การทำแผนความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1

Information System's Security Plan for Special Branch Division 1

โดย

ร้อยตำรวจโท อนุเทพ ชมพูธวัช

รหัส 44067292

อาจารย์ที่ปรึกษา

ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2545

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

การทำแผนความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1

Information System's Security Plan for Special Branch Division 1

โดย

ร้อยตำรวจโท อนุเทพ ชมพูธวัช

รหัส 44067292

อาจารย์ที่ปรึกษา

ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2545

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การทำแผนความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1
นักศึกษา	ร้อยตำรวจโท อนุเทพ ชมพูธวัช
อาจารย์ที่ปรึกษา	ดร.จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

กองตำรวจสันติบาล 1 เป็นหน่วยงานที่มีภารกิจในการปฏิบัติงานด้านการข่าวเกี่ยวกับความมั่นคงของประเทศ ซึ่งข้อมูลสารสนเทศถือเป็นทรัพยากรหลักที่สำคัญที่สุดในการปฏิบัติงาน การนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการปฏิบัติงานนั้น แม้ว่าจะช่วยให้การปฏิบัติงานเป็นไปด้วยความสะดวกรวดเร็ว และเพิ่มประสิทธิภาพการทำงานก็ตาม แต่ความปลอดภัยของระบบสารสนเทศนั้นเป็นสิ่งที่สำคัญอย่างยิ่ง ดังนั้น จึงจำเป็นต้องมีการศึกษาวิเคราะห์ถึงความปลอดภัยของระบบสารสนเทศ เพื่อกำหนดแนวทางและมาตรการต่างๆ ที่เหมาะสม ในการป้องกันระบบสารสนเทศให้มีความปลอดภัย โดยในโครงการศึกษากรณีพิเศษนี้ได้อิงมาตรฐาน ISO/IEC 17799:2000 ซึ่งเป็นมาตรฐานด้านการจัดการความปลอดภัยระบบสารสนเทศ เป็นแนวทางในการศึกษาวิเคราะห์และจัดทำแผนความปลอดภัยระบบสารสนเทศ

Title	Information System's Security Plan for Special Branch Division 1
Student	Police Lieutenant Anuthep Chomputawat
Advisor	Dr. Chanboon Sathitwiriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2002

ABSTRACT

The Special Branch Division 1 is responsible for performing intelligence about the national's security. Information is the most important resources for operations. Although using the Information and Communication Technology (ICT) to enhance operating efficiency, the security of information systems is vital. Thus security of information systems studying is essential to determine the appropriate policies, procedures and guidelines. This special study project is based on ISO/IEC 17799:2000 (International Standard of Information Security Management) for the analysis and implementation of information system's security plan.

กิตติกรรมประกาศ

โครงการศึกษากรณีพิเศษนี้ สำเร็จลุล่วงไปด้วยดี เนื่องจากได้รับการสนับสนุนด้านต่างๆ จากบุคคลหลายฝ่าย ผู้เขียนจึงใคร่ขอขอบพระคุณ บุคคลต่างๆ ดังต่อไปนี้

1. คุณพ่อ คุณแม่ ญาติ และน้องๆ ในครอบครัว ที่เป็นกำลังใจและให้การสนับสนุนช่วยเหลือในด้านต่างๆ เสมอมา
2. ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษา ที่กรุณาให้ข้อมูล คำปรึกษาและแนะนำแนวทางในการศึกษา
3. คณาจารย์ทุกท่าน ที่กรุณาให้ความรู้แขนงวิชาต่างๆ อันเป็นประโยชน์
4. พ.ต.ต.กษิดิศ เพิ่มพูนวิวัฒน์ ร.ต.ท.นันทวุฒิ รอดมณี คุณไชยยศ นันวณิชย์ คุณกนกพร แป้นสุข คุณธนาวุฒิ โบสีทธิพิเชฏฐ์ และคุณจรินทร์ทร โบสิทธิพิเชฏฐ์ ที่ให้คำแนะนำและช่วยเหลือด้านต่างๆ
5. เพื่อนๆ ITM 9.2 ทุกคน โดยเฉพาะ คุณสุชาติ จันทร์พงษ์ คุณเชิดชัย กัลยาวุฒิพงศ์ คุณรัชภูมิ พจนาวราพันธุ์ และคุณวีรพงศ์ หอมชื่น ที่ให้ความช่วยเหลือในด้านต่างๆ เสมอมา

ร้อยตำรวจโท อนุเทพ ชมพูธวัช

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญตาราง (ต่อ)

หน้า

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญตาราง (ต่อ)

สารบัญภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความเป็นมา

ในปัจจุบัน เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communications Technology หรือ ICT) เข้ามามีบทบาทสำคัญช่วยให้การปฏิบัติงานเกี่ยวกับข้อมูลสารสนเทศ เช่น การจัดเก็บ ค้นคืน ประมวลผล และการรับส่งข้อมูลสารสนเทศ เป็นไปด้วยความสะดวกรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น ทำให้หน่วยงานหรือองค์กรต่างๆ ทั้งภาครัฐและเอกชนมีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับระบบสารสนเทศอย่างกว้างขวาง

กองตำรวจสันติบาล 1 เป็นอีกหน่วยงานหนึ่งที่เล็งเห็นถึงความสำคัญและประโยชน์ดังกล่าวของเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีแนวความคิดที่จะพัฒนาระบบสารสนเทศจากเดิมที่มีการจัดเก็บข้อมูลในรูปแบบของเอกสาร และติดต่อสื่อสารด้วยระบบวิทยุ โทรศัพท์ โทรสาร ไปรษณีย์ และเจ้าหน้าที่นำสาร ซึ่งประสบกับปัญหาในการดูแลจัดเก็บเอกสาร การค้นคืนข้อมูลทำได้ล่าช้า ข้อมูลมีความซ้ำซ้อนและไม่ถูกต้องตรงกัน การรับส่งข้อมูลล่าช้า ไม่ชัดเจน และไม่ปลอดภัยเท่าที่ควร ให้เป็นระบบสารสนเทศที่มีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ อันจะช่วยแก้ไขปัญหาต่างๆ ดังกล่าวที่เกิดขึ้นได้

แต่เนื่องจากในปัจจุบัน มีภัยคุกคามที่ก่อความเสียหายต่อระบบสารสนเทศในรูปแบบของการทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ จำนวนมาก ข้อมูลสารสนเทศถือเป็นทรัพยากรหลักที่สำคัญที่สุดในการปฏิบัติงานของ กองตำรวจสันติบาล 1 ความปลอดภัยของข้อมูลและระบบสารสนเทศจึงเป็นสิ่งที่สำคัญอย่างยิ่ง ดังนั้นจึงจำเป็นต้องมีการศึกษาวิเคราะห์ถึงความปลอดภัยของข้อมูลและระบบสารสนเทศเพื่อกำหนดแนวทางมาตรการต่างๆ ที่เหมาะสมในการป้องกันข้อมูลและระบบสารสนเทศให้มีความปลอดภัย ซึ่งปัจจุบันมีมาตรฐานสากลด้านการจัดการความปลอดภัยระบบสารสนเทศ คือ มาตรฐาน ISO/IEC 17799:2000 โครงการศึกษากรณีพิเศษนี้จึงได้อิงมาตรฐานดังกล่าว เป็นแนวทางในการศึกษาวิเคราะห์และจัดทำแผนความปลอดภัยระบบสารสนเทศ

1.2 วัตถุประสงค์

เพื่อศึกษาวิเคราะห์ความเสี่ยง กำหนดความต้องการด้านความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 หากมีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการปฏิบัติงาน และกำหนดแนวทางมาตรการต่างๆ จัดทำแผนความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1โดยอิงมาตรฐาน ISO/IEC 17799:2000

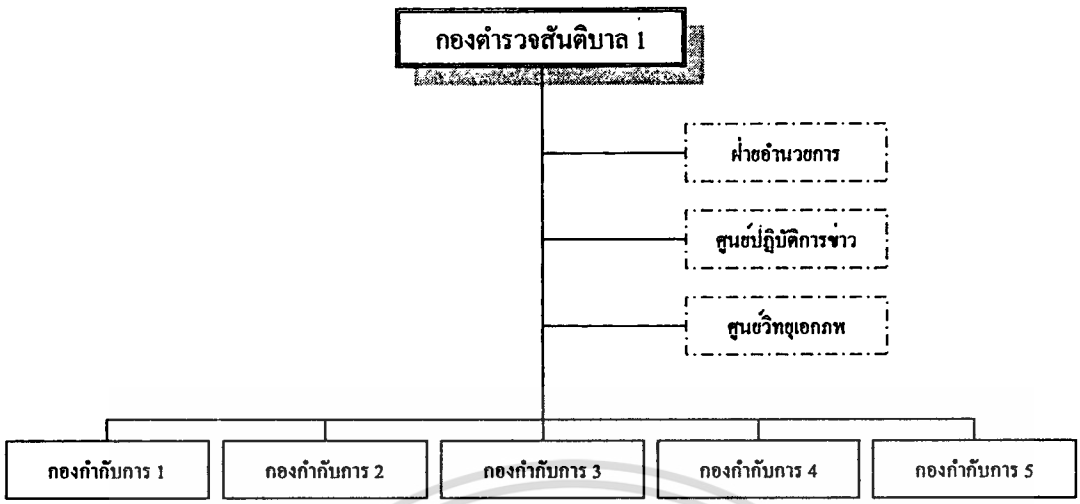
1.3 ขอบเขตการศึกษา

โครงการศึกษากรณีพิเศษนี้เป็นการศึกษาวิเคราะห์และจัดทำแผนความปลอดภัยระบบสารสนเทศ ของกองตำรวจสันติบาล 1 ที่มีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการปฏิบัติงาน โดยอิงมาตรฐาน ISO/IEC 17799:2000 ซึ่งเป็นมาตรฐานด้านการจัดการความปลอดภัยระบบสารสนเทศ แต่เนื่องจากระบบสารสนเทศในปัจจุบันของกองตำรวจสันติบาล 1 ยังไม่มีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้กับการปฏิบัติงาน ดังนั้นเพื่อความชัดเจนในการศึกษาวิเคราะห์ จึงจำเป็นต้องกำหนดขอบเขตของระบบสารสนเทศเบื้องต้นสำหรับการวิเคราะห์และจัดทำแผนความปลอดภัย ซึ่งมีรายละเอียดต่างๆ ดังนี้

1.3.1 ภารกิจและโครงสร้างของกองตำรวจสันติบาล 1

กองตำรวจสันติบาล 1 มีภารกิจปฏิบัติงานการข่าว เกี่ยวกับบุคคลหรือกลุ่มบุคคลซึ่งมิใช่ชาวต่างประเทศ ที่มีพฤติการณ์เป็นภัยต่อความมั่นคงของประเทศ รวมทั้งการสืบสวนสอบสวนเกี่ยวกับคดีความผิดดังกล่าว ดำเนินการเกี่ยวกับงานดำเนินกรรมวิธีข่าวกรอง ปฏิบัติงานร่วมหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย กองตำรวจสันติบาล 1 ประกอบด้วยส่วนต่างๆ ดังต่อไปนี้

- ฝ่ายอำนวยการ มีหน้าที่ปฏิบัติงานอำนวยการของ กองตำรวจสันติบาล 1
- ศูนย์ปฏิบัติการข่าว มีหน้าที่ปฏิบัติงานเป็นศูนย์กลางในการควบคุมสั่งการการปฏิบัติงาน และดำเนินกรรมวิธีข่าวกรอง ของ กองตำรวจสันติบาล 1
- ศูนย์วิทยุเอกภพ มีหน้าที่ปฏิบัติงานเป็นศูนย์กลางในการติดต่อสื่อสาร รวมถึงปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองตำรวจสันติบาล 1
- กองกำกับการ 1 มีหน้าที่ปฏิบัติงานการข่าวในเขตพื้นที่ภาคกลางและภาคตะวันออก
- กองกำกับการ 2 มีหน้าที่ปฏิบัติงานการข่าวในเขตพื้นที่ภาคตะวันออกเฉียงเหนือ
- กองกำกับการ 3 มีหน้าที่ปฏิบัติงานการข่าวในเขตพื้นที่ภาคเหนือ
- กองกำกับการ 4 มีหน้าที่ปฏิบัติงานการข่าวในเขตพื้นที่ภาคใต้
- กองกำกับการ 5 มีหน้าที่ปฏิบัติงานการข่าวในเขตพื้นที่จังหวัดกรุงเทพมหานคร

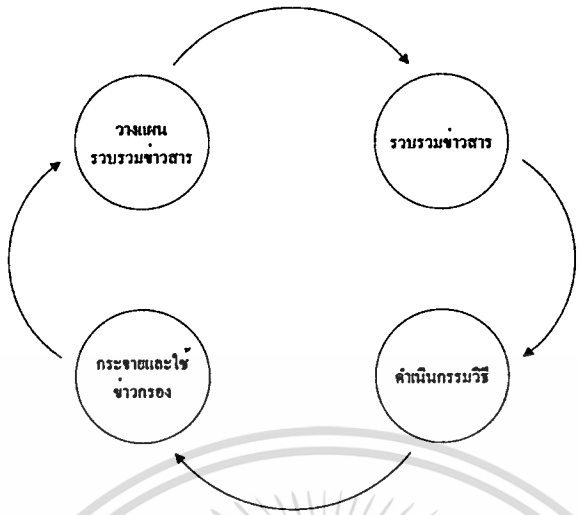


ภาพที่ 1.1 แสดงผังโครงสร้างของ กองตำรวจสันติบาล 1

1.3.2 การปฏิบัติงานการข่าวของ กองตำรวจสันติบาล 1

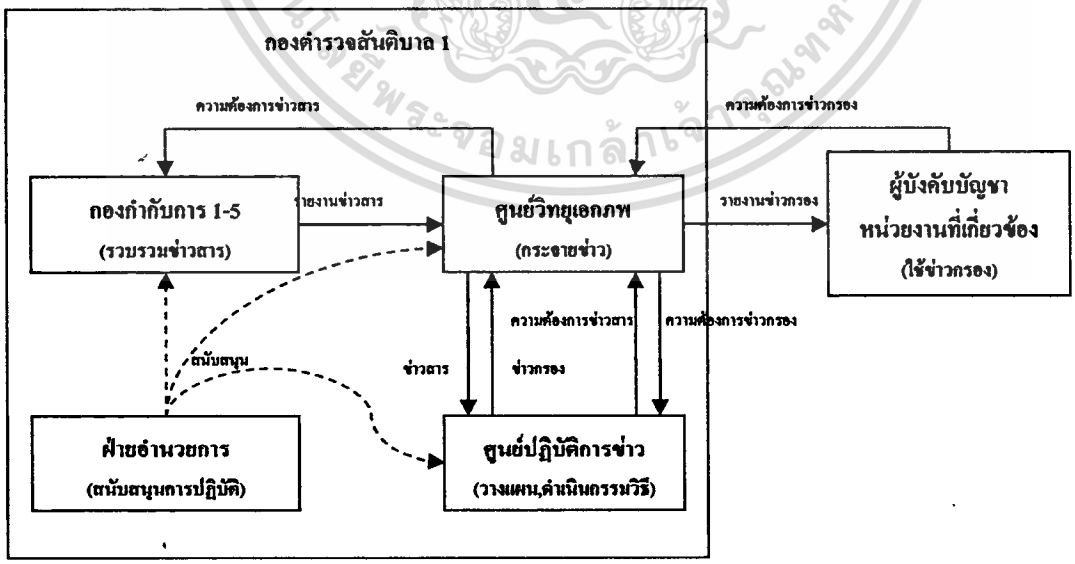
การปฏิบัติงานการข่าวของ กองตำรวจสันติบาล 1 เป็นการรวบรวมข่าวสารตามความต้องการข่าวกรองของผู้บังคับบัญชา ที่เกี่ยวกับบุคล กลุ่มบุคคล ที่มีพฤติการณ์เป็นภัยต่อความมั่นคงของประเทศ ซึ่งข้อมูลข่าวสารที่รวบรวมได้จะถูกนำไปประเมินค่า วิเคราะห์ สังเคราะห์ เพื่ออนุมานเป็นสมมติฐานข่าวกรอง ที่สามารถวินิจฉัยได้ว่าบุคคลหรือกลุ่มบุคคลที่ปรากฏในรายงานข่าวเป็นใคร รวมกลุ่มกันเพื่อกระทำผิดกฎหมายประการใดหรือไม่ หากเป็นเรื่องผิดกฎหมาย ใช้รูปแบบและวิธีการอย่างไร พฤติการณ์ตามพยานหลักฐานที่รวบรวมมาอยู่ในขั้นตอนใดของการกระทำความผิด เพื่อนำไปเป็นข้อมูลสารสนเทศในการวางแผนการปฏิบัติต่อบุคคลหรือกลุ่มบุคคลดังกล่าวต่อไป ซึ่งขั้นตอนการปฏิบัติดังกล่าวเป็นการดำเนินการต่อข่าวสารเพื่อให้เป็นข่าวกรอง มีวิธีการปฏิบัติที่เป็นลำดับและต่อเนื่องกันไปในลักษณะที่เป็นวงรอบ เรียกว่า วงรอบข่าวกรอง ประกอบด้วย 4 ขั้นตอน คือ

- การวางแผนรวบรวมข่าวสาร เป็นการกำหนดความต้องการข่าวกรองของผู้บังคับบัญชา
- การรวบรวมข่าวสาร เป็นการดำเนินการให้ได้มาซึ่งข่าวสารตามความต้องการที่กำหนดไว้ในขั้นของการวางแผน
- การดำเนินกรรมวิธี เป็นการดำเนินการเพื่อเปลี่ยนข่าวสารที่ได้ให้เป็นข่าวกรอง
- การใช้และกระจายข่าวสารและข่าวกรอง



ภาพที่ 1.2 แสดงวงรอบข่าวกรอง

การปฏิบัติงานการข่าวของ กองตำรวจสันติบาล 1 ตามวงรอบข่าวกรองนั้น สามารถแสดงความสัมพันธ์ระหว่างส่วนราชการต่างในสังกัด กองตำรวจสันติบาล 1 ได้ ดังภาพที่ 1.3



ภาพที่ 1.3 แสดงการปฏิบัติงานการข่าวของ กองตำรวจสันติบาล 1

1.3.3 ระบบสารสนเทศของ กองตำรวจสันติบาล 1

1.3.3.1 เป็นระบบสารสนเทศแบบ Client/Server Architecture

1.3.3.2 ระบบงาน

1.3.3.2.1 ระบบงานหลัก (Major Applications) ประกอบด้วย

- ระบบงานข่าว(Intelligence System) เป็นระบบสำรับดำเนินงานด้านการข่าว เป็นแบบ Web Application

1.3.3.2.2 ระบบงานสนับสนุน (Support Applications) ประกอบด้วย

- ระบบงานบริหาร (Management System) เป็นระบบสำหรับดำเนินงานบริหารต่างๆ เช่น กำลังพล บัญชี การเงิน พัสดุฯลฯ
- ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail System)
- ระบบประชาสัมพันธ์และข้อมูลเผยแพร่ (Public Relations System)

1.3.3.3 ระบบเครือข่าย

1.3.3.3.1 ระบบเครือข่าย Intranet

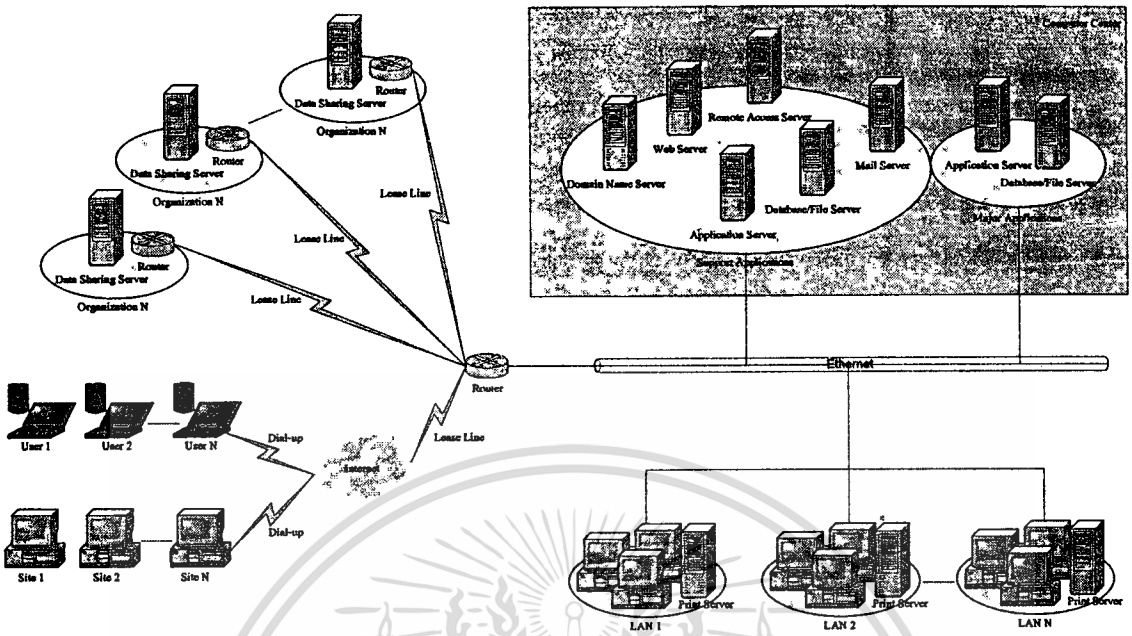
- Local Area Network (LAN) เชื่อมต่อเครื่องคอมพิวเตอร์ต่างๆ เป็นแบบ Ethernet
- Backbone Network (BN) เชื่อมต่อ LAN ต่างๆ ภายในอาคาร และระหว่างอาคารใกล้เคียง เป็นแบบ Ethernet
- Metropolitan Area Network (MAN) และ Wide Area Network (WAN) เชื่อมต่อหน่วยตำรวจสันติบาลในต่างจังหวัด และเจ้าหน้าที่ที่ปฏิบัติงานนอกสถานที่ เป็นแบบ Dial-up ผ่านเครือข่าย Internet

1.3.3.3.2 ระบบเครือข่าย Extranet

- เชื่อมต่อกับหน่วยงานต่างๆ ที่เกี่ยวข้องในการปฏิบัติงานเพื่อรับส่งหรือแลกเปลี่ยนข้อมูลข่าวสารต่างๆ แบบ Remote Access ผ่าน Lease Line

1.3.3.3.3 ระบบเครือข่าย Internet

- เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตผ่านผู้ให้บริการอินเทอร์เน็ต แบบ Remote Access ผ่าน Lease Line เพื่อใช้บริการต่างๆ จากเครือข่าย Internet ให้บริการข้อมูลเผยแพร่ประชาสัมพันธ์ และให้บริการเจ้าหน้าที่ที่ปฏิบัติงานนอกสถานที่สามารถเข้าสู่ระบบเครือข่าย Intranet ได้



ภาพที่ 1.4 แสดงระบบเครือข่าย กองตำรวจสันติบาล 1

1.3.4 ประเภทข้อมูลสารสนเทศ ของกองตำรวจสันติบาล 1

1.3.4.1 ข้อมูลการปฏิบัติงาน แบ่งข้อมูลข่าวสารออกตาม พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และ ระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ.2544 ได้ดังนี้

- ลับที่สุด (TOP SECRET) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ลับมาก (SECRET) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ลับ (CONFIDENTIAL) หมายความถึง ข้อมูลข่าวสารลับซึ่งหาเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลข่าวสารที่มิใช่ข้อมูลข่าวสารลับ

1.3.4.2 ข้อมูลประชาสัมพันธ์ภายในหน่วยงาน

1.3.4.3 ข้อมูลประชาสัมพันธ์ทั่วไป

1.4 ขั้นตอนการดำเนินงาน

โครงการศึกษากรณีพิเศษนี้เป็นการศึกษาวิเคราะห์ความเสี่ยง และกำหนดความต้องการด้านความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 หากมีการนำอาเทคโนโลยีสารสนเทศและการสื่อสาร มาประยุกต์ใช้กับการปฏิบัติงาน และกำหนดแนวทางมาตรการต่างๆ จัดทำแผนความปลอดภัยระบบสารสนเทศ โดยอิงมาตรฐาน ISO/IEC 17799:2000 ซึ่งมีขั้นตอนการดำเนินงาน เรียงตามเนื้อหา ดังนี้

บทที่ 1 กล่าวถึงความเป็นมา วัตถุประสงค์ ขอบเขตการศึกษา และขั้นตอนการดำเนินงาน และประโยชน์ที่คาดว่าจะได้รับจากของโครงการศึกษากรณีพิเศษ

บทที่ 2 กล่าวถึงทฤษฎีที่เกี่ยวข้องกับโครงการศึกษากรณีพิเศษ ได้แก่ ความปลอดภัยระบบสารสนเทศ การบริหารความเสี่ยง มาตรฐาน ISO/IEC 17799:2000 และเทคโนโลยีด้านความปลอดภัยระบบสารสนเทศ

บทที่ 3 เป็นการวิเคราะห์ความต้องการด้านความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 ซึ่งมีขั้นตอนตั้งแต่การกำหนดประเภทรายการทรัพย์สิน กำหนดเกณฑ์การประเมินความเสี่ยง แล้วจึงประเมินความเสี่ยง และกำหนดความต้องการด้านความปลอดภัย

บทที่ 4 เป็นการจัดการความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 โดยกำหนดแนวทางมาตรการต่างๆ จัดทำแผนความปลอดภัยระบบสารสนเทศอิงมาตรฐาน ISO/IEC 17799:2000

บทที่ 5 เป็นการสรุปผลที่ได้จากการศึกษา ปัญหาอุปสรรค และแนวทางการพัฒนาต่อไป

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ทราบถึงความเสี่ยงต่อความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 ที่อาจประสบกับภัยคุกคามอันก่อให้เกิดความเสียหายต่อระบบสารสนเทศในรูปแบบต่างๆ

1.5.2 ทราบถึงความต้องการด้านความปลอดภัยระบบสารสนเทศของกองตำรวจสันติบาล 1

1.5.3 กองตำรวจสันติบาล 1 มีแนวทางมาตรการต่างๆ หรือแผนความปลอดภัยระบบสารสนเทศ ในการดำเนินการต่างๆให้เกิดความปลอดภัยของข้อมูลและระบบสารสนเทศ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 ความปลอดภัยระบบสารสนเทศ

2.1.1 ความปลอดภัยระบบสารสนเทศ

ความปลอดภัยระบบสารสนเทศ คือ การป้องกันระบบสารสนเทศให้สามารถบรรลุวัตถุประสงค์ที่สามารถปฏิบัติจริงได้ในการรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) ของทรัพยากรต่างๆ ในระบบสารสนเทศ (Pfleeger. 1997)

- ความลับ (Confidentiality) คือ การทำให้ข้อมูลสารสนเทศสามารถถูกเข้าถึงได้เฉพาะผู้มีสิทธิหรืออำนาจโดยชอบเท่านั้น
- บูรณภาพ (Integrity) คือ การรักษาป้องกันให้ระบบสารสนเทศสามารถทำงานได้อย่างถูกต้องสมบูรณ์
- สภาพพร้อมใช้งาน (Availability) คือ การทำให้ผู้มีสิทธิสามารถเข้าถึงระบบสารสนเทศได้เมื่อต้องการ

2.1.2 ภัยคุกคามต่อความปลอดภัยระบบสารสนเทศ

ภัยคุกคามต่อความปลอดภัยในระบบสารสนเทศ คือเหตุการณ์หรือกรณีที่มีโอกาสก่อความเสียหายต่อระบบสารสนเทศในรูปแบบ การทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ (Pfleeger. 1997)

ภัยคุกคามสามารถแบ่งออกได้ตามลักษณะที่เกิดขึ้นกับระบบ เป็น 4 ประเภท คือ

2.1.2.1 Interruption (การขัดจังหวะ) หมายถึงสถานการณ์ที่ทรัพย์สินของระบบเกิดการสูญหาย ไม่อยู่ในสภาพพร้อมใช้งาน หรือไม่เสถียร สถานการณ์ดังกล่าวเรียกว่าการโจมตีสภาพพร้อมใช้งาน (availability attack) ทำให้ระบบขาดสภาพพร้อมใช้งานบางส่วนหรือทั้งหมด

2.1.2.2 Interception (การยึดครอง) หมายถึง การกระทำโดยที่บุคคลที่ไม่มีสิทธิอำนาจเข้าถึงทรัพย์สินในระบบ เพื่อต้องการสำเนาโปรแกรม หรือแฟ้มข้อมูลอย่างผิดกฎหมาย ดักจับข้อมูลจากเครือข่าย เป็นต้น สถานการณ์แบบนี้เรียกว่า การโจมตีความลับ (confidentiality attack)

2.1.2.3 Modification (การดัดแปร) หมายถึง การกระทำโดยที่บุคคลที่ไม่มีสิทธิอำนาจเข้าถึงทรัพย์สินในระบบ เพื่อต้องการเปลี่ยนแปลงแก้ไขสิ่งต่อไปนี้ เช่น การเปลี่ยนแปลงค่าต่างๆ ในฐานข้อมูล การดัดแปลงโปรแกรม การเปลี่ยนแปลงข้อมูลที่กำลังส่งผ่านตัวกลางสื่อสาร และการดัดแปลงฮาร์ดแวร์ เป็นต้น สถานการณ์แบบนี้เรียกว่า การโจมตีบูรณ-ภาพ (Integrity attack)

2.1.2.4 Fabrication (การปลอมแต่ง) หมายถึง การสร้างหรือประดิษฐ์วัตถุแปลกปลอมขึ้นมาในระบบคอมพิวเตอร์เพื่อจุดประสงค์ในการหลอกลวง เช่น การเพิ่มทรานแซคชั่นปลอมในเครือข่ายสื่อสาร การเพิ่มเรคคอร์ดปลอมในฐานข้อมูลเดิม เป็นต้น ซึ่งสามารถป้องกันได้ด้วยการพิสูจน์ตัวจริงหรือหลักในการระบุตัวบุคคล (Authentication) สถาน-การณ์แบบนี้เรียกว่า การโจมตีการพิสูจน์ตัวจริง (authenticity attack)

2.1.3 ความบกพร่อง (Vulnerability)

ความบกพร่อง คือ จุดอ่อนหรือจุดบกพร่องในระบบสารสนเทศ ที่อาจถูกภัยคุกคามต่างๆ ก่อความเสียหายต่อระบบสารสนเทศ (ทศพล กนกนุวัตร์. 2542)

ความบกพร่องดังกล่าว สามารถแบ่งออกได้เป็น 6 ประเภท คือ

2.1.3.1 ความบกพร่องจากมนุษย์ (Human Vulnerabilities) เป็นความบกพร่องที่เกิดจากการกระทำของมนุษย์ ทั้งที่เกิดจากความตั้งใจและความไม่ตั้งใจ

2.1.3.2 ความบกพร่องจากสภาพทางกายภาพ (Physical Vulnerabilities) เป็นความบกพร่องที่เกิดจากสภาพหรือลักษณะทางกายภาพ

2.1.3.3 ความบกพร่องจากฮาร์ดแวร์ (Hardware Vulnerabilities) เป็นความบกพร่องที่เกิดจากการทำงานของฮาร์ดแวร์

2.1.3.4 ความบกพร่องจากซอฟต์แวร์ (Software Vulnerabilities) เป็นความบกพร่องที่เกิดจากการทำงานของซอฟต์แวร์

2.1.3.5 ความบกพร่องจากการติดต่อสื่อสาร (Communication Vulnerabilities) เป็นความบกพร่องที่เกิดขึ้นจากการติดต่อสื่อสารต่างๆ

2.1.3.6 ความบกพร่องจากเหตุการณ์ธรรมชาติ (Natural Incident Vulnerabilities) เป็นความบกพร่องที่เกิดขึ้นจากเหตุการณ์ธรรมชาติ

2.1.4 การควบคุมความปลอดภัย

การควบคุมความปลอดภัย เป็นการดำเนินการใดๆ เพื่อป้องกันมิให้เกิดภัยคุกคามต่อความปลอดภัย การควบคุมความปลอดภัยแบ่งออกเป็น 3 ระดับ คือ

- การควบคุมการจัดการ เป็นนโยบาย มาตรการต่างๆ ของผู้บริหารในการจัดการความเสี่ยงและความปลอดภัยในระบบสารสนเทศขององค์กร
- การควบคุมการปฏิบัติการ เป็นมาตรการความปลอดภัยที่เน้นในเรื่องการควบคุม/สั่งการโดยบุคคล เพื่อเพิ่มความปลอดภัยของระบบสารสนเทศ
- การควบคุมทางเทคนิค เป็นการควบคุมความปลอดภัยในขณะที่เครื่องคอมพิวเตอร์กำลังทำงาน

2.1.5 เป้าหมายการรักษาความปลอดภัย

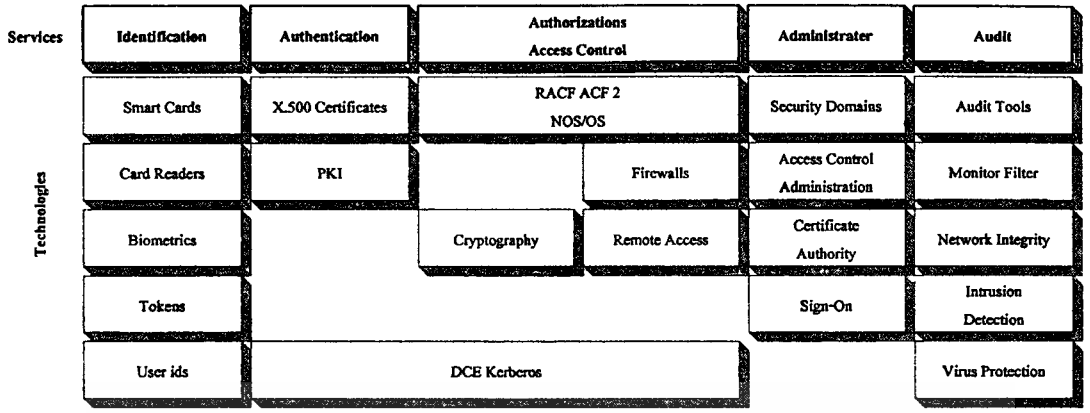
บริการทางด้านความปลอดภัย (Security service) ทั้งหลายทั้งปวง เกิดขึ้นมา เพื่อจุดมุ่งหมายดังต่อไปนี้

- ความลับ (Confidentiality)
- บูรณภาพ (Integrity)
- สภาพพร้อมใช้งาน (Availability)
- การพิสูจน์ตัวจริง (Authentication)
- ความไม่สามารถปฏิเสธความรับผิด (Non-Repudiation)
- การควบคุมการเข้าถึง (Access control)

2.1.6 ภาพรวมระบบรักษาความปลอดภัยระบบสารสนเทศ

บริการทางด้านความปลอดภัย (Security services) ที่พึงมีในการปกป้องความปลอดภัยระบบสารสนเทศ มีดังนี้

- การระบุตัว (Identification)
- การพิสูจน์ตัวจริง (Authentication)
- การควบคุมการเข้าถึง(Access control)
- การจัดการบริหาร (Administration)
- การตรวจสอบ (Audit)



ภาพที่ 2.1แสดงความสัมพันธ์ระหว่างบริการทางด้านความปลอดภัยและเทคโนโลยี

2.1.7 การวางแผนความปลอดภัยระบบสารสนเทศ

การวางแผนความปลอดภัยระบบสารสนเทศ เป็นการกำหนดแนวทางการดำเนินการเพื่อรักษาความปลอดภัยระบบสารสนเทศ แบ่งออกเป็น 5 ระยะ ดังนี้

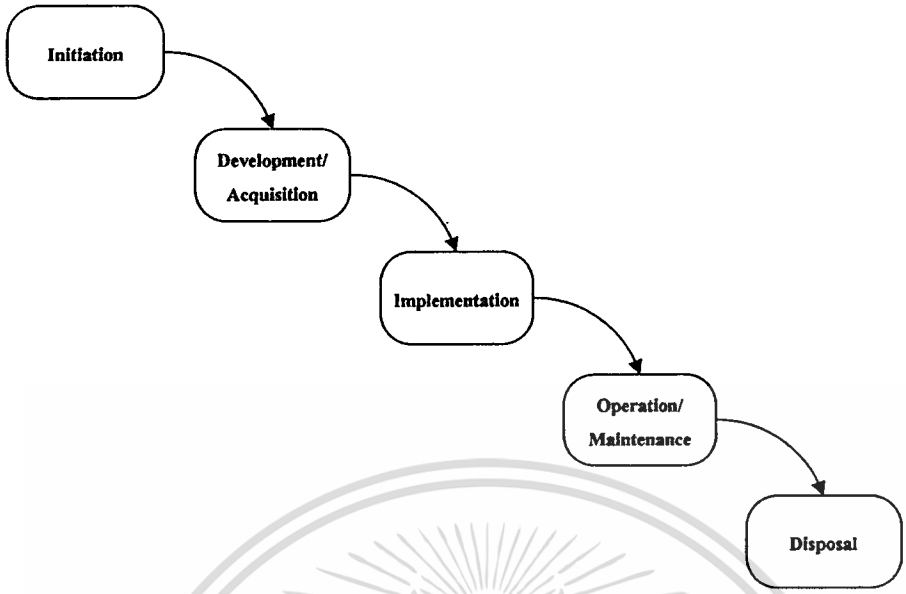
2.1.7.1 ระยะเริ่มต้น (Initiation Phase) เป็นขั้นตอนแรกของการวางแผน โดยเก็บรวบรวมข้อมูลต่างๆ เพื่อศึกษาองค์กร วิเคราะห์ความสำคัญของข้อมูล และความเสี่ยงต่างๆ ที่อาจเกิดขึ้นต่อข้อมูลและระบบสารสนเทศ

2.1.7.2 ระยะพัฒนาและจัดทำ (Development/Acquisition Phase) เป็นการนำข้อมูลที่ได้จากขั้นตอนแรกมาจัดทำแผน โดยกำหนดความต้องการทางด้านความปลอดภัย และกำหนดขอบเขต เป้าหมาย และแนวทางหรือมาตรการต่างๆ เพื่อใช้ในการรักษาความปลอดภัย

2.1.7.3 ระยะนำไปใช้ (Implementation Phase) เป็นการนำมาตรการต่างๆ ที่ได้กำหนดไว้ในแผนมาดำเนินการปรับเปลี่ยนให้เป็นไปตามมาตรการที่กำหนดในแผน

2.1.7.4 ระยะปฏิบัติการและบำรุงรักษา (Operation/ Maintenance Phase) เป็นการนำเอามาตรการต่างๆ ที่ได้กำหนดไว้ในแผนมาใช้ในการควบคุม ตรวจสอบความปลอดภัยขณะที่ระบบกำลังทำงาน

2.1.7.5 ระยะการกำจัด (Disposal Phase) เป็นการจัดการกับข้อมูล ฮาร์ดแวร์ และซอฟต์แวร์ ที่ไม่ได้ใช้ในการปฏิบัติงานหรือเลิกใช้งานแล้ว เช่น การเก็บรักษา การทิ้ง และการทำลาย



ภาพที่ 2.2 แสดงขั้นตอนการวางแผนความปลอดภัย

2.2 การบริหารความเสี่ยง

2.2.1 ความเสี่ยงต่อความปลอดภัยระบบสารสนเทศ (Risk)

ความเสี่ยงต่อความปลอดภัยระบบสารสนเทศ หมายถึง โอกาสที่ระบบสารสนเทศอาจจะประสบกับภัยคุกคามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศในรูปแบบการทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ

2.2.2 การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง คือ กระบวนการในการกำหนด การควบคุม ลดหรือบรรเทาความเสี่ยงต่อความปลอดภัยระบบสารสนเทศ ซึ่งสามารถกระทำได้หลายแนวทางดังนี้

- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือการยุติการดำเนินการหรือการกระทำบางอย่างที่มีความเสี่ยงสูง
- การผ่องถ่ายความเสี่ยง (Risk Transfer) คือการที่มอบหมายให้บุคคล หรือองค์กรอื่นมาทำหน้าที่ที่มีความเสี่ยงแทน
- การลดความเสี่ยง (Risk Reduction) คือการการดำเนินการหรือกระทำบางอย่างเพื่อลดความเสี่ยง
- การยอมรับความเสี่ยง (Risk Acceptance) คือการยอมให้ความเสี่ยงเกิดขึ้นได้

2.2.3 ขั้นตอนการบริหารความเสี่ยง

2.2.3.1 กำหนดรายการทรัพย์สิน

2.2.3.2 วิเคราะห์ความบกพร่อง

2.2.3.3 วิเคราะห์ภัยคุกคาม

2.2.3.4 วิเคราะห์โอกาสเกิดภัยคุกคาม

2.2.3.5 ประเมินความเสี่ยง

2.2.3.6 กำหนดการควบคุม ลดหรือบรรเทาความเสี่ยง

2.3 มาตรฐาน ISO/IEC 17799:2000

2.3.1 มาตรฐาน ISO/IEC 17799:2000 เป็นมาตรฐานด้าน Information Technology ที่ออกโดย ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) ในการจัดการด้านความปลอดภัยของระบบสารสนเทศ

2.3.2 ISO/IEC 17799:2000 ได้กำหนดแนวทางในการจัดการด้านความปลอดภัย ดังต่อไปนี้

2.3.2.1 นโยบายความปลอดภัย

- นโยบายความปลอดภัยระบบสารสนเทศ มีวัตถุประสงค์เพื่อ กำหนดแนวทางในการรักษาความปลอดภัยของระบบสารสนเทศ

2.3.2.2 ความปลอดภัยองค์กร

- โครงสร้างองค์กรด้านความปลอดภัยระบบสารนเทศ มีวัตถุประสงค์เพื่อจัดการความปลอดภัยระบบสารสนเทศในองค์กร
- ความปลอดภัยของการเข้าถึงจากบุคคลภายนอก มีวัตถุประสงค์เพื่อ คงไว้ซึ่งความปลอดภัยของระบบสารสนเทศในการดำเนินการหรือเข้าถึงทรัพยากรสารสนเทศจากบุคคลภายนอก
- การจ้าง มีวัตถุประสงค์เพื่อ คงไว้ซึ่งความปลอดภัยระบบสารสนเทศจากการจ้างองค์กรภายนอกมาดำเนินการเกี่ยวกับระบบสารสนเทศ

2.3.2.3 การแบ่งแยกประเภททรัพย์สินและการควบคุม

- บัญชีรายการทรัพย์สิน มีวัตถุประสงค์เพื่อ คงไว้ซึ่งการปกป้องทรัพย์สินระบบสารสนเทศขององค์กร
- การจัดหมวดหมู่ข้อมูลสารสนเทศ มีวัตถุประสงค์เพื่อ ทำให้ข้อมูลสารสนเทศได้รับการปกป้องในระดับที่เหมาะสม

2.3.2.4 ความปลอดภัยเกี่ยวกับบุคคล

- ความปลอดภัยในตำแหน่งหน้าที่ และการทำงาน มีวัตถุประสงค์เพื่อ ลดความเสี่ยงที่เกิดจากความผิดพลาดของมนุษย์ หรือกระทำความผิด
- การอบรม มีวัตถุประสงค์เพื่อ ทำให้ผู้ใช้ทราบพึงระลึกถึงภัยคุกคามต่อระบบสารสนเทศ และปฏิบัติตามนโยบายความปลอดภัยขององค์กร
- การปฏิบัติเมื่อเกิดเหตุการณ์ต่อความปลอดภัย มีวัตถุประสงค์เพื่อ ตรวจสอบเรียนรู้ และลดความเสียหายจากเหตุการณ์ต่อความปลอดภัย

2.3.2.5 ความปลอดภัยทางกายภาพและสภาพแวดล้อม

- พื้นที่ปลอดภัย มีวัตถุประสงค์เพื่อ ป้องกันผู้ที่ไม่มีสิทธิเข้ามาทำลายหรือก่อความเสียหายต่อสถานที่และระบบสารสนเทศ
- อุปกรณ์ความปลอดภัย มีวัตถุประสงค์เพื่อ ป้องกันความเสียหาย อันตรายที่มีต่อทรัพย์สิน และการดำเนินงานขององค์กร
- การควบคุมทั่วไป มีวัตถุประสงค์เพื่อ ป้องกันความเสียหายของระบบสารสนเทศ

2.3.2.6 การติดต่อสื่อสารและการบริหารจัดการ

- การปฏิบัติงานและความรับผิดชอบ มีวัตถุประสงค์เพื่อ ตรวจสอบแก้ไข และปฏิบัติงานด้านความปลอดภัยของระบบสารสนเทศ
- การวางแผนและการรับระบบ มีวัตถุประสงค์เพื่อ ลดความเสี่ยงของความล้มเหลวของระบบ
- การป้องกันซอฟต์แวร์ประสงค์ร้าย มีวัตถุประสงค์เพื่อ ปกป้องบูรณภาพของซอฟต์แวร์และข้อมูลสารสนเทศ
- การดูแลรักษา มีวัตถุประสงค์เพื่อ คงไว้ซึ่งบูรณภาพ และสภาพพร้อมใช้งานของระบบสารสนเทศ และการติดต่อสื่อสาร
- การบริหารจัดการเครือข่าย มีวัตถุประสงค์เพื่อ ปกป้องข้อมูลสารสนเทศในเครือข่าย
- การจัดการสื่อบันทึก มีวัตถุประสงค์เพื่อ ควบคุมจัดการและป้องกันสื่อบันทึก
- การแลกเปลี่ยนข้อมูลสารสนเทศและซอฟต์แวร์ มีวัตถุประสงค์เพื่อ ป้องกันการสูญหาย การดัดแปลง หรือนำไปใช้ในทางที่ผิด ของการแลกเปลี่ยนข้อมูลระหว่างองค์กร

2.3.2.7 การควบคุมการเข้าถึง

- ความต้องการขององค์กรในการควบคุมการเข้าถึง มีวัตถุประสงค์เพื่อ ควบคุมการเข้าถึงระบบสารสนเทศ
- การจัดการการเข้าถึงของผู้ใช้ มีวัตถุประสงค์เพื่อ ป้องกันผู้ที่ไม่มีสิทธิเข้าถึงระบบสารสนเทศ
- ความรับผิดชอบของผู้ใช้ มีวัตถุประสงค์เพื่อ ป้องกันผู้ใช้ที่ไม่มีสิทธิเข้าถึง
- การควบคุมการเข้าถึงระบบเครือข่าย มีวัตถุประสงค์เพื่อ ป้องกันบริการระบบเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ มีวัตถุประสงค์เพื่อ ป้องกันผู้ที่ไม่มีสิทธิเข้าถึงคอมพิวเตอร์
- การควบคุมการเข้าถึงโปรแกรมประยุกต์ มีวัตถุประสงค์เพื่อ ป้องกันการเข้าถึงข้อมูลสารสนเทศในระบบสารสนเทศโดยไม่มีสิทธิ
- การเฝ้าดูการเข้าถึงและการใช้ระบบ มีวัตถุประสงค์เพื่อ ตรวจจับกิจกรรมที่ไม่มีสิทธิ
- การใช้งานคอมพิวเตอร์เคลื่อนที่ มีวัตถุประสงค์เพื่อ รักษาความปลอดภัยระบบสารสนเทศเมื่อใช้งานคอมพิวเตอร์เคลื่อนที่

2.3.2.8 การพัฒนาและการบำรุงรักษาระบบ

- ความต้องการความปลอดภัยของระบบ มีวัตถุประสงค์เพื่อ ให้ระบบสารสนเทศถูกสร้างให้มีความปลอดภัย
- ความปลอดภัยในระบบงาน มีวัตถุประสงค์เพื่อ ป้องกันการสูญหาย การดัดแปลง หรือการนำไปใช้ในทางที่ผิด ของการใช้ข้อมูลในระบบงาน
- การควบคุมการเข้ารหัส มีวัตถุประสงค์เพื่อ ป้องกันความลับ การให้สิทธิหรือบูรณภาพของข้อมูลสารสนเทศ
- เอกสารความปลอดภัยระบบ มีวัตถุประสงค์เพื่อ ให้โครงการเทคโนโลยีสารสนเทศและการสื่อสาร และกิจกรรมต่างๆ ถูกนำไปปฏิบัติ
- ความปลอดภัยในการพัฒนาและสนับสนุนการปฏิบัติงาน มีวัตถุประสงค์เพื่อคงไว้ซึ่งความปลอดภัยของซอฟต์แวร์ระบบงานและข้อมูลสารสนเทศ

2.3.2.9 การบริหารจัดการอย่างต่อเนื่อง

- เกณฑ์ของการบริหารจัดการอย่างต่อเนื่อง มีวัตถุประสงค์เพื่อ ป้องกัน แก้ไขการขัดจังหวะการดำเนินงานในองค์กร จากความล้มเหลวหายนะต่างๆ

2.3.2.10 การนำไปปฏิบัติ

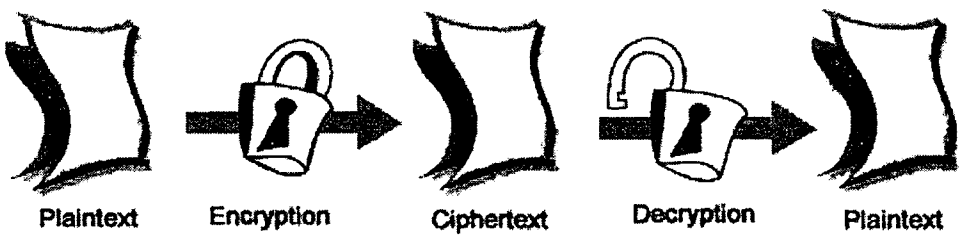
- การนำไปปฏิบัติตามความต้องการของ กฎ ระเบียบ ข้อบังคับ และกฎหมาย มีวัตถุประสงค์เพื่อ อุดช่องโหว่ของกฎ ระเบียบ ข้อบังคับ กฎหมาย
- ทบทวนนโยบายความปลอดภัย และการนำไปปฏิบัติทางเทคนิค มีวัตถุประสงค์เพื่อ ให้สมารถนำไปปฏิบัติกับของระบบสารสนเทศ ตามนโยบายความปลอดภัยขององค์กรและมาตรฐาน

2.4 เทคโนโลยีด้านความปลอดภัย

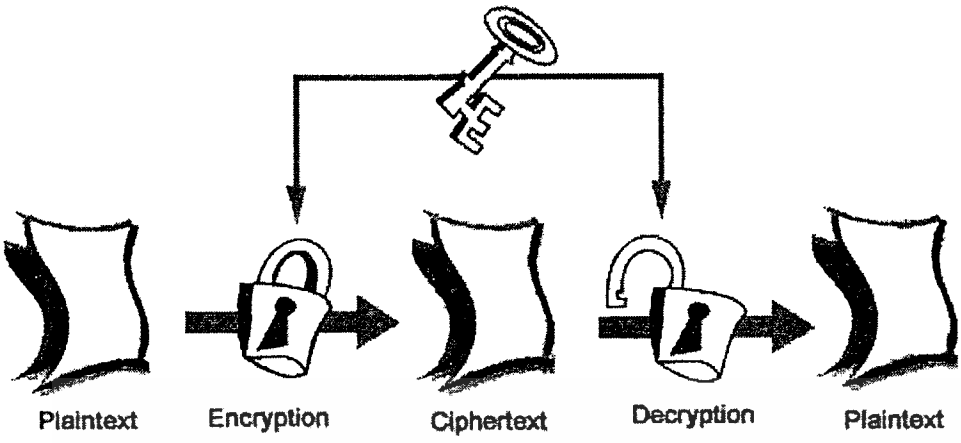
2.4.1 วิทยาการเข้ารหัสลับ (Cryptography)

วิทยาการเข้ารหัสลับ เป็นเทคนิคในการแปลงข้อมูลหรือข้อความที่สามารถอ่านเข้าใจได้ (Plain text หรือ Clear text) ให้เป็นข้อมูลที่เข้ารหัสแบบข้อมูลตัวอักษร (Text) หรือข้อมูลไบนารี่ (Binary) ที่ไม่สามารถอ่านเข้าใจได้ (Cipher text) สามารถแบ่งออกเป็น 2 ระบบ คือ

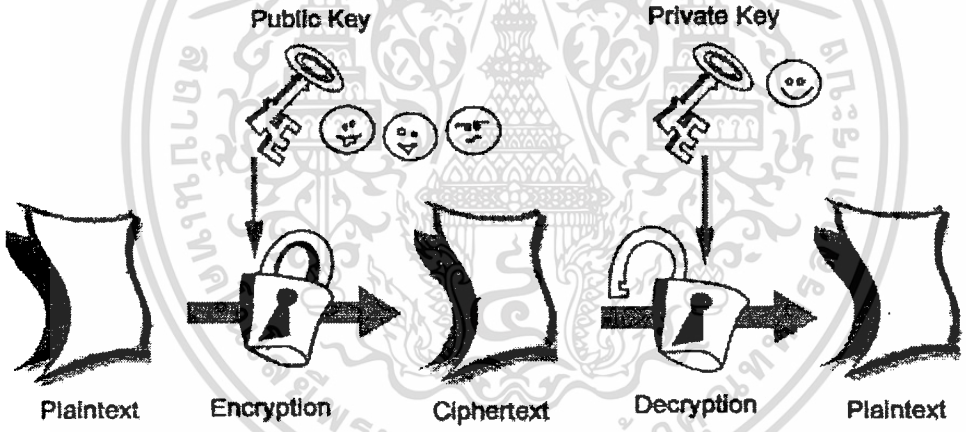
- ระบบการเข้ารหัสแบบสมมาตร(Symmetric Cryptosystems) ใช้กุญแจเดียวในการเข้ารหัสลับข้อความและถอดรหัสลับข้อความ เรียกกุญแจนี้ว่า กุญแจลับ (Secret Key) หรือกุญแจเดี่ยว (Single Key)
- ระบบการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptosystems) ใช้กุญแจสาธารณะ (Public Key) ในการเข้ารหัสลับข้อความ และใช้กุญแจส่วนตัว (Private Key) ในการถอดรหัสลับข้อความนั้น เรียกได้อีกอย่างว่า ระบบการเข้ากุญแจสาธารณะ (Public key cryptosystems) หรือการเข้ารหัสลับแบบกุญแจคู่ (Two-key encryption)



ภาพที่ 2.3 แสดง Basic Encryption/Decryption Process



ภาพที่ 2.4 แสดง Symmetric Cryptography



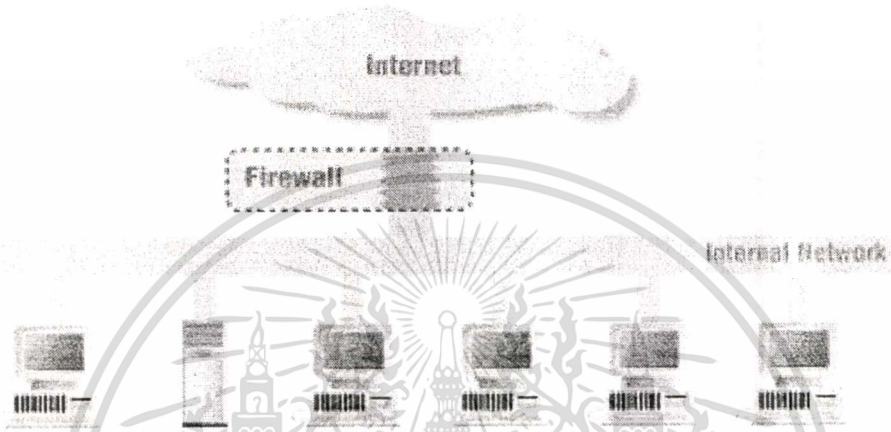
ภาพที่ 2.5 แสดง Asymmetric Cryptography

วิทยาการเข้ารหัสลับถูกนำมาใช้ในระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อทำหน้าที่หลัก/พื้นฐาน 3 ประการคือ

- ความลับหรือภาวะส่วนตัว (Confidentiality or Privacy)
- บูรณภาพข้อมูล (Data Integrity)
- การพิสูจน์ตัวจริง (Authentication)

2.4.2 ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเทอร์เน็ต หรือเครือข่ายภายนอก โดยไฟร์วอลล์ มีหน้าที่ในการควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกหรือเครือข่ายที่ไม่ปลอดภัย กับ เครือข่ายภายในหรือเครือข่ายที่ต้องการป้องกัน



ภาพที่ 2.6 แสดงการใช้ไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน

การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้หลายระดับและหลายรูปแบบขึ้นอยู่กับชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น สามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้บริการอะไรบ้าง จากที่ไหน เป็นต้น

ไฟร์วอลล์ สามารถแบ่งได้เป็น 2 ประเภท คือ

- Network Layer Firewalls ได้แก่ Packet-Filtering Router หรือ Packet Filter
- Application Layer Firewalls ได้แก่ Application-Level Gateway (Proxy Server) และ Circuit-Level Gateway

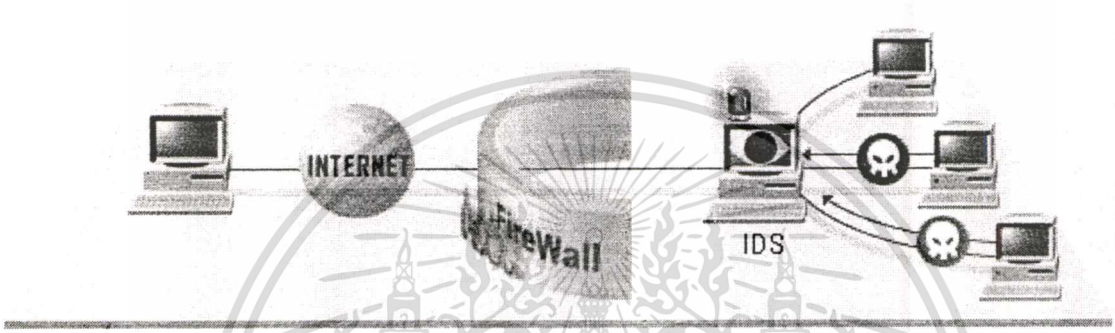
2.4.3 ระบบตรวจจับผู้บุกรุก (Intrusion Detection System)

ผู้บุกรุกระบบคอมพิวเตอร์ (Intruder) หมายถึง บุคคลที่พยายามบุกรุก หรือได้ บุกรุกเข้ามาในระบบโดยที่ไม่มีสิทธิ การบุกรุกสามารถแบ่งจากสถานที่ที่เข้ามาของผู้ บุกรุก สามารถแบ่งได้เป็น 2 ประเภท คือ การบุกรุกจากภายในเครือข่าย และการบุกรุกจากภายนอกเครือข่าย

ระบบตรวจจับผู้บุกรุก สามารถแบ่งออกได้เป็น 4 ประเภท คือ

- Application-Base Monitoring Approaches เป็นแบบที่มีการเก็บข้อมูลในระดับ Application เช่น log file ของ DBMS

- Host-Base Monitoring Approaches เป็นแบบที่มี Agent คอย Sensor เก็บข้อมูลกิจกรรมต่างๆ
- Target-Base Monitoring Approaches เป็นแบบที่วิเคราะห์บูรณภาพของไฟล์ที่ต้องการหรือกำหนดไว้
- Network-Base Monitoring Approaches เป็นแบบที่มีการเก็บข้อมูลในเครือข่าย



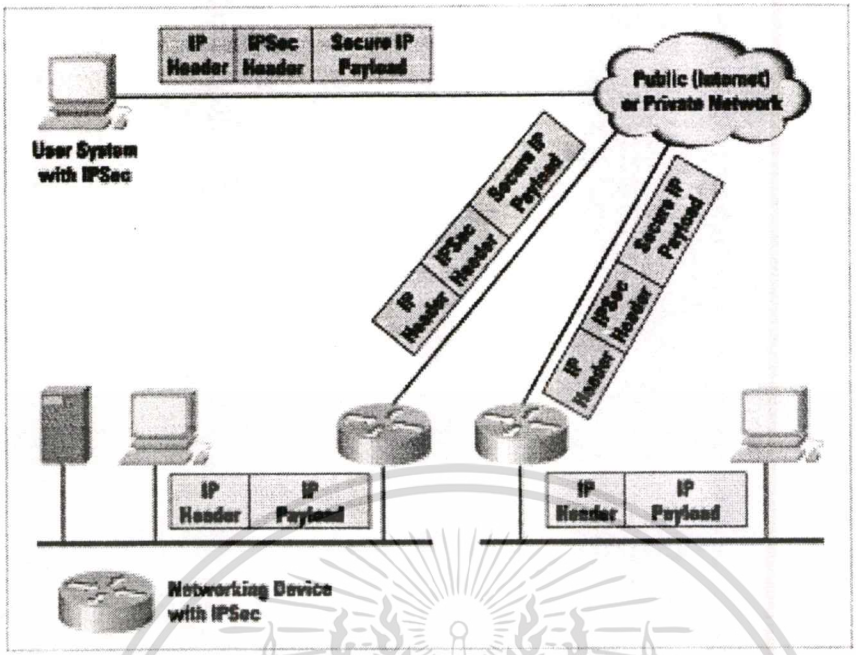
ภาพที่ 2.7 แสดงตัวอย่างการวางระบบตรวจจับการบุกรุก

2.4.4 IP Security (IPSec)

การรักษาความปลอดภัยระดับ IP หรือเรียกย่อๆ ว่า IPSec นั้น มีหน้าที่ในการให้บริการ 3 อย่าง คือ การพิสูจน์ตน (Authentication), การรักษาความลับ (Confidential) และการบริหารคีย์ (Key Management)

IPSec ใช้ในการเชื่อมต่อระหว่างสำนักงานสาขา (Branch Office) โดยผ่านเครือข่ายอินเทอร์เน็ต หรือใช้ในการเชื่อมต่อระยะไกล (Remote Access) ผ่านเครือข่ายอินเทอร์เน็ต หรือใช้ในการเชื่อมต่อระหว่างระหว่างองค์กรที่เรียกว่า เอ็กซ์ทราเน็ต (Extranet)

จากรูปแบบการใช้งานปกติของ IPSec โดยการสื่อสารภายในวงแลน (Local Area Network) แต่ละวงจะเป็นการสื่อสารตามปกติ แต่เมื่อการสื่อสารออกไปข้างนอกจะมีการใช้ IPSec โดยการนำ IPSec มาใช้นี้จะเริ่มที่เราท์เตอร์ (Router) และไฟร์วอลล์ (Firewall) หรือเกตเวย์ (Gateway) ของเครือข่าย โดยจะมีการเข้ารหัสข้อมูลแล้วจึงส่งออกไป เมื่อถึงปลายทางก็จะถอดรหัสออกมา ซึ่งการทำงานทั้งหมดนี้จะเกิดขึ้นโดยที่เครื่องคอมพิวเตอร์ไม่มีส่วนรับทราบเลย นอกจากนั้น IPSec ยังสามารถใช้งานในกรณีที่ผู้ใช้การเชื่อมต่อแบบ Dial-up ได้อีกด้วย สามารถใช้ในการเชื่อมต่อเข้ามาที่หน่วยงานนั้นๆ โดยตรง



ภาพที่ 2.8 แสดงรูปแบบการใช้งานปกติของ IPSec

2.4.5 VPN (Virtual Private Network)

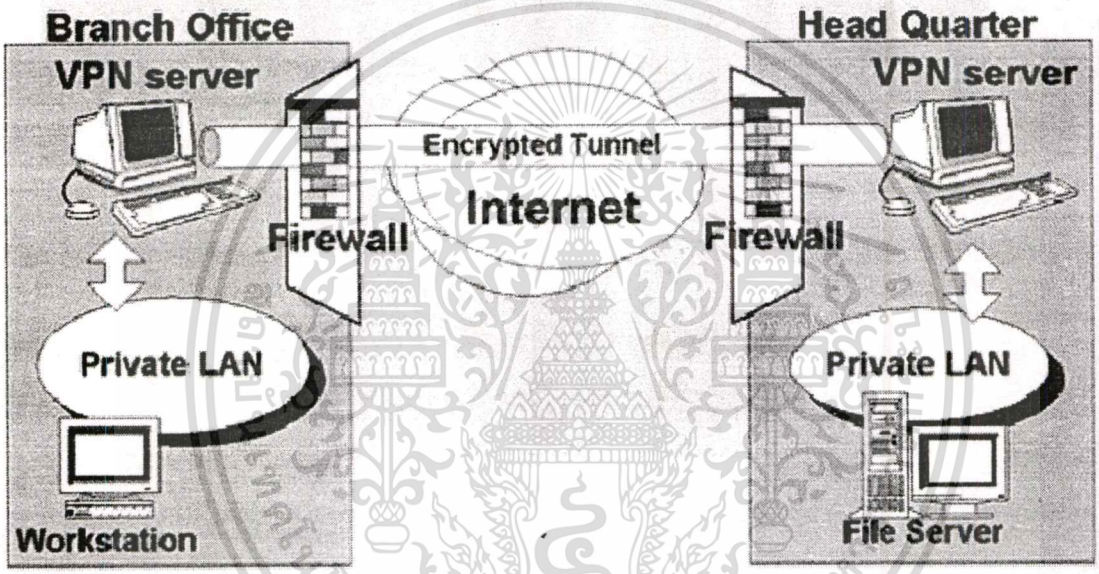
VPN (Virtual Private Network) เป็นการจำลองเครือข่ายภายในบนเครือภายภายนอก อย่างเช่น อินเทอร์เน็ตที่เรียกว่า "virtual" ก็เพราะมันขึ้นอยู่กับการใช้การเชื่อมต่อเสมือน (virtual connections) ซึ่งเป็นคอนเน็กชั่นชั่วคราว ไม่ได้เป็นการติดต่อทางกายภาพ แต่มันประกอบด้วยแพ็กเก็ตที่ถูกเราท์ไปมาโดยผ่านเครื่องหลากหลายบนอินเทอร์เน็ต การเชื่อมต่อเสมือนที่มีความปลอดภัยนี้อาจถูกสร้างขึ้นระหว่างเครื่องสู่เครื่อง หรือเป็นแบบเครื่องสู่เครือข่าย หรือระหว่างเครือข่ายก็ได้

การพัฒนาเอาเทคโนโลยี VPN ไปใช้ในองค์กร เพื่อช่วยอำนวยความสะดวกและปลอดภัย สามารถจำแนกได้เป็น 2 รูปแบบ คือ

2.4.5.1 Site-to-Site

เมื่อองค์กรใดๆ ต้องการติดต่อกับระบบเครือข่ายของสาขาขององค์กรตนข้ามเครือข่ายอินเทอร์เน็ตและใช้ VPN ในการควบคุมความปลอดภัยข้ามเครือข่าย สิ่งที่ทุกองค์กรจะต้องมีในการทำระบบ VPN คือ VPN เซิร์ฟเวอร์เพื่อตรวจสอบทำการเข้ารหัส-ถอดรหัส แพ็กเกจต่างๆ ที่ส่งเข้าออกระหว่างภายในและภายนอกเครือข่าย ถ้าหากไม่มี VPN เซิร์ฟเวอร์ในด้านใดด้านหนึ่ง การติดต่อจะเป็นไปไม่ได้เลย ดังรูป สมมติว่าบริษัทหนึ่งติดตั้ง VPN เซิร์ฟเวอร์ ที่สำนักงานของตน และให้สาขาที่อยู่ห่างไกลต่อผ่าน

เครือข่ายอินเทอร์เน็ตเข้ามาเพื่อติดต่อส่งข้อมูลภายในกัน สาขานั้นจะต้องมี VPN เซิร์ฟเวอร์ เพื่อเป็นตัวควบคุมแพ็กเกจเข้าออกระบบเครือข่ายของสาขานั้นด้วย โดยที่ VPN เซิร์ฟเวอร์ทั้งสองข้างจะต้องเป็น เซิร์ฟเวอร์ชนิดเดียวกัน คือ คุยกันได้ มีระบบการเข้าและถอดรหัสเดียวกัน ซึ่งส่วนใหญ่จะใช้ VPN เซิร์ฟเวอร์ยี่ห้อเดียวกัน VPN เซิร์ฟเวอร์ของทั้งสองฝั่งจะสร้างทันเนลต่อตรงระหว่างกัน ดังนั้นเครื่องลูกข่ายที่อยู่หลังเซิร์ฟเวอร์นี้ จะส่งข้อมูลออกระบบเครือข่ายอีกฝั่งหนึ่งผ่านทางทันเนลนี้ด้วย



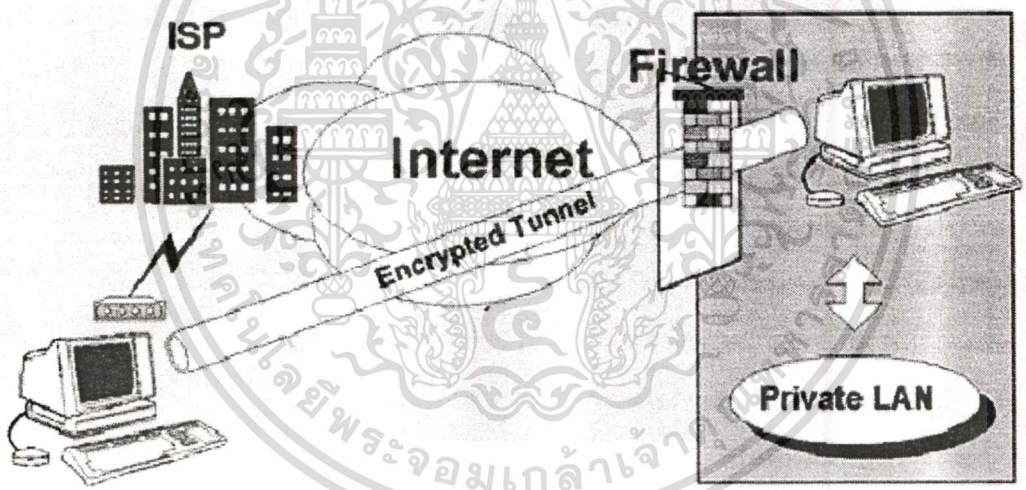
ภาพที่ 2.9 แสดงการ Implement VPN ในรูปแบบ site-to-site

2.4.5.2 SPC-to-site

เนื่องจากทุกวันนี้มีความต้องการที่จะให้ผู้ที่ออกไปปฏิบัติงานนอกสำนักงาน ไม่ว่าจะเป็นที่ต่างจังหวัด, ต่างประเทศ หรือร้านค้าขายปลีกสามารถติดต่อและส่งผ่านข้อมูลกับสำนักงานใหญ่ได้อย่างสะดวก, รวดเร็ว และประหยัด ไม่ว่าจะอยู่ที่ไหน หรือติดต่อเมื่อไหร่ จากที่เราได้อธิบายไปในตอนต้นแล้วว่าเมื่อสำนักงานใหญ่ต่อเข้าระบบอินเทอร์เน็ตที่มีเครือข่ายเชื่อมต่อกันทั่วโลก และเปิดให้ผู้ใช้งานจากภายนอกติดต่อผ่าน ISP ได้ การเชื่อมต่อที่เกิดขึ้นจะถูกควบคุมโดยระบบ VPN ระบบ VPN ในรูปแบบนี้ ทำได้ 2 ลักษณะ คือ

- Client- initiated

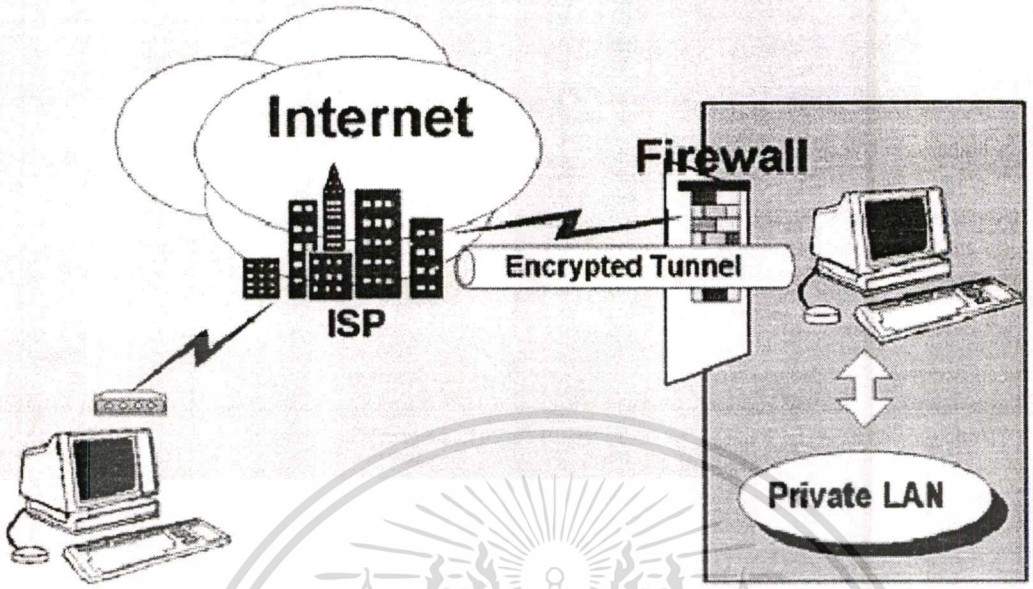
ผู้ใช้งานที่ต้องการติดต่อกับเครือข่ายภายในของบริษัทจะโทรเข้าหา ISP หลังจากที่ผ่านการตรวจสอบชื่อและรหัสผ่านที่ ISP จะต้องตรวจสอบเพื่อดูว่าผู้ที่โทรเข้ามานั้นเป็นสมาชิกของตนหรือไม่ ถ้าใช่ ISP นั้นก็จะอนุญาตให้ผู้ใช้นั้นสามารถผ่านเข้าสู่ระบบอินเทอร์เน็ตได้ หลังจากนั้นผู้ใช้งานก็จะสร้างทันเนลจากเครื่องเวิร์กสเตชันของตนไปสู่เครื่อง VPN เซิร์ฟเวอร์ เพื่อส่งข้อมูลกัน ทันเนลนั้นจะถูกสร้างโดย ซอฟแวร์ที่ติดตั้งที่เครื่องเวิร์กสเตชันนั้น ดังนั้นถ้าเครื่องเวิร์กสเตชันนั้นต้องการดึงข้อมูลจากไฟล์เซิร์ฟเวอร์ภายในระบบเครือข่ายของบริษัท ก็จะสามารถทำได้โดยผ่านทันเนลนี้



ภาพที่ 2.10 แสดง Client- initiated

- Network access server

บริษัทที่ต้องการให้ผู้ใช้งานสามารถโทรเข้า ISP และติดต่อมาที่ระบบเครือข่ายของบริษัท จะต้องทำการติดต่อกับ ISP ที่บริษัทตนเชื่อมสายเข้ามาดังรูป



ภาพที่ 2.11 แสดง Network access server

บริษัทเดินสายวงจรเช่ามายัง ISP และให้ ISP นั้นทราบว่าทางบริษัทต้องการให้ผู้ใช้ติดต่อผ่านระบบ VPN มายังบริษัทของตนได้ เมื่อผู้ใช้ล็อกเข้าสู่ระบบอินเทอร์เน็ตที่ ISP แล้ว ISP จะตรวจสอบดูว่าผู้ใช้งานนั้นเป็นสมาชิกของเครือข่ายบริษัทใด ซึ่งเมื่อตรวจสอบพบแล้ว ISP นั้นก็จะสร้างทันเนลจาก ISP ถึงที่บริษัทนั้น และให้ผู้ใช้ส่งผ่านข้อมูลไปยังบริษัทของตนเองผ่านทันเนลที่มีความปลอดภัย

ทั้ง 2 ลักษณะนี้มีข้อดีข้อเสียแตกต่างกันไป แบบ Client-initiated มีความยืดหยุ่นในการต่อเข้า ISP ใดๆก็ได้ เนื่องจากทันเนลสร้างขึ้นที่ตัวผู้ใช้เองโดยตรงโดยไม่ต้องพึ่ง ISP ในขณะที่แบบ Network access server ต้องใช้ ISP หรือกลุ่มของ ISP เดียวกับที่บริษัทต่อระบบเครือข่าย ทำให้มีข้อจำกัดในการใช้งานจากที่ต่างๆ แต่แบบ Network access server นี้ผู้ใช้งานภายนอกสามารถใช้งานได้ทันทีไม่ว่าจะเป็นเครื่องโน้ตบุ๊คหรือพีซีใดๆ ในขณะที่แบบ Client-initiated ก่อนการใช้งาน ผู้ใช้ต้องติดตั้งโปรแกรมซึ่งเป็น VPN ไคลเอนต์ ลงที่เครื่องก่อน จึงจะติดต่อเข้าไปยังเซิร์ฟเวอร์ ของตนได้

บทที่ 3
วิเคราะห์ความต้องการด้านความปลอดภัย

การกำหนดความต้องการด้านความปลอดภัยระบบสารสนเทศของกองตำรวจสันติบาล 1 นั้น อาศัยการหลักการบริหารความเสี่ยงเป็นเครื่องมือช่วยในการกำหนดความต้องการ ซึ่งการบริหารความเสี่ยงนั้น มีขั้นตอนตั้งแต่ การกำหนดประเภทรายการทรัพย์สิน วิเคราะห์สภาพไม่มั่นคง และภัยคุกคาม แล้วจึงทำการประเมินความเสี่ยง เพื่อกำหนดความต้องการด้านความปลอดภัย อันจะนำไปสู่การกำหนดแนวทางหรือมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ของ กองตำรวจสันติบาล 1 ต่อไป

3.1 กำหนดประเภทรายการทรัพย์สิน

ทรัพย์สินต่างๆ ในระบบสารสนเทศของ กองตำรวจสันติบาล 1 สามารถจำแนกออกเป็นประเภทหลักๆ ได้ 4 ประเภท คือทรัพย์สินประเภทข้อมูล (Information Assets) ทรัพย์สินประเภทซอฟต์แวร์ (Software Assets) ทรัพย์สินประเภทกายภาพ (Physical Assets) และ บริการ (Services) ซึ่งรายละเอียดรายการทรัพย์สินแต่ละประเภท มีดังนี้

ตารางที่ 3.1 รายการทรัพย์สินประเภทข้อมูล (Information Assets)

ลำดับ	รายการ
1.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับที่สุด)
2.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับมาก)
3.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับ)
4.	ข้อมูลปฏิบัติงานระบบงานหลัก
5.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับที่สุด)
6.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับมาก)
7.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับ)
8.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน
9.	ข้อมูลประชาสัมพันธ์ภายในหน่วยงาน
10.	ข้อมูลประชาสัมพันธ์ทั่วไป

ตารางที่ 3.2 รายการทรัพย์สินประเภทซอฟต์แวร์ (Software Assets)

ลำดับ	รายการ
1.	OS DB/File Server ระบบงานหลัก
2.	OS Application Server ระบบงานหลัก
3.	OS DB/File Server ระบบงานสนับสนุน
4.	OS Application Server ระบบงานสนับสนุน
5.	OS Mail Server
6.	OS Remote Access Server
7.	OS Web Server
8.	OS Domain Name Server
9.	OS Print Server
10.	OS Workstation
11.	OS Client
12.	DBMS ระบบงานหลัก
13.	Application ระบบงานหลัก
14.	DBMS ระบบงานสนับสนุน
15.	Application ระบบงานสนับสนุน
16.	Mail Server Application
17.	Remote Access Server Application
18.	Web Server Application
19.	Domain Name Server Application
20.	Print Server Application
21.	Workstation Application
22.	Client Application
23.	Management Tools
24.	Development Tools
25.	Server Utility
26.	Client Utility

ตารางที่ 3.3 รายการทรัพย์สินประเภทกายภาพ (Physical Assets)

ลำดับ	รายการ
1.	สถานที่ กองตำรวจสันติบาล 1 (SB1 Area)
2.	อาคาร กองตำรวจสันติบาล 1 (SB1 Buildings)
3.	อาคาร ศูนย์คอมพิวเตอร์ (CC Building)
4.	ศูนย์คอมพิวเตอร์ (Computer Center)
5.	DB/File Server ระบบงานหลัก
6.	Application Server ระบบงานหลัก
7.	DB/File Server ระบบงานสนับสนุน
8.	Application Server ระบบงานสนับสนุน
9.	Mail Server
10.	Remote Access Server
11.	Web Server
12.	Domain Name Server
13.	Print Server
14.	Workstation
15.	Client
16.	ระบบงานหลัก Network Equipment & Cable
17.	ระบบงานสนับสนุน Network Equipment & Cable
18.	Backbone Network Equipment & Cable
19.	Client Network Equipment & Cable
20.	Computer Center Media
21.	Users Media
22.	Computer Center Furniture and Accommodations
23.	Furniture and Accommodations
24.	Computer Center Air Condition
25.	ระบบงานหลัก Power Equipment & Cable
26.	ระบบงานสนับสนุน Power Equipment & Cable
27.	Client Power Equipment & Cable

ตารางที่ 3.4 รายการทรัพย์สินประเภทบริการ (Services)

ลำดับ	รายการ
1.	Computer Center Electricity Supply
2.	Working Area Electricity Supply
3.	Computer Center Water Supply
4.	Working Area Water Supply
5.	Computer Center Air Condition
6.	Working Area Air Condition
7.	Computer Center Lighting
8.	Working Area Lighting
9.	Lease Line Service
10.	Internet Service

3.2 วิเคราะห์ความบกพร่อง

การวิเคราะห์ความบกพร่อง (Vulnerabilities) เป็นการวิเคราะห์ถึงจุดอ่อนหรือจุดบกพร่องในระบบสารสนเทศ ที่อาจถูกภัยคุกคามต่างๆ ก่อความเสียหายต่อระบบสารสนเทศ ซึ่งความบกพร่องต่างๆ ในระบบสารสนเทศนั้นได้แก่ การควบคุมการเข้าถึงที่ไม่ดี (Poor Access Control) การชำรุดทรุดโทรมขาดการซ่อมแซม (Disrepair) การทำงานผิดพลาดของฮาร์ดแวร์ (Miss Process of Hardware) การทำงานผิดพลาดของซอฟต์แวร์ (Miss Process of Software) ความผิดพลาดในการติดต่อสื่อสาร (Miss Process of Communication) และ การไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention) ซึ่งสามารถวิเคราะห์ความบกพร่องของทรัพย์สินแต่ละประเภท ได้ดังนี้

ตารางที่ 3.5 ความบกพร่องของทรัพย์สินประเภทข้อมูล

Type of Vul.	Vulnerabilities
Human	Poor Logical Access Control
Physical	-
Hardware	Miss Process
Software	Miss Process
Communication	Miss Process
Natural Incident	Poor Prevention

ตารางที่ 3.6 ความบกพร่องของทรัพย์สินประเภทซอฟต์แวร์

Type of Vul.	Vulnerabilities
Human	Poor Logical Access Control
Physical	-
Hardware	-
Software	Miss Process
Communication	-
Natural Incident	Poor Prevention

ตารางที่ 3.7 ความบกพร่องของทรัพย์สินประเภทกายภาพ

Type of Vul.	Vulnerabilities
Human	Poor Physical Access Control
Physical	Disrepair
Hardware	Miss Process
Software	Miss Process
Communication	-
Natural Incident	Poor Prevention

ตารางที่ 3.8 ความบกพร่องของทรัพย์สินประเภทบริการ

Type of Vul.	Vulnerabilities
Human	Poor Logical Access Control
Physical	-
Hardware	-
Software	-
Communication	-
Natural Incident	Poor Prevention

3.3 วิเคราะห์ภัยคุกคาม

ภายหลังจากที่วิเคราะห์ถึงสภาพบกพร่องในระบบสารสนเทศของทรัพย์สินแต่ละประเภทตามประเภทความบกพร่องแล้วนั้น ก็จะเป็นการวิเคราะห์ถึงภัยคุกคาม (Threat) ต่างๆ ที่อาจเกิดขึ้นจากความบกพร่องที่ได้วิเคราะห์ไว้ข้างต้น พร้อมทั้งกำหนดแนวทางการบริหารความเสี่ยง (Risk Management) เพื่อควบคุมลดหรือบรรเทาความเสี่ยงจากภัยคุกคามต่างๆ ซึ่งสามารถวิเคราะห์จำแนกตามประเภททรัพย์สินได้ดังนี้

3.3.1 ทรัพย์สินประเภทข้อมูล

วิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นจากความบกพร่องต่างๆ และแนวทางการบริหารความเสี่ยง จำแนกออกตามประเภทของภัยคุกคาม ได้ดังนี้

3.3.1.1 การควบคุมการเข้าถึงทางลอจิคอลที่ไม่ดี (Poor Logical Access Control)

3.3.1.1.1 การขัดจังหวะ (Interruption)

- ผู้บุกรุกเข้ามาลบข้อมูล (Intruder intrude to Delete) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้ลบข้อมูลโดยไม่เจตนา (User not intent to Delete) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)
- ผู้ใช้เจตนาลบข้อมูล (User Intent to Delete) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.1.1.2 การยึดครอง (Interception)

- ผู้บุกรุกเข้ามาสำเนาข้อมูล (Intruder intrude to Copy) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้เจตนาสำเนาข้อมูล (User Intent to Copy) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.1.1.3 การดัดแปร (Modification)

- ผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล (Intruder intrude to Modify) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้แก้ไขเปลี่ยนแปลงข้อมูลโดยไม่เจตนา (User not intent to Modify)บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

- ผู้ใช้แก้ไขเปลี่ยนแปลงข้อมูลโดยเจตนา (User Intent to Modify) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.1.1.4 การปลอมแต่ง (Fabrication)

- ผู้บุกรุกเข้ามาเพิ่มข้อมูล (Intruder intrude to Insert) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้เพิ่มข้อมูลโดยไม่เจตนา (User not intent to Insert) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)
- ผู้ใช้เพิ่มข้อมูลโดยเจตนา (User Intent to Insert) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.1.2 การทำงานผิดพลาดของฮาร์ดแวร์ (Miss Process of Hardware)

3.3.1.2.1 การขัดจังหวะ (Interruption)

- ข้อมูลถูกลบ (Be Deleted) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.2.2 การดัดแปร (Modification)

- ข้อมูลถูกเปลี่ยนแปลงแก้ไข (Be Modified) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.3 การทำงานผิดพลาดของซอฟต์แวร์ (Miss Process of Software)

3.3.1.3.1 การขัดจังหวะ (Interruption)

- ข้อมูลถูกลบ (Be Deleted) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.3.2 การดัดแปร (Modification)

- ข้อมูลถูกเปลี่ยนแปลงแก้ไข (Be Modified) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.4 ความผิดพลาดในการติดต่อสื่อสาร (Miss Process of Communication)

3.3.1.4.1 การขัดจังหวะ (Interruption)

- ข้อมูลสูญหาย (Be Lost) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.4.2 การดัดแปร (Modification)

- ข้อมูลถูกเปลี่ยนแปลงแก้ไข (Be Modified) บริหารความเสี่ยงโดย การสำรองข้อมูล (Backup)

3.3.1.5 การไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention)

3.3.1.5.1 การขัดจังหวะ (Interruption)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)
- ถูกดักจับข้อมูล (Sniffer)บริหารความเสี่ยงโดยการเข้ารหัสข้อมูล (Encryption)

3.3.1.5.2 การยึดครอง (Interception)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)
- ถูกดักจับข้อมูล (Sniffer)บริหารความเสี่ยงโดยการเข้ารหัสข้อมูล (Encryption)

3.3.1.5.3 การดัดแปร (Modification)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)
- ถูกดักจับข้อมูล (Sniffer)บริหารความเสี่ยงโดยการเข้ารหัสข้อมูล (Encryption)

3.3.1.5.4 การปลอมแต่ง (Fabrication)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)
- ถูกดักจับข้อมูล (Sniffer)บริหารความเสี่ยงโดยการเข้ารหัสข้อมูล (Encryption)

ตารางที่ 3.9 ภัยคุกคาม และแนวทางการบริหารความเสี่ยงของทรัพย์สินประเภทข้อมูล

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Risk Management
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	Logical Access Control
			User not intent to Delete	Backup
			User Intent to Delete	Policy
		Interception	Intruder intrude to Copy	Logical Access Control
			User Intent to Copy	Policy
		Modification	Intruder intrude to Modify	Logical Access Control
			User not intent to Modify	Backup
			User Intent to Modify	Policy
		Fabrication	Intruder intrude to Insert	Logical Access Control
			User not intent to Insert	Backup
			User Intent to Insert	Policy
Hardware	Miss Process	Interruption	Be Deleted	Backup
		Interception	-	-
		Modification	Be Modified	Backup
		Fabrication	-	-
Software	Miss Process	Interruption	Be Deleted	Backup
		Interception	-	-
		Modification	Be Modified	Backup
		Fabrication	-	-
Communication	Miss Process	Interruption	Be Lost	Encryption
		Interception	-	-
		Modification	Be Modified	Encryption
		Fabrication	-	-
Natural Incident	Poor Prevention	Interruption	Malicious Software	Malicious Scan Software
			Sniffer	Encryption
		Interception	Malicious Software	Malicious Scan Software
			Sniffer	Encryption
		Modification	Malicious Software	Malicious Scan Software
			Sniffer	Encryption
		Fabrication	Malicious Software	Malicious Scan Software
			Sniffer	Encryption

3.3.2 ทรัพย์สินประเภทซอฟต์แวร์

วิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นจากความบกพร่องต่างๆ และแนวทางการบริหารความเสี่ยง จำแนกออกตามประเภทของภัยคุกคาม ได้ดังนี้

3.3.2.1 การควบคุมการเข้าถึงทางลอจิคอลที่ไม่ดี (Poor Logical Access Control)

3.3.2.1.1 การขัดจังหวะ (Interruption)

- ผู้บุกรุกเข้ามาลบซอฟต์แวร์ (Intruder intrude to Delete or Uninstall) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้ลบซอฟต์แวร์โดยไม่เจตนา (User not intent to Delete or Uninstall) บริหารความเสี่ยงโดย การมีซอฟต์แวร์สำรอง (Reserve Software)
- ผู้ใช้เจตนาลบซอฟต์แวร์ (User Intent to Delete or Uninstall) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.2.1.2 การยึดครอง (Interception)

- ผู้บุกรุกเข้ามาสำเนาซอฟต์แวร์ (Intruder intrude to Copy) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้เจตนาสำเนาซอฟต์แวร์ (User Intent to Copy) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.2.1.3 การดัดแปร (Modification)

- ผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงซอฟต์แวร์ (Intruder intrude to Configure) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)
- ผู้ใช้แก้ไขเปลี่ยนแปลงซอฟต์แวร์โดยไม่เจตนา (User not intent to Configure)บริหารความเสี่ยงโดย การมีซอฟต์แวร์สำรอง (Reserve Software)
- ผู้ใช้แก้ไขเปลี่ยนแปลงซอฟต์แวร์โดยเจตนา (User Intent to Configure) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.2.2 การทำงานผิดพลาดของซอฟต์แวร์ (Miss Process of Software)

3.3.2.2.1 การขัดจังหวะ (Interruption)

- ซอฟต์แวร์หยุดทำงาน (Error or Hang) บริหารความเสี่ยงโดย การมีซอฟต์แวร์สำรอง (Reserve Software)

3.3.2.3 การไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention)

3.3.2.3.1 การขัดจังหวะ (Interruption)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

3.3.2.3.2 การยึดครอง (Interception)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

3.3.2.3.3 การดัดแปร (Modification)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

3.3.2.3.4 การปลอมแต่ง (Fabrication)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

ตารางที่ 3.10 ภัยคุกคาม และแนวทางการบริหารความเสี่ยงของทรัพย์สินประเภทซอฟต์แวร์

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Risk Management
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete or Uninstall	Logical Access Control
			User not intent to Delete or Uninstall	Reserve Software
			User Intent to Delete or Uninstall	Policy
		Interception	Intruder intrude to Copy	Logical Access Control
			User Intent to Copy	Policy
		Modification	Intruder intrude to Configure	Logical Access Control
			User not intent to Configure	Reserve Software
			User Intent to Configure	Policy
		Fabrication	-	-
Software	Miss Process	Interruption	Error or Hang	Reserve Software
		Interception	-	-
		Modification	-	-
		Fabrication	-	-
Natural Incident	Poor Prevention	Interruption	Malicious Software	Malicious Scan Software
		Interception	Malicious Software	Malicious Scan Software
		Modification	Malicious Software	Malicious Scan Software
		Fabrication	Malicious Software	Malicious Scan Software

3.3.3 ทรัพย์สินประเภทกายภาพ

วิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นจากความบกพร่องต่างๆ และแนวทางการบริหารความเสี่ยง จำแนกออกตามประเภทของภัยคุกคาม ได้ดังนี้

3.3.3.1 การควบคุมการเข้าถึงทางกายภาพที่ไม่ดี (Poor Physical Access Control)

3.3.3.1.1 การขัดจังหวะ (Interruption)

- ผู้บุกรุกเข้ามาทำความเสียหาย (Intruder intrude to Destroy) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)

- ผู้ใช้ทำความเสียหายโดยไม่เจตนา (User not intent to Destroy) บริหารความเสี่ยงโดย การมีสถานที่หรือสิ่งของสำรอง (Reserve Site or Hardware)
- ผู้ใช้เจตนาทำความเสียหาย (User Intent to Destroy) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.3.1.2 การยึดครอง (Interception)

- ผู้บุกรุกเข้ามาขโมยสิ่งของ (Intruder intrude to Steal) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)
- ผู้ใช้เจตนาขโมยสิ่งของ (User Intent to Steal) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.3.1.3 การดัดแปร (Modification)

- ผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงสิ่งต่างๆ (Intruder intrude to Configure) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)
- ผู้ใช้แก้ไขเปลี่ยนแปลงสิ่งต่างๆ โดยเจตนา (User Intent to Configure) บริหารความเสี่ยงโดย การกำหนด กฎระเบียบ ข้อบังคับ (Policy)

3.3.3.2 การชำรุดทรุดโทรมขาดการซ่อมแซม (Disrepair)

3.3.3.2.1 การขัดจังหวะ (Interruption)

- สถานที่และสิ่งของต่างๆ เสียหายเนื่องจากชำรุดทรุดโทรม (Lose) บริหารความเสี่ยงโดย มีการบำรุงรักษา (Maintenance)

3.3.3.3 การทำงานผิดพลาดของฮาร์ดแวร์ (Miss Process of Hardware)

3.3.3.3.1 การขัดจังหวะ (Interruption)

- ฮาร์ดแวร์หยุดทำงาน (Error or Hang) บริหารความเสี่ยงโดย การมีสถานที่หรือสิ่งของสำรอง (Reserve Site or Hardware)

3.3.3.4 การทำงานผิดพลาดของซอฟต์แวร์ (Miss Process of Software)

3.3.3.4.1 การขัดจังหวะ (Interruption)

- สถานที่และสิ่งของต่างๆ เสียหาย (Be Lose) บริหารความเสี่ยงโดย การมีสถานที่หรือสิ่งของสำรอง (Reserve Site or Hardware)

3.3.3.5 การไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention)

3.3.3.5.1 การขัดจังหวะ (Interruption)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)
- อัคคีภัย (Fire) บริหารความเสี่ยงโดย มีระบบป้องกัน ตรวจจับ และระงับอัคคีภัย (Fire Detection, Fire Protection and Fire Extinction)
- แผ่นดินไหว (Earthquake) บริหารความเสี่ยงโดย มีการวางแผนการปฏิบัติเมื่อเกิดเหตุ (Disaster Plan)
- อุทกภัย (Flood) บริหารความเสี่ยงโดย มีการวางแผนการปฏิบัติเมื่อเกิดเหตุ (Disaster Plan)
- ไฟฟ้าดับ (Power Supply Break) บริหารความเสี่ยงโดย มีระบบสำรองและผลิตกระแสไฟฟ้า (UPS and Generator)
- เหตุหายนะต่างๆ (Sabotage) บริหารความเสี่ยงโดย มีการวางแผนการปฏิบัติเมื่อเกิดเหตุ (Disaster Plan)

3.3.3.5.2 การยึดครอง (Interception)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

3.3.3.5.3 การดัดแปร (Modification)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

3.3.3.5.4 การปลอมแต่ง (Fabrication)

- ถูกโจมตีด้วยซอฟต์แวร์ประสงค์ร้าย (Malicious Software) บริหารความเสี่ยงโดย การใช้ซอฟต์แวร์ป้องกัน (Malicious Scan Software)

ตารางที่ 3.11 ภัยคุกคาม และแนวทางการบริหารความเสี่ยงของทรัพย์สินประเภทกายภาพ

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Risk Management
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	Physical Access Control
			User not intent to Destroy	Reserve Site or Hardware
			User Intent to Destroy	Policy
		Interception	Intruder intrude to Steal	Physical Access Control
			User Intent to Steal	Policy
		Modification	Intruder intrude to Configure	Physical Access Control
			User Intent to Configure	Policy
		Fabrication	-	-
Physical	Disrepair	Interruption	Lose	Maintenance
		Interception	-	-
		Modification	-	-
		Fabrication	-	-
Hardware	Miss Process	Interruption	Error or Hang	Reserve Site or Hardware
		Interception	-	-
		Modification	-	-
		Fabrication	-	-
Software	Miss Process	Interruption	Be Lost	Reserve Site or Hardware
		Interception	-	-
		Modification	-	-
		Fabrication	-	-
Natural Incident	Poor Prevention	Interruption	Malicious Software	Malicious Scan Software
			Fire	Fire Detection Fire Protection Fire Extinction
			Earthquake	Disaster Plan
			Flood	Disaster Plan
			Power Supply Break	UPS and Generator
			Sabotage	Disaster Plan
		Interception	Malicious Software	Malicious Scan Software
		Modification	Malicious Software	Malicious Scan Software
		Fabrication	Malicious Software	Malicious Scan Software

3.3.4 ทรัพย์สินประเภทบริการ

วิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นจากความบกพร่องต่างๆ และแนวทางการบริหารความเสี่ยง จำแนกออกตามประเภทของภัยคุกคาม ได้ดังนี้

3.3.4.1 การควบคุมการเข้าถึงทางลอจิคอลที่ไม่ดี (Poor Logical Access Control)

3.3.4.1.1 การยึดครอง (Interception)

- ผู้บุกรุกเข้ามาลักลอบขโมยใช้บริการ (Larceny) บริหารความเสี่ยงโดย การควบคุมการเข้าถึงทางลอจิคอล (Logical Access Control)

3.3.4.2 การไม่มีการป้องกันเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น (Poor Prevention)

3.3.4.2.1 การขัดจังหวะ (Interruption)

- บริการขัดข้องหรือหยุดให้บริการ (Down or Denied of Services) บริหารความเสี่ยงโดย การมีระบบสำรอง (Reserve Services)

ตารางที่ 3.12 ภัยคุกคาม และแนวทางการบริหารความเสี่ยงของทรัพย์สินประเภทบริการ

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Risk Management
Human	Poor Logical Access Control	Interruption	-	-
		Interception	Larceny	Logical Access Control
		Modification	-	-
		Fabrication	-	-
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	Reserve Services
		Interception	-	-
		Modification	-	-
		Fabrication	-	-

3.4 ประเมินความเสี่ยง

การประเมินความเสี่ยงด้านความปลอดภัยระบบสารสนเทศของกองตำรวจสันติบาล 1 นั้น เป็นการวิเคราะห์ถึงโอกาสที่ระบบสารสนเทศอาจจะประสบกับภัยคุกคามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศในรูปแบบต่างๆ เช่น การทำลาย การเปิดเผย เปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ โดยเมื่อวิเคราะห์กำหนดถึงความบกพร่อง (Vulnerabilities) และภัยคุกคาม (Threat) แล้ว จากนั้นจึงวิเคราะห์ประเมินผลกระทบที่อาจต่อความปลอดภัย (Impact) และโอกาสเกิดภัยคุกคาม (Probability) ตามเกณฑ์ที่กำหนดไว้ เพื่อประเมินความเสี่ยง (Risk) อันจะ

นำไปสู่การกำหนดความต้องการด้านความปลอดภัย และกำหนดแนวทางมาตรการป้องกันระบบสารสนเทศให้มีความปลอดภัยต่อไป

3.4.1 เกณฑ์การประเมินความเสี่ยง

ในการประเมินวิเคราะห์ความเสี่ยง จำเป็นจะต้องมีการกำหนดเกณฑ์ในการประเมินวิเคราะห์เพื่อให้ทราบถึงแนวทางหรือเหตุผลในการวิเคราะห์ ซึ่งความเสี่ยงต่อความปลอดภัยระบบสารสนเทศ คือโอกาสที่ระบบสารสนเทศอาจจะประสบกับภัยคุกคามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ในรูปแบบการทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูล และการปฏิเสธการให้บริการของระบบ ดังนั้น ความเสี่ยงต่อระบบสารสนเทศ (Risk) จึงเกิดจากผลกระทบหรือความเสียหายต่อความปลอดภัยของระบบ (Impact) กับ โอกาสในการเกิดภัยคุกคาม (Probability) ซึ่งพอจะกำหนดเป็นเกณฑ์การประเมินความเสี่ยงได้ ดังนี้

ความเสี่ยง = ผลกระทบต่อความปลอดภัย X โอกาสในการเกิดภัยคุกคาม

Risk = Impact X Probability

โดยเกณฑ์การประเมินผลกระทบต่อความปลอดภัย เกณฑ์การประเมินโอกาสการเกิดภัยคุกคาม และเกณฑ์การประเมินความเสี่ยง ได้กำหนดดังแสดงในตาราง ที่ 3.13, 3.14 และ 3.15 ตามลำดับ

ตารางที่ 3.13 เกณฑ์การประเมินผลกระทบต่อความปลอดภัย

ระดับ	ความหมาย
0	ไม่มีผลกระทบต่อความปลอดภัยใดๆ
1	มีผลกระทบต่อความปลอดภัยเล็กน้อย ระบบสามารถใช้งานได้ตามปกติ
2	มีผลกระทบต่อความปลอดภัย บางส่วนของระบบเสียหายไม่สามารถใช้งานได้ชั่วคราว
3	มีผลกระทบต่อความปลอดภัย ระบบทั้งหมดเสียหายไม่สามารถใช้งานได้ชั่วคราว
4	มีผลกระทบต่อความปลอดภัย บางส่วนของระบบเสียหายไม่สามารถใช้งานได้อีกต่อไป
5	มีผลกระทบต่อความปลอดภัย ระบบทั้งหมดเสียหายไม่สามารถใช้งานได้อีกต่อไป

ตารางที่ 3.14 เกณฑ์การประเมินโอกาสเกิดภัยคุกคาม

ระดับ	ความหมาย
1	แทบจะไม่มีโอกาสเกิดขึ้นเลย (น้อยกว่า 1 ครั้ง ในรอบ 20 ปี)
2	มีโอกาสเกิดน้อยมาก (มากกว่า 1 ครั้งในรอบ 20 ปี)
3	มีโอกาสเกิดน้อย (มากกว่า 1 ครั้งในรอบ 5 ปี)
4	มีโอกาสเกิดปานกลาง (มากกว่า 1 ครั้งใน 1 ปี)
5	มีโอกาสเกิดสูง (มากกว่า 1 ครั้งใน 1 เดือน)
6	มีโอกาสเกิดขึ้นเป็นประจำ (มากกว่า 1 ครั้งใน 1 วัน)

ตารางที่ 3.15 เกณฑ์การประเมินความเสี่ยง

ผลกระทบต่อความปลอดภัย \ โอกาสเกิดภัยคุกคาม	1	2	3	4	5	6
0	0	0	0	0	0	0
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24
5	5	10	15	20	25	30

ความสำคัญลำดับ 1 (ดำเนินการจัดทำแผนรองรับและควบคุมอย่างใกล้ชิด)

ความสำคัญลำดับ 2 (ดำเนินการจัดทำแผนรองรับ)

ความสำคัญลำดับ 3 (ไม่ต้องจัดทำแผนรองรับ)

3.4.2 ประเมินความเสี่ยง

การประเมินความเสี่ยงด้านความปลอดภัยนี้ เป็นการประเมินวิเคราะห์แยกตามรายการทรัพย์สินต่างๆ ตามที่ได้กำหนดไว้ ดังนี้

ตารางที่ 3.16 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับที่สุด)

Type of Vul	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.17 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับมาก)

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.18 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับ)

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.19 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.20 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับที่สุด)

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.21 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับมาก)

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.22 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับ)

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.23 ประเมินความเสี่ยงของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	4	6	24 (1)
			User not intent to Delete	4	6	24 (1)
			User Intent to Delete	4	6	24 (1)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	4	6	24 (1)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	4	4	16 (1)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.24 ประเมินความเสี่ยงของ ข้อมูลประชาสัมพันธ์ภายในหน่วยงาน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	2	6	12 (2)
			User not intent to Delete	2	6	12 (2)
			User Intent to Delete	2	6	12 (2)
		Interception	Intruder intrude to Copy	4	6	24 (1)
			User Intent to Copy	0	6	0 (3)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	2	4	8 (2)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	2	4	8 (2)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	0	4	0 (3)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	2	6	12 (2)
			Sniffer	0	6	0 (3)
		Interception	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.25 ประเมินความเสี่ยงของ ข้อมูลประชาสัมพันธ์ทั่วไป

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete	2	6	12 (2)
			User not intent to Delete	2	6	12 (2)
			User Intent to Delete	2	6	12 (2)
		Interception	Intruder intrude to Copy	0	6	0 (3)
			User Intent to Copy	0	6	0 (3)
		Modification	Intruder intrude to Modify	4	6	24 (1)
			User not intent to Modify	4	6	24 (1)
			User Intent to Modify	4	6	24 (1)
		Fabrication	Intruder intrude to Insert	4	6	24 (1)
			User not intent to Insert	4	6	24 (1)
			User Intent to Insert	4	6	24 (1)
Hardware	Miss Process	Interruption	Be Deleted	2	4	8 (2)
		Modification	Be Modified	4	4	16 (1)
Software	Miss Process	Interruption	Be Deleted	2	4	8 (2)
		Modification	Be Modified	4	4	16 (1)
Communication	Miss Process	Interruption	Be Lost	0	4	0 (3)
		Modification	Be Modified	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	2	6	12 (2)
			Sniffer	0	6	0 (3)
		Interception	Malicious Software	0	6	0 (3)
			Sniffer	0	6	0 (3)
		Modification	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)
			Sniffer	4	6	24 (1)

ตารางที่ 3.26 ประเมินความเสี่ยงของ OS DB/File Server ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.27 ประเมินความเสี่ยงของ OS Application Server ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.28 ประเมินความเสี่ยงของ OS DB/File Server ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.29 ประเมินความเสี่ยงของ OS Application Server ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.30 ประเมินความเสี่ยงของ OS Mail Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.31 ประเมินความเสี่ยงของ OS Remote Access Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.32 ประเมินความเสี่ยงของ OS Web Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.33 ประเมินความเสี่ยงของ OS Domain Name Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.34 ประเมินความเสี่ยงของ OS Print Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.35 ประเมินความเสี่ยงของ OS Workstation

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.36 ประเมินความเสี่ยงของ OS Client

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.37 ประเมินความเสี่ยงของ DBMS ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.38 ประเมินความเสี่ยงของ Application ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.39 ประเมินความเสี่ยงของ DBMS ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.40 ประเมินความเสี่ยงของ Application ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.41 ประเมินความเสี่ยงของ Mail Server Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.42 ประเมินความเสี่ยงของ Remote Access Server Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.43 ประเมินความเสี่ยงของ Web Server Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.44 ประเมินความเสี่ยงของ Domain Name Server Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	4	6	24 (1)
			User not intent to Delete,Uninstall	4	6	24 (1)
			User Intent to Delete,Uninstall	4	6	24 (1)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	4	6	24 (1)
			User not intent to Configure	4	6	24 (1)
			User Intent to Configure	4	6	24 (1)
Software	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.45 ประเมินความเสี่ยงของ Print Server Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.46 ประเมินความเสี่ยงของ Workstation Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.47 ประเมินความเสี่ยงของ Client Application

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.48 ประเมินความเสี่ยงของ Management Tools

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.49 ประเมินความเสี่ยงของ Development Tools

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.50 ประเมินความเสี่ยงของ Server Utility

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	1	6	6 (2)
			User not intent to Delete,Uninstall	1	6	6 (2)
			User Intent to Delete,Uninstall	1	6	6 (2)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.51 ประเมินความเสี่ยงของ Client Utility

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interruption	Intruder intrude to Delete,Uninstall	0	6	0 (3)
			User not intent to Delete,Uninstall	0	6	0 (3)
			User Intent to Delete,Uninstall	0	6	0 (3)
		Interception	Intruder intrude to Copy	1	6	6 (2)
			User Intent to Copy	1	6	6 (2)
		Modification	Intruder intrude to Configure	1	6	6 (2)
			User not intent to Configure	1	6	6 (2)
			User Intent to Configure	1	6	6 (2)
Software	Miss Process	Interruption	Error or Hang	0	4	0 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	0	6	0 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.52 ประเมินความเสี่ยงของ สถานที่ กองตำรวจสันติบาล 1

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	5	4	20 (1)
			User not intent to Destroy	5	4	20 (1)
			User Intent to Destroy	5	4	20 (1)
Physical	Disrepair	Interruption	Lose	5	4	20 (1)
Natural Incident	Poor Prevention	Interruption	Fire	5	3	15 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	3	4	12 (2)
			Sabotage	5	2	10 (2)

ตารางที่ 3.53 ประเมินความเสี่ยงของ อาคาร กองตำรวจสันติบาล 1

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	3	4	12 (2)
			Sabotage	4	2	8 (2)

ตารางที่ 3.54 ประเมินความเสี่ยงของ อาคาร ศูนย์คอมพิวเตอร์

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	5	4	20 (1)
			User not intent to Destroy	5	4	20 (1)
			User Intent to Destroy	5	4	20 (1)
Physical	Disrepair	Interruption	Lose	5	4	20 (1)
Natural Incident	Poor Prevention	Interruption	Fire	5	3	15 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	3	4	12 (2)
			Sabotage	5	2	10 (2)

ตารางที่ 3.55 ประเมินความเสี่ยงของ ศูนย์คอมพิวเตอร์

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	5	4	20 (1)
			User not intent to Destroy	5	4	20 (1)
			User Intent to Destroy	5	4	20 (1)
Physical	Disrepair	Interruption	Lose	5	4	20 (1)
Natural Incident	Poor Prevention	Interruption	Fire	5	3	15 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	3	4	12 (2)
			Sabotage	5	2	10 (2)

ตารางที่ 3.56 ประเมินความเสี่ยงของ DB/File Server ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.57 ประเมินความเสี่ยงของ Application Server ระบบงานหลัก

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.58 ประเมินความเสี่ยงของ DB/File Server ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.59 ประเมินความเสี่ยงของ Application Server ระบบงานสนับสนุน

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.60 ประเมินความเสี่ยงของ Mail Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.61 ประเมินความเสี่ยงของ Remote Access Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.62 ประเมินความเสี่ยงของ Web Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.63 ประเมินความเสี่ยงของ Domain Name Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.64 ประเมินความเสี่ยงของ Print Server

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.65 ประเมินความเสี่ยงของ Workstation

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.66 ประเมินความเสี่ยงของ Client

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.67 ประเมินความเสี่ยงของ ระบบงานหลัก Network Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.68 ประเมินความเสี่ยงของ ระบบงานสนับสนุน Network Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.69 ประเมินความเสี่ยงของ Backbone Network Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.70 ประเมินความเสี่ยงของ Client Network Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.71 ประเมินความเสี่ยงของ Computer Center Media

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.72 ประเมินความเสี่ยงของ Users Media

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.73 ประเมินความเสี่ยงของ Computer Center Furniture and Accommodations

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Fire	1	6	6 (2)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)

ตารางที่ 3.74 ประเมินความเสี่ยงของ Furniture and Accommodations

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Fire	1	6	6 (2)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)

ตารางที่ 3.75 ประเมินความเสี่ยงของ Computer Center Air Condition

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.76 ประเมินความเสี่ยงของ ระบบงานหลัก Power Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.77 ประเมินความเสี่ยงของ ระบบงานสนับสนุน Power Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	4	4	16 (1)
			User not intent to Destroy	4	4	16 (1)
			User Intent to Destroy	4	4	16 (1)
		Interception	Intruder intrude to Steal	4	4	16 (1)
			User Intent to Steal	4	4	16 (1)
		Modification	Intruder intrude to Configure	4	4	16 (1)
			User Intent to Configure	4	4	16 (1)
Physical	Disrepair	Interruption	Lose	4	4	16 (1)
Hardware	Miss Process	Interruption	Error or Hang	4	4	16 (1)
Software	Miss Process	Interruption	Be lost	4	4	16 (1)
Natural Incident	Poor Prevention	Interruption	Malicious Software	4	6	24 (1)
			Fire	4	3	12 (2)
			Earthquake	4	1	4 (3)
			Flood	1	4	4 (3)
			Power Supply Break	4	4	16 (1)
			Sabotage	4	2	8 (2)
		Interception	Malicious Software	4	6	24 (1)
		Modification	Malicious Software	4	6	24 (1)
		Fabrication	Malicious Software	4	6	24 (1)

ตารางที่ 3.78 ประเมินความเสี่ยงของ Client Power Equipment & Cable

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Physical Access Control	Interruption	Intruder intrude to Destroy	1	4	4 (3)
			User not intent to Destroy	1	4	4 (3)
			User Intent to Destroy	1	4	4 (3)
		Interception	Intruder intrude to Steal	1	4	4 (3)
			User Intent to Steal	1	4	4 (3)
		Modification	Intruder intrude to Configure	1	4	4 (3)
			User Intent to Configure	1	4	4 (3)
Physical	Disrepair	Interruption	Lose	1	4	4 (3)
Hardware	Miss Process	Interruption	Error or Hang	1	4	4 (3)
Software	Miss Process	Interruption	Be lost	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Malicious Software	1	6	6 (2)
			Fire	1	3	3 (3)
			Earthquake	1	1	1 (3)
			Flood	1	4	4 (3)
			Power Supply Break	1	4	4 (3)
			Sabotage	1	2	2 (3)
		Interception	Malicious Software	1	6	6 (2)
		Modification	Malicious Software	1	6	6 (2)
		Fabrication	Malicious Software	1	6	6 (2)

ตารางที่ 3.79 ประเมินความเสี่ยงของ Computer Center Electricity Supply

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	3	4	12 (2)

ตารางที่ 3.80 ประเมินความเสี่ยงของ Working Area Electricity Supply

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	2	4	8 (2)

ตารางที่ 3.81 ประเมินความเสี่ยงของ Computer Center Water Supply

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	2	4	8 (2)

ตารางที่ 3.82 ประเมินความเสี่ยงของ Working Area Water Supply

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	1	4	4 (3)

ตารางที่ 3.83 ประเมินความเสี่ยงของ Computer Center Air Condition

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	3	4	12 (2)

ตารางที่ 3.84 ประเมินความเสี่ยงของ Working Area Air Condition

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	1	4	4 (3)

ตารางที่ 3.85 ประเมินความเสี่ยงของ Computer Center Lighting

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	1	4	4 (3)

ตารางที่ 3.86 ประเมินความเสี่ยงของ Working Area Lighting

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	1	4	4 (3)

ตารางที่ 3.87 ประเมินความเสี่ยงของ Lease Line Service

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	3	4	12 (2)

ตารางที่ 3.88 ประเมินความเสี่ยงของ Internet Service

Type of Vul.	Vulnerabilities	Type of Threat	Threat	Impact	Prob.	Risk
Human	Poor Logical Access Control	Interception	Larceny	1	4	4 (3)
Natural Incident	Poor Prevention	Interruption	Down or Denied of Services	3	4	12 (2)

3.5 ความต้องการด้านความปลอดภัย

จากเกณฑ์การประเมินความเสี่ยงใน ตารางที่ 3.15 ได้กำหนดแบ่งค่าความเสี่ยงต่างๆ ออกเป็น 3 กลุ่ม คือ

- ความสำคัญลำดับ 1 (ดำเนินการจัดทำแผนรองรับ และควบคุมอย่างใกล้ชิด)
- ความสำคัญลำดับ 2 (ดำเนินการจัดทำแผนรองรับ)
- ความสำคัญลำดับ 3 (ไม่ต้องจัดทำแผนรองรับ)

ซึ่งการประเมินความเสี่ยงด้านความปลอดภัยระบบสารสนเทศของรายการทรัพย์สินต่างๆ นั้น สามารถนำมากำหนดความต้องการด้านความปลอดภัยต่างๆ จำแนกตามรายการทรัพย์สินต่างๆ ได้ดังนี้

3.5.1 ทรัพย์สินประเภทข้อมูล

ตารางที่ 3.89 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับที่สุด)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.90 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับมาก)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.91 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานหลัก (ลับ)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.92 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.93 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับที่สุด)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.94 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับมาก)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.95 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับ)

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.96 ความต้องการความปลอดภัยของ ข้อมูลปฏิบัติงานระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.97 ความต้องการความปลอดภัยของ ข้อมูลประชาสัมพันธ์ภายในหน่วยงาน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

ตารางที่ 3.98 ความต้องการความปลอดภัยของ ข้อมูลประชาสัมพันธ์ทั่วไป

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Backup	1
4.	Encryption on Communications	1
5.	Malicious Scan Software	1

3.5.2 ทรัพย์สินประเภทซอฟต์แวร์

ตารางที่ 3.99 ความต้องการความปลอดภัยของ OS DB/File Server ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.100 ความต้องการความปลอดภัยของ OS Application Server ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.101 ความต้องการความปลอดภัยของ OS DB/File Server ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.102 ความต้องการความปลอดภัยของ OS Application Server ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.103 ความต้องการความปลอดภัยของ OS Mail Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.104 ความต้องการความปลอดภัยของ OS Remote Access Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.105 ความต้องการความปลอดภัยของ OS Web Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.106 ความต้องการความปลอดภัยของ OS Domain Name Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.107 ความต้องการความปลอดภัยของ OS Print Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.108 ความต้องการความปลอดภัยของ OS Workstation

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.109 ความต้องการความปลอดภัยของ OS Client

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.110 ความต้องการความปลอดภัยของ DBMS ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.111 ความต้องการความปลอดภัยของ Application ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.112 ความต้องการความปลอดภัยของ DBMS ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.113 ความต้องการความปลอดภัยของ Application ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.114 ความต้องการความปลอดภัยของ Mail Server Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.115 ความต้องการความปลอดภัยของ Remote Access Server Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.116 ความต้องการความปลอดภัยของ Web Server Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.117 ความต้องการความปลอดภัยของ Domain Name Server Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	1
2.	Policy	1
3.	Reserve Software	1
4.	Malicious Scan Software	1

ตารางที่ 3.118 ความต้องการความปลอดภัยของ Print Server Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.119 ความต้องการความปลอดภัยของ Workstation Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.120 ความต้องการความปลอดภัยของ Client Application

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.121 ความต้องการความปลอดภัยของ Management Tools

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.122 ความต้องการความปลอดภัยของ Development Tools

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.123 ความต้องการความปลอดภัยของ Server Utility

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

ตารางที่ 3.124 ความต้องการความปลอดภัยของ Client Utility

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	2
2.	Policy	2
3.	Reserve Software	2
4.	Malicious Scan Software	2

3.5.3 ทรัพย์สินประเภทภายภาพ

ตารางที่ 3.125 ความต้องการความปลอดภัยของ สถานที่ กองตำรวจสันติบาล 1

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	2
7.	Disaster Plan	2

ตารางที่ 3.126 ความต้องการความปลอดภัยของ อาคาร กองตำรวจสันติบาล 1

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	2
7.	Disaster Plan	2

ตารางที่ 3.127 ความต้องการความปลอดภัยของ อาคาร ศูนย์คอมพิวเตอร์

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	2
7.	Disaster Plan	2

ตารางที่ 3.128 ความต้องการความปลอดภัยของ ศูนย์คอมพิวเตอร์

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	2
7.	Disaster Plan	2

ตารางที่ 3.129 ความต้องการความปลอดภัยของ DB/File Server ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.130 ความต้องการความปลอดภัยของ Application Server ระบบงานหลัก

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.131 ความต้องการความปลอดภัยของ DB/File Server ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.132 ความต้องการความปลอดภัยของ Application Server ระบบงานสนับสนุน

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.133 ความต้องการความปลอดภัยของ Mail Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.134 ความต้องการความปลอดภัยของ Remote Access Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.135 ความต้องการความปลอดภัยของ Web Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.136 ความต้องการความปลอดภัยของ Domain Name Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.137 ความต้องการความปลอดภัยของ Print Server

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

ตารางที่ 3.138 ความต้องการความปลอดภัยของ Workstation

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

ตารางที่ 3.139 ความต้องการความปลอดภัยของ Client

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

ตารางที่ 3.140 ความต้องการความปลอดภัยของ ระบบงานหลัก Network Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.141 ความต้องการความปลอดภัยของ ระบบงานสนับสนุน Network Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Backup or Reserve	1
3.	Maintenances	1
4.	Scan Malicious Software	1
5.	Fire Protection	2
6.	UPS and Generator	1
7.	Disaster Plan	2

ตารางที่ 3.142 ความต้องการความปลอดภัยของ Backbone Network Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.143 ความต้องการความปลอดภัยของ Client Network Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

ตารางที่ 3.144 ความต้องการความปลอดภัยของ Computer Center Media

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.145 ความต้องการความปลอดภัยของ Users Media

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

ตารางที่ 3.146 ความต้องการความปลอดภัยของ Computer Center Furniture and Accommodations

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	3
7.	Disaster Plan	3

ตารางที่ 3.147 ความต้องการความปลอดภัยของ Furniture and Accommodations

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Fire Detection, Fire Protection and Fire Extinction	2
6.	UPS and Generator	3
7.	Disaster Plan	3

ตารางที่ 3.148 ความต้องการความปลอดภัยของ Computer Center Air Condition

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.149 ความต้องการความปลอดภัยของ ระบบงานหลัก Power Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.150 ความต้องการความปลอดภัยของ ระบบงานสนับสนุน Power Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	1
2.	Policy	1
3.	Reserve Site or Hardware	1
4.	Maintenances	1
5.	Malicious Scan Software	1
6.	Fire Detection, Fire Protection and Fire Extinction	2
7.	UPS and Generator	1
8.	Disaster Plan	2

ตารางที่ 3.151 ความต้องการความปลอดภัยของ Client Power Equipment & Cable

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Physical Access Control	3
2.	Policy	3
3.	Reserve Site or Hardware	3
4.	Maintenances	3
5.	Malicious Scan Software	2
6.	Fire Detection, Fire Protection and Fire Extinction	3
7.	UPS and Generator	3
8.	Disaster Plan	3

3.5.4 ทรัพย์สินประเภทบริการ

ตารางที่ 3.152 ความต้องการความปลอดภัยของ Computer Center Electricity Supply

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

ตารางที่ 3.153 ความต้องการความปลอดภัยของ Working Area Electricity Supply

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

ตารางที่ 3.154 ความต้องการความปลอดภัยของ Computer Center Water Supply

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

ตารางที่ 3.155 ความต้องการความปลอดภัยของ Working Area Water Supply

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	3

ตารางที่ 3.156 ความต้องการความปลอดภัยของ Computer Center Air Condition

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

ตารางที่ 3.157 ความต้องการความปลอดภัยของ Working Area Air Condition

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	3

ตารางที่ 3.158 ความต้องการความปลอดภัยของ Computer Center Lighting

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	3

ตารางที่ 3.159 ความต้องการความปลอดภัยของ Working Area Lighting

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	3

ตารางที่ 3.160 ความต้องการความปลอดภัยของ Lease Line Service

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

ตารางที่ 3.161 ความต้องการความปลอดภัยของ Internet Service

ลำดับ	ความต้องการความปลอดภัย	ความสำคัญ
1.	Logical Access Control	3
2.	Reserve Services	2

บทที่ 4

การจัดการความปลอดภัยระบบสารสนเทศ

ในการจัดการความปลอดภัยระบบสารสนเทศของ กองตำรวจสันติบาล 1 นั้นได้อิงมาตรฐาน ISO/IEC 17799:2000 ซึ่งเป็นมาตรฐานด้านการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ เป็นแนวทางในการกำหนดแนวทาง หรือมาตรการต่างๆ ในการรักษาความปลอดภัยระบบสารสนเทศ โดยสอดคล้องกับความต้องการด้านความปลอดภัยของ กองตำรวจสันติบาล 1 ที่ได้ประเมินวิเคราะห์ไว้ ซึ่งมีรายละเอียด ดังต่อไปนี้

4.1 ความปลอดภัยองค์กร

4.1.1 โครงสร้างองค์กรด้านความปลอดภัยระบบสารสนเทศ

ในการรักษาความปลอดภัยระบบสารสนเทศนั้น จำเป็นจะต้องมีการกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการรักษาความปลอดภัย สามารถกำหนดบทบาทและหน้าที่ความรับผิดชอบได้ดังนี้

4.1.1.1 หน่วยงานหรือผู้รับผิดชอบด้านความปลอดภัยระบบสารสนเทศ

4.1.1.1.1 คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Committee) มีหน้าที่ที่เกี่ยวข้องในด้านความปลอดภัยระบบสารสนเทศคือ เป็นผู้กำหนดนโยบาย และควบคุมการปฏิบัติให้เป็นไปตามนโยบายด้านความปลอดภัยที่กำหนด คณะกรรมการฯ ประกอบด้วยส่วนต่างๆ ดังต่อไปนี้

- หัวหน้าหน่วยงาน (Superintendent) จาก ฝ่ายอำนวยการ, ศูนย์ปฏิบัติการข่าว, ศูนย์วิทยุเอกภพ และ กองกำกับการ 1-5 เป็นคณะกรรมการ
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Manager) เป็นคณะกรรมการ
- ที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Advisor) เป็น ที่ปรึกษาให้คำปรึกษาด้านความปลอดภัยต่างๆ

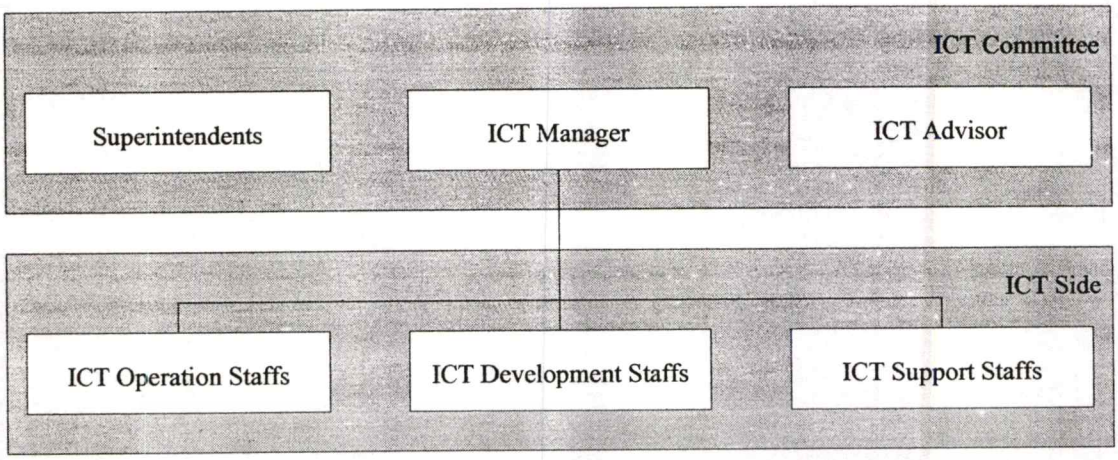
ภาพที่ 4.1 แสดงผังโครงสร้างคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

4.1.1.1.2 ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร

ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Side) การปฏิบัติการต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศและการสื่อสารให้มีความปลอดภัย พร้อมทั้งประสานงานด้านความปลอดภัยระบบสารสนเทศระหว่างหน่วยงานๆ และองค์กรต่างๆ ที่เกี่ยวข้อง โดยสามารถแบ่งหน้าที่ความรับผิดชอบได้ดังนี้

- เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (ICT Operation Staffs) มีหน้าที่ในการดำเนินการควบคุมการปฏิบัติการต่างๆ ให้เกิดความปลอดภัย
- เจ้าหน้าที่พัฒนาระบบ (ICT Development Staffs) มีหน้าที่ในการศึกษา วิเคราะห์พัฒนาระบบให้มีความปลอดภัย
- เจ้าหน้าที่สนับสนุน (ICT Support Staffs) มีหน้าที่ในการช่วยเหลือและให้บริการต่างๆ กับผู้ใช้งานระบบให้เกิดความปลอดภัย

ภาพที่ 4.2 แสดงผังโครงสร้างฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร



ภาพที่ 4.3 แสดงการจัดโครงสร้างองค์กรด้านความปลอดภัย

4.1.2 การเข้าถึงจากบุคคลภายนอก

การรักษาความปลอดภัยจากการเข้าถึงจากบุคคลภายนอก นั้นจะต้องมีการกำหนดเหตุผลความจำเป็นในการเข้าถึง (Reasons for Access) รูปแบบวิธีการเข้าถึง (Type of Access) กำหนดผู้ตัวผู้ติดต่อประสานงานของหน่วยงาน (On-site Contractor) รวมถึงข้อกำหนดความต้องการในการติดต่อประสานงานของบุคคลภายนอก (Security requirement in third party) โดยการกำหนดเป็นข้อกำหนด ข้อตกลง หรือสัญญา

4.1.3 การจ้าง

ในการจ้าง(Outsourcing) เพื่อดำเนินการเกี่ยวกับระบบสารสนเทศนั้นจะต้องมีการกำหนดความต้องการในด้านความปลอดภัยของการจ้าง และจะต้องมีการจัดทำข้อตกลงหรือสัญญาต่างๆ ในการดำเนินการของบุคคลภายนอกที่รับจ้างมาดำเนินการต่างๆ

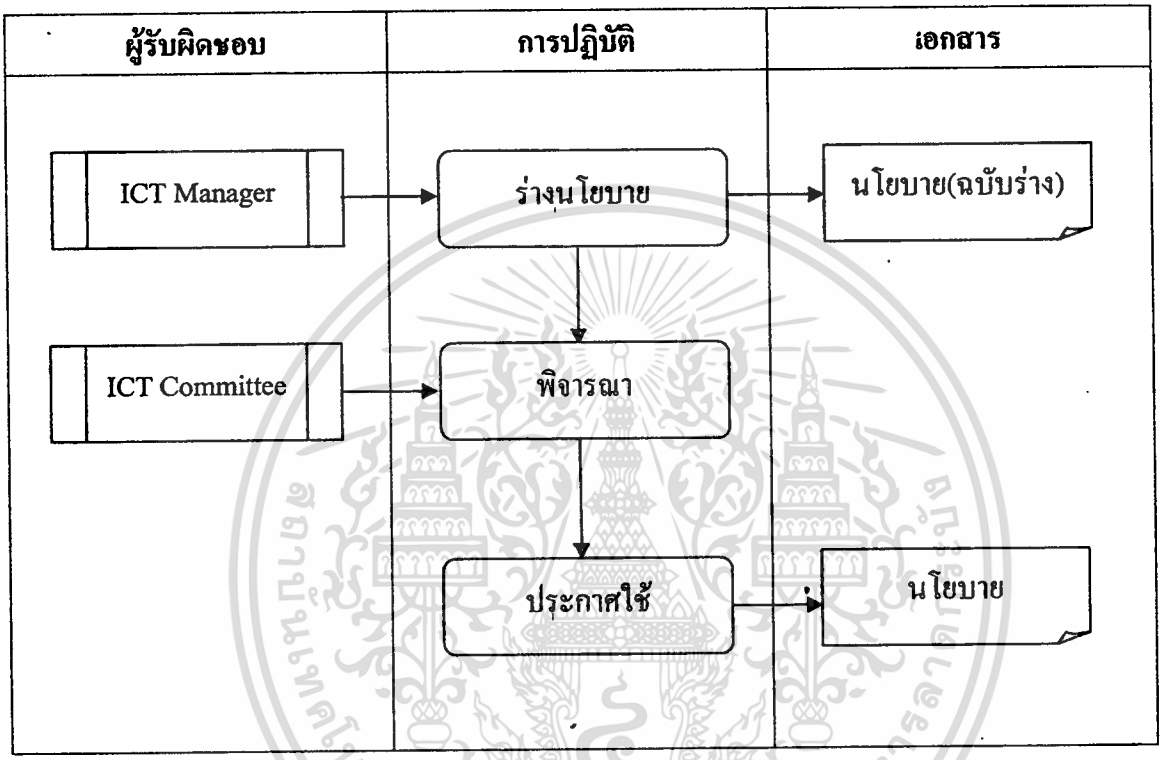
4.2 นโยบายความปลอดภัย

นโยบายความปลอดภัยสำหรับเป็นเครื่องมือในการบริหารจัดการควบคุมการดำเนินการต่างๆ ให้เป็นไปตามแนวทางหรือมาตรฐานเดียวกัน เป็นส่วนช่วยให้เกิดความชัดเจนในการปฏิบัติต่างๆ เพื่อการรักษาความปลอดภัยระบบสารสนเทศ ซึ่งการจัดการเกี่ยวกับนโยบายความปลอดภัยนั้นเริ่มตั้งแต่การสร้างหรือจัดทำนโยบายความปลอดภัย และการปรับปรุงนโยบายความปลอดภัยให้มีความสมบูรณ์ครบถ้วน สอดคล้องกับสถานการณ์ปัจจุบันอย่างสม่ำเสมอ ซึ่งการดำเนินการดังกล่าวมีขั้นตอนดังต่อไปนี้

4.2.1 ขั้นตอนการสร้างนโยบายความปลอดภัย

4.2.1.1 หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารร่างนโยบาย

4.2.1.2 นำร่างนโยบายเข้าที่ประชุมคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อพิจารณาและประกาศใช้



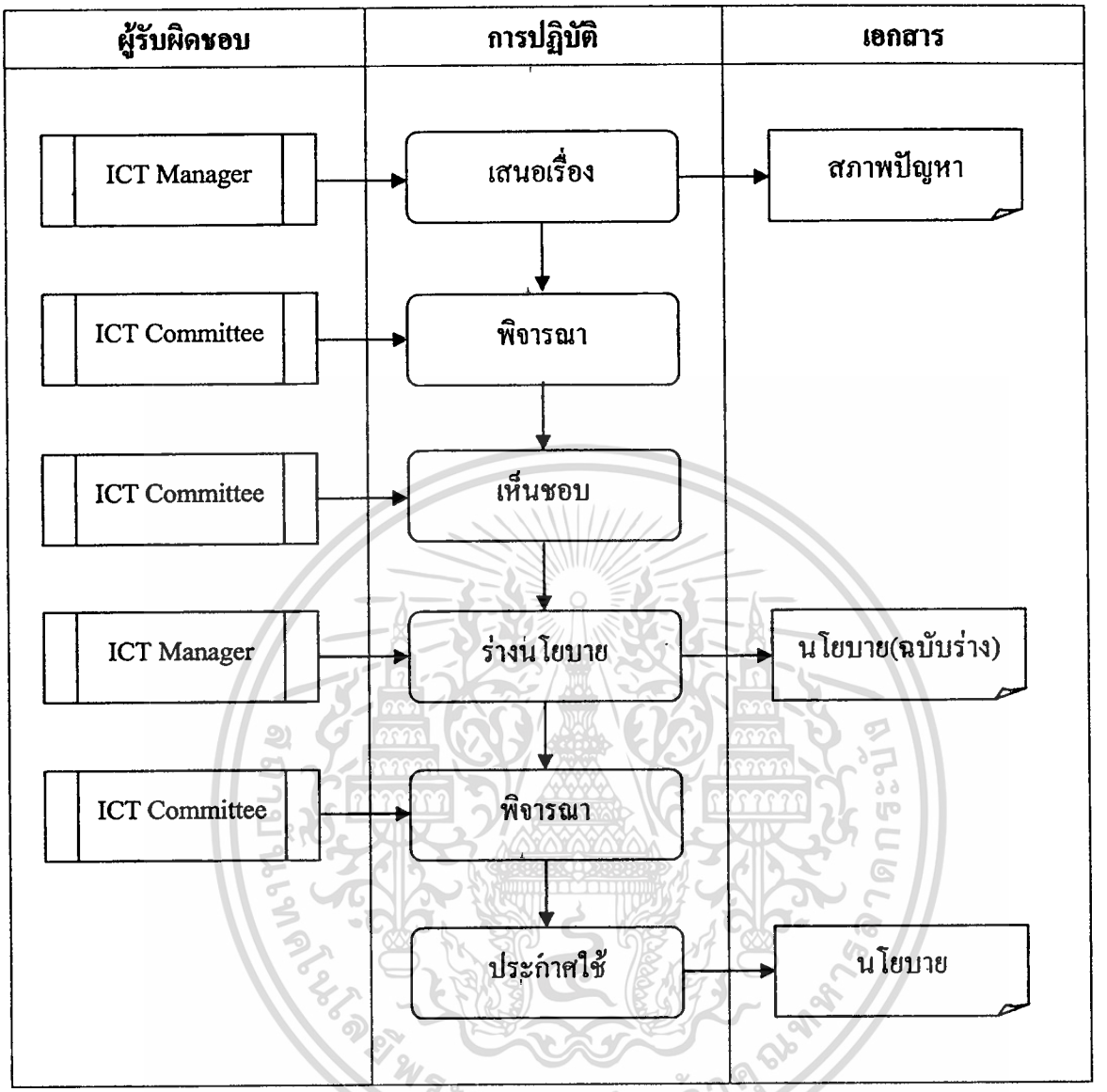
ภาพที่ 4.4 ขั้นตอนการสร้างนโยบายความปลอดภัย

4.2.2 ขั้นตอนการปรับปรุงนโยบายความปลอดภัย

4.2.2.1 เมื่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร เห็นสมควรที่จะปรับปรุงนโยบาย ให้นำเรื่องเข้าที่ประชุมคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อพิจารณาให้ความเป็นชอบในการปรับปรุงนโยบาย

4.2.2.2 เมื่อที่ประชุมเห็นชอบในการปรับปรุงนโยบายแล้ว หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารดำเนินการร่างนโยบายฉบับปรับปรุง

4.2.2.3 นำร่างนโยบายฉบับปรับปรุงเข้าที่ประชุมคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารเพื่อพิจารณาประกาศใช้และยกเลิกฉบับเดิม



ภาพที่ 4.5 ขั้นตอนการปรับปรุงนโยบายความปลอดภัย

4.2.3 นโยบายความปลอดภัยระบบสารสนเทศของกองตำรวจสันติบาล1

นโยบายความปลอดภัยระบบสารสนเทศนั้นจะต้องกำหนดรายละเอียดแนวทางปฏิบัติต่างๆ ดังต่อไปนี้

- กล่าวนำหรือความเป็นมาเป้าหมายในการรักษาความปลอดภัย
- คำนิยามความหมาย
- กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

- ข้อปฏิบัติของพนักงานในการใช้งานเครือข่ายคอมพิวเตอร์
- ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

โดยนโยบายความระบบสารสนเทศของกองตำรวจสันติบาล 1 นั้นมีรายละเอียดตาม ภาคผนวก ก.

4.3 การแบ่งประเภทสินทรัพย์และการควบคุม

ในการรักษาความปลอดภัยระบบสารสนเทศนั้น เพื่อความสะดวกและปกป้องทรัพย์สินต่างๆ ให้มีความปลอดภัยนั้น จำเป็นต้องมีการแบ่งแยกประเภททรัพย์สิน เพื่อที่จะกำหนดมาตรการในการควบคุมความปลอดภัยได้อย่างมีประสิทธิภาพ ซึ่งการแบ่งแยกประเภททรัพย์สินนั้นแบ่งออกเป็น 4 ประเภท คือ ข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์ และบริการ

นอกจากนี้ รายการทรัพย์สินต่างๆ จำเป็นจะต้องมีการกำหนดผู้ดูแลรับผิดชอบด้านความปลอดภัย และสถานที่ตั้ง ของทรัพย์สินต่างๆ ซึ่งรายละเอียดรายการทรัพย์สินแต่ละประเภทมีดังนี้

ตารางที่ 4.1 รายการทรัพย์สินประเภทข้อมูล (Information Assets)

ลำดับ	รายการ	ผู้ดูแลรับผิดชอบ	สถานที่ตั้ง
1.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับที่สุด)	ICT Operation Staffs	Computer Center
2.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับมาก)	ICT Operation Staffs	Computer Center
3.	ข้อมูลปฏิบัติงานระบบงานหลัก (ลับ)	ICT Operation Staffs	Computer Center
4.	ข้อมูลปฏิบัติงานระบบงานหลัก	ICT Operation Staffs	Computer Center
5.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับที่สุด)	ICT Operation Staffs	Computer Center
6.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับมาก)	ICT Operation Staffs	Computer Center
7.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน (ลับ)	ICT Operation Staffs	Computer Center
8.	ข้อมูลปฏิบัติงานระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
9.	ข้อมูลประชาสัมพันธ์ภายในหน่วยงาน	ICT Operation Staffs	Computer Center
10.	ข้อมูลประชาสัมพันธ์ทั่วไป	ICT Operation Staffs	Computer Center

ตารางที่ 4.2 รายการทรัพย์สินประเภทซอฟต์แวร์ (Software Assets)

ลำดับ	รายการ	ผู้ดูแลรับผิดชอบ	สถานที่ตั้ง
1.	OS DB/File Server ระบบงานหลัก	ICT Operation Staffs	Computer Center
2.	OS Application Server ระบบงานหลัก	ICT Operation Staffs	Computer Center
3.	OS DB/File Server ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
4.	OS Application Server ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
5.	OS Mail Server	ICT Operation Staffs	Computer Center
6.	OS Remote Access Server	ICT Operation Staffs	Computer Center
7.	OS Web Server	ICT Operation Staffs	Computer Center
8.	OS Domain Name Server	ICT Operation Staffs	Computer Center
9.	OS Print Server	Power Users	Working Area
10.	OS Workstation	ICT Operation Staffs	Computer Center
11.	OS Client	Users	Working Area
12.	DBMS ระบบงานหลัก	ICT Operation Staffs	Computer Center
13.	Application ระบบงานหลัก	ICT Operation Staffs	Computer Center
14.	DBMS ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
15.	Application ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
16.	Mail Server Application	ICT Operation Staffs	Computer Center
17.	Remote Access Server Application	ICT Operation Staffs	Computer Center
18.	Web Server Application	ICT Operation Staffs	Computer Center
19.	Domain Name Server Application	ICT Operation Staffs	Computer Center
20.	Print Server Application	Power Users	Working Area
21.	Workstation Application	ICT Operation Staffs	Computer Center
22.	Client Application	Users	Working Area
23.	Management Tools	ICT Operation Staffs	Computer Center
24.	Development Tools	Development Staffs	Computer Center
25.	Server Utility	ICT Operation Staffs	Computer Center
26.	Client Utility	Users	Working Area

ตารางที่ 4.3 รายการทรัพย์สินประเภทกายภาพ (Physical Assets)

ลำดับ	รายการ	ผู้ดูแลรับผิดชอบ	สถานที่ตั้ง
1.	สถานที่ กองตำรวจสันติบาล 1 (SB1 Area)	Guardedness	SB1 Area
2.	อาคาร กองตำรวจสันติบาล 1 (SB1 Buildings)	Guardedness	SB1 Building
3.	อาคาร ศูนย์คอมพิวเตอร์ (CC Building)	Guardedness	CC Building
4.	ศูนย์คอมพิวเตอร์ (Computer Center)	Guardedness	Computer Center
5.	DB/File Server ระบบงานหลัก	ICT Operation Staffs	Computer Center
6.	Application Server ระบบงานหลัก	ICT Operation Staffs	Computer Center
7.	DB/File Server ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
8.	Application Server ระบบงานสนับสนุน	ICT Operation Staffs	Computer Center
9.	Mail Server	ICT Operation Staffs	Computer Center
10.	Remote Access Server	ICT Operation Staffs	Computer Center
11.	Web Server	ICT Operation Staffs	Computer Center
12.	Domain Name Server	ICT Operation Staffs	Computer Center
13.	Print Server	ICT Users	Working Area
14.	Workstation	ICT Operation Staffs	Computer Center
15.	Client	Users	Working Area
16.	ระบบงานหลัก Network Equipment & Cable	ICT Operation Staffs	Computer Center
17.	ระบบงานสนับสนุน Network Equipment&Cable	ICT Operation Staffs	Computer Center
18.	Backbone Network Equipment & Cable	ICT Operation Staffs	Computer Center
19.	Client Network Equipment & Cable	Users	Working Area
20.	Computer Center Media	ICT Operation Staffs	Computer Center
21.	Users Media	Users	Working Area
22.	Computer Center Furniture and Accommodations	ICT Operation Staffs	Computer Center
23.	Furniture and Accommodations	Users	Working Area
24.	Computer Center Air Condition	ICT Operation Staffs	Computer Center
25.	ระบบงานหลัก Power Equipment & Cable	ICT Operation Staffs	Computer Center
26.	ระบบงานสนับสนุน Power Equipment & Cable	ICT Operation Staffs	Computer Center
27.	Client Power Equipment & Cable	Users	Working Area

ตารางที่ 4.4 รายการทรัพย์สินประเภทบริการ (Services)

ลำดับ	รายการ	ผู้ดูแลรับผิดชอบ	สถานที่ตั้ง
1.	Computer Center Electricity Supply	ICT Operation Staffs	Computer Center
2.	Working Area Electricity Supply	Users	Working Area
3.	Computer Center Water Supply	ICT Operation Staffs	Computer Center
4.	Working Area Water Supply	Users	Working Area
5.	Computer Center Air Condition	ICT Operation Staffs	Computer Center
6.	Working Area Air Condition	Users	Working Area
7.	Computer Center Lighting	ICT Operation Staffs	Computer Center
8.	Working Area Lighting	Users	Working Area
9.	Lease Line Service	ICT Operation Staffs	Service Provider
10.	Internet Service	ICT Operation Staffs	Service Provider

สำหรับการควบคุมความปลอดภัยทรัพย์สินนั้น แบ่งออกเป็น

- Logical Access Controls สำหรับทรัพย์สินประเภทข้อมูล ซอฟต์แวร์ และบริการ
- Physical Access Controls สำหรับทรัพย์สินประเภทฮาร์ดแวร์

4.4 การจัดการความปลอดภัยเกี่ยวกับบุคคล

4.4.1 ความปลอดภัยในตำแหน่งหน้าที่และการทำงาน

ในการรักษาความปลอดภัยระบบสารสนเทศนั้น บุคคลเป็นปัจจัยหนึ่งที่ส่งผลกระทบต่อความปลอดภัยระบบสารสนเทศ ดังนั้นจึงจำเป็นต้องมีมาตรการในการจัดการความปลอดภัยที่อาจเกิดจากการกระทำของบุคคลอันเกี่ยวกับการตรวจสอบประวัติ ทำข้อตกลง กำหนดสิทธิ และยกเลิกสิทธิ

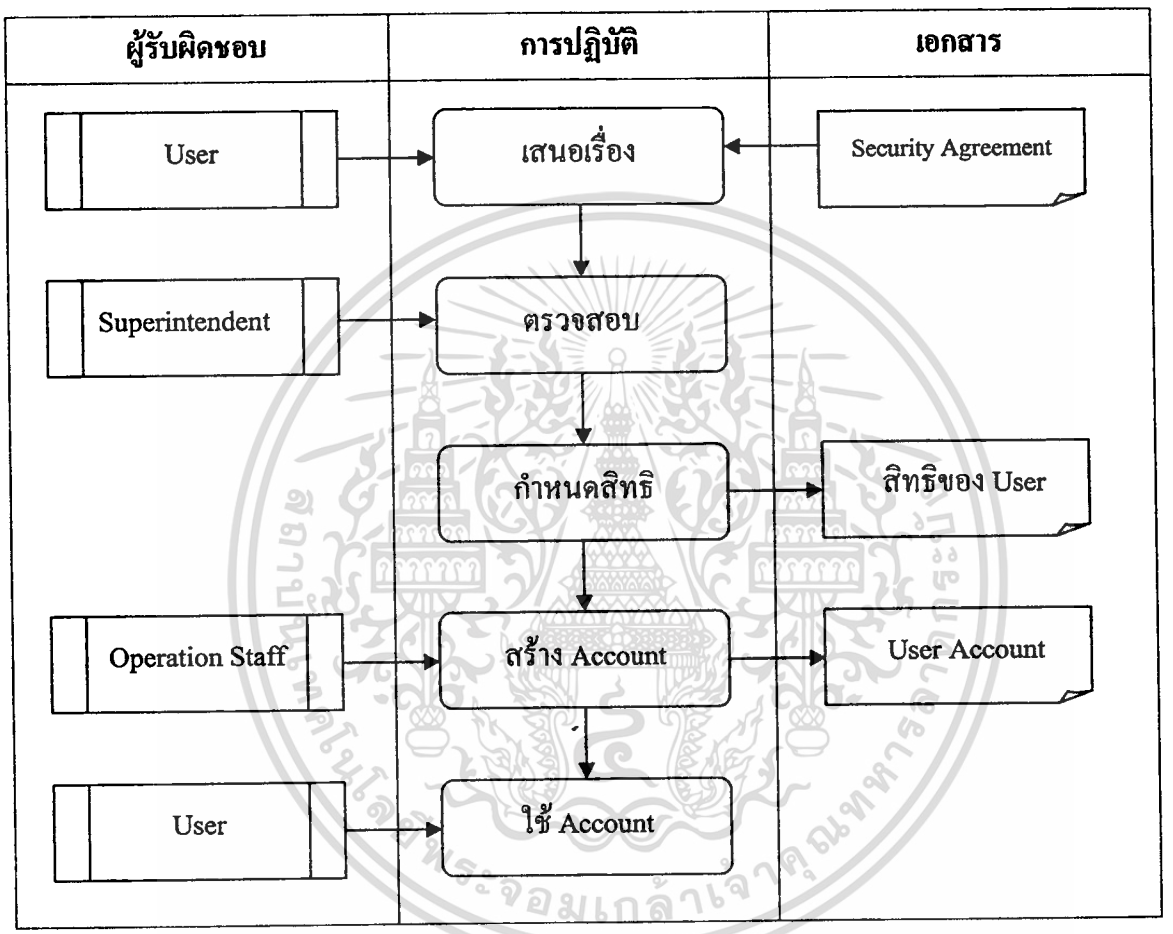
4.4.1.1 ขั้นตอนการให้สิทธิการทำงานในระบบ

4.4.1.1.1 เจ้าหน้าที่ลงนามในหนังสือข้อตกลงด้านความปลอดภัยตามระเบียบที่กำหนดและเสนอให้หัวหน้าของตนพิจารณา

4.4.1.1.2 หัวหน้าของเจ้าหน้าที่กำหนดสิทธิในการใช้งานทั้งนี้ไม่เกินสิทธิที่หัวหน้าได้รับ

4.4.1.1.3 หลังจากที่หัวหน้ากำหนดสิทธิแล้วดำเนินการส่งเรื่องให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ดำเนินการสร้าง Account สำหรับการใช้งานระบบ

4.4.1.1.4 เจ้าหน้าที่แจ้ง User Account ให้เจ้าหน้าที่ทราบเพื่อนำ Account ไปใช้



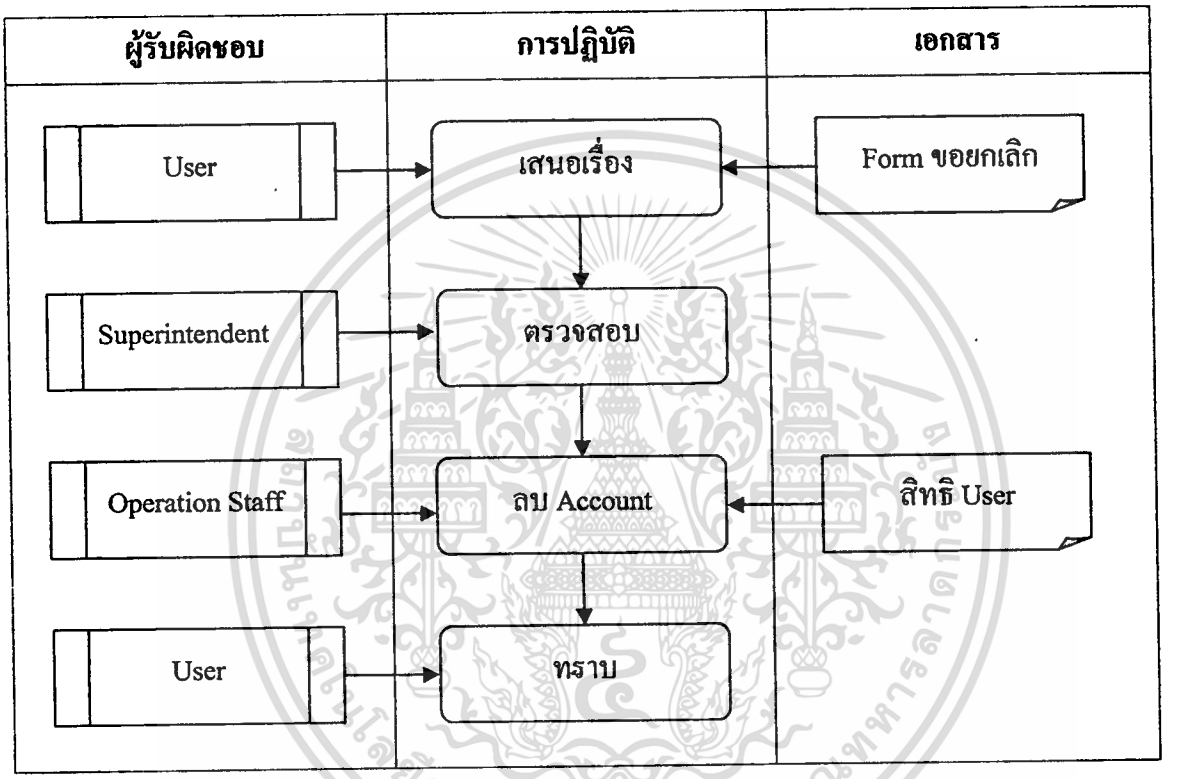
ภาพที่ 4.6 แสดงขั้นตอนการให้สิทธิการใช้งานระบบ

4.4.1.2 ขั้นตอนการยกเลิกสิทธิการทำงานในระบบ

4.4.1.2.1 เจ้าหน้าที่ทำเรื่องเพื่อขอยกเลิกการใช้งานระบบ เสนอหัวหน้าผู้รับผิดชอบ

4.4.1.2.2 หัวหน้าผู้รับผิดชอบตรวจสอบความถูกต้องแล้วส่งเรื่องไปยังเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (หัวหน้าสามารถเสนอเรื่องเพื่อยกเลิกสิทธิโดยไม่ต้องรับเรื่องจากเจ้าหน้าที่ก็ได้)

4.4.1.2.3 เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์รับเรื่องจากหัวหน้าผู้รับผิดชอบ แล้วดำเนินการลบAccount ของ User พร้อมทั้งแจ้งให้ User ทราบ (หากเกิดความผิดปกติเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์สามารถระงับสิทธิของ User ได้เพื่อป้องกันความปลอดภัยของระบบ และต้องแจ้งให้หัวหน้าผู้รับผิดชอบ และเจ้าหน้าที่ทราบ)



ภาพที่ 4.7 แสดงขั้นตอนการยกเลิกสิทธิการใช้งานระบบ

4.4.2 การอบรม

การอบรมเป็นการช่วยให้บุคลากรทราบและพึงระลึกถึงภัยคุกคามต่อระบบสารสนเทศพร้อมทั้งความรู้ในการป้องกัน และปฏิบัติเพื่อให้เกิดความปลอดภัย ซึ่งการอบรมนั้นจำเป็นจะต้องจัดอบรมให้สอดคล้องกับภารกิจหน้าที่ความรับผิดชอบของบุคลากรแต่ละคน โดย กองตำรวจสันติบาล 1 จัดแบ่งประเภทบุคลากรสำหรับการฝึกอบรม และหลักสูตรการฝึกอบรบดังนี้

4.4.2.1 ผู้บริหาร

4.4.2.1.1 ความรู้พื้นฐานทั่วไปเกี่ยวกับความปลอดภัยระบบสารสนเทศ

4.4.2.1.2 การบริหารจัดการความปลอดภัยระบบสารสนเทศ

4.4.2.2 เจ้าหน้าที่ปฏิบัติงาน

4.4.2.2.1 ความรู้พื้นฐานทั่วไปเกี่ยวกับความปลอดภัยระบบสารสนเทศ

4.4.2.2.2 การปฏิบัติเมื่อเกิดเหตุการณ์ต่อความปลอดภัยระบบสารสนเทศต่างๆ

4.4.2.3 เจ้าหน้าปฏิบัติงานด้านระบบสารสนเทศ

4.4.2.3.1 ความรู้พื้นฐานทั่วไปเกี่ยวกับความปลอดภัยระบบสารสนเทศ

4.4.2.3.2 เทคโนโลยีด้านความปลอดภัยระบบสารสนเทศ

4.4.3 การปฏิบัติเมื่อเกิดเหตุการณ์ต่อความปลอดภัย

เหตุการณ์ต่างๆ ที่อาจเกิดขึ้นและมีผลต่อความปลอดภัยระบบสารสนเทศ เช่น อัคคีภัย วาตภัย อุทกภัย แผ่นดินไหว ระบบกระแสไฟฟ้าขัดข้อง หรือเหตุการณ์หายนะต่างๆ นั้น จำเป็นจะต้องมีการซักซ้อมการปฏิบัติเมื่อเกิดเหตุ เพื่อเมื่อเกิดเหตุการณ์จริงจะสามารถปฏิบัติได้อย่างถูกต้อง ช่วยลดความเสียหายลงได้

4.5 การควบคุมทางกายภาพ และสภาพแวดล้อม

การรักษาความปลอดภัยทางการภาพเป็นสิ่งที่สำคัญในการป้องกันทรัพย์สินและระบบสารสนเทศทางกายให้มีความปลอดภัย เนื่องจากข้อมูลและอุปกรณ์ต่างๆ จะต้องทำงานบนอุปกรณ์และสถานที่ ดังนั้นจึงจำเป็นจะต้องมีการควบคุมความปลอดภัยทางกายภาพ ซึ่งจากการวิเคราะห์ความเสี่ยงนั้น จำเป็นที่จะต้องปกป้องทรัพยากรด้านฮาร์ดแวร์ซึ่งอยู่ในศูนย์คอมพิวเตอร์ ซึ่งประกอบด้วยส่วนต่างๆ ดังนี้

4.5.1 สถานที่ตั้งและสภาพของศูนย์คอมพิวเตอร์

4.5.1.1 อยู่ห่างจากวัตถุหรือสถานที่ที่อาจก่อให้เกิดความเสียหายต่อระบบ เช่น ระบบทำความร้อน สถานที่เก็บวัตถุไวไฟ วัตถุระเบิด

4.5.1.2 ไม่อยู่ใกล้โรงงานก่อมลพิษและฝุ่น

4.5.1.3 ห่างจากบริเวณพลุกพล่าน ทางเดิน/ประตูทางเข้าหลัก

4.5.1.4 ตั้งอยู่บริเวณที่ปลอดภัยจากภัยของน้ำ เช่น บริเวณที่น้ำท่วมไม่ถึง

4.5.1.5 ผนังและเพดานป้องกันการรั่วซึมของน้ำ

4.5.1.6 มีระบบกำจัดของเหลวที่เกิดขึ้นได้อย่างรวดเร็ว

4.5.2 การป้องกันความปลอดภัยของอุปกรณ์คอมพิวเตอร์

4.5.2.1 ทำเครื่องหมายที่ตัวอุปกรณ์

4.5.2.2 ติดตั้งอุปกรณ์กับเฟอร์นิเจอร์ พื้น หรือผนัง ที่แข็งแรง ด้วยวิธีที่เหมาะสม

4.5.2.3 ติดตั้งอุปกรณ์ในสถานที่ที่ปลอดภัยเป็นสัดส่วน

4.5.2.4 ใช้อุปกรณ์ในการป้องกันการเคลื่อนย้ายอุปกรณ์ต่างๆ

4.5.2.5 ใช้อุปกรณ์เตือนภัยในการเคลื่อนย้ายอุปกรณ์

4.5.3 การควบคุมการเข้าถึง

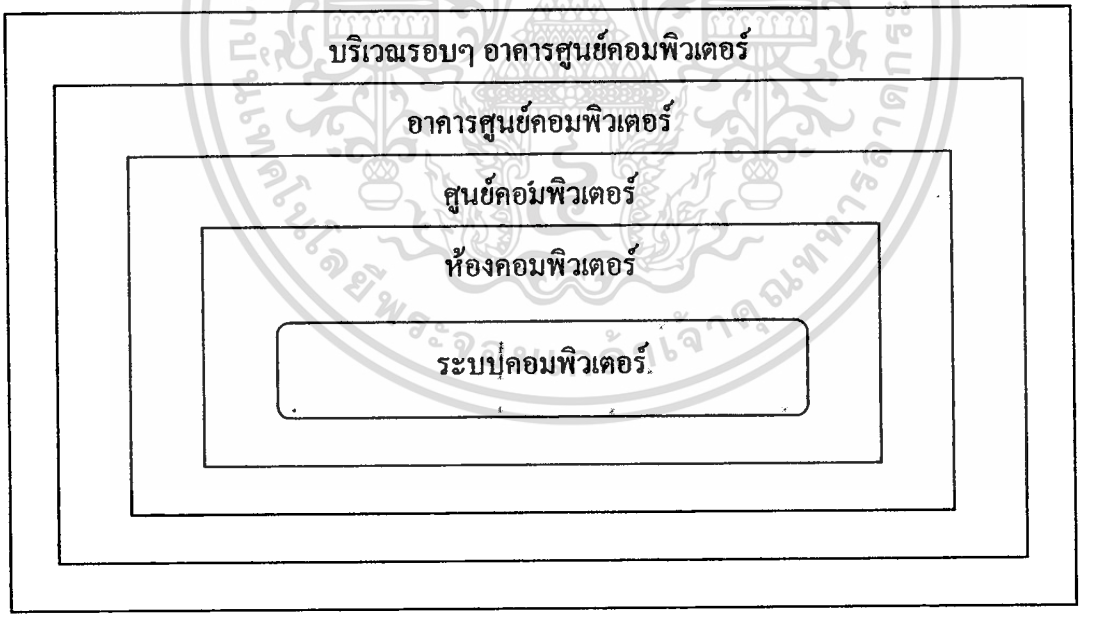
4.5.3.1 จำกัดการใช้อาคารสถานที่เฉพาะผู้ที่มีส่วนเกี่ยวข้องเท่านั้น

4.5.3.2 ใช้เครื่องกั้นทาง เพื่อควบคุมจุดเข้าออก

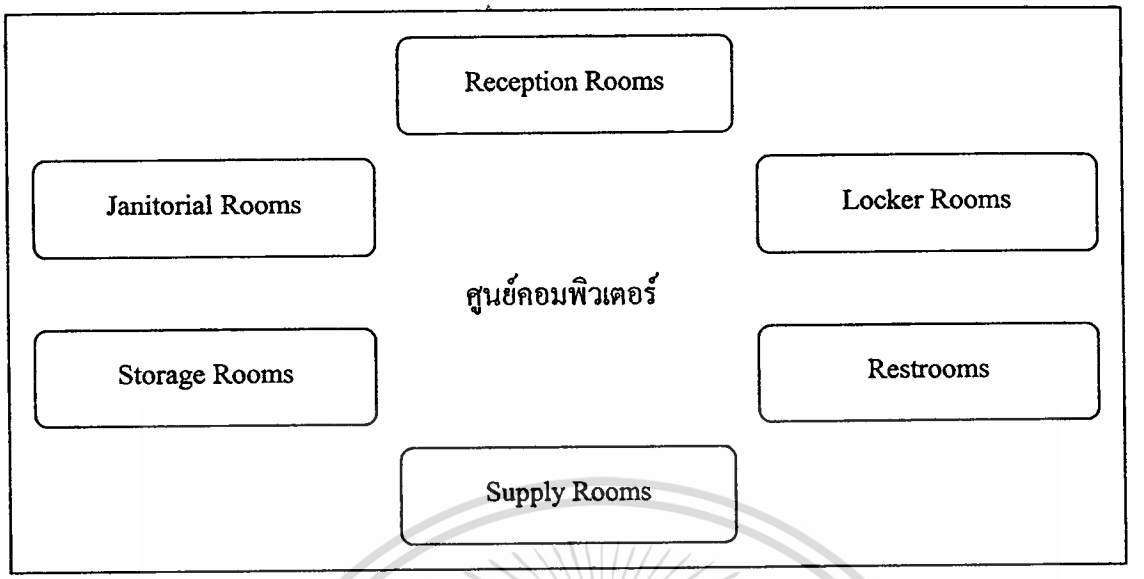
4.5.3.3 มีเจ้าหน้าที่ยามรักษาความปลอดภัยตลอด 24 ชั่วโมง

4.5.3.4 มีระบบกล้องโทรทัศน์วงจรปิด เพื่อบันทึกและเฝ้าดูความเคลื่อนไหวต่างๆ

4.5.3.5 มีระบบสัญญาณเตือนภัยผู้บุกรุก



ภาพที่ 4.6 แสดงชั้นการป้องกันระบบคอมพิวเตอร์



ภาพที่ 4.7 แสดงเขตพื้นที่รักษาความปลอดภัยบริเวณศูนย์คอมพิวเตอร์

4.5.4 ระบบปรับอากาศ

4.5.4.1 เป็นระบบปรับอากาศแยกส่วนจากระบบอื่น

4.5.4.2 ระบบปรับอากาศสามารให้ความเย็นพื้นที่ให้บริการและสำนักงานที่อยู่บริเวณข้างเคียงได้ เพื่อให้การปฏิบัติการดำเนินต่ไป

4.5.4.3 เชื่อมโยงกับระบบตรวจจับความร้อนและควันไฟ และระบบดับเพลิง

4.5.5 ระบบจ่ายกำลังไฟฟ้า

4.5.5.1 ติดตั้งระบบจ่ายไฟฟ้าสำรอง (UPS)

4.5.5.2 ติดตั้งระบบจ่ายไฟฟ้าฉุกเฉิน เพื่อส่องสว่างพื้นที่ปฏิบัติงานที่จำเป็น เช่น ทางเดิน บริเวณทางขึ้นลงบันได ฯลฯ

4.5.6 ระบบป้องกันและระงับอัคคีภัย

4.5.6.1 มีอุปกรณ์ในการระงับอัคคีภัยอย่างเพียงพอ

4.5.6.2 มีระบบตรวจจับความร้อน และระบบดับเพลิงอัตโนมัติ

4.6 การจัดการการปฏิบัติการและการติดต่อสื่อสาร

4.6.1 การปฏิบัติงานและความรับผิดชอบ

ในการปฏิบัติทั้งผู้ใช้และผู้ดูแลระบบจำเป็นจะต้องมีระเบียบ และวิธีการปฏิบัติงานต่างๆ พร้อมทั้งการตรวจสอบและแก้ไขสิ่งต่างๆ เพื่อให้เกิดความปลอดภัย ซึ่ง

ได้แก่ ขั้นตอนในการปฏิบัติงานทั่วไป ขั้นตอนการปฏิบัติเมื่อเกิดการเปลี่ยนแปลงสิ่งต่างๆ ขั้นตอนในการตรวจพบ รายงานแหตุการณ์ต่อความปลอดภัย การปฏิบัติเพื่อลดความเสี่ยงหรือความเสียหายที่เกิดขึ้น

4.6.2 การวางแผนและการรับระบบ

ในการพัฒนาระบบหรือบำรุงรักษาระบบนั้นจำเป็นจะต้องมีการวางแผนในการพัฒนาระบบถึงขั้นตอนการดำเนินการต่างๆ เพื่อให้ระบบที่พัฒนาหรือทำการบำรุงรักษานั้นมีความปลอดภัย โดยการกำหนดข้อยอมรับระบบ

4.6.3 การป้องกันซอฟต์แวร์ประสงค์ร้าย

ซอฟต์แวร์ประสงค์ร้ายต่างๆ เกิดขึ้นอยู่ตลอดเวลา และสามารถโจมตีหรือทำลายระบบได้ทุกเมื่อดังนั้นจึงจำเป็นจะต้องมีระบบในการตรวจสอบ ป้องกัน และกำจัดซอฟต์แวร์ประสงค์ร้ายต่างๆ

4.6.4 การดูแลรักษา

การบำรุงดูแลรักษาระบบนั้นจะเป็นที่จะต้องมีการสำรองข้อมูล ฮาร์ดแวร์ ซอฟแวร์และบริการต่างๆ สำหรับเมื่อเวลาเกิดปัญหาจะได้นำมาใช้ได้ นอกจากนี้จะต้องมีการเก็บข้อมูลการปฏิบัติงาน และข้อผิดพลาดต่างๆ สำหรับวินิจฉัยในการแก้ไขปัญหา

4.6.5 การจัดการเครือข่าย

ระบบเครือข่ายนั้นมีความสำคัญมากในการปฏิบัติงาน จึงจำเป็นต้องมีการการตรวจสอบควบคุม และจัดการเครือข่ายเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา

4.6.6 การจัดเก็บสื่อบันทึกและความปลอดภัย

สื่อบันทึกข้อมูลต่างๆ นั้นจำเป็นจะต้องมีการบริหารจัดการ เช่น การใช้งาน การทิ้งหรือทำลายสื่อ เพื่อให้ข้อมูลที่ถูกจัดเก็บและถูกทำลายนั้นมีความปลอดภัย

4.6.7 การแลกเปลี่ยนข้อมูลและซอฟต์แวร์

การแลกเปลี่ยนข้อมูลและซอฟต์แวร์นั้น จะต้องมีการกำหนดมาตรการ และใช้เทคโนโลยีในการควบคุมการปฏิบัติในการแลกเปลี่ยนข้อมูลทั้งภายในองค์กร และระหว่างองค์กร ให้มีความปลอดภัย อันได้แก่ การป้องกันการสูญหาย ดัดแปลง หรือนำไปใช้ในทางที่ผิดกฎ ระเบียบ ข้อบังคับหรือกฎหมาย

4.7 การควบคุมการเข้าถึง

4.7.1 ความต้องการในการควบคุมการเข้าถึง

การเข้าถึงระบบสารสนเทศ นั้นจำเป็นจะต้องมีการกำหนดระเบียบนโยบายในการเข้าถึงข้อมูลหรือระบบสารสนเทศ เพื่อใช้เป็นแนวทางการในการปฏิบัติ เพื่อให้เกิดความปลอดภัยในการเข้าถึงข้อมูลและระบบสารสนเทศ

4.7.2 การจัดการการเข้าถึงของผู้ใช้

การเข้าถึงข้อมูลของผู้ใช้นั้นจะต้องมีการลงทะเบียนผู้ใช้ ซึ่งจำเป็นการอนุญาตสิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศต่างๆ โดยในการใช้งานระบบนั้นจะต้องมีการระบุตัว ตรวจสอบสิทธิ และให้สิทธิในการใช้งานระบบ นอกจากนี้สิทธิของผู้ใช้นั้นอาจมีการเปลี่ยนแปลงจำเป็นจะต้องมีการตรวจสอบ ทบทวนสิทธิของผู้ใช้งานอยู่ตลอดเวลาด้วย

4.7.3 ความรับผิดชอบของผู้ใช้

ผู้ใช้งานนั้นเมื่อมีสิทธิที่ในการเข้าถึงข้อมูลหรือระบบสารสนเทศแล้ว อาจมีการใช้สิทธิในทางที่ผิด หรือทำให้ข้อมูลหรือระบบสารสนเทศเสียหายโดยไม่เจตนาจึงเป็นที่จะต้องมีการกำหนดความรับผิดชอบต่อการกระทำของผู้ใช้ เพื่อเป็นการป้องกันมิให้ผู้ใช้ใช้สิทธิในทางที่ผิด และไม่ประมาทในการดำเนินการต่างๆ กับข้อมูลหรือระบบสารสนเทศ

4.7.4 การควบคุมการเข้าถึงเครือข่าย

การควบคุมการเข้าถึงเครือข่ายนั้นเป็นการปกป้องชั้นหนึ่งในการเข้าถึงข้อมูลและระบบสารสนเทศ ซึ่งการควบคุมการเข้าถึงเครือข่ายนั้น เป็นการตรวจสอบสิทธิในการเข้าถึงเครือข่ายเพื่อใช้งานข้อมูลหรือระบบสารสนเทศ

4.7.5 การควบคุมการเข้าถึงระบบปฏิบัติ

การควบคุมการเข้าถึงในระดับระบบปฏิบัติการเป็นการปกป้องชั้นหนึ่งในการเข้าถึงข้อมูลและระบบสารสนเทศ ซึ่งการควบคุมการเข้าถึงในระดับระบบปฏิบัติการนั้นจะเป็นการตรวจสอบสิทธิในการเข้าถึงเครื่องคอมพิวเตอร์ที่ใช้งาน

4.7.6 การควบคุมการเข้าถึงโปรแกรมประยุกต์

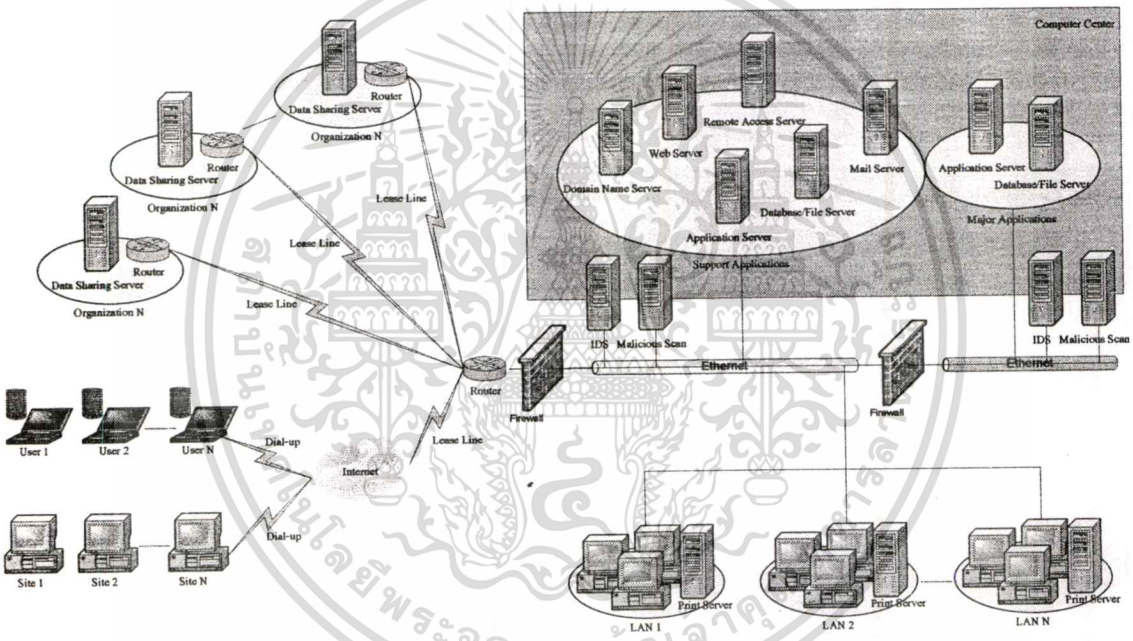
การควบคุมการเข้าถึงในระดับโปรแกรมประยุกต์เป็นการปกป้องชั้นหนึ่งในการเข้าถึงข้อมูลและระบบสารสนเทศ ซึ่งการควบคุมการเข้าถึงในระดับโปรแกรมประยุกต์นั้นจะเป็นการตรวจสอบสิทธิในการเข้าข้อมูลและระบบสารสนเทศ

4.7.7 ระบบการเฝ้าดูการเข้าถึงและการใช้งาน

ระบบการเฝ้าดูการการเข้าถึงและการใช้งาน เป็นการตรวจสอบกิจกรรมต่างๆ ในระบบสารสนเทศ ที่อาจมีผลกระทบต่อความปลอดภัยของข้อมูลและระบบสารสนเทศ

4.7.8 คอมพิวเตอร์พกพาและเครื่องมือสื่อสาร

ในการใช้งานคอมพิวเตอร์พกพาและเครื่องมือสื่อสารเพื่อเข้าเชื่อมต่อเข้าสู่ระบบสารสนเทศนั้นทั้งการเชื่อมต่อโดยตรงกับระบบ และการเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตนั้น จำเป็นจะต้องมีการกำหนดวิธีการปฏิบัติ และใช้เทคโนโลยีที่เหมาะสมในการเชื่อมต่อเข้าสู่ระบบ



ภาพที่ 4.8 แสดง Logical Access Controls

4.8 การพัฒนาและบำรุงรักษาระบบ

4.8.1 ความต้องการด้านความปลอดภัยของระบบ

ในการพัฒนาและบำรุงรักษาระบบนั้น จำเป็นจะต้องมีการกำหนดความต้องการด้านความปลอดภัย สำหรับใช้เป็นแนวทางในการพัฒนาและบำรุงรักษาระบบสารสนเทศให้มีความปลอดภัย

4.8.2 ความปลอดภัยในระบบงาน

ความปลอดภัยในระบบงาน นั้นจะต้องกำหนดแนวทางการปฏิบัติ เพื่อป้องกันการสูญหาย การเปลี่ยนแปลงแก้ไข หรือมีการนำข้อมูลในระบบงานมาใช้ในทางที่ผิด

4.8.3 การควบคุมการเข้ารหัส

การเข้ารหัสเป็นการรักษาความลับและความถูกต้องของข้อมูล พร้อมทั้งตรวจสอบสิทธิและให้สิทธิในการเข้าถึงข้อมูล

4.8.4 เอกสารความปลอดภัยระบบ

ในการพัฒนาระบบและบำรุงรักษาระบบจำเป็นต้องมีเอกสารคู่มือการใช้งาน ปรับตั้งค่าต่างๆ ของระบบ เพื่อการใช้งานระบบและบำรุงรักษาระบบได้อย่างถูกต้อง เกิดความปลอดภัย

4.8.5 ความปลอดภัยในการพัฒนาและสนับสนุนการทำงาน

ในการพัฒนาและปฏิบัติงานนั้นจำเป็นจะต้องมีส่วนสนับสนุนการปฏิบัติงานให้เป็นไปด้วยความปลอดภัยในข้อมูลและระบบสารสนเทศ

4.9 การจัดการอย่างต่อเนื่อง

เกณฑ์ในการจัดการอย่างต่อเนื่อง เป็นการดำเนินการในการตรวจสอบ ป้องกัน และแก้ไขสถานการณ์ต่างๆ ที่อาจก่อความเสียหายให้กับข้อมูลและระบบสารสนเทศ อันได้แก่การสำรองข้อมูล และการกู้ข้อมูลหรือระบบให้สามารถทำงานได้ตามปกติ ซึ่งสถานการณ์ต่างๆ จะมีสภาพการเกิด และแนวทางการระวังป้องกันระดับที่แตกต่างกันไป ดังนั้นจึงจำเป็นที่จะต้องมีการวางแผนในการปฏิบัติเมื่อเกิดเหตุการณ์ต่างๆ อันจะเป็นการป้องกัน หรือลดบรรเทาความเสียหายที่เกิดขึ้นได้ นอกจากนี้จำเป็นที่จะต้องมีการซักซ้อมการปฏิบัติจริง เพื่อเมื่อเกิดเหตุการณ์จะได้สามารถปฏิบัติได้อย่างถูกต้องมีประสิทธิภาพ

4.10 การนำไปใช้งาน

การวางแผนความปลอดภัยระบบสารสนเทศนั้น จะไม่เกิดประโยชน์หากไม่มีการนำไปใช้งานซึ่งการนำไปใช้งานนั้นสามารถกระทำได้โดยการประกาศใช้ เป็นเกณฑ์ ข้อกำหนด กฎระเบียบ ข้อบังคับ หรือกฎหมาย ในการปฏิบัติ นอกจากนี้ จำเป็นจะต้องมีการตรวจสอบและประเมินผลการปฏิบัติให้เป็นไปตามแผนที่กำหนด และสรุปผลการปฏิบัติเพื่อนำมาหาข้อผิดพลาดและปรับปรุงแผนให้สามารถรักษาความปลอดภัยได้ดียิ่งขึ้น

บทที่ 5
สรุป

5.1 ปัญหาอุปสรรคที่พบ

ในการศึกษาวิเคราะห์เพื่อจัดทำแผนความปลอดภัยเทคโนโลยีสารสนเทศนี้เนื่องจากระบบสารสนเทศปัจจุบันของกองตำรวจสันติบาล 1 ยังคงเป็นระบบสารสนเทศที่ยังไม่มีการประยุกต์ใช้ระบบสารสนเทศในการปฏิบัติงาน จึงทำให้การศึกษาวิเคราะห์ขาดความชัดเจนและไม่สามารถดำเนินการศึกษาวิเคราะห์ได้ในบางเรื่อง เนื่องจากมีในการศึกษาวิเคราะห์นั้นจะเป็นที่จะต้องมีการศึกษาวิเคราะห์ลงไปในรายละเอียด และค่อนข้างมีรายละเอียดหรือความเป็นไปได้ในแนวทางต่างๆ มากมาย จึงทำให้การศึกษาวิเคราะห์จัดทำแผนความปลอดภัยระบบสารสนเทศนี้เป็นการกำหนดแนวทางกว้างๆ ในการรักษาความปลอดภัยระบบสารสนเทศ

5.2 แนวทางการพัฒนาต่อไป

การรักษาความปลอดภัยระบบสารสนเทศ นั้นจะต้องพิจารณา และคำนึงถึงทุกส่วนของระบบทั้งด้านการบริหารจัดการ และการปฏิบัติการต่างๆ ของ อุปกรณ์คอมพิวเตอร์ โปรแกรมระบบ โปรแกรมประยุกต์ โปรแกรมจัดการฐานข้อมูล ระบบเครือข่าย และบุคคลที่เกี่ยวข้องกับระบบ โดยพิจารณาจากระบบที่มีอยู่ว่าเป็นอย่างไร มีจุดอ่อนตรงไหน มีความเสี่ยงเป็นเช่นไร แล้วจึงวิเคราะห์หาแนวทางหรือมาตรการในการป้องกันระบบให้มีความปลอดภัย อีกทั้งต้องมีการทบทวนการวิเคราะห์จุดอ่อน ความเสี่ยง และแนวทาง มาตรการต่างๆ อย่างสม่ำเสมอ

บรรณานุกรม

ทศพล กนกนุวัตร์. 2542. **How to Protect from Hackers เข้ารหัส ป้องกันระบบ.** กรุงเทพฯ: เอช.เอ็น. กรุ๊ป.

ธีรา ทานตวณิช. 2542. **Virtual Private Network.** [Online]. Available: http://www.vpn.th.com/VPN-concepts.htm

ปราการ โกลากุล. 2544. **ความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์ (Firewall).** [Online]. Available: http://www.thaicert.nectec.or.th/paper/firewall/fwbasics.php

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย. 2544. **ตัวอย่างระเบียบว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย.** [Online]. Available: http://thaicert.nectec.or.th/paper/basic/policy.php

Carlson T. 2001. **Information Security Management: Understanding ISO 17799.** n.p.: Lucent Technologies

Howard, J.D. and Thomas A.L. 2544. **คำศัพท์ที่เกี่ยวข้องกับ computer security และ intrusion detection.** แปลจาก A Common Language for Computer Security. โดย ปนิวัธน์ ทรัพย์รุ่งเรือง, พ.ต. [Online]. Available: http://thaicert.nectec.or.th/paper/basic/terms.htm

ISO/IEC 17799. 2000. **Information Technology – Code of practice for information security managemrnt.** [Online]. Available: http://www.iso.ch

Jack L.B., Jr. **Information Security Risk Assessment Practices of Leading Organizations.** [Online]. Available: http://www.gao.gov/special.pubs/ai00033.pdf

Jakub A.S. 2001. **The Project of Information Security System based on ISO 17799 regulations for AVET INS.** Master's Thesis carried out at the Faculty of Production Engineering, Warsaw University of Technology and Department of Production Economics, Linköping Institute of Technology

SANS Institute. 2544. **คำศัพท์ที่เกี่ยวข้องกับ computer security และ intrusion detection.** แปลจาก NSA Glossary of Terms Used in Security and Intrusion Detection. โดย ปนิวัธน์ ทรัพย์รุ่งเรือง, พ.ต. [Online]. Available: http://thaicert.nectec.or.th/paper/basic/terms.htm

Swanson M. 1988. Guide **for Developing Security Plans for Information Technology Systems.** n.p.

ภาคผนวก

ผนวก ก.

ระเบียบ กองตำรวจสันติบาล 1

ว่าด้วย ความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

พ.ศ. .....

ด้วย กองตำรวจสันติบาล 1 ได้จัดให้มีระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกในการปฏิบัติงาน ดังนั้นเพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ กองตำรวจสันติบาล 1 เป็นไปอย่างเหมะสมและมีประสิทธิภาพ รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง อันส่งผลกระทบต่อความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ จึงเห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

ข้อ 1 "องค์กร" หมายความถึง กองตำรวจสันติบาล 1

ข้อ 2 "เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ระบบสารสนเทศ ของกองตำรวจสันติบาล 1

ข้อ 3 "ผู้บังคับบัญชา" หมายความถึง ผู้มีอำนาจสั่งการตามโครงสร้างของกองตำรวจสันติบาล 1

ข้อ 4 "เจ้าหน้าที่" หมายความถึง ข้าราชการตำรวจ พนักงานและลูกจ้างของกองตำรวจสันติบาล 1 รวมถึงบุคคลอื่นที่ กองตำรวจสันติบาล 1 มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

ข้อ 5 "ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

ข้อ 6 "ผู้ดูแลเครือข่ายคอมพิวเตอร์" หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ให้มี "คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กองตำรวจสันติบาล 1" ที่ผู้บังคับบัญชาแต่งตั้งจากเจ้าหน้าที่ขององค์กร โดย คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กองตำรวจสันติบาล 1 มีอำนาจหน้าที่ดังต่อไปนี้

- กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้
- ให้คำปรึกษาแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์เกี่ยวกับการปฏิบัติตามระเบียบนี้
- ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม
- ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้
- ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3 ข้อปฏิบัติของเจ้าหน้าที่ในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ 1 เจ้าหน้าที่มีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้

การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่เจ้าหน้าที่ที่ฝ่าฝืนตามความเหมาะสมต่อไป

ข้อ 2 .เจ้าหน้าที่พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ 3 เจ้าหน้าที่พึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย อาทิ เช่น ไม่ใช้การส่ง mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ 4 เจ้าหน้าที่มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ 5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล เจ้าหน้าที่จะต้อง

- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองใช้งานอยู่ ทั้งในระดับ BIOS และระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ 6 เจ้าหน้าที่จะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือขององค์กร หรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น

- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังเจ้าหน้าที่หรือบุคคลอื่น เป็นต้น
- เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของเจ้าหน้าที่อื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ
- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ (web site) ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

ข้อ 7 เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม เจ้าหน้าที่จะต้อง

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน
- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กร ได้
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (server) ที่ต้องใช้งานตลอด 24 ชั่วโมง
- ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กร ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กร จัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล
- ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งองค์กร จัดให้สำหรับใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร
- ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กองตำรวจสันติบาล 1 ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการดังกล่าวด้วย
- ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต
- คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่องค์กร รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากองค์กร ภายในกำหนด 7 วันนับแต่วันพ้นสภาพการเป็นเจ้าหน้าที่

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

ข้อ 1 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่เพื่อให้เป็นไปตามระเบียบนี้

หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าพนักงานผู้ใดมีพฤติการณ์ล่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที

ข้อ 2 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ 3 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

ข้อ 4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ 5 เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่องค์กร ในทันทีที่พ้นหน้าที่ และให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ 6 ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กร จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป

ประวัติผู้เขียน

ชื่อ : ร้อยตำรวจโท อนุเทพ ชมพูธวัช

เกิดเมื่อ : 7 มีนาคม 2520

สถานที่เกิด : อ.เมือง จว.นครปฐม

ประวัติการศึกษา

ระดับประถมศึกษา โรงเรียนเบญจมินทร์ กรุงเทพฯ

ระดับมัธยมศึกษาตอนต้น โรงเรียนสารวิทยา กรุงเทพฯ

ระดับมัธยมศึกษาตอนปลาย (ม.4-5) โรงเรียนสารวิทยา กรุงเทพฯ

ระดับมัธยมศึกษาตอนปลาย โรงเรียนเตรียมทหาร กรุงเทพฯ รุ่นที่ 37

ระดับอุดมศึกษา ปริญญาบัตรรัฐประศาสนศาสตร์ (ตำรวจ) โรงเรียนนายร้อยตำรวจ

ประวัติการทำงาน

รองสารวัตร ประจำโรงเรียนนายร้อยตำรวจ พ.ศ.2543-2543

รองสารวัตร งาน 3 กองกำกับการ 3 กองตำรวจสันติบาล 1 พ.ศ.2543-ปัจจุบัน