดยมีเจ้าหน้าที่ได้รับมอบหมายชัดเจน
4.3	ข้อมูลระบบและเครื่องคอมพิวเตอร์ขององค์กรขาดความมั่นคงปลอดภัย	ขาดการสร้างความรู้ สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยซึ่งทำให้ผู้ใช้งานสามารถป้องกันตนเองได้	5	3	15/กลาง	สถานะปัจจุบัน : ยังไม่เคยมีการอบรมให้ความรู้ ความเข้าใจ ด้านรักษาความปลอดภัยระบบสารสนเทศ

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.4	บุคลากรไม่เกรงกลัวต่อการละเมิดนโยบายด้านความมั่นคงปลอดภัยซึ่งอาจทำให้องค์กรเกิดความเสียหายมากขึ้นและมากขึ้น	ขาดกระบวนการลงโทษทางวินัยเมื่อมีการละเมิดนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย	3	3	9/กลาง	สถานะปัจจุบัน : การลงโทษส่วนใหญ่จะเป็นการว่ากล่าวตักเตือน
4.5	บุคลากรขาดความรู้ความสามารถในการปฏิบัติงานตามหน้าที่ความรับผิดชอบของตนเอง/บุคลากรที่รับเข้ามาเคยมีประวัติเสียและอาจก่อให้เกิดความเสียหายต่อองค์กร	ขั้นตอนสำหรับการคัดเลือกบุคลากรเข้ามาปฏิบัติงานในองค์กร	4	2	8/ต่ำ	สถานะปัจจุบัน : มีการสัมภาษณ์และตรวจสอบประวัติการทำงานรวมทั้งตรวจสอบประวัติอาชญากรจากกรมตำรวจ
4.6	การปฏิเสธความรับผิดชอบเนื่องจากลักษณะงานหรือหน้าที่ความรับผิดชอบไม่ชัดเจน	การกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ชัดเจนของบุคลากรที่เข้ามาปฏิบัติงานกับองค์กร	5	5	25/สูง	สถานะปัจจุบัน :ไม่มีการกำหนดบทบาทหน้าที่ความรับผิดชอบที่ชัดเจนเฉพาะส่วนงานในแผนกของตัวเองจึงขาดการประสานงานที่ชัดเจนระหว่างแผนก

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อ	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.7	(W) ขาดและให้ความรู้ด้านความมั่นคงปลอดภัย ให้แก่เจ้าหน้าที่ ผู้ใช้ระบบ	ทำให้เกิดการสร้างความตระหนักการทำงานผิดพลาด	5	3	15/กลาง	กำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
4.8	(W) มีการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียดเพื่อความปลอดภัยสำหรับสารสนเทศขององค์กร	ป้องกันการเข้าถึงข้อมูลและอุปกรณ์	3	2	6/ต่ำ	ยังไม่มีการควบคุมและการตรวจสอบเรื่องนี้
4.9	(W) ไม่มีการกำหนดให้ผู้ที่สิ้นสุดการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน	ทรัพย์สินสูญหาย	3	5	15/กลาง	ต้องมีข้อกำหนดในการคืนอุปกรณ์และการถอดถอนสิทธิเมื่อสิ้นสุดการจ้างงาน

ตารางที่ 16 (ต่อ)

5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environnent Security) – A9						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.1	การจัดวางอุปกรณ์อยู่ในที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	ทำให้อุปกรณ์มีการทำงานผิดพลาด	5	3	15/กลาง	สถานะปัจจุบัน : สำหรับเครื่องเซิร์ฟเวอร์ทุกเครื่องได้ต่อไฟเข้ากับระบบสำรองไฟ ส่วนคอมพิวเตอร์ทั่วไปก็มีบ้างที่ต่อเข้ากับเครื่องสำรองไฟ
5.2	ผู้ไม่ประสงค์ดี อาจเข้าถึงอุปกรณ์และข้อมูลได้ง่าย	กำแพงและประตูสามารถเปิดสะดวกและมีส่วนประกอบของกระจกธรรมดาซึ่งผู้ไม่ประสงค์ดีสามารถเข้าถึงอุปกรณ์ได้โดยง่าย	5	4	20/สูง	ปัจจุบัน : ประตูและกำแพงสามารถเปิดง่ายและสะดวกและเป็นส่วนประกอบและประตู ข้อเสนอแนะ:ประตูควรเป็นประตูกระจกนิรภัย

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.3	ข้อมูลสำคัญในคอมพิวเตอร์เก่า ถูกเข้าถึงโดยผู้ไม่ได้รับอนุญาต	ขาดขั้นตอนกำจัดอุปกรณ์และการทำลายข้อมูลในเครื่องคอมพิวเตอร์เก่า ที่บริจาคหรือขายต่อ	4	4	16/กลาง	สถานะปัจจุบัน : ไม่มีการทำลายข้อมูลในเครื่องคอมพิวเตอร์เก่าที่ไม่ใช้แล้ว ข้อเสนอแนะ : ควรทำลายสื่อบันทึกข้อมูลก่อนนำออกนอกองค์กร
5.4	ห้ามนำทรัพย์สินในองค์กรออกไปภายนอก นอกจากได้รับอนุญาตเท่านั้น	ไม่มีการตรวจสอบการนำทรัพย์สินออกนอกสถานที่	4	3	12/กลาง	สถานะปัจจุบัน : ยังไม่มีการเซ็นชื่อในใบนำทรัพย์สินออกนอกสถานที่ทุกครั้ง
5.5	อุปกรณ์ได้รับความเสียหายจากภัยธรรมชาติ และ เข้าถึงได้โดยง่าย เนื่องจากสถานที่ตั้งไม่เหมาะสม	การออกแบบสถานที่ตั้งและบริเวณโดยรอบของห้องเซิร์ฟเวอร์	3	2	6/ต่ำ	สถานะปัจจุบัน : ห้องเซิร์ฟเวอร์ได้รับการออกแบบให้อยู่บริเวณกลางๆ ของตัวอาคารภายในและมีพื้นที่จำกัด

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.6	ทรัพย์สินขององค์กรเกิดการสูญหายหรือเสียหาย	มีการควบคุมทางกายภาพในการเข้า-ออกสถานที่ต่างๆขององค์กร	4	3	12/กลาง	สถานะปัจจุบัน : มีเจ้าหน้าที่รักษาความปลอดภัยควบคุม ในการเข้า-ออกสถานที่ต่างๆและมาการตรวจค้นร่างกายในสถานที่เป็นจุดเสี่ยง
5.7	มีการวางแผนในการบำรุงรักษาเครื่องเซิร์ฟเวอร์และอุปกรณ์อย่างต่อเนื่องสม่ำเสมอ	อุปกรณ์อาจจะเสีย หรือไม่สามารถทำงนได้ มีการดูแลรักษาภายในห้องเซิร์ฟเวอร์ ให้อยู่ในระหว่างอุณหภูมิ 15-22 °c อยู่เสมอ	5	1	5/ต่ำ	สถานะปัจจุบัน : มีการวางแผนการบำรุงรักษาทุกปี
5.8	เมื่อไฟดับ เครื่อง UPS ทำให้ Server ดับ เมื่อไฟติด ไฟเข้าสู่ Server แล้วทำให้ ไม่สามารถเข้าสู่ระบบได้ HW เสีย	การ Restart ตัวเองของ Server ทำให้ค่าต่างๆของอุปกรณ์ที่กำหนดไว้ผิดพลาดและไม่สามารถทำงานต่อได้	5	4	20/สูง	สถานะปัจจุบัน : มีระบบไฟสำรองได้ไม่เกิน 3 ชั่วโมง /ยังต้องมีการปิดระบบ Server ด้วยระบบมือ

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.9	มีการอนุญาตให้ผ่านเข้า-ออกในห้อง Server	เฉพาะผู้มีบัตรเท่านั้น	4	3	12/กลาง	สถานะปัจจุบัน : ไม่ค่อยมีการควบคุมการเข้า-ออกในห้อง Server แต่ไม่ได้ใช้บัตรในการผ่านเข้า - ออก

ตารางที่ 16 (ต่อ)

6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communicatios and Operating Management) - A10						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.1	ข้อมูลไม่ได้รับการสำรองอย่างถูกวิธีในเครื่องคอมพิวเตอร์เฉพาะทางอย่างสม่ำเสมอ	ขาดแผนการสำรองข้อมูลที่ครบถ้วน เช่น เอกสารวิธีการสำรองข้อมูลแต่ละระบบ/ข้อมูลที่สำรอง (Backup) ที่จัดเก็บไว้ไม่สามารถใช้งานได้/ไม่มีการวางแผนที่ดี	5	5	25/สูง	สถานะปัจจุบัน : ให้เจ้าหน้าที่ของบริษัท Outsource ทำการสำรองข้อมูลให้อย่างเดียว และใช้ Server สำรองอยู่ในที่เดียวกัน ข้อเสนอแนะ : ควรมีเอกสารขั้นตอนวิธีการสำรองข้อมูล และควรมีการบันทึกการสำรองข้อมูลและทดสอบการใช้งาน
6.2	ไม่มีอุปกรณ์ควบคุม/ตรวจสอบข้อมูลและการเชื่อมต่อทางเครือข่ายเพื่อความปลอดภัย	ขาดการควบคุม/การตรวจสอบข้อมูลและการเชื่อมต่อทางเครือข่าย	5	5	25/สูง	สถานะปัจจุบัน : ไม่มีอุปกรณ์การควบคุมการตรวจสอบใช้งานข้อมูลหรือตรวจสอบระบบเครือข่าย

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
6.3	การปฏิบัติงานผิดพลาด	ขาดการจัดทำและปรับปรุงเอกสารคู่มือขั้นตอนการปฏิบัติงานไว้ให้เป็นระบบ	4	4	16/กลาง	สถานะปัจจุบัน : ไม่มีเอกสารและคู่มีการปฏิบัติงานเพียงบางส่วน ข้อเสนอแนะ : ควรจัดทำและปรับปรุงเอกสารคู่มือขั้นตอนปฏิบัติงานอยู่เสมอ
6.4	การไม่สามารถติดตั้งระบบกลับคืนในกรณีที่เกิดภัยพิบัติกับสถานที่ที่ใช้สำหรับจัดเก็บข้อมูลที่ได้สำรองไว้และการไม่มีข้อมูลในการใช้งาน	ขาดการจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่	5	5	25/สูง	สถานะปัจจุบัน : ข้อมูลที่สำรองไว้เก็บไว้ใกล้กับเครื่องเซิร์ฟเวอร์ ข้อเสนอแนะ : ข้อมูลที่สำรองควรเก็บไว้ในตู้เซฟกันไฟและควรเก็บไว้ที่ห้องอื่นที่อยู่ห่างจากห้องเซิร์ฟเวอร์

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.5	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/ การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต/ข้อมูลสำคัญรั่วไหล	ยังไม่มีนโยบายการปฏิบัติและการแลกเปลี่ยนข้อมูลกันระหว่างองค์กร เพื่อป้องกันการถูกเข้าถึง การเปลี่ยนแปลงแก้ไข การสำเนา และการทำลายโดยไม่ได้รับอนุญาต	4	4	16/กลาง	สถานะปัจจุบัน : ยังไม่มีนโนยายเรื่องความลับ และมีการระบุข้อตกลงเรื่องความลับลงในสัญญาเสมอ โดยจะมีแผนกกฎหมายเป็นผู้ตรวจทานให้
6.6	เอกสารและคู่มือเกิดการสูญหาย/ ข้อมูลสำคัญในเอกสารคู่มือนั้นถูกเข้าถึงโดยไม่ได้รับอนุญาต	การจัดเก็บเอกสารและคู่มือการปฏิบัติงานไว้ในสถานที่ที่มีความปลอดภัย	5	4	20/สูง	สถานะปัจจุบัน : มีการจัดเก็บและScanเอกสารบางอย่างเป็น Soft file และจัดเก็บใน Server ซึ่งมีระบบสำรองข้อมูล และกำหนดสิทธิ์ในการเข้าถึงข้อมูล

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.7	ไม่มีคู่มือการปฏิบัติงานที่เป็นลายลักษณ์อักษร	ขั้นตอนการทำงานผิดพลาด	4	5	20/สูง	ไม่มีคู่มือในการดูแลระบบเครือข่าย ดูแลระบบงานประยุกต์
6.8	โปรแกรมป้องกันไวรัส ไม่สามารถป้องกันไวรัสใหม่ๆได้ ทำให้ไวรัสแพร่กระจาย	ขาดการตรวจสอบการปรับปรุงฐานข้อมูลของไวรัสอย่างสม่ำเสมอ ไม่มีระเบียบปฏิบัติในการป้องกันไวรัสอย่างจริงจังและทั่วถึง	4	1	4/ต่ำ	สถานะปัจจุบัน : มีตรวจสอบการปรับปรุงฐานข้อมูลไวรัสเดือนละ 1 ครั้ง เนื่องจากเป็นโปรแกรมไวรัสรวมกับการบำรุงรักษาระบบ PC ข้อเสนอแนะ : ควรกำหนดนโยบายป้องกันไวรัส และ ระเบียบปฏิบัติในการป้องกันไวรัสอย่างจริงจัง

ตารางที่ 16 (ต่อ)

7.การควบคุมการเข้าถึง(Access Control)- A11						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
7.1	ไม่มีการจัดทำนโยบายการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร	มีการละเมิดการเข้าถึงข้อมูล	5	4	20/กลาง	ไม่มีเอกสารเป็นลายลักษณ์อักษร
7.2	มีการกำหนดการบริหารการกำหนดสิทธิในการใช้งานระบบ	ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	4	2	8/ต่ำ	มีการกำหนดสิทธิในการใช้งานระบบงานต่างๆ
7.3	การใช้งานรหัสผ่าน (Password Use)	ป้องกันการเข้าถึงข้อมูลและการเจาะระบบ	5	4	20/สูง	ข้อเสนอแนะ : ควรกำหนด User และ Password อย่างน้อง 8 ตัวอักษร
7.4	การเข้าใช้งานระบบเครือข่ายที่อยภายนอกองค์กร ต้องมีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ใช้	ป้องกันการเข้าถึงเครือข่ายจากคนภายนอก	5	4	20/สูง	ข้อเสนอแนะ : ควรมีกำหนดสิทธิการเข้าถึงระบบ จากภายนอกให้เป็นลายลักษณ์อักษร
7.5	ไม่มีการจำกัดการเข้าถึงซอร์สโค้ด (Source Code)สำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด/ละเมิดการเข้าถึงข้อมูล	3	5	15/กลาง	ข้อเสนอแนะ : ต้องมีการกำหนดสิทธิและระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
7.6	(W) ขาดการควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ	เข้าถึงได้ง่าย	3	5	15/กลาง	สถานะปัจจุบัน : ยังไม่มีการกำหนดให้มีขั้นตอนการปฏิบัติที่ชัดเจน เพื่อควบคุมการติดตั้งโปรแกรมต่างๆ ในระบบปฏิบัติการที่ใช้
7.7	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/ทำให้ข้อมูลสำคัญเกิดการรั่วไหล	ขาดขั้นตอนปฏิบัติสำหรับการจัดการกับระบบสารสนเทศตามชั้นความลับที่กำหนดไว้	4	5	20/สูง	สถานะปัจจุบัน : แผนก ICT สามารถเข้าถึงข้อมูลสำคัญได้ทุกอย่าง

ตารางที่ 16 (ต่อ)

8.การจัดหา การบำรุงรักษาระบบสารสนเทศ (Information System Acquistion Development and Maintenance)-A12						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.1	ข้อมูลรั่วไหลจากการนำข้อมูลออกจากองค์กรผ่านทางระบบของแอปพลิเคชัน	ต้องมีการกำหนด กลไกสำหรับตรวจสอบการนำข้อมูลออกจากระบบแอปพลิเคชันต่างๆ	5	4	20/กลาง	สถานะปัจจุบัน : ระบบมีการกำหนดสิทธิ์ในการนำข้อมูลออกจากแอปพลิเคชัน โดยประมวลผลตามสิทธิ์ของผู้ใช้ที่เข้ามาใช้งานระบบ
8.2	การจัดหาและการพัฒนา ระบบสารสนเทศ ที่ไม่มีประสิทธิภาพทำให้องค์กรได้มาซึ่งระบบที่ไม่มีความมั่นคงปลอดภัย	ไม่มีการวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ	3	4	12/กลาง	สถานะปัจจุบัน : จัดทำข้อกำหนดของระบบต่างๆตามความเข้าใจในการจัดหาหรือพัฒนาระบบสารสนเทศตามข้อเท็จจริงที่ได้รับ

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.3	ข้อมูลสำคัญถูกเข้าถึงจากผู้ไม่ได้รับอนุญาต	การเข้ารหัสข้อมูลที่สำคัญขององค์กร เช่น Web application และข้อมูลในคอมพิวเตอร์	4	4	16/กลาง	สถานะปัจจุบัน : ระบบ Web Application ยังไม่มีการเข้ารหัสส่วนที่เป็นคอมพิวเตอร์ของผู้บริหารนั้น
8.4	เกิดความผิดพลาด หรือ การสูญหายของข้อมูล	ระบบงานนำเข้าซึ่งข้อมูล และเกิดการประมวลผลที่ไม่ถูกต้อง	5	4	20/สูง	นำเข้าข้อมูลในระบบโดย Application ต่างๆ ที่เป็นโปรแกรมประยุกต์ ยังไม่มีการตรวจสอบระบบฐานข้อมูล
8.5	ผู้ไม่ประสงค์ดีนำอาศัยช่องโหว่ของระบบปฏิบัติการโจมตีระบบให้เสียหาย	ขาดการอัพเดท Patch ของระบบปฏิบัติการอย่างมีประสิทธิภาพ เพื่ออุดช่องโหว่ของระบบปฏิบัติการ	5	5	25/สูง	สถานะปัจจุบัน : มีการตรวจสอบช่องโหว่ของระบบปฏิบัติการ แต่ไม่มีระบบบริหารจัดการ Patch จากศูนย์กลาง(centralized patch management)

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.6	ใช้ซอฟท์แวร์ละเมิดลิขสิทธิ์และซอฟท์แวร์ที่ดาวโหลดมามีไวรัสทำให้ระบบเสียหาย	ขาดการควบคุมการติดตั้งซอฟท์แวร์ โดยพนักงานติดตั้งซอฟท์แวร์ได้เอง	3	1	3/ต่ำ	สถานะปัจจุบัน : ผู้ใช้ติดตั้งซอฟท์แวร์เอง ไม่ได้มีการควบคุมทางเทคนิคอย่างจริงจัง เช่น ผู้ใช้มีสิทธิ์เป็น Admin
8.7	ระบบเสียหาย และ แก้ไขกลับคืนได้ล่าช้า อันเนื่องมาจากการเปลี่ยนแปลงที่ไม่มีการควบคุมที่ดี	ขั้นตอนปฏิบัติสำหรับควบคุมเปลี่ยนแปลงหรือแก้ไขระบบทั้งHardwareและ Software เช่น การบันทึกการเปลี่ยนแปลง การทำทดสอบระบบก่อนมีการเปลี่ยนแปลง	5	4	20/สูง	สถานะปัจจุบัน :ยังไม่มีขั้นตอนปฏิบัติสำหรับควบคุมเปลี่ยนแปลงหรือแก้ไขระบบ ทั้ง Hardware และ Software

ตารางที่ 16 (ต่อ)

9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Incident Management) A13						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
9.1	ระบบเสียหายกับเกิดเหตุการณ์เดิมๆ ที่เกิดขึ้นในด้านการละเมิดความมั่นคงปลอดภัย	ต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อเตรียมการป้องกันไว้ล่วงหน้า	5	3	15/กลาง	สถานะปัจจุบัน : มีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยการเก็บ Log
9.2	เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุฉุกเฉินไม่ได้รับการจัดการภายในระยะเวลาที่เหมาะสมซึ่งทำให้เหตุการณ์เกิดการลุกลามหรือบานปลาย/เหตุการณ์ฉุกเฉินถูกละเลยโดยไม่มีการแจ้งเหตุเหล่านั้น	ขั้นตอนปฏิบัติสำหรับการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	3	15/กลาง	สถานะปัจจุบัน : ยังไม่มีแผนสำรองฉุกเฉินในการจัดการระบบสารสนเทศได้ทันท่วงที

ตารางที่ 16 (ต่อ)

10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Bisiness Continuty Management) -A14						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
10.1	การกู้คืนธุรกิจสำคัญและระบบงานสนับสนุนไม่ได้รับการกู้คืนหรือสร้างความต่อเนื่องภายในระยะเวลาที่เหมาะสมภายหลังจากที่เกิดเหตุภัยพิบัติ	การระบุและจัดลำดับความสำคัญของกระบวนการทางธุรกิจสำคัญกล่าวคือกระบวนการทางธุรกิจใดก่อนหลังที่ต้องได้รับการกู้คืนให้สำเร็จเรียงตามลำดับความสำคัญ	5	5	25/สูง	สถานะปัจจุบัน :ยังไม่มีการกำหนดระดับความสำคัญของระบบสารสนเทศแต่ละประเภทโดยแบ่งทั้งทาง Business Value และ IT Value
10.2	การขาดความชัดเจนในกระบวนการสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญและระบบงานสนับสนุน /การขาดแผนการสร้างความต่อเนื่องสำหรับกระบวนการทางธุรกิจที่สำคัญ	นโยบายและวัตถุประสงค์เพื่อสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญ	5	5	25/สูง	สถานะปัจจุบัน : ยังไม่มีนโยบายการปฏิบัติงานเพื่อสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญ

ตารางที่ 16 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
10.3	กระบวนการทางธุรกิจสำคัญไม่สามารถกู้คืนได้สำเร็จภายในระยะเวลาที่เหมาะสม	ทางธุรกิจ (Business การจัดทำแผนสร้างความต่อเนื่องContinuityPlan -- BCP) และ ปรับปรุงแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง	5	4	20/สูง	สถานะปัจจุบัน : ยังไม่มีแผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Plan BCP) แต่ขาดการทบทวนและปรับปรุงให้ทันสมัย
10.4	ผู้บริหารขาดข้อมูลเพื่อใช้ในการตัดสินใจว่าจำเป็นต้องมีการสร้างความต่อเนื่องให้แก่กระบวนการทางธุรกิจหนึ่งหรือไม่	ไม่มีการวิเคราะห์และจัดทำรายงานการประเมินผลกระทบที่มีต่อกระบวนการทางธุรกิจสำคัญ (Business Impact Analysis) ในกรณีที่เกิดภัยพิบัติและทำให้กระบวนการเหล่านี้เกิดการหยุดชะงักทำให้ผู้บริหารไม่เห็นถึงความสำคัญและจัดสรรงบประมาณเพื่อการสร้างความต่อเนื่องให้แก่ธุรกิจนั้น	5	5	25/สูง	สถานะปัจจุบัน : ยังไม่มีการวิเคราะห์และจัดทำรายงานการประเมินผลกระทบที่มีต่อกระบวนการทางธุรกิจสำคัญ (Business Impact Analysis) ในกรณีที่เกิดภัยพิบัติ กระบวนการทางธุรกิจสำคัญ ยังไม่มีแผนรองรับ

ตารางที่ 16 (ต่อ)

11.การปฏิบัติตามข้อกำหนด (Compliance) -A15						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
11.1	การใช้งานระบบไม่ตรงตามเงื่อนไขข้อกำหนดที่กำหนดไว้/ไม่ตรงตามวัตถุประสงค์	ขั้นตอนการขออนุมัติเพื่อใช้ระบบงานขององค์กร ขาดการระบุลักษณะหรือประเภทของการใช้	4	3	12/กลาง	สถานะปัจจุบัน : ไม่มีขั้นตอนการขออนุมัติเพื่อใช้ระบบงานขององค์กร ต้องได้รับการอนุมัติจากหัวหน้างานก่อนจากนั้นเจ้าหน้าที่ ICT จะดำเนินการจัดหาตามสิ่งที่ผู้ใช้ได้ขอใช้งานระบบ
11.2	เอกสารข้อมูลสำคัญบางประเภทไม่ได้รับการจัดเก็บไว้นานและอาจมีการละเมิดกฎหมายที่กำหนดไว้	การกำหนดระยะเวลาสำหรับการจัดเก็บเอกสารข้อมูลแต่ละประเภทที่มีความสำคัญ	4	2	8/ต่ำ	สถานะปัจจุบัน : ไม่มีกำหนดระยะเวลาสำหรับการจัดเก็บเอกสารข้อมูลสำคัญ โดยการจัดการแต่ละประเภทของเอกสาร
11.3	ข้อมูลเอกสารที่สำคัญสูญหายหรือรั่วไหล	การจัดเก็บข้อมูลสำคัญ รวมทั้งข้อมูลส่วนตัว ที่ไม่มีประสิทธิภาพ	4	2	8/ต่ำ	สถานะปัจจุบัน : มีการทำสำเนาเอกสารสำคัญที่ต้องใช้อ้างอิงและจัดเก็บเอกสารต้นฉบับไว้สถานที่ปลอดภัยภายนอกองค์กร ส่วนข้อมูลเอกสารที่จัดเก็บภายในองค์กรก็มีการแบ่งระดับสิทธิ์การเข้าถึง

ภาคผนวก ง

ตารางผลการวิเคราะห์และประเมินความเสี่ยง

(หลังการดำเนินโครงการ)

ตารางที่ 17 ผลการวิเคราะห์และประเมินความเสี่ยง (หลังการดำเนินโครงการ)

1.นโยบายความมั่นคงปลอดภัย (Security policy)=A5						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
1.1	ยังไม่มีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัยในองค์กรอย่างเป็นทางการ	ยังไม่ได้จัดทำ/กำลังอยู่ระหว่างการดำเนินการ	5	5	25/สูง	ควรจัดทำร่างนโยบายความมั่นคงปลอดภัยสารสนเทศและประกาศใช้อย่างเป็นทางการเพื่อลดความเสี่ยง
1.2	ยังไม่มีการกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการจัดทำนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ไม่มีแนวปฏิบัติในการจัดทำนโยบาย มีโอกาสโดนเจาะระบบได้ง่าย	5	2	10/กลาง	มีการกำหนดผู้รับผิดชอบในการจัดทำนโยบายความมั่นคงปลอดภัยเรียบร้อยแล้ว
1.3	ยังไม่มีการทบทวน ปรับปรุงการจัดทำนโยบายความมั่นคงปลอดภัยและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	มีการละเมิดความปลอดภัยสูง	4	2	8/ต่ำ	มีการทบทวนและพัฒนาปรับปรุงจัดทำร่างนโยบายมั่นคงปลอดภัยของระบบสารสนเทศ(กำลังดำเนินการ)

ตารางที่ 17 (ต่อ)

2.โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) – A6						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
2.1	ไม่สามารถผลักดันนโยบายด้านความมั่นคงปลอดภัยให้มีผลชัดเจนและสำเร็จอย่างเป็นรูปธรรม	ขาดการกำหนดให้มีตัวแทนพนักงานจากสำนัก/กองต่างๆเพื่อประสานงาน ในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ	5	3	15/กลาง	มีการนำเสนอให้ผู้บริหารให้มีตัวแทนจากสำนัก/กองต่างๆ เพื่อประสานงานด้านความปลอดภัย
2.2	ระบบสารสนเทศไม่มีความมั่นคงปลอดภัยเนื่องจากขาดผู้รับผิดชอบและดูแลอย่างจริงจังและชัดเจน	ไม่มีการกำหนดหน้าที่และผู้รับผิดชอบในการดูแลระบบสารสนเทศอย่างชัดเจนและไม่มีการกำหนดทิศทางที่ชัดเจน	5	2	10/กลาง	สถานะปัจจุบัน:มีการกำหนดผู้รับผิดชอบด้านสารสนเทศและแบ่งแยกความรับผิดชอบที่ชัดเจน แต่อาจจะมีซ้ำซ้อนเพราะเจ้าหน้าที่ ITไม่ เพียงพอ

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
2.3	การเข้าถึงระบบและข้อมูลสำคัญโดยไม่ได้รับอนุญาต	มีการระบุข้อกำหนดหรือเงื่อนไขด้านความมั่นคงปลอดภัยในการเข้าถึงระบบงานหรือสารสนเทศขององค์กร	5	1	5/ต่ำ	สถานะปัจจุบัน:มีการกำหนดความปลอดภัยในการเข้าถึงและใช้งานระบบสารสนเทศขององค์กรและมีรูปแบบเอกสารที่ชัดเจน
2.4	ข้อมูลสำคัญรั่วไหลหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต แก่บุคลคลผู้ไม่มีสิทธิ์ทั้งภายในและนอกองค์กร	ไม่มีการจัดทำข้อตกลงการไม่เปิดเผยความลับ	5	4	20/สูง	สถานะปัจจุบัน : ยังไม่มีนโยบายเรื่องการรักษาความลับและ ให้พนักงานลงชื่อรับทราบ
2.5	ไม่มีการจัดทำแผนฉุกเฉิน กรณีระบบมีปัญหา	ไม่สามารถกู้ระบบ ได้ตามเวลาที่เหมาะสม อาจส่งผลกระทบต่อการทำงาน	4	4	16/กลาง	สถานะปัจจุบัน : ควรจัดทำแผนฉุกเฉินรองรับ กรณีระบบมีปัญหาและไม่สามารถใช้งานได้

ตารางที่ 17 (ต่อ)

3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) = A7						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
3.1	ขาดการบริหารจัดการด้านทรัพย์สินต่างๆ ให้ชัดเจน เช่น การใช้งานผิดพลาด	- มีการจัดทำป้ายชื่อและบัญชีทรัพย์สินสารสนเทศขององค์กร - มีการควบคุมการใช้ทรัพย์สินขององค์กรอย่างเหมาะสม	3	4	12/กลาง	สถานะปัจจุบัน : ยังไม่มีการทำและปรับปรุงบัญชีสินทรัพย์ที่มีความสำคัญ ให้ถูกต้องอยู่เสมอ
3.2	การปฏิเสธความรับผิดชอบเมื่อเกิดการสูญหายของทรัพย์สิน/ขาดการดูแลอย่างเหมาะสม	มีการกำหนดผู้ดูแลหรือผู้ถือครองทรัพย์สินในบัญชีทรัพย์สิน	4	3	12/กลาง	สถานะปัจจุบัน :ยังไม่มีการกำหนดผู้ดูแลในบัญชีทรัพย์สิน
3.3	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตเนื่องจากมีการป้องกันที่ไม่เหมาะสม	ยังไม่มีแนวทางการจัดหมวดหมู่ความสำคัญข้อมูลสารสนเทศ (classification guidelines)	4	3	12/กลาง	สถานะปัจจุบัน : ยังไม่มีแนวทางการจัดหมวดหมู่ข้อมูลและไม่มีเอกสารระบุชัดเจน

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
3.4	การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)	ยังไม่มีการจัดหมวดหมู่ความสำคัญของข้อมูลสารสนเทศและระบุความเป็นเจ้าของระบบ	4	4	16/กลาง	สถานะปัจจุบัน : ยังไม่มีแนวทางการจัดหมวดหมู่ข้อมูลและไม่มีเอกสารระบุชัดเจนและระบุความเป็นเจ้าของระบบ
3.5	ไม่มีการจัดเก็บทะเบียนครุภัณฑ์คอมพิวเตอร์ให้ถูกต้อง	ไม่มีการบำรุงรักษาอย่างเหมาะสม	4	1	4/ต่ำ	กำหนดให้มีการจัดเก็บทะเบียนครุภัณฑ์ (อยู่ระหว่างดำเนินการ)

ตารางที่ 17 (ต่อ)

4.ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร (Human Resources Security) –A8						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.1	การเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยใช้ User ID ของพนักงานคนก่อน	ขาดการติดตาม เรื่องการถอดถอนสิทธิของพนักงานที่ลาออก หรือย้ายแผนก/ขาดการปรับปรุงข้อมูลในการจัดการสิทธิของระบบงานต่างๆ	4	2	8/ต่ำ	สถานะปัจจุบัน:เริ่มมีการกำหนดสิทธิในการถอดถอนสิทธิของเจ้าหน้าที่ที่ลาออกหรือย้ายแผนก ข้อเสนอแนะ:ควรมีการกำหนดหน้าที่และขั้นตอนปฏิบัติให้ชัดเจน
4.2	ทรัพย์สินขององค์กรเกิดการสูญหายไป/หรือไม่มีการเก็บข้อมูลการยืมคืนทรัพย์สินอย่างเป็นระบบ	มีขั้นตอนปฏิบัติสำหรับการยืม-คืนทรัพย์สินขององค์กรเมื่อพนักงานมีการลาออกหรือเข้าใหม่	3	4	12/กลาง	สถานะปัจจุบัน : มีขั้นตอนปฏิบัติสำหรับการคืนทรัพย์สินขององค์กรโดยมีเจ้าหน้าที่ได้รับมอบหมายชัดเจน
4.3	ข้อมูล ระบบ และเครื่องคอมพิวเตอร์ขององค์กรขาดความมั่นคงปลอดภัย	ขาดการสร้างความรู้ สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยซึ่งทำให้ผู้ใช้งานสามารถป้องกันตนเองได้ในระดับพื้นฐาน	4	2	8/ต่ำ	สถานะปัจจุบัน : เริ่มมีการอบรมให้ความรู้ ความเข้าใจ ด้านรักษาความปลอดภัยระบบสารสนเทศ กำลังดำเนินการจัดทำนโยบาย

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.4	บุคลากรไม่เกรงกลัวต่อการละเมิดนโยบายด้านความมั่นคงปลอดภัยซึ่งอาจทำให้องค์กรเกิดความเสียหายมากขึ้นและมากขึ้น	ขาดกระบวนการลงโทษทางวินัยเมื่อมีการละเมิดนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย	3	3	9/ต่ำ	สถานะปัจจุบัน : การลงโทษส่วนใหญ่จะเป็นการว่ากล่าวตักเตือน
4.5	บุคลากรขาดความรู้ความสามารถในการปฏิบัติงานตามหน้าที่ความรับผิดชอบของตนเอง/บุคลากรที่รับเข้ามาเคยมีประวัติเสียและอาจก่อให้เกิดความเสียหายต่อองค์กร	ขั้นตอน สำหรับการคัดเลือกบุคลากรเข้ามาปฏิบัติงานในองค์กร	4	2	8/ต่ำ	สถานะปัจจุบัน : มีการสัมภาษณ์และตรวจสอบประวัติการทำงานรวมทั้งตรวจสอบประวัติอาชญากร จากกรมตำรวจ
4.6	การปฏิเสธความรับผิดชอบเนื่องจากลักษณะงานหรือหน้าที่ความรับผิดชอบไม่ชัดเจน	การกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ชัดเจนของบุคลากร ที่เข้ามาปฏิบัติงานกับองค์กร	5	3	15/กลาง	สถานะปัจจุบัน :เริ่มมีการกำหนดบทบาทหน้าที่ความรับผิดชอบที่ชัดเจนเฉพาะส่วนงานในแผนกของตัวเองจึงขาดการประสานงานที่ชัดเจนระหว่างแผนก

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
4.7	(W) ขาดและให้ความรู้ด้านความมั่นคงปลอดภัย ให้แก่เจ้าหน้าที่ ผู้ใช้ระบบ	ทำให้เกิดการสร้างความตระหนักการทำงานผิดพลาด	5	1	5/ต่ำ	มีการจัดฝึกอบรมด้าน Security Awareness Training ให้แก่เจ้าหน้าที่ภายในองค์กรและกำหนดระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
4.8	(W) มีการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียดเพื่อความปลอดภัยสำหรับสารสนเทศขององค์กร	ป้องกันการเข้าถึงข้อมูลและอุปกรณ์	3	2	6/ต่ำ	ยังไม่มีการควบคุมและการตรวจสอบในเรื่องนี้ ให้ชัดเจน
4.9	(W) ไม่มีการกำหนดให้ผู้ที่สิ้นสุดการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน	ทรัพย์สินสูญหาย	3	5	15/กลาง	ยังไม่มีข้อกำหนดในการคืนอุปกรณ์และการถอดถอนสิทธิเมื่อสิ้นสุดการจ้างงาน

ตารางที่ 17 (ต่อ)

5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environnent Security) – A9						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.1	การจัดวางอุปกรณ์อยู่ในที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	ทำให้อุปกรณ์มีการทำงานผิดพลาด	5	3	3/ต่ำ	สถานะปัจจุบัน : สำหรับเครื่องเซิร์ฟเวอร์ทุกเครื่องได้ต่อไฟเข้ากับระบบสำรองไฟ ส่วนคอมพิวเตอร์ทั่วไปก็มีบ้างที่ต่อเข้ากับเครื่องสำรองไฟ
5.2	ผู้ไม่ประสงค์ดี อาจเข้าถึงอุปกรณ์และข้อมูลได้ง่าย	กำแพงและประตูสามารถเปิดสะดวกและมีส่วนประกอบของกระจกธรรมดาซึ่งผู้ไม่ประสงค์ดีสามารถเข้าถึงอุปกรณ์ได้โดยง่าย	5	4	20/สูง	ปัจจุบัน : ประตูและกำแพงสามารถเปิดง่ายสะดวกและเป็นส่วนประกอบและประตู ข้อเสนอแนะ : ประตูควรเป็นประตูนิรภัย

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.3	ข้อมูลสำคัญในคอมพิวเตอร์เก่าถูกเข้าถึงโดยผู้ไม่ได้รับอนุญาต	ขาดขั้นตอนกำจัดอุปกรณ์และการทำลายข้อมูลในเครื่องคอมพิวเตอร์เก่า ที่บริจาคหรือขายต่อ	4	2	8/ต่ำ	สถานะปัจจุบัน : ไม่มีการทำลายข้อมูลในเครื่องคอมพิวเตอร์ที่ไม่ใช้ ข้อเสนอแนะ : ควรทำลายสื่อบันทึกข้อมูลก่อนการนำออกนอกองค์กร
5.4	ห้ามนำทรัพย์สินในองค์กรออกไปภายนอก นอกจากได้รับอนุญาตเท่านั้น	ไม่มีการตรวจสอบการนำทรัพย์สินออกนอกสถานที่	4	2	8/ต่ำ	สถานะปัจจุบัน : เริ่มมีการกำกับให้เซ็นใบนำทรัพย์สินออกนอกสถานที่ทุกครั้ง
5.5	อุปกรณ์ได้รับความเสียหายจากภัยธรรมชาติ และ เข้าถึงได้โดยง่าย เนื่องจากสถานที่ตั้งไม่เหมาะสม	การออกแบบสถานที่ตั้งและบริเวณโดยรอบของห้องเซิร์ฟเวอร์	3	3	9/ต่ำ	สถานะปัจจุบัน : ห้องเซิร์ฟเวอร์ได้รับการออกแบบให้อยู่บริเวณกลางๆ ของตัวอาคารภายในและมีพื้นที่จำกัด

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.6	ทรัพย์สินขององค์กรเกิดการสูญหายหรือเสียหาย่	มีการควบคุมทางกายภาพในการ เข้า-ออกสถานที่ต่างๆ ขององค์กร	4	1	4/ต่ำ	สถานะปัจจุบัน : มีเจ้าหน้าที่รักษาความ ปลอดภัยควบคุม ในการเข้า-ออกสถานที่ต่างๆและมาการตรวจค้นร่างกายในสถานที่เป็นจุดเสี่ยง
5.7	มีการวางแผนในการบำรุงรักษาเครื่องเซิร์ฟเวอร์และอุปกรณ์อย่างต่อเนื่องสม่ำเสมอ	อุปกรณ์อาจจะเสีย หรือไม่สามารถทำงนได้ มีการดูแลรักษาภายในห้องเซิร์ฟเวอร์ ให้อยู่ในระหว่างอุณหภูมิ 15-22 °c อยู่เสมอ	5	1	5/ต่ำ	สถานะ ปัจจุบัน : มีการวางแผนการบำรุงรักษาระบบและอุปกรณ์ทุกปี
5.8	เมื่อไฟดับ เครื่อง UPS ทำให้ Server ดับ เมื่อไฟติด ไฟเข้าสู่ Server แล้วทำให้ ไม่สามารถเข้าสู่ระบบได้ HW เสีย	การ Restart ตัวเองของ Server ทำให้ค่าต่างๆของอุปกรณ์ที่กำหนดไว้ผิดพลาดและไม่สามารถทำงานต่อได้	5	2	10/กลาง	สถานะปัจจุบัน : มีระบบไฟสำรองได้ไม่เกิน 3 ชั่วโมง

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
5.9	มีการอนุญาตให้ผ่านเข้า - ออกในห้อง Server เฉพาะกิจเท่านั้น	เฉพาะผู้มีบัตรเท่านั้น	4	1	4/ต่ำ	สถานะ ปัจจุบัน : มีการควบคุมการเข้า-ออกในห้อง Server และผู้ได้รับอนุญาตเท่านั้น

ตารางที่ 17 (ต่อ)

6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and Operations Management) A.10						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.1	ข้อมูลไม่ได้รับการสำรองอย่างถูกวิธีในเครื่องคอมพิวเตอร์เฉพาะทางอย่างสม่ำเสมอ	ขาดแผนการสำรองข้อมูลที่ครบถ้วน เช่น เอกสารวิธีการสำรองข้อมูลแต่ละระบบ/ข้อมูลที่สำรอง (Backup) ที่จัดเก็บไว้ไม่สามารถใช้งานได้/ไม่มีการวางแผนที่ดี	5	3	15/กลาง	สถานะปัจจุบัน : ให้เจ้าหน้าที่ของบริษัท Outsource ทำการสำรองข้อมูลให้อย่างเดียว และใช้ Server สำรองอยู่ในที่เดียวกันและกำหนดให้มีการจัดทำเอกสารคู่มือการใช้งาน ข้อเสนอแนะ : ต้องมีเอกสารขั้นตอนวิธีการสำรองข้อมูล และควรมีบันทึกการสำรองข้อมูลและทดสอบในเบื้องต้นเพื่อการใช้งาน
6.2	ไม่มีอุปกรณ์ควบคุม/ตรวจสอบข้อมูลและการเชื่อมต่อทางเครือข่ายเพื่อความปลอดภัย	ขาดการควบคุม/การตรวจสอบข้อมูลและการเชื่อมต่อทางเครือข่าย	5	1	5/ต่ำ	สถานะปัจจุบัน : ได้จัดซื้อมีอุปกรณ์การควบคุมป้องกันการบุกรุกเพื่อตรวจสอบระบบเครือข่าย

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ข้อเสนอแนะ
6.3	การปฏิบัติงานผิดพลาด	ขาดการจัดทำและปรับปรุงเอกสารคู่มือ ขั้นตอนการปฏิบัติงานไว้ให้เป็นระบบ	4	2	8/ต่ำ	สถานะปัจจุบัน : ไม่มีเอกสารและคู่มือการปฏิบัติงานเพียงบางส่วน ข้อเสนอแนะ : ควรจัดทำและปรับปรุงเอกสารคู่มือขั้นตอนปฏิบัติงานให้ทันสมัยอยู่เสมอ
6.4	การไม่สามารถติดตั้งระบบกลับคืนในกรณีที่เกิดภัยพิบัติกับสถานที่ที่ใช้สำหรับจัดเก็บข้อมูลที่ได้สำรองไว้และการไม่มีข้อมูลในการใช้งาน	ขาดการจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่	5	5	25/สูง	สถานะปัจจุบัน : ข้อมูลสำรองเก็บในเครื่องเซิร์ฟเวอร์ ข้อเสนอแนะ : ควรเก็บไว้ในตู้เซฟกันไฟและควรเก็บไว้ที่ห้องอื่นๆ

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.5	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต/ข้อมูลสำคัญรั่วไหล	ยังไม่มีนโยบายการปฏิบัติและการแลกเปลี่ยนข้อมูลกันระหว่างองค์กร เพื่อป้องกันการถูกเข้าถึง การเปลี่ยนแปลงแก้ไข การสำเนา และการทำลายโดยไม่ได้รับอนุญาต	4	2	8/ต่ำ	สถานะปัจจุบัน : มีนโนยายเรื่องความลับ และมีการระบุข้อตกลงเรื่องความลับลงในสัญญาเสมอ โดยจะมีแผนกกฎหมายเป็นผู้ตรวจทานให้
6.6	เอกสารและคู่มือเกิดการสูญหาย ข้อมูลสำคัญในเอกสารคู่มือนั้นถูกเข้าถึงโดยไม่ได้รับอนุญาต	การจัดเก็บเอกสารและคู่มือการปฏิบัติงานไว้ในสถานที่ที่มีความปลอดภัย	5	1	5/ต่ำ	สถานะปัจจุบัน : มีการจัดเก็บและScanเอกสารบางอย่างเป็น Soft file และจัดเก็บใน Server ซึ่งมีระบบสำรองข้อมูล และกำหนดสิทธิ์ในการเข้าถึงข้อมูล มีเอกสารชัดเจน

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
6.7	ไม่มีคู่มือการปฏิบัติงานที่เป็นลายลักษณ์อักษร	ขั้นตอนการทำงานผิดพลาด	4	3	12/กลาง	มีคู่มือในการดูแลระบบเครือข่าย ดูแลระบบงานประยุกต์แต่ยังไม่มีการจัดเก็บอย่างระบบ
6.8	โปรแกรมป้องกันไวรัส ไม่สามารถป้องกันไวรัสใหม่ๆได้ ทำให้ไวรัสแพร่กระจาย	ขาดการตรวจสอบการปรับปรุงฐานข้อมูลรูปแบบของไวรัส อย่างสม่ำเสมอ ขาดนโยบายป้องกันไวรัส และระเบียบปฏิบัติในการป้องกันไวรัสอย่างจริงจังและทั่วถึง	4	1	4/ต่ำ	สถานะปัจจุบัน : มีตรวจสอบการปรับปรุงฐานข้อมูลไวรัสเดือนละ 1 ครั้ง เนื่องจากเป็นโปรแกรมไวรัสรวมกับการบำรุงรักษาระบบ PC ข้อเสนอแนะ : ควรกำหนดนโยบายป้องกันไวรัส และ ระเบียบปฏิบัติในการป้องกันไวรัสอย่างจริงจัง

ตารางที่ 17 (ต่อ)

7.การควบคุมการเข้าถึง(Access Control)- A11						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
7.1	ไม่มีการจัดทำนโยบายการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร	มีการละเมิดการเข้าถึงข้อมูล	5	2	10/กลาง	กำลังอยู่ระหว่างดำเนินการจัดทำเอกสารเป็นลายลักษณ์อักษร
7.2	มีการกำหนดการบริหารการกำหนดสิทธิในการใช้งานระบบ	ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	4	1	4/ต่ำ	มีการกำหนดสิทธิในการใช้งานระบบงานต่างๆ
7.3	การใช้งานรหัสผ่าน (Password Use)	ป้องกันการเข้าถึงข้อมูลและการเจาะระบบ	5	2	10/กลาง	กำหนดนโยบายแล้วแต่ยังไม่ได้จัดฝึกอบรมเรื่องความปลอดภัย ข้อเสนอแนะ : ควรกำหนด User และ Password อย่างน้อง 8 ตัวอักษร
7.4	การเข้าใช้งานระบบเครือข่ายที่อยภายนอกองค์กร ต้องมีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ใช้	ป้องกันการเข้าถึงเครือข่ายจาก บุคคลที่ไม่เกี่ยวข้อง	5	1	5/ต่ำ	มีกำหนดสิทธิการเข้าถึงระบบจากภายนอกให้เป็นลายลักษณ์

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
7.5	ไม่มีการจำกัดการเข้าถึงซอร์สโค้ด (Source Code)สำหรับระบบที่ให้บริการ	ระบบทำงานผิดพลาด/ละเมิดการเข้าถึงข้อมูล	3	2	6/ต่ำ	มีการกำหนดนโยบายในการกำหนดสิทธิและระดับในการเข้าถึงเฉพาะผู้ที่รับผิดชอบเท่านั้น
7.6	มีการควบคุมการติดตั้งโปรแกรมต่างๆ ในระบบปฏิบัติการที่ให้บริการ	เข้าถึงได้ง่าย	3	2	6/ต่ำ	สถานะปัจจุบัน :มีการกำหนดให้มีขั้นตอนการปฏิบัติที่ชัดเจนเพื่อควบคุมการติดตั้งโปรแกรมต่างๆ ในระบบ ปฏิบัติการที่ใช้
7.7	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/ทำให้ข้อมูลสำคัญเกิดการรั่วไหล	ขาดขั้นตอนปฏิบัติสำหรับการจัดการกับระบบสารสนเทศตามชั้นความลับที่กำหนดไว้	4	2	8/ต่ำ	มีการกำหนดนโยบายและแนวปฏิบัติให้ชัดเจนในการเข้าถึงข้อมูลสำคัญ แต่ยังไม่ได้ประกาศใช้

ตารางที่ 17 (ต่อ)

8.การจัดหา การบำรุงรักษาระบบสารสนเทศ (Information System Acquistion Development and Maintenance) A12						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.1	ข้อมูลรั่วไหลจากการนำข้อมูลออกจากองค์กรผ่านทางระบบของแอปพลิเคชัน	ต้องมีการกำหนด กลไกสำหรับตรวจสอบการนำข้อมูลออกจากระบบแอปพลิเคชันต่างๆ	5	2	10/กลาง	สถานะปัจจุบัน : ระบบมีการกำหนดสิทธิ์ในการนำข้อมูลออกจากแอปพลิเคชัน โดยประมวลผลตามสิทธิ์ของผู้ใช้ที่เข้ามาใช้งานระบบ
8.2	การจัดหาและการพัฒนา ระบบสารสนเทศ ที่ไม่มีประสิทธิภาพทำให้องค์กรได้มาซึ่งระบบที่ไม่มีความมั่นคงปลอดภัย	ไม่มีการวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ	3	2	6/ต่ำ	สถานะปัจจุบัน : จัดทำข้อกำหนดของระบบต่างๆตามความเข้าใจในการจัดหาหรือพัฒนาระบบสารสนเทศตามข้อเท็จจริงที่ได้รับ

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.3	ข้อมูลสำคัญถูกเข้าถึงจากผู้ไม่ได้รับอนุญาต	การเข้ารหัสข้อมูลที่สำคัญขององค์กร เช่น Web Application และ ข้อมูลในคอมพิวเตอร์	4	2	8/ต่ำ	สถานะปัจจุบัน : เริ่มมีการกำหนดสิทธิการเข้าถึงระบบ เช่น ระบบ Web Application ยังไม่มีการเข้ารหัส ส่วนที่เป็นคอมพิวเตอร์ของผู้บริหารนั้น
8.4	เกิดความผิดพลาด หรือ การสูญหายของข้อมูล	ระบบงานนำเข้าซึ่งข้อมูล และเกิดการประมวลผลที่ไม่ถูกต้อง	5	1	5/ต่ำ	มีการกำหนดเป็นนโยบายและมีการกำหนด การนำเข้าข้อมูลโดย Application ต่างๆ ที่เป็นโปรแกรมประยุกต์ และมีการตรวจสอบระบบฐานข้อมูล
8.5	ผู้ไม่ประสงค์ดีนำอาศัยช่องโหว่ของระบบปฏิบัติการโจมตีระบบให้เสียหาย	ขาดการอัพเดท Patch ของระบบ ปฏิบัติการอย่างมีประสิทธิภาพ เพื่ออุดช่องโหว่ของระบบ ปฏิบัติการ	5	2	10/กลาง	สถานะปัจจุบัน : มีการตรวจสอบช่องโหว่ของระบบปฏิบัติการ แต่ไม่มีระบบบริหารจัดการ Patch จากศูนย์กลาง(centralized patch management)

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
8.6	ใช้ซอฟท์แวร์ละเมิดลิขสิทธิ์และซอฟท์แวร์ที่ดาวโหลดมามีไวรัสทำให้ระบบเสียหาย	ขาดการควบคุมการติดตั้งซอฟท์แวร์ โดยพนักงานติดตั้งซอฟท์แวร์ได้เอง	3	1	3/ต่ำ	สถานะปัจจุบัน : ผู้ใช้ติดตั้งซอฟท์แวร์เอง ไม่ได้มีการควบคุมทางเทคนิคอย่างจริงจัง เช่น ผู้ใช้มีสิทธิ์เป็น Admin
8.7	ระบบเสียหายและแก้ไขกลับคืนได้ล่าช้า อันเนื่องมาจากการเปลี่ยนแปลงที่ไม่มีการควบคุมที่ดี	ขั้นตอนปฏิบัติสำหรับควบคุมเปลี่ยนแปลงหรือแก้ไขระบบทั้งHardwareและ Software เช่น การบันทึกการเปลี่ยนแปลง การทดสอบระบบ	5	3	15/กลาง	สถานะปัจจุบัน :มีแผนการจัดทำขั้นตอนปฏิบัติสำหรับควบคุมเปลี่ยนแปลงหรือแก้ไขระบบ ทั้ง Hardware และ Software ในรูปแบบเอกสาร

ตารางที่ 17 (ต่อ)

9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Incident Management)-A13						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
9.1	ระบบเสียหายกับเกิดเหตุการณ์เดิมๆ ที่เกิดขึ้นในด้านการละเมิดความมั่นคงปลอดภัย	ต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อเตรียมการป้องกันไว้ล่วงหน้า	5	2	10/กลาง	สถานะปัจจุบัน : มีการตรวจสอบการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยการเก็บ Log และมีระบบรายงาน (Report)
9.2	เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุฉุกเฉินไม่ได้รับการจัดการภายในระยะเวลาที่เหมาะสมซึ่งทำให้เหตุการณ์เกิดการลุกลามหรือบานปลาย เหตุการณ์ฉุกเฉินถูกละเลยโดยไม่มีการแจ้งเหตุเหล่านั้น	ขั้นตอนปฏิบัติสำหรับการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5	3	15/กลาง	สถานะปัจจุบัน : ยังไม่มีแผนสำรองฉุกเฉินในการจัดการระบบสารสนเทศได้ทันท่วงที

ตารางที่ 17 (ต่อ)

10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Bisiness Continuty Management) -A14						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
10.1	การกู้คืนธุรกิจสำคัญและระบบงานสนับสนุนไม่ได้รับการกู้คืนหรือสร้างความต่อเนื่องภายในระยะเวลาที่เหมาะสมภายหลังจากที่เกิดเหตุภัยพิบัติ	การระบุและจัดลำดับความสำคัญกระบวนการทางธุรกิจสำคัญกล่าวคือกระบวนการทางธุรกิจใดก่อนหลังที่ต้องได้รับการกู้คืนให้สำเร็จเรียงตามลำดับความสำคัญ	5	5	25/สูง	สถานะปัจจุบัน : มีการกำหนดระดับความสำคัญของระบบสารสนเทศแต่ละประเภทโดยแบ่งทั้งทาง Business Value และ IT Value
10.2	การขาดความชัดเจนในกระบวนการสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญและระบบงานสนับสนุน /การขาดแผนการสร้างความต่อเนื่องทางธุรกิจสำหรับกระบวนการทางธุรกิจสำคัญ	นโยบายและวัตถุประสงค์เพื่อสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญ	5	3	15/กลาง	สถานะปัจจุบัน : มีนโยบาย และ การปฏิบัติงานเพื่อสร้างความต่อเนื่องให้กับกระบวนการทางธุรกิจสำคัญ

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
10.3	กระบวนการทางธุรกิจสำคัญไม่สามารถกู้คืนได้สำเร็จภายในระยะเวลาที่เหมาะสม	ทางธุรกิจ (Business การจัดทำแผนสร้างความต่อเนื่อง ContinuityPlan - BCP) และ ปรับปรุงแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง	5	4	20/สูง	สถานะปัจจุบัน : มีแผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Plan BCP) แต่ขาดการทบทวนและปรับปรุงให้ทันสมัย
10.4	ผู้บริหารขาดข้อมูลเพื่อใช้ในการตัดสินใจว่าจำเป็นต้องมีการสร้างความต่อเนื่องให้แก่กระบวนการทางธุรกิจหนึ่งหรือไม่	ไม่มีการวิเคราะห์และจัดทำรายงานการประเมินผลกระทบที่มีต่อกระบวนการทางธุรกิจสำคัญ (Business Impact Analysis) ในกรณีที่เกิดภัยพิบัติและทำให้กระบวนการเหล่านี้เกิดการหยุดชะงักขาดความต่อเนื่องให้แก่ธุรกิจนั้น	5	4	20/สูง	สถานะปัจจุบัน : ยังไม่มีการวิเคราะห์และจัดทำรายงานการประเมินผลกระทบที่มีต่อกระบวนการทางธุรกิจสำคัญ (Business Impact Analysis) ในกรณีที่เกิดภัยพิบัติ กระบวนการทางธุรกิจสำคัญยังไม่มีแผนรองรับ

ตารางที่ 17 (ต่อ)

11.การปฏิบัติตามข้อกำหนด (Compliance) - A15						
วัตถุประสงค์						
ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
11.1	การใช้งานระบบไม่ตรงตามเงื่อนไขข้อกำหนดที่กำหนดไว้/ไม่ตรงตามวัตถุประสงค์	ขั้นตอนการขออนุมัติเพื่อใช้ระบบงานขององค์กร ขาดการระบุหรือกล่าวถึงลักษณะหรือประเภทของการใช้งานใดที่ถือว่าเหมาะสมและตรงกับความต้องการทางธุรกิจ	5	5	25/สูง	สถานะปัจจุบัน : ไม่มีขั้นตอนการขออนุมัติเพื่อใช้ระบบงานขององค์กร โดยต้องระบุจุดประสงค์และได้รับการอนุมัติจากหัวหน้างานก่อน จากนั้นเจ้าหน้าที่ ICT จะดำเนินการจัดหา ตามสิ่งที่ผู้ใช้ได้ขอใช้งานระบบ
11.2	เอกสารข้อมูลสำคัญบางประเภทไม่ได้รับการจัดเก็บไว้อย่างยาวนานเพียงพอและอาจมีการละเมิดกฎหมายที่กำหนดไว้	การกำหนดระยะเวลาสำหรับการจัดเก็บเอกสารข้อมูลแต่ละประเภทที่มีความสำคัญ	4	3	12/กลาง	สถานะปัจจุบัน : เริ่มมีการวางแผนงาน ในการกำหนดระยะเวลาสำหรับการจัดเก็บเอกสารข้อมูลที่สำคัญตามแต่ละประเภทของเอกสาร

ตารางที่ 17 (ต่อ)

ข้อ	ประเด็นความเสี่ยง/ช่องโหว่/จุดอ่อน	ปัจจัยเสี่ยง/ภัยคุกคาม	ผลกระทบ	โอกาส	ผล/ระดับความเสี่ยง	สถานะปัจจุบัน/ ข้อเสนอแนะ
11.3	ข้อมูลเอกสารที่สำคัญสูญหายหรือรั่วไหล	การจัดเก็บข้อมูลสำคัญรวมทั้งข้อมูลส่วนตัวที่ไม่มีประสิทธิภาพ	4	3	12	สถานะปัจจุบัน : มีการทำสำเนาเอกสารสำคัญที่ต้องใช้อ้างอิงและจัดเก็บเอกสารต้นฉบับไว้สถานที่ปลอดภัยภายนอกองค์กร ส่วนข้อมูลเอกสารที่จัดเก็บภายในองค์กรก็มีการแบ่งระดับสิทธิ์การเข้าถึงและจัดเก็บอย่างปลอดภัย

ภาคผนวก จ

ร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

- ร่าง -

ประกาศสำนักงานคณะกรรมการคุ้มครองผู้บริโภค
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการ ใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ เลขาธิการคณะกรรมการคุ้มครองผู้บริโภคโดยความเห็นชอบของคณะกรรมการธุรกรรม ทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานคณะกรรมการคุ้มครองผู้บริโภค เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค"

ข้อ ๒ ประกาศนี้ มีผลใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓ คำนิยาม ในประกาศนี้

"**หน่วยงาน**" หมายถึง สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

"**การรักษาความมั่นคงปลอดภัย**" หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของหน่วยงาน

"**ผู้ใช้งาน**" หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน รวมถึงบุคคลภายนอกที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้บริการหรือใช้งาน เครื่องคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน

"**ผู้ดูแลระบบ (System Administrator)**" หมายถึง ผู้ใช้งานที่ได้รับมอบหมายจากผู้บังคับ บัญชาให้มีหน้าที่รับผิดชอบดูแลรักษา บริหารจัดการระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศ

"**สิทธิ์ของผู้ใช้งาน**" หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษและสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"บัญชีผู้ใช้บริการ (Account)" หมายถึง รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ และบริการในระบบเครือข่ายของหน่วยงาน

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง(Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด(Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด(Unwanted or Unexpected)ซึ่งทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"หน่วยงาน" หมายถึง สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่สำนักงานคณะกรรมการคุ้มครองผู้บริโภคอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

"โปรแกรมประสงค์ร้าย (Malware)" หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"การพิสูจน์ยืนยันตัวตน (Authentication)" หมายถึง ขั้นตอนการรักษาความปลอดภัย ในการเข้าใช้งานระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน โดยทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน เข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย (Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (Local Area Network) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

"ระบบแลน (Local Area Network)" และ **"ระบบอินทราเน็ต (Intranet)"** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่าย ที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"ระบบอินเทอร์เน็ต (Internet)" หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

"ระบบสารสนเทศ (Information System)" ห มายถึง ร ะบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

"พื้นที่ใช้งานระบบสารสนเทศ" หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

๑. พื้นที่ทำงาน หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์ แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

๒. พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย หมายถึง ห้องปฏิบัติการสารสนเทศ (Information Operational Room) ที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศ ระบบเครือข่าย รวมถึงข้อมูลคอมพิวเตอร์ของหน่วยงาน ประกอบด้วย ห้องเซิร์ฟเวอร์ (Server Room) ห้อง NOC (Network Operating Center) และห้อง FAC (Facility)

๓. พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายถึง พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย (Wireless Lan) ครอบคลุมพื้นที่การให้บริการทั้งหน่วยงาน

"เจ้าของข้อมูล" หมายถึง หน่วยงานภายในเจ้าของข้อมูล ผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"จดหมายอิเล็กทรอนิกส์ (e-Mail)" หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้

ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารถึงผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP POP3 และ IMAP เป็นต้น

"ชุดคำสั่งไม่พึงประสงค์" หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

"เวลาอ้างอิงสากล (Stratum 0)" หมายถึง การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์ แม่ข่าย ที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้อง ในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ข้อ ๔ ขอบเขตของนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศของหน่วยงาน ทุกระดับชั้นตำแหน่ง

ข้อ ๕ ผู้รับผิดชอบ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chef Information Officer : CIO) ประจำสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน เป็นผู้รับผิดชอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ หน่วยงาน หรือผู้หนึ่งผู้ใด ไม่ว่ากรณีใด ๆ

ข้อ ๖ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๖.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๗ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค

๗.๒ กำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๗.๓ กำหนดให้การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ การเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ และการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น ให้สามารถให้บริการแก่ผู้ใช้งานและประชาชนได้อย่างทั่วถึง สะดวก รวดเร็ว รวมทั้งให้มีการคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๗.๔ กำหนดกฎเกณฑ์การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้เข้าถึงหรือควบคุมการใช้งานสารสนเทศ และกำกับดูแลการดำเนินงาน เพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๗.๕ ดำเนินการจัดทำระบบสารสนเทศและระบบสำรองข้อมูลของสารสนเทศ ให้ อยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการได้ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๗.๖ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๗.๗ ดำเนินการติดตาม ตรวจสอบการดำเนินงาน ทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง ให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยีในยุคปัจจุบัน พร้อมรองรับการเปลี่ยนแปลงในอนาคต

๗.๘ ดำเนินการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ ตลอดจนส่งเสริมให้มีการศึกษานโยบายด้านความปลอดภัยสารสนเทศอย่างต่อเนื่อง

๗.๙ จัดทำนโยบายเป็นลายลักษณ์อักษร โดยประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ให้บุคลากรทุกระดับในหน่วยงาน ผู้ใช้งานระบบและผู้ที่เกี่ยวข้องได้รับทราบและให้ถือปฏิบัติตามอย่างเคร่งครัด ผ่านทางเว็บไซต์สำนักงานคณะกรรมการคุ้มครองผู้บริโภค

๗.๑๐ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chef Information Officer : CIO) ประจำหน่วยงาน ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน เป็นผู้รับผิดชอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศ หน่วยงานหรือผู้หนึ่งผู้ใด ไม่ว่ากรณีใด ๆ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๘ แนวปฏิบัติการควบคุมการเข้าออกห้องปฏิบัติการสารสนเทศ (Information Operational Room)

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศของหน่วยงาน

๘.๑ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศ หรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๘.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้อนุญาตการกำหนดสิทธิ์ในการเข้าถึงการมอบอำนาจ การกำหนดมาตรการควบคุม รวมถึงการอนุญาตการเข้า-ออกห้องปฏิบัติการสารสนเทศ (Information Operational Room) และปฏิบัติหน้าที่ตามได้รับมอบหมาย ประกอบด้วย

(๑) จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิ์และหน้าที่ที่ได้รับมอบหมาย

(๒) จัดทำ “ทะเบียนบันทึกการเข้าออกพื้นที่” และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว

(๓) สิทธิ์ในการเข้าออกห้องปฏิบัติการสารสนเทศ ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

(๔) ผู้ติดต่อจากหน่วยงานภายนอกต้องขออนุญาตเข้าออกห้องปฏิบัติการสารสนเทศ และต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

(๕) ผู้ติดต่อจากหน่วยงานภายนอกที่ต้องการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อื่น ๆ มาใช้ในการปฏิบัติงานในห้องปฏิบัติการสารสนเทศ ต้องแจ้งรายการอุปกรณ์วัตถุประสงค์ การใช้งาน ประกอบการขออนุญาตเข้าออกห้องปฏิบัติการสารสนเทศให้ถูกต้องชัดเจนและต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๘.๓ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๙ แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ (Access Control)

เพื่อกำหนดมาตรการควบคุมการเข้าถึงสารสนเทศของหน่วยงาน ป้องกันการใช้งานจากผู้ไม่ประสงค์ดี ป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกหรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่สินทรัพย์สารสนเทศ ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของหน่วยงานได้อย่างถูกต้อง

๙.๑ แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศ ร่วมกับหน่วยงานภายในเจ้าของข้อมูล เจ้าของระบบงาน เป็นผู้อนุญาตการกำหนดสิทธิ์ในการเข้าถึง การกำหนดมาตรการควบคุมการเข้าถึงสารสนเทศและการเข้าใช้งานระบบสารสนเทศของหน่วยงาน เพื่อดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

(๑.๑) กำหนดเกณฑ์ในการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้เข้าถึงการใช้งานสารสนเทศ เช่น

- กำหนดผู้ใช้งานตามกลุ่มผู้ใช้งาน (กลุ่มผู้บริหาร/ ผู้อำนวยการ-หัวหน้างาน/ ผู้ปฏิบัติงาน/ ผู้ดูแลระบบ)
- กำหนดสิทธิ์ของผู้ใช้งานตามกลุ่มผู้ใช้งาน (อ่านอย่างเดียว/ เพิ่มข้อมูล/ แก้ไขข้อมูล/ ลบข้อมูล/ อนุมัติ)

(๑.๒) กำหนดเกณฑ์การระงับสิทธิ์และการมอบอำนาจ ในการยกเลิก เพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดจากการจ้าง เป็นต้น

(๒) ผู้ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องลงทะเบียนผู้ใช้งาน โดยกรอกแบบฟอร์มขอใช้บริการระบบสารสนเทศเสนอขออนุมัติผู้บังคับบัญชา และต้องได้รับอนุญาตอย่างเป็นทางการ

(๓) ผู้ดูแลระบบ (System Administrator) ต้องตรวจสอบและกำหนดสิทธิ์ การใช้งานระบบ การเข้าถึงข้อมูลและระบบสารสนเทศ ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนการเข้าใช้ระบบสารสนเทศ รวมทั้งมีการตรวจสอบ ทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ พร้อมบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

(๓.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

(๓.๒) ส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๓.๓) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ใน ที่เปิดเผย หรือไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้มีการป้องกันการเข้าถึง

(๔) ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งาน ระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศที่สำคัญ

(๕) ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

(๖) ผู้ดูแลระบบต้องกำหนดให้ระบบสามารถยุติการใช้งานระบบสารสนเทศนั้น โดยอัตโนมัติเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-Out) หากเป็นระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบให้เร็วขึ้นตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง กำหนดให้ใช้งานได้ เฉพาะในช่วงวัน-เวลาราชการเท่านั้น

๙.๒ แนวปฏิบัติการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) ผู้ดูแลระบบต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ดังนี้

- ประเภทของข้อมูล เช่น ข้อมูลด้านการบริหาร/การบริการ ข้อมูลภายในหน่วยงาน/ภายนอกหน่วยงาน
- ลำดับความสำคัญ เช่น ระดับความสำคัญมาก/ ปานกลาง
- ลำดับชั้นความลับ เช่น ข้อมูลลับที่สุด/ ลับมาก/ ลับ/ ทั่วไป
- ระดับชั้นการเข้าถึง เช่น สำหรับผู้บริหาร/ผู้ใช้งานทั่วไป
- เวลาที่ได้เข้าถึง เช่น วัน-เวลาราชการ/ นอกราชการ
- ช่องทางการเข้าถึง เช่น อินเทอร์เน็ต/ อินทราเน็ต

(๒) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ผู้ดูแลระบบ/เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) ผู้ดูแลระบบต้องกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๙.๓ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ เช่น การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องทำการสำรองและลบข้อมูลที่สำคัญออกก่อน เป็นต้น

๙.๔ ผู้ดูแลระบบ ผู้ใช้งาน ต้องรักษาความลับราชการ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๙.๕ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๐ แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงาน เข้าถึงระบบสารสนเทศและระบบเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวตนผู้ใช้งานระบบสารสนเทศหน่วยงาน

๑๐.๑ แนวปฏิบัติการลงทะเบียนผู้ใช้งาน (User Registration)

(๑) ผู้ดูแลระบบต้องจัดทำแบบฟอร์มการขอใช้บริการระบบสารสนเทศให้ผู้ใช้งานลงทะเบียนในแบบฟอร์มเสนอผู้บังคับบัญชา เพื่อขออนุมัติใช้บริการระบบสารสนเทศของหน่วยงาน ตามสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น

(๒) ผู้ดูแลระบบต้องกำหนดให้มีการแจ้งเวียนเอกสาร หรือสิ่งที่แสดงเป็นลายลักษณ์อักษร ให้แก่ผู้ใช้งานรับทราบสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบสารสนเทศของหน่วยงานและต้องปฏิบัติตามอย่างเคร่งครัด

(๓) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์/ทบทวนสิทธิ์ การเข้าถึงระบบสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออก เปลี่ยนตำแหน่งงาน โอน ย้าย ยกเลิกการใช้งาน

(๔) ผู้ดูแลระบบต้องทำการตรวจสอบ หรือทบทวนบัญชีการลงทะเบียนผู้ใช้งาน อย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

(๕) บุคลากรใหม่ของหน่วยงาน / ผู้ใช้งานที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องลงทะเบียนผู้ใช้งาน โดยกรอกแบบฟอร์มขอใช้บริการระบบสารสนเทศ เสนอขออนุมัติผู้บังคับบัญชาระดับผู้อำนวยการสำนัก/กอง/กลุ่ม หรือผู้ได้รับมอบหมาย เป็นลายลักษณ์อักษร เสนอสำนักแผนและการคุ้มครองผู้บริโภค ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและต้องได้รับอนุญาตอย่างเป็นทางการ

๑๐.๒ แนวปฏิบัติการบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

(๑) ผู้ดูแลระบบต้องตรวจสอบและกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่สำคัญ ให้เหมาะสมต่อหน้าที่รับผิดชอบ โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสมสำหรับระบบสารสนเทศ

(๓) ผู้ดูแลระบบต้องมอบหมายสิทธิ์ให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

(๕) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

๑๐.๓ แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารรับรหัสผ่าน สิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน

(๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่าน ที่มีความมั่นคงปลอดภัย

(๓) ผู้ดูแลระบบต้องกำหนดขั้นตอนการตั้งรหัสผ่าน (Password) และการเก็บข้อมูลในระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน ต้องไม่ปรากฏหรือแสดงรหัสผ่าน (Password) ออกมาโดยตรง โดยให้แสดงผลในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น ๆ เช่น ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร และการจัดเก็บข้อมูลส่วนบุคคลแทน

(๔) ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านเริ่มต้น (Default Password) หรือรหัสผ่านชั่วคราวที่ได้รับโดยทันที เมื่อทำการล๊อกอิน (Login) เข้าสู่การใช้งานในครั้งแรก และควรกำหนดรหัสผ่านใหม่ให้มีความยากแก่การคาดเดาโดยผู้อื่น (Strong Password)

(๕) ผู้ดูแลระบบต้องให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของหน่วยงานทุก ๖ – ๑๒ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๑๐.๔ แนวปฏิบัติการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

(๑) ผู้ดูแลระบบต้องทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน ๑ ครั้ง/ปี

(๒) ผู้ดูแลระบบต้องทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

(๓) ผู้ดูแลระบบต้องทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งาน ที่มีสิทธิ์ในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๑๐.๕ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๑ แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อควบคุม กำหนดมาตรการให้ผู้ใช้งานได้รับทราบถึงหน้าที่ความรับผิดชอบในการใช้งานคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน เพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) รวมทั้งทำความเข้าใจ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและ มีความพร้อมใช้งานอยู่เสมอ และเพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน ให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลการใช้งานของผู้ใช้งานให้เป็นไปตามนโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๑.๑ แนวปฏิบัติการใช้งานคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย

(๑) ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย โดยมีวัตถุประสงค์ ดังต่อไปนี้

(๑.๑) ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๑.๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๑.๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือแก่ประชาชน

(๑.๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๑.๕) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะ อันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๑.๖) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(๑.๗) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตามข้อ ๑.๑ ๑.๒ ๑.๓ ๑.๔ ๑.๕ หรือ ๑.๖

(๒) ผู้ใช้งานจะต้องไม่สนับสนุน หรือยินยอมให้มีการกระทำความผิดตาม ข้อ ๑. ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

(๓) ผู้ใช้งานจะต้องไม่กระทำการดังต่อไปนี้

(๓.๑) เข้าถึงโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

(๓.๒) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓.๓) เข้าถึงโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

(๓.๔) กระทำด้วยประการใดโดยมิชอบ ด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๓.๕) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๓.๖) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๓.๗) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-Mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น โดยปกติสุข

(๓.๘) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

(๓.๙) จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้ เป็นเครื่องมือในการกระทำความผิดตามข้อ ๓.๑) ๓.๒) ๓.๓) ๓.๔) ๓.๕) ๓.๖) ๓.๗) หรือ ๓.๘)

(๔) การใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายผู้ใช้งานต้องปฏิบัติดังต่อไปนี้

(๔.๑) ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุดแก่ทางราชการ

(๔.๒) ไม่คัดลอกโปรแกรมต่าง ๆ ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๔.๓) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยศูนย์เทคโนโลยีสารสนเทศเท่านั้น

(๔.๔) ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

(๔.๕) ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในหน่วยงาน

(๔.๖) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบ ข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๔.๗) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใด เพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน เพื่อให้บุคคลอื่น สามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๔.๘) ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

(๕) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงานร่วมกัน

(๖) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน และเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๗) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานระบบสารสนเทศและระบบเครือข่าย หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๘) ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุก เข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

(๙) ห้ามมิให้ผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลสารสนเทศที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของหน่วยงาน

(๑๐) ห้ามมิให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือ การแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้ บริการโฆษณาสินค้า หรือการเปิดให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

(๑๑) ผู้ใช้งานจะต้องไม่ละเมิดสิทธิ์ของผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหาย เสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น

(๑๒) ผู้ใช้งานต้องรักษาความลับราชการ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทาง

ราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๑.๒ แนวปฏิบัติการใช้งานบัญชีผู้ใช้บริการ (User Account)

(๑) ผู้ใช้งานต้องรับทราบสิทธิ์และหน้าที่ เกี่ยวกับการใช้งานระบบสารสนเทศ และต้องปฏิบัติตามอย่างเคร่งครัด

(๒) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (User Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ เครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๓) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

(๔) หน่วยงานให้บัญชีผู้ใช้บริการ (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานเจ้าของบัญชีผู้ใช้บริการ จะต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่ายหรือจ่ายแจกให้กับผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๑๑.๓ แนวปฏิบัติการใช้งานรหัสผ่าน (Password)

(๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเริ่มต้น (Default Password) หรือรหัสผ่านชั่วคราวที่ได้รับโดยทันที เมื่อทำการล๊อกอิน (Login) เข้าสู่การใช้งานในครั้งแรก และควรกำหนดรหัสผ่านใหม่ให้มีความยากแก่การคาดเดาโดยผู้อื่น (Strong Password)

(๒) ผู้ใช้งานต้องตั้งรหัสผ่าน (Password) ให้มีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจผสมระหว่างตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลขหรือตัวอักขระพิเศษ และสัญลักษณ์ต่าง ๆ ด้วย

(๓) ผู้ใช้งานไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อหรือนามสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ และไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในที่เปิดเผย หรือไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้มีการป้องกันการเข้าถึง

(๔) ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของหน่วยงานทุก ๖ – ๑๒ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ผู้ใช้งานจะต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศ โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๑๑.๔ แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

(๑) เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงาน ศูนย์เทคโนโลยีสารสนเทศได้ติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(๒) ผู้ใช้งานควรทำการอัพเดท (Update) ระบบปฏิบัติการและโปรแกรม การใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่อาจเกิดขึ้นจากซอฟต์แวร์ และเพื่อเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

(๓) ห้ามมิให้ผู้ใช้งานทำการปิด หรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๔) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ให้แจ้งศูนย์เทคโนโลยีสารสนเทศโดยทันที เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ และก่อนการรับ-ส่งข้อมูลคอมพิวเตอร์ ห รือข้อมูลสารสนเทศ (Information) ผ่านระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบข้อมูลโดยใช้โปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อน เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

(๖) ผู้ใช้งานต้องทำการตรวจสอบไฟล์ก่อนเปิดใช้งาน โดยใช้โปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) เพื่อป้องกันการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๑๑.๕ แนวปฏิบัติของผู้ดูแลระบบ (System Administrator)

(๑) ผู้ดูแลระบบ (System Administrator) มีหน้าที่ ดังต่อไปนี้

(๑.๑) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบรายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวทันที

(๑.๒) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์ สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

(๑.๓) ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่ายอย่างสม่ำเสมอ

(๑.๔) ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ขาย (Server) อย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงาน บนเครื่องคอมพิวเตอร์ เมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธีการตามมาตรฐาน DOD 5220.22-M

(๑.๕) ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งาน

(๑.๖) ดูแลรักษาและปรับปรุงบัญชีผู้ใช้บริการ (User Account) ระบบสารสนเทศและระบบเครือข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

(๑.๗) ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

(๑.๘) ดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน ๑ ครั้ง/ปี เป็น อย่างน้อย ทบทวนสิทธิสำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้บริหาร ผู้ดูแลระบบ และทบทวนสิทธิ์เมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การเลื่อนตำแหน่ง การโอน-ย้ายหน่วยงานหรือการสิ้นสุดการจ้างอย่างสม่ำเสมอ

(๑.๙) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน โดยไม่มีเหตุผลอันสมควร

(๑.๑๐) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์ หรือข้อมูลส่วนบุคคลของผู้ใช้งาน ที่ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(๑.๑๑) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

(๑.๑๒) ต้องรักษาความลับราชการ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑.๑๓) เมื่อผู้ดูแลระบบพ้นจากหน้าที่รับผิดชอบ จะต้องส่งมอบงานและ คืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันที โดยให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตรวจสอบการส่งมอบงานและการคืนทรัพย์สิน

(๒) ผู้ดูแลระบบ (System Administrator) จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ และเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ด้วยวิธีการที่มั่นคงปลอดภัย เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๑๑.๖ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๒ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเครือข่าย เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติงานหรือที่ไม่ได้รับอนุญาต กระทำการใด ๆ อันเป็นการเข้าถึง

ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายของหน่วยงาน ที่จะสร้างความเสียหายแก่ข้อมูลและระบบสารสนเทศของหน่วยงาน โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้บริการระบบเครือข่ายที่แตกต่างกัน รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๑๒.๑ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

(๑) ศูนย์เทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการเข้าถึงระบบเครือข่าย ผู้ใช้งานที่ต้องการใช้บริการระบบเครือข่ายของหน่วยงาน จะต้องได้รับอนุญาตจากผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศ และสามารถเข้าถึงระบบสารสนเทศตามสิทธิ์การเข้าถึงที่ได้รับอนุญาตเท่านั้น และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

(๒) ผู้ใช้งานที่ต้องการนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๓) การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

(๔) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๕) ผู้ดูแลระบบต้องบริหารการควบคุมการเข้าถึงระบบเครือข่าย และบริหารจัดการการเข้าถึงระบบเครือข่ายอย่างมีประสิทธิภาพ ดังต่อไปนี้

(๕.๑) ออกแบบระบบเครือข่าย โดยทำการแบ่งแยกเครือข่าย (Segregation In Networks) ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น Internal Zone External Zone Application Zone Database Zone DMZ Zone เป็นต้น เพื่อให้การบริหารจัดการ ควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

(๕.๒) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียด เกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์บนเครือข่ายต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๕.๓) กำหนดให้มีวิธีการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ระบุตามค่า IP Address และปฏิบัติตามวิธีการหรือกระบวนการที่สามารถ ระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้ ๑) มีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ ๒) มีการควบคุมการใช้งานอย่างเหมาะสม ๓) มีการจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(๕.๔) กำหนดให้มีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๕.๕) กำหนดให้มีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง ตามข้อ ๙ แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ (Access Control) โดยให้มีการตรวจสอบการเชื่อมต่อเข้าสู่ระบบเครือข่าย การจำกัดสิทธิ์ การเข้าถึงข้อมูลของผู้ใช้งาน เป็นต้น และต้องควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

(๕.๖) กำหนดให้มีการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง และการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๖) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบโดย

(๖.๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ตรวจสอบโปรโตคอล (Protocol) และพอร์ต (Port) ที่ใช้ ตรวจสอบแอพพลิเคชั่นที่ทำงานบนเครื่องเป้าหมาย

(๖.๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย โดยการปิดเซอร์วิส (Service) และพอร์ต (Port) ที่ไม่จำเป็น การใช้เครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

(๖.๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ให้มีการจำกัดการใช้งานเฉพาะเท่าที่จำเป็นและภายในระยะเวลาที่กำหนด

(๗) กำหนดให้มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) โดยต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๗.๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานหมายเลขเครือข่าย (IP Address)

(๗.๒) กำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๘) ระบบเครือข่ายทั้งหมดของหน่วยงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆรวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๙) ระบบเครือข่ายต้องมีการติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System : IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๑๐) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย รวมถึงการติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศหรือ ผู้ที่ได้รับอนุญาตเท่านั้น โดยต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและให้มีการจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๑) การเข้าสู่ระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์ และระบบสารสนเทศต้องมีการลงบันทึกเข้าใช้งาน (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

(๑๒) IP address ภายในของระบบงานเครือข่ายภายในของหน่วยงานจำเป็น ต้องมีการป้องกันมิให้บุคคลภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

(๑๓) ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังต่อไปนี้

(๑๓.๑) การเข้าสู่ระบบระยะไกล (Remote Access) ด้วยวิธีการใด ๆ ที่สามารถเข้าถึงข้อมูลหรือระบบเครือข่ายของหน่วยงาน ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและมีการควบคุมการเข้าถึงอย่างเข้มงวด และผู้ใช้งานต้องปฏิบัติตามนโยบายของหน่วยงานอย่างเคร่งครัด

(๑๓.๒) การทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็น ในการดำเนินงานต่อศูนย์เทคโนโลยีสารสนเทศและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศอย่างเป็นทางการ

(๑๓.๓) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๑๓.๔) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเครือข่ายจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดช่องทาง (Port) ทิ้งไว้โดยไม่จำเป็น ช่องทาง (Port) ดังกล่าว ต้องตัดการเชื่อมต่อเมื่อและจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

(๑๓.๕) การเชื่อมต่อระบบสารสนเทศ ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑๓.๖) การเข้าใช้งาน ผู้ใช้งานต้องทำการพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งก่อนใช้ระบบเครือข่าย เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเครือข่ายของหน่วยงาน

(๑๔) ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ตามแนวทางดังต่อไปนี้

(๑๔.๑) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูล ที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(๑๔.๒) ต้องกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๑๔.๓) ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้อย่างสม่ำเสมอ

(๑๔.๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๑๔.๕) จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ และเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ด้วยวิธีการที่มั่นคงปลอดภัย

๑๒.๒ แนวปฏิบัติการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๑) ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการบริหารและรับผิดชอบดูแลในจัดการระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(๒) กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software)

(๓) กำหนดให้มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

(๔) ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet FTP Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยต้องมีมาตรการเพิ่มเติมด้วย

(๕) ต้องดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server Mail Server Application Server ต่าง ๆ เป็นต้น

(๖) ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๑๒.๓ แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

(๑) ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

(๒) ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

(๓) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวของที่ได้รับมอบหมายเท่านั้น

๑๒.๔ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๑) แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน ระบบเครือข่ายไร้สาย (Wireless Lan สคบ. : BGC-Hotspot)

(๑.๑) ผู้ใช้งาน ที่เป็นบุคลากร สคบ. ที่ต้องการขอใช้บริการระบบเครือข่ายไร้สาย ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการ ตามแบบฟอร์มการขอใช้บริการระบบ Wireless Lan สคบ. เสนอผู้บังคับบัญชา และมีหนังสือถึงสำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค เพื่อศูนย์เทคโนโลยีสารสนเทศดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการ (User) และรหัสผ่าน (Password)

(๑.๒) ผู้ใช้งาน ประชาชนทั่วไป ที่ต้องการขอใช้บริการระบบเครือข่ายไร้สาย ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการ ตามแบบฟอร์มการขอใช้บริการระบบ Wireless Lan สคบ. เสนอเจ้าหน้าที่ประชาสัมพันธ์ สคบ. ณ ศูนย์รับเรื่องราวร้องทุกข์ ๑๑๖๖ ผ่านหัวหน้าศูนย์รับเรื่องราวร้องทุกข์ ๑๑๖๖ เพื่อสำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค ศูนย์เทคโนโลยีสารสนเทศ ดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการ (User) และรหัสผ่าน (Password)

(๑.๓) ผู้ใช้งานไม่ควรใช้บัญชีผู้ใช้บริการ (User) และรหัสผ่าน (Password) ของผู้อื่นเพื่อใช้งานระบบ ยกเว้นแต่จะได้รับความยินยอมจากเจ้าของบัญชีผู้ใช้บริการ และให้ถือว่าเจ้าของบัญชีผู้ใช้บริการระบบเครือข่ายไร้สายนั้น เป็นผู้รับผิดชอบต่อการใช้งานระบบ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๑.๔) หลังจากการใช้งานระบบเครือข่ายไร้สายเสร็จสิ้น ผู้ใช้งานต้องทำการออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันมิให้บุคคลอื่นเข้าใช้งานระบบ

(๑.๕) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) ของตน เป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

(๒) แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๒.๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบเครือข่ายไร้สาย กำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งาน โดยจะอนุญาตเฉพาะชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(๒.๒) ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบ และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่าย ไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบทันที

(๒.๓) ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอก ที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สาย

(๒.๔) ผู้ดูแลระบบต้องจัดทำทะเบียนบัญชีผู้ใช้บริการ และมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

๑๒.๕ แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

(๑) ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามมิให้ผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

(๒) ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับ ตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

(๓) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

(๔) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

(๕) การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่น ๆ

(๖) การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ หรือเป็นความลับของหน่วยงาน

(๗) การนำเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพา ของภายนอกหน่วยงาน มาทำการเชื่อมต่ออินเทอร์เน็ตภายในหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการ อุดช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์

(๘) การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต ผู้ใช้งานจะต้องทำการทดสอบไวรัส (Virus Scan) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

(๙) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

(๑๐) ผู้ใช้งานต้องรักษาความลับราชการ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๒.๖ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๓ แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อควบคุม กำหนดมาตรการให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ ร วมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อั นจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๑๓.๑ แนวปฏิบัติการการควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ดูแลระบบต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ของหน่วยงาน และกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งาน เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(๒) ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่าน (Password Management System) ให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีระบบ Active Directory (AD) และกำหนด AD Policy เพื่อตรวจสอบการตั้งรหัสผ่าน การกำหนดให้เปลี่ยนรหัสผ่านชั่วคราว การกำหนดให้รหัสผ่านหมดอายุ เป็นต้น

(๓) ผู้ดูแลระบบต้องกำหนดให้ระบบสามารถยุติการใช้งานระบบสารสนเทศนั้น โดยอัตโนมัติเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-Out) และต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น ตามข้อ ๙ แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ (Access Control)

(๔) ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ใหม่ ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ที่รับผิดชอบ และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดาโดยผู้อื่น (Strong Password)

(๕) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบใหม่

(๖) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๗) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๓.๒ แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

(๑) ผู้ใช้งานต้องมีชื่อในบัญชีผู้ใช้บริการ (Account) มีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่มีสิทธิ์เข้าใช้งานสารสนเทศของหน่วยงาน และทำการพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบสารสนเทศของ

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(๓) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์ระบบสารสนเทศและระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๔) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(๕) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๑๓.๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิด สามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อเป็นการป้องกันระบบสารสนเทศที่มีความสำคัญให้ดำเนินการดังนี้

(๑) จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์ในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์อย่างรัดกุม โดยกำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์บางครั้ง

(๒) กำหนดให้มีการถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ โดยให้จัดเก็บไว้ในสื่อภายนอก หากไม่มีการใช้งานเป็นประจำ

๑๓.๔ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๔ แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของหน่วยงาน ป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศของหน่วยงานให้หยุดชะงัก และสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของหน่วยงานได้อย่างถูกต้อง

๑๔.๑ แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งาน ให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่งงาน โอน ย้าย หรือขอยกเลิกการใช้งาน

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบสารสนเทศและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

(๓.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย ยกเลิกการใช้งานหรือสิ้นสุดจากการจ้าง

(๓.๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓.๓) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๓.๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในที่เปิดเผย หรือไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้มีการป้องกันการเข้าถึง

(๓.๕) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง

(๔) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๔.๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๔.๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานในแต่ละชั้นความลับของข้อมูล

(๔.๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔.๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption

(๔.๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๔.๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๔.๒ แนวปฏิบัติการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

(๑) แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน ระบบจดหมายอิเล็กทรอนิกส์สำนักงาน โดเมน : @ocpb.go.th (http://mail.ocpb.go.th/owa) และ ระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ โดเมน : @ocpb.mail.go.th (http://ocpb.mail.go.th)

(๑.๑) ผู้ใช้งานที่ต้องการขอใช้บริการระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการ ตามแบบฟอร์มการขอใช้บริการระบบสารสนเทศสำนักงานคณะกรรมการคุ้มครองผู้บริโภค เสนอผู้บังคับบัญชาให้ความเห็นชอบ และมีหนังสือถึงสำนักแผน และการพัฒนาการคุ้มครองผู้บริโภค ศูนย์เทคโนโลยีสารสนเทศ เพื่อขอให้ดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการ (User) และรหัสผ่าน (Password)

(๑.๒) ผู้ใช้งานที่ได้รับรหัสผ่านชั่วคราว (Default Password) ในการเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) เมื่อทำการเข้าสู่ระบบในครั้งแรก จะต้องทำการเปลี่ยนรหัสผ่าน (Password) ใหม่ โดยทันที

(๑.๓) ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของบัญชีผู้ใช้บริการ และให้ถือว่าเจ้าของบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-Mail) นั้น เป็นผู้รับผิดชอบต่อการใช้งานใด ๆ ในจดหมายอิเล็กทรอนิกส์ (e-Mail) ของตน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๑.๔) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-Mail)

(๑.๕) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อบัญชีผู้ใช้บริการ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

(๑.๖) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ โดยใช้โปรแกรมป้องกันไวรัสก่อนการเปิดทุกครั้ง เพื่อป้องกันการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น และต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของ

ตนเองเป็นประจำ ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ในระบบ

(๑.๗) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) เสร็จสิ้น ผู้ใช้งานต้องทำการออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันมิให้บุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) ของตน

(๒) แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๒.๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒.๒) ผู้ดูแลระบบต้องจัดทำทะเบียนบัญชีผู้ใช้บริการ และมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

(๓) ผู้ใช้งานต้องรักษาความลับราชการ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๔.๓ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องดำเนินการดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน ตรวจสอบและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ต่าง ๆ เช่น ระบบควบคุมอุณหภูมิ ระบบตรวจจับความชื้น ในห้องปฏิบัติการสารสนเทศ และปฏิบัติตาม**ข้อ ๘** แนวปฏิบัติการควบคุมการเข้าออกห้องปฏิบัติการสารสนเทศ (Information Operational Room)

(๒) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking) โดยผู้ใช้งานต้องขออนุมัติผู้บังคับบัญชาระดับผู้อำนวยการสำนัก/กอง/กลุ่ม หรือผู้ได้รับมอบหมาย เป็นลายลักษณ์อักษร เสนอสำนักแผนและการคุ้มครองผู้บริโภค ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องได้รับอนุญาตอย่างเป็นทางการ และมีการเพิ่มค่า Mac Address ของอุปกรณ์ในระบบควบคุมการใช้งาน

๑๔.๔ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยกำหนดให้มีการจัดเก็บ Mac Address พร้อมรายละเอียดผู้ใช้งาน กำหนดสิทธิ์การเข้าถึงสารสนเทศ ตรวจสอบการเข้าใช้งานและผู้บุกรุกที่พยายามเข้าใช้งานโดยไม่ได้รับอนุญาต และรายงานผู้บังคับบัญชาทราบ

๑๔.๕ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๕ แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศจากหน่วยงานภายนอก อันอาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบสารสนเทศโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศของหน่วยงานเป็นไปอย่างมั่นคงปลอดภัย

๑๕.๑ ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดให้มีการประเมินความเสี่ยง จากการเข้าถึงระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศได้

๑๕.๒ การควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายนอก รวมถึงการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(๑) หน่วยงานภายนอก/บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค จะต้องขออนุมัติผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(๒) ผู้ดูแลระบบต้องจัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงาน/บุคคลภายนอกทำการขออนุมัติการเข้าใช้งานระบบสารสนเทศ ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้ โดยมีรายละเอียดอย่างน้อยคือ เหตุผลในการขอใช้ ระยะเวลาในการใช้ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย และการกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๑๕.๓ หน่วยงานภายนอกที่ทำงานให้กับสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในสำนักงานคณะกรรมการคุ้มครองผู้บริโภคหรือนอกสถานที่ จำเป็น ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศของหน่วยงาน

๑๕.๔ สำนักงานคณะกรรมการคุ้มครองผู้บริโภคควรพิจารณาการเข้าไปประเมินความเสี่ยง หรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบสารสนเทศที่เข้าไปปฏิบัติงาน

๑๕.๕ เจ้าของโครงการ/เจ้าของระบบงาน/เจ้าของข้อมูล ซึ่งรับผิดชอบต่อโครงการ/ระบบงาน ที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๑๕.๖ สำหรับโครงการ/ระบบงานที่มีความสำคัญ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๑๕.๗ สำหรับโครงการ/ระบบงานซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ผู้ดูแลระบบต้องกำหนดให้มีการควบคุม

อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และกำหนดข้อปฏิบัติ แผนงานและขั้นตอนการปฏิบัติงานในการเข้าถึงระบบของหน่วยงานภายนอก

๑๕.๘ ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างครบถ้วน ถูกต้อง เป็นไปตามขอบเขตที่กำหนดไว้

๑๕.๙ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๖ แนวปฏิบัติการจัดทำระบบสำรองข้อมูล

เพื่อกำหนดมาตรการ ข้อปฏิบัติในการสำรองข้อมูลและการกู้คืนระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินหรือสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน เพื่อให้ผู้ดูแลระบบสามารถดำเนินการสำรองข้อมูลและการกู้คืนระบบได้อย่างถูกต้องภายในระยะเวลาที่เหมาะสม

๑๖.๑ แนวปฏิบัติการจัดทำระบบสำรองข้อมูลและการกู้คืนระบบ

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศ ร่วมกับหน่วยงานภายในเจ้าของข้อมูล เจ้าของระบบงาน พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม โดยจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง

(๒) ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดหน้าที่และความรับผิดชอบของ ผู้ดูแลระบบ (System Administrator) ให้มีผู้ดูแลระบบหลัก/ผู้ดูแลระบบสำรอง ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินให้ชัดเจน ให้ผู้ดูแลระบบสำรองปฏิบัติงานแทนกรณีที่ผู้ดูแลระบบหลักไม่สามารถปฏิบัติงานได้

(๓) ผู้ดูแลระบบต้องจัดทำการสำรองข้อมูลและซอฟต์แวร์ ของระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศที่สำคัญ และทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศที่สำคัญของหน่วยงาน

(๔) กำหนดให้มีขั้นตอนปฏิบัติการจัดทำการสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศ แต่ละระบบ

(๕) กำหนดให้มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการระบุชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่-เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

(๖) กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ข้อมูลที่จะทำการสำรอง เช่น Data Backup หรือ System Backup

(๗) กำหนดให้มีการเข้ารหัสในการสำรองข้อมูลที่สำคัญ (Encrypted Backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผยได้

(๘) ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ผู้ดูแลระบบรายงานข้อผิดพลาด (Fault logging) จากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๙) นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

(๑๐) ต้องมีการทดสอบและทบทวนสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๖.๒ การปฏิบัติเกี่ยวกับการสำรองข้อมูลและการกู้คืนระบบ

(๑) ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
- Web Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้งต่อสัปดาห์
- Database Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	๑ ครั้งต่อวัน
- Mail Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลในเมลบ็อกซ์	๑ ครั้งต่อสัปดาห์
- Firewall Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูล Rule ของ Firewall	๑ ครั้งต่อเดือน
- Server อื่น ๆ เช่น ระบบงานต่าง ๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลบนเซิร์ฟเวอร์อื่น ๆ	๑ ครั้งต่อเดือน

(๒) ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูล ว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้น ถูกต้อง ครบถ้วนสมบูรณ์หรือไม่

(๓) ผู้ดูแลระบบต้องทดสอบการกู้คืนระบบอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง และดำเนินการดังนี้

(๓.๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศ เป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการกู้คืนระบบ พร้อมบันทึกและรายงานสรุป ผลการปฏิบัติการกู้คืนระบบต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

(๓.๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อการกู้คืนระบบ

(๓.๓) หากความเสียหายที่เกิดขึ้นกับระบบสารสนเทศ กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้งานระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๑๖.๓ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) ในกรณีที่ ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง เพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมดให้ชัดเจน กำหนดช่องทางในการติดต่อกับผู้เกี่ยวข้อง และผู้ให้บริการภายนอก เช่น บริษัทผู้รับจ้างต่าง ๆ เมื่อเกิดเหตุจำเป็นที่ต้องการติดต่อ

(๒) ประเมินความเสี่ยงสำหรับระบบสารสนเทศที่มีผลกระทบและมีความสำคัญสูง พร้อมกำหนดมาตรการ กระบวนการในการวางแผนรับมือเพื่อลดความเสี่ยง

(๓) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล ขั้นตอนปฏิบัติในการกู้คืนระบบและทดสอบการกู้คืนระบบ

(๔) ทดสอบ ซ้อม ประเมินและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยให้มีการทบทวนแผนอย่างน้อยปีละ ๑ ครั้ง

(๕) เผยแพร่แผนเตรียมความพร้อมกรณีฉุกเฉินนี้ ให้บุคลากรที่เกี่ยวข้อง ได้รับทราบ และให้ถือปฏิบัติตามอย่างเคร่งครัด

๑๖.๔ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๗ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

เพื่อกำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยง เพื่อควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจนและสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๑๗.๑ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๓.๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศ เป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการกู้คืนระบบ พร้อมบันทึกและรายงานสรุป ผลการปฏิบัติการกู้คืนระบบต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

(๓.๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อการกู้คืนระบบ

(๓.๓) หากความเสียหายที่เกิดขึ้นกับระบบสารสนเทศ กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้งานระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๑๖.๓ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) ในกรณีที่ ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง เพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมดให้ชัดเจน กำหนดช่องทางในการติดต่อกับผู้เกี่ยวข้อง และผู้ให้บริการภายนอก เช่น บริษัทผู้รับจ้างต่าง ๆ เมื่อเกิดเหตุจำเป็นที่ต้องการติดต่อ

(๒) ประเมินความเสี่ยงสำหรับระบบสารสนเทศที่มีผลกระทบและมีความสำคัญสูง พร้อมกำหนดมาตรการ กระบวนการในการวางแผนรับมือเพื่อลดความเสี่ยง

(๓) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล ขั้นตอนปฏิบัติในการกู้คืนระบบและทดสอบการกู้คืนระบบ

(๔) ทดสอบ ซ้อม ประเมินและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยให้มีการทบทวนแผนอย่างน้อยปีละ ๑ ครั้ง

(๕) เผยแพร่แผนเตรียมความพร้อมกรณีฉุกเฉินนี้ ให้บุคลากรที่เกี่ยวข้อง ได้รับทราบ และให้ถือปฏิบัติตามอย่างเคร่งครัด

๑๖.๔ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๗ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

เพื่อกำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยง เพื่อควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจนและสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๑๗.๑ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๗.๒ ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน และจัดทำรายงานพร้อมข้อเสนอแนะ

๑๗.๓ ดำเนินการระบุความเสี่ยง เหตุการณ์ความเสี่ยงและผลกระทบของความเสี่ยง ให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ดังต่อไปนี้

(๑) ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์ แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

(๒) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน ไวรัสคอมพิวเตอร์ ระบบไฟฟ้าขัดข้อง

(๓) ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

(๔) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

(๕) ความเสี่ยงที่เกิดจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจสร้างความเสียหายแก่ระบบสารสนเทศของหน่วยงาน เช่น เหตุจารจล เหตุเพลิงไหม้ เหตุภัยพิบัติทางธรรมชาติ

๑๗.๔ ดำเนินการกำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น โดยคำนึงถึงองค์ประกอบดังต่อไปนี้

(๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๑๗.๕ ประเมินผลภาพรวมของความเสี่ยง และกำหนดให้มีเกณฑ์ในการพิจารณาว่าความเสี่ยงที่ระบุนั้น ต้องมีการบริหารจัดการลดความเสี่ยงนั้นหรือไม่

๑๗.๖ ทบทวนกระบวนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๗.๗ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย และผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบอิสระจากภายนอก (External Auditor) เป็นผู้รับผิดชอบ

ข้อ ๑๘ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงาน

เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้กับบุคลากรและผู้ที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการ

รักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๑๘.๑ ประชาสัมพันธ์แจ้งเวียนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้บุคลากรทุกระดับภายในหน่วยงานรับทราบ และให้ถือปฏิบัติโดยเคร่งครัด

๑๘.๒ ประชาสัมพันธ์แจ้งเวียนสร้างความตระหนัก ความรู้ความเข้าใจให้บุคลากรได้รับทราบ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๑๘.๓ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ข้อ ๑๙ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

๑๙.๑ ระบบป้องกันผู้บุกรุก

แผนดำเนินการรายวัน

(๑) ตรวจสอบไฟล์ล็อก (Log File) หรือรายงานของระบบป้องกันการบุกรุกสิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

(๑.๑) การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก

(๑.๒) ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

(๑.๓) ระดับความรุนแรงมากน้อยเพียงใด

(๑.๔) หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

(๒) ระบบไฟร์วอลล์ (Firewall)

(๒.๑) ตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒.๒) ตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ (Firewall) สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟล์วอลล์ (Firewall) ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๒.๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้รายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๑๙.๒ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ต หรือมัลแวร์ (Malware) ประกอบด้วย ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์ต่าง ๆ

แผนดำเนินการรายวัน / รายสัปดาห์ / รายเดือน

(๑) ตรวจสอบไฟล์ล็อก (Log File) และรายงานของอุปกรณ์ที่เกี่ยวข้องกับ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ควรตรวจสอบมีดังนี้

(๑.๑) มัลแวร์ (Malware) ประเภทใดถูกพบเป็นจำนวนมาก

(๑.๒) มัลแวร์ (Malware) ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

(๑.๓) มีการส่งมัลแวร์ (Malware) จากเครือข่ายภายในหน่วยงานไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (Malware) โดยเฉพาะมัลแวร์ (Malware) ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของหน่วยงาน

(๓) หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายใดติดมัลแวร์ (Malware) หรือส่งมัลแวร์ (Malware) ออกไปภายนอก ต้องระงับการเชื่อมต่อระบบเครือข่ายกับเครื่องคอมพิวเตอร์นั้น แล้วทำการแก้ไขเครื่องทันที

๑๙.๓ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ สำนักแผนและการพัฒนาการคุ้มครองผู้บริโภค และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ

ประกาศ ณ วันที่ มีนาคม พ.ศ. ๒๕๕๖

นายจิรชัย มูลทองโร่ย

(นายจิรชัย มูลทองโร่ย)
เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค

ประวัติผู้เขียน

ชื่อ-นามสกุล	สุพรรณี ชาติสุข
ประวัติการศึกษา	สำเร็จการศึกษาระดับปริญญาตรี คณะวิทยาศาสตร์ สาขาคณิตศาสตร์ มหาวิทยาลัยรามคำแหง ปีการศึกษา 2534
ตำแหน่งและสถานที่ทำงานปัจจุบัน	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค สำนักนายกรัฐมนตรี ที่อยู่ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา อาคารรัฐประศาสนภักดี(อาคารบี) ชั้น ๕ ถ.แจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
ประสบการณ์การทำงาน	ปี 25325-2536 เจ้าหน้าที่ระบบงานคอมพิวเตอร์ สำนักปลัดกระทรวงคมนาคม ปี 2537-2554 นักวิชาการคอมพิวเตอร์ 3- 7 สำนักงานประกันสังคม กระทรวงแรงงาน 1 มิถุนายน 2554 – ปัจจุบัน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค สำนักนายกรัฐมนตรี