แผนความปลอดภัยระบบสารสนเทศของ บมจ. ปตท. สผ.

PTTEP Information System Security Plan

โดย

นายญาณพัฒน์ ช้างโต

รหัส 44067251

อาจารย์ที่ปรึกษา

ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2545

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	แผนความปลอดภัยระบบสารสนเทศของ บมจ. ปตท. สผ.
นักศึกษา	นายญาณพัฒน์ ช้างโต
อาจารย์ที่ปรึกษา	ดร. จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

แผนความปลอดภัยระบบสารสนเทศเป็นเครื่องมือที่องค์กรต้องจัดทำขึ้นเพื่อดำรงไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้และตอบสนองต่อบริการความปลอดภัยของข้อมูลสารสนเทศอันเนื่องมาจากภัยคุกคามต่าง ๆ ความเสี่ยง จุดอ่อนของระบบ เงื่อนไข กฎหมาย จริยธรรม และผลกระทบอื่น ๆ โดยแผนความปลอดภัยระบบสารสนเทศจะได้รับการตอบสนองจากการกำหนดนโยบายความปลอดภัย มาตรฐานความปลอดภัย ข้อแนะนำ และวิธีการปฏิบัติงานเกี่ยวกับความปลอดภัยของระบบสารสนเทศ

แผนความระบบสารสนเทศของบริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน) หรือ บมจ. ปตท. สผ. ในกรณีศึกษานี้มีจุดประสงค์เพื่อศึกษาถึงหลักการ องค์ประกอบ แนวทาง ความเหมาะสมของแผนความปลอดภัยรวมถึงเครื่องมือความปลอดภัยต่าง ๆ ในระบบสารสนเทศขององค์กร โดยนำมาเปรียบเทียบกับมาตรฐานความปลอดภัยสากล ISO/IEC 17799

Title	PTTEP Information System Security Plan
Student	Mr. Yanaphat Changto
Adviser	Ph.D. Chanboon Sathitwiriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2002

ABSTRACT

Information Security Plan is established tool for Corporate Information System Security to ensure that confidentiality, integrity, availability and information security services met. By objective, information security protects information asset from threats vulnerability, risk, impact, laws, ethics and other damages sources. Information Security Plan are responsible with information security policy, standard, guideline, procedures and others suitable set of controls. PTTEP Information System Security Plan Project study about existing principles, components, vision, guideline and implementation information security plan and to be compare with International Standard ISO/IEC 17799 – Code of practice for information security management

กิตติกรรมประกาศ

ในการจัดทำโครงการศึกษากรณีพิเศษเรื่องแผนความปลอดภัยระบบสารสนเทศของ บริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน) ในครั้งนี้สำเร็จได้ด้วยดีเนื่องจากการได้รับคำปรึกษา คำแนะนำ อย่างดีจากอาจารย์ ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาโครงการพัฒนาระบบงาน จึงขอขอบพระคุณเป็นอย่างสูง รวมทั้งคณาจารย์ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่านที่ได้อบรมสั่งสอน ปูพื้นความรู้แก่ข้าพเจ้ามาโดยตลอด

ขอขอบคุณแผนกเทคโนโลยีสารสนเทศ บมจ. ปตท. สผ. ที่ให้ข้อมูลและการศึกษาค้นคว้าข้อมูลในการจัดทำโครงการนี้

ญาณพัฒน์ ช้างโต

14 มีนาคม 2546

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

บทคัดย่อภาษาอังกฤษ II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญภาพ VII

สารบัญตาราง VIII

บทที่

1. บทนำ 1
   - 1.1 ความสำคัญและที่มา 1
   - 1.2 วัตถุประสงค์ 1
   - 1.3 ขอบเขตการศึกษา 2
   - 1.4 ผลหรือประโยชน์ที่คาดว่าจะได้รับจากการศึกษา 2
2. แนวคิดที่เกี่ยวข้อง 3
   - 2.1 นิยาม 3
   - 2.2 การป้องกันข้อมูลสารสนเทศ 3
   - 2.3 ความจำเป็นในการคุ้มครองระบบสารสนเทศ 4
   - 2.4 การกำหนดความต้องการด้านความปลอดภัยขององค์กร 4
   - 2.5 การจัดทำระบบความปลอดภัยสารสนเทศขององค์กร 4
   - 2.6 การบริหารความปลอดภัยข้อมูลสารสนเทศขององค์กร 7
   - 2.7 แผนความปลอดภัยเทคโนโลยีสารสนเทศ 8
   - 2.8 นโยบาย มาตรฐาน ข้อเสนอแนะ และขั้นตอนปฏิบัติงานรักษาความปลอดภัยข้อมูลสารสนเทศ 10
3. สภาพการณ์ปัจจุบัน 12
   - 3.1 ข้อมูลบริษัทเบื้องต้น 12
   - 3.2 ภารกิจขององค์กร 14

สารบัญ (ต่อ)

หน้า

3.3 หลักการกำกับดูแลกิจการที่ดี 14
3.4 โครงสร้างองค์กร และการบริหาร 16
3.5 โครงสร้างและหน้าที่แผนกเทคโนโลยีสารสนเทศ 18
3.6 โครงสร้างสถาปัตยกรรมระบบสารสนเทศ 21
3.7 นโยบายเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ และสื่อโทรคมนาคม 26
3.8 แผนความปลอดภัยระบบเทคโนโลยีสารสนเทศ 29
3.9 แผนว่าด้วยการจัดการปัญหา 29
4. การบริหารความเสี่ยง 37
4.1 วงจรชีวิตของการบริหารความเสี่ยง 37
4.2 ขั้นตอนในการวิเคราะห์ความเสี่ยง 39
4.3 การวิเคราะห์ความเสี่ยงในกรณีของ บมจ. ปตท. สผ. 41
4.4 ผลการวิเคราะห์ความเสี่ยงในกรณีของ บมจ. ปตท. สผ. 46
5. การพัฒนาแผนความปลอดภัยระบบสารสนเทศ 60
5.1 วัตถุประสงค์ 60
5.2 ขอบเขตของการประยุกต์ใช้แผนความปลอดภัยและหน่วยงานที่รับผิดชอบ 61
5.3 ความรับผิดชอบในเรื่องของระบบความปลอดภัยสารสนเทศ 62
5.4 เป้าหมายของการทำแผนความปลอดภัยระบบสารสนเทศ 62
5.5 การทบทวน การปรับปรุง และการประยุกต์ใช้แผน 63
5.6 แผนความปลอดภัยสารสนเทศ 63
5.7 การพัฒนานโยบายความปลอดภัย 76
6. สรุปและข้อเสนอแนะ 82
6.1 ผลการศึกษา 82
6.2 ประโยชน์ที่คาดว่าได้รับ 83
6.3 ข้อเสนอแนะ 83
บรรณานุกรม 85

สารบัญ (ต่อ)

หน้า

ภาคผนวก

ก. PTT Exploration & Production PCL IT Policy 86

ข. มาตรฐานสากล ISO/IEC 17799 111

ประวัติผู้เขียน 128

สารบัญรูป

หน้า

รูปที่

2.1 แสดงความสัมพันธ์ของวัตถุประสงค์ความปลอดภัย 3
2.2 แสดงขั้นตอนในการจัดการประเมินความเสี่ยง 6
2.3 Information Security Administration Diagram 8
3.1 แสดงโครงการลงทุนของ ปตท. สผ. 13
3.2 แสดงโครงสร้างองค์กร 17
3.3 แสดงโครงสร้างแผนกบริการเทคโนโลยีสารสนเทศ 18
3.4 แสดงระบบเครือข่ายท้องถิ่น 21
3.5 แสดงระบบเครือข่ายระยะไกล 22
3.6 แสดงการเชื่อมต่อของระบบงานธุรกิจเบ็ดเสร็จ 23
3.7 แสดงระบบสารสนเทศงานธรณีวิทยาและธรณีฟิสิกส์ 24
3.8 แสดงการเชื่อมต่อของ SAN 25
3.9 แสดงการเชื่อมต่อของ NAS 26
3.10 แสดงขั้นตอนในการทำแผน 30
4.1 แสดงวงจรชีวิตของการบริหารความเสี่ยง 38
5.1 แสดงโครงสร้างองค์กรแผนกเทคโนโลยีสารสนเทศที่ควรรวมงานด้านความปลอดภัยระบบสารสนเทศ 61
5.2 แสดงตัวอย่างสัญญาจ้างงานที่รวมประเด็นด้านความปลอดภัยระบบสารสนเทศ 70
5.3 แสดงตัวอย่างแบบรายงานเหตุสุดวิสัย 75

สารบัญตาราง

หน้า

ตารางที่

4.1 ตารางจัดลำดับความสำคัญ 40
4.2 แสดงลำดับความสำคัญทรัพย์สินเชิงตัวเลข 42
4.3 แสดงความน่าจะเป็นในการเกิดภัยคุกคาม 45
4.4 แสดงค่าความเสี่ยง 46
4.5 แสดงกลุ่มของเซิฟเวอร์ขององค์กร 47
4.6 แสดงกลุ่มของอุปกรณ์เครือข่ายสื่อสาร 48
4.7 แสดงกลุ่มของอุปกรณ์ต่าง ๆ ของเครือข่าย 50
4.8 แสดงกลุ่มของอุปกรณ์โทรคมนาคม 51
4.9 แสดงอุปกรณ์โครงสร้างพื้นฐานห้องคอมพิวเตอร์ขององค์กร 52
4.10 แสดงกลุ่มของทรัพย์สินฮาร์ดแวร์ของระบบคอมพิวเตอร์ 53
4.11 แสดงข้อมูลของหน่วยงานต่าง ๆ ตามโครงสร้างองค์กร 54
4.12 แสดงกลุ่มของซอฟท์แวร์ที่ใช้ในองค์กร 57

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ระบบสารสนเทศได้แก่ ข้อมูล ฮาร์ดแวร์ ซอฟท์แวร์ บุคลากร และวิธีปฏิบัติงานต่าง ๆ ถือว่าเป็นทรัพย์สินขององค์กรมีมูลค่าสำหรับองค์กรที่จะต้องหาทางปกป้องคุ้มครองให้เกิดความปลอดภัย การจัดทำเครื่องมือสำหรับความปลอดภัยด้านระบบสารสนเทศจึงเป็นสิ่งจำเป็นในการควบคุมความเสี่ยง ภัยคุกคาม กฎหมาย จริยธรรม รวมทั้งผลกระทบต่าง ๆ เช่นการสูญเสียข้อมูลลูกค้า ข้อมูลทางการเงินและการบัญชี ข้อมูลผลิตภัณฑ์ใหม่ ๆ การถูกลงโทษทางกฎหมาย การสูญเสียส่วนแบ่งการตลาด รวมทั้งการเสียชื่อเสียงและความเชื่อมั่นต่อองค์กร

ดังนั้นการลดความเสี่ยงหรือปัจจัยในแง่ลบต่าง ๆ ที่จะเกิดขึ้นกับองค์กรหรือเกิดขึ้นแล้วกับองค์กร องค์กรจะต้องจัดทำชุดเครื่องมือในการบริหารปกป้องคุ้มครองแก่ระบบสารสนเทศที่สำคัญคือแผนความปลอดภัยระบบสารสนเทศที่ได้รับการปฏิบัติตอบสนองต่อจากการกำหนดนโยบายความปลอดภัย มาตรฐาน วิธีการปฏิบัติงาน ข้อแนะนำและข้อเสนอแนะที่เกี่ยวกับความปลอดภัยของระบบสารสนเทศที่กำหนดขึ้นเพื่อให้ฝ่ายเทคโนโลยีสารสนเทศและพนักงานได้ตระหนักและปฏิบัติตาม

โครงการวิเคราะห์ระบบงานนี้จึงมุ่งเน้นการศึกษาแผนความปลอดภัยระบบสารสนเทศของ บมจ. ปตท. สผ. ที่ใช้ปฏิบัติอยู่ว่ามีแผนใดบ้าง มีความเหมาะสม มีประสิทธิภาพและมีความสอดคล้องกับมาตรฐานสากล ISO/IEC 17799 เพื่อเป็นแนวทางในการบริหาร พัฒนา จัดทำและแก้ไขแผนความปลอดภัยระบบสารสนเทศและเครื่องมือความปลอดภัยอื่น ๆ เพื่อความปลอดภัยในระบบสารสนเทศที่มีประสิทธิภาพและประสิทธิผลมากขึ้นรวมทั้งอาจนำไปใช้ในการขอใบรับรองด้านความปลอดภัยระบบสารสนเทศต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาถึงหลักการ ขั้นตอน แนวทางของการจัดทำแผนความปลอดภัยระบบสารสนเทศรวมถึงเครื่องมือความปลอดภัยต่าง ๆ

1.2.2 ศึกษามาตรฐานความปลอดภัยระบบสารสนเทศสากล ISO/IEC 17799

1.2.3 วิเคราะห์ เปรียบเทียบระหว่างแผนและเครื่องมือความปลอดภัยระบบสารสนเทศที่องค์กรใช้ปฏิบัติอยู่กับมาตรฐานสากล ISO/IEC 17799

1.2.4 เพื่อเป็นแนวทางในการกำหนด ปรับปรุง เปลี่ยนแปลง เพิ่มเติม ข้อพึงระวัง การประยุกต์ใช้แผนและเครื่องมือความปลอดภัยต่าง ๆ ให้กับระบบความปลอดภัยสารสนเทศของ บมจ. ปตท. สผ. ให้สอดคล้องกับมาตรฐานความปลอดภัยระบบสารสนเทศสากล

1.3 ขอบเขตการศึกษา

1.3.1 สำรวจและศึกษาสภาพการณ์ระบบเทคโนโลยีสารสนเทศและเครื่องมือความปลอดภัยระบบสารสนเทศขององค์กรในปัจจุบัน

1.3.2 ศึกษามาตรฐานความปลอดภัยระบบสารสนเทศสากล ISO/IEC 17799

1.3.3 ศึกษาเปรียบเทียบระบบความปลอดภัยระบบสารสนเทศขององค์กรกับมาตรฐานสากล ISO/IEC 17799

1.3.4 พัฒนาแผนแม่บทความปลอดภัยและนโยบายความปลอดภัยเทคโนโลยีสารสนเทศขององค์กร

1.4 ผลหรือประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

1.4.1 ได้ทราบถึงหลักการ แนวทางในการจัดทำแผนความปลอดภัยระบบสารสนเทศขององค์กร

1.4.2 ได้ทราบถึงหลักปฏิบัติด้านความปลอดภัยระบบสารสนเทศตามมาตรฐานสากล ISO/IEC 17799

1.4.3 เพื่อเป็นแนวทางในการกำหนด ปรับปรุง เปลี่ยนแปลง ข้อพึงระวังในการพัฒนาแผนแม่บทความปลอดภัยขององค์กรต่อไป

1.4.4 เพื่อเป็นแนวทางให้องค์กรอื่นได้นำไปศึกษาและนำไปประยุกต์ใช้ในองค์กร

บทที่ 2
แนวคิดที่เกี่ยวข้อง

2.1 นิยาม

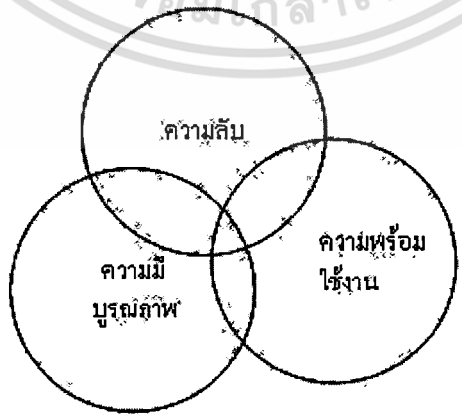
ความหมายของการปกป้องคุ้มครองความปลอดภัยของข้อมูลสารสนเทศ องค์กร The International Organization for Standardization (ISO) และ องค์กร The International Electro technical Commission (IEC) ได้นิยามไว้ว่า ข้อมูลสารสนเทศเป็นเสมือนทรัพย์สินชนิดหนึ่งขององค์กรที่มีมูลค่าและต้องการป้องกันเพื่อคุ้มครองข้อมูลสารสนเทศ จากภัยคุกคามต่าง ๆ เพื่อทำให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อลดความเสียหายที่อาจเกิดขึ้นให้น้อยลง และทำให้องค์กรสามารถลดต้นทุน และเพิ่มโอกาสทางธุรกิจได้มากขึ้น (ISO. 2001: VIII)

2.2 การป้องกันข้อมูลสารสนเทศเพื่อบรรลุวัตถุประสงค์ 3 ประการคือ

2.2.1 ความลับของข้อมูล (Confidentiality) คือความต้องการที่จะไม่เปิดเผยข้อมูลสารสนเทศที่เป็นความลับ หรือส่วนตัว

2.2.2 บูรณภาพ (Integrity) คือการที่ข้อมูล หรือโปรแกรม มีความทันสมัย ทันเวลา ถูกต้องและสมบูรณ์

2.2.3 ความพร้อมใช้งาน (Availability) คือระบบสามารถทำงานได้ทันทีที่ต้องการ และผู้มีสิทธิ์ไม่ถูกปฏิเสธการใช้งาน



รูปที่ 2.1 ความสัมพันธ์ของวัตถุประสงค์ความปลอดภัย

2.3 ความจำเป็นในการคุ้มครองระบบสารสนเทศ (ISO. 2001 : 8)

ความจำเป็นในการปกป้องคุ้มครองข้อมูลสารสนเทศ เพื่อประโยชน์ดังต่อไปนี้

2.3.1 ความลับของข้อมูล ความถูกต้องของข้อมูล ความพร้อมใช้ของข้อมูล ทำให้องค์กรสามารถแข่งขันทางธุรกิจ การจัดทำงบการเงิน ความสามารถทำกำไร เพื่อบรรลุข้อผูกพันทางกฎหมาย และเพื่อภาพพจน์ขององค์กร

2,3.2 เป็นการป้องกันภัยคุกคาม จากสาเหตุต่าง ๆ เช่น ความล้มเหลวของระบบคอมพิวเตอร์ ไวรัส การถูกเจาะระบบ การปฏิเสธการให้บริการ ไฟไหม้ น้ำท่วม การจารกรรม การก่อวินาศกรรม เป็นต้น

2.3.3 เนื่องจากการเชื่อมต่อข้อมูลผ่านอินเตอร์เน็ต หรือ เครือข่ายสาธารณะ ทำให้เกิดปัญหาต่อการควบคุมความปลอดภัย

2.3.4 เนื่องจากระบบสารสนเทศ ไม่ได้ออกแบบมาเพื่อเน้นด้านความปลอดภัย จึงต้องมีการจัดการ หรือมีวิธีการเข้ามาคุ้มครอง โดยอาศัยความร่วมมือจากผู้บริหาร พนักงาน คู่ค้า พันธมิตร และหุ้นส่วนต่าง ๆ

2.3.5 การควบคุมความปลอดภัยของข้อมูลที่ตรงกับความต้องการ รวมทั้งการออกแบบที่ถูกต้องทำให้ประหยัดค่าใช้จ่าย และเกิดประสิทธิผลแก่องค์กร

2.4 การกำหนดความต้องการด้านความปลอดภัยขององค์กร

องค์กรจะต้องแยกแยะความต้องการด้านความปลอดภัย โดยพิจารณาจากเหตุปัจจัยต่าง ๆ 3 ประการ คือ

2.4.1 พิจารณาความเสี่ยง (Risk) โดยการประเมินความเสี่ยงที่จะเกิดขึ้น จากภัยคุกคามและผลกระทบด้านลบแก่องค์กร

2.4.2 พิจารณาจากข้อกฎหมาย ข้อบังคับ สนธิสัญญาต่าง ๆ รวมทั้งความต้องการของลูกค้า คู่ค้า หุ้นส่วน คู่สัญญา เป็นต้น

2.4.3 พิจารณาจากหลักเกณฑ์ จุดประสงค์ วิสัยทัศน์ และความต้องการอื่น ๆ ขององค์กร

2.5 การจัดทำระบบความปลอดภัยสารสนเทศขององค์กร (Swanson. 1998 : 6)

2.5.1 ในการจัดทำระบบความปลอดภัยสารสนเทศขององค์กร สามารถแบ่งได้เป็น 2 แนวคิดคือ

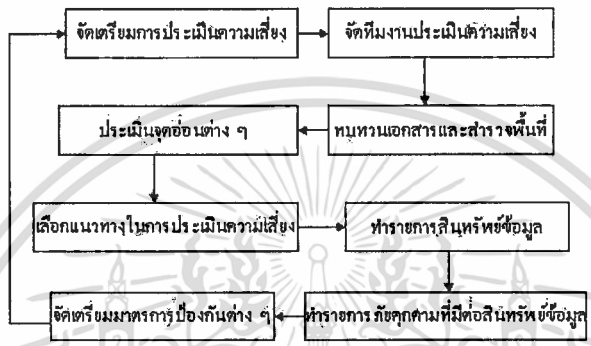
1. แนวคิดจากล่างขึ้นบน (Bottom up Approach) ซึ่งจะได้ความรวดเร็ว แต่ไม่ชัดเจนมากนัก มีลักษณะขั้นตอนคือ

- ศึกษา เข้าใจนโยบายสารสนเทศที่มีอยู่ในขณะนั้น รวมทั้งรูปแบบของเครือข่าย ขั้นตอนการปฏิบัติงาน และกิจกรรมของพนักงานที่ปฏิบัติอยู่ ณ เวลานั้น ๆ
- พิจารณาการโจมตีระบบข้อมูลสารสนเทศที่เกิดขึ้นในขณะนั้น ๆ
- สรุปจุดอ่อนต่าง ๆ ที่องค์กรมีอยู่
- กำหนดนโยบายความปลอดภัยสารสนเทศ และให้ความรู้แก่พนักงาน
- จัดทำนโยบายให้ผู้ใช้งาน และให้ความรู้แก่ผู้ใช้ทุกคน
- สร้างข้อแนะนำทางเทคนิคเพื่อเป็นแนวทางในการติดตั้ง บำรุงรักษา และตรวจสอบระบบสารสนเทศ

2. แนวคิดจากบนลงล่าง (Top Down Approach) เป็นแนวคิดเชิงวิธีการ ซึ่งมีความชัดเจนแต่มีความล่าช้า และมีต้นทุนเริ่มต้นสูง โดยจะต้องอาศัยวิสัยทัศน์ ความชัดเจน ความเข้าใจและความสนับสนุนจากฝ่ายบริหาร มีขั้นตอนคือ
   - ประเมินทรัพย์สิน(Asset Analysis) ว่าจะต้องปกป้อง คุ้มครองระบบสารสนเทศใดบ้าง มีมูลค่าเท่าใด และอย่างไร
   - วิเคราะห์กฎเกณฑ์ นโยบาย และข้อปฏิบัติด้านความปลอดภัย (ถ้ามี)
   - กำหนดวัตถุประสงค์ด้านความปลอดภัยเบื้องต้นขึ้น
   - วิเคราะห์ภัยคุกคาม (Threat Analysis) ต่อระบบสารสนเทศโดยแบ่งเป็นระดับ (likelihood of a threat)
   - วิเคราะห์ผลกระทบอื่น ๆ (Impact Analysis) ต่อข้อมูลสารสนเทศโดยอาจมีการแบ่งเป็นระดับ ๆ
   - คำนวณความเสี่ยง (Calculate Risk)
   - วิเคราะห์ข้อจำกัดต่าง ๆ (Constraints Analysis) เช่นกฎหมายในประเทศ กฎหมายระหว่างประเทศ วัฒนธรรมองค์กร ศีลธรรมจรรยา พันธะคู่สัญญา
   - พิจารณากำหนดกลยุทธ์มาใช้โดยมีการกำหนดวัตถุประสงค์ กำหนดมาตรฐานในการควบคุม
   - การประยุกต์ใช้ (Implementation) โดยพัฒนาแผนและนโยบาย ข้อแนะนำ วิธีปฏิบัติการ ขึ้นมาใช้ในองค์กร
   - รับประกันความปลอดภัย (Assurance) โดยมีการจัดทำประเมินความเสี่ยงซ้ำ จัดทำทบทวนแผน นโยบาย กฎเกณฑ์ ทุก ๆ 2 ปี

2.5.2 การจัดการความเสี่ยง (Risk Management) (Peltier. 2001 : 12)

ความเสี่ยง คือเหตุการณ์ในแง่ลบต่าง ๆ ที่อาจเกิดขึ้นต่อองค์กร และมีผลกระทบต่อความปลอดภัยของข้อมูลสารสนเทศ ความเสี่ยงขึ้นกับปัจจัยต่าง ๆ คือ ผลกระทบ (Impact) ภัยคุกคาม (Threat) และความจุดอ่อนต่าง ๆ (Vulnerabilities) ซึ่งการจัดการความเสี่ยงย่อมมีขั้นตอนในการจัดทำได้หลายรูปแบบ



รูปที่ 2.2 ขั้นตอนในการจัดการประเมินความเสี่ยง

ภัยคุกคาม (Threat) ที่เกิดขึ้นกับระบบสารสนเทศแบ่งได้ดังนี้

- ภัยคุกคามทั่ว ๆ ไป (General Threats) ได้แก่ เกิดจากมนุษย์ เช่น การละเลย การไม่ระมัดระวัง การใช้ซอฟท์แวร์ และฮาร์ดแวร์ที่ไม่ถูกต้อง การโจมตีโดยวิธีทางสังคม (Social Engineering) การออกแบบระบบปฏิบัติการที่ผิดพลาด หรือซอฟท์แวร์ทำงานผิดพลาด
- ภัยคุกคามจากการพิสูจน์ และแยกแยะตัวตน (Identification/Authorization Threats) ได้แก่ โปรแกรมที่ซ่อนตัวมา เกิดจากฮาร์ดแวร์ เกิดจากนักบุกรุกที่ปลอมตัวเข้ามาในระบบ เกิดจากผู้ใช้ภายในระบบปลอมตัว
- ภัยคุกคามที่ลดความน่าเชื่อถือ หรือความไว้วางใจในการให้บริการ (Reliability of Service Threats) ได้แก่ ภัยธรรมชาติ เช่น ไฟ ควัน น้ำท่วม แผ่นดินไหว ไฟฟ้าดับ การทำลายล้างเผ่าพันธุ์ของมนุษย์ เช่น สงคราม ระเบิดสารเคมี นิวเคลียร์ เกิดจากการทำงานของอุปกรณ์ล้มเหลว เช่น สายเคเบิล ระบบติดต่อสื่อสารเครือข่าย เกิดการปฏิเสธการให้บริการ เกิดจากการจารกรรมหรือวินาศกรรมต่าง ๆ
- ภัยคุกคามความเป็นส่วนตัว
- ภัยคุกคามต่อบูรณภาพและความถูกต้อง

- ภัยคุกคามชนิดควบคุมการเข้าถึง ได้แก่การแกะรหัสผ่าน การดักจับข้อมูลในเครือข่าย การใช้ประตูหลัง
- ภัยคุกคามต่อการทำให้เสื่อมเสียชื่อเสียง (Repudiation threats)
- ภัยคุกคามต่อข้อบังคับหรือกฎหมาย

แหล่งที่มาของภัยคุกคามได้แก่ การเมือง การค้า พนักงานในองค์กร แฮกเกอร์ แคร็กเกอร์ คู่สัญญา คู่ค้าที่สามารถเข้าถึงระบบ อาชญากรขององค์กร นักสืบสวนสอบสวนต่าง ๆ ข้อบังคับทางกฎหมายหรือองค์กรของรัฐ และนักข่าว เป็นต้น

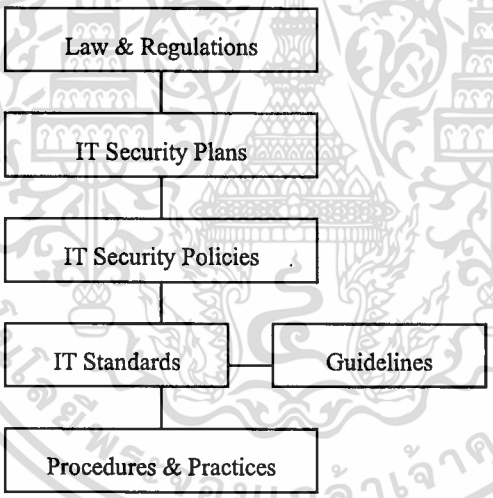
ผลกระทบ (Impact) ผลกระทบที่อาจเกิดขึ้นแก่องค์กรได้แก่

- ความลับขององค์กร ความลับของลูกค้า ความลับทางบัญชี การเงินขององค์กรถูกเปิดเผย
- เกิดการเปลี่ยนแปลงข้อมูลทางการเงินและการบัญชี
- บุคลากรในองค์กรสูญเสียความเป็นส่วนตัวด้านข้อมูล
- ภาพพจน์องค์กรเสียหาย
- หน่วยงานธุรกิจหลักขององค์กรชะงักงัน
- เครือข่ายคอมพิวเตอร์ล้มเหลว
- ลูกค้าขาดความเชื่อมั่นและเชื่อถือทำให้สูญเสียส่วนแบ่งการตลาด
- องค์กรถูกลงโทษทางกฎหมาย
- คุณภาพการให้บริการลดลง
- คู่แข่งได้เปรียบทางธุรกิจและทำให้สูญเสียรายได้
- นักโจมตีระบบใช้ระบบเครือข่ายขององค์กรเป็นฐานทำร้ายเว็บไซต์อื่น ๆ
- ระบบอิเล็กทรอนิกส์ทำงานล้มเหลว

2.6 การบริหารความปลอดภัยข้อมูลสารสนเทศขององค์กร (Peltier. 2001 : 95)

ข้อมูลสารสนเทศของทุกองค์กรย่อมมีความสำคัญและมีผลต่อการดำเนินธุรกิจขององค์กร ดังนั้นการจำแนกแยกแยะข้อมูลขององค์กรจะช่วยให้สามารถจัดการความปลอดภัยข้อมูลสารสนเทศได้ถูกทิศทางและประสิทธิผล ข้อมูลทั่วไปที่เป็นความลับขององค์กรที่พบได้เกือบทุกองค์กรได้แก่ ข้อมูลเงินเดือน ข้อมูลแผนการตลาด ข้อมูลลิขสิทธ์ ข้อมูลกำไร ข้อมูลลูกค้า ข้อมูลบัญชี ข้อมูลการประเมินผล ข้อมูลผู้ถือหุ้น ข้อมูลแผนงานธุรกิจ ข้อมูลแผนงานดำเนินงาน ข้อมูลเครื่องหมายการค้า ข้อมูลคู่แข่งทางการค้า ข้อมูลทางด้านสวัสดิการ ข้อมูลรายรับ รายจ่ายขององค์กร ข้อมูลงบดุล ข้อมูลของ

ผู้บริหาร ข้อมูลระบบเครือข่ายสารสนเทศขององค์กร เป็นต้น เมื่อองค์กรได้จัดทำแยกประเภทความลับของข้อมูลในองค์กรและได้จัดทำการประเมินความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศขององค์กรแล้ว องค์กรจะต้องมีการจัดทำเครื่องมือในการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สอดคล้องกับวิสัยทัศน์ พันธะสัญญาและวัฒนธรรมขององค์กร ซึ่งได้แก่มีการจัดทำแผนความปลอดภัย (Security Plan) นโยบายความปลอดภัย (Security Policy) มาตรฐานความปลอดภัย (Standard) ข้อแนะนำ (Guidelines) และขั้นตอนการปฏิบัติงาน (Procedures) นอกจากนี้แผนกเทคโนโลยีสารสนเทศหรือฝ่ายบริหารจะต้องมีการทบทวนและมีการพัฒนาแผนต่าง ๆ นโยบายต่างๆ มาตรฐาน ขั้นตอนการปฏิบัติงาน และข้อเสนอแนะในการทำงานอยู่เป็นประจำ ซึ่งจะทำให้ระบบรักษาความปลอดภัยขององค์กรมีความเข้มแข็งและทันเหตุการณ์อยู่ตลอดเวลา นอกจากนี้องค์กรควรจะต้องมีการจัดตั้งทีมงานทางด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศขึ้นมาดูแลและรับผิดชอบระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศขององค์กร



รูปที่ 2.3 Information Security Administration Diagram

2.7 แผนความปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Plan) (Swanson. 1998 : 8)

การจัดทำแผนความปลอดภัยสารสนเทศ เป็นการจัดทำ จัดหา ความต้องการด้านความปลอดภัยในเชิงกว้างของระบบความปลอดภัย รวมทั้งอธิบายการควบคุมแผนงานให้ตรงตามความต้องการ และกำหนดหน้าที่ความรับผิดชอบให้แก่บุคคลต่าง ๆ ในองค์กร เพื่อให้สอดคล้องกับข้อกำหนดทางกฎหมายในประเทศ และกฎหมายระหว่างประเทศ วิสัยทัศน์ และพันธะกิจขององค์กร และสนับสนุนระบบธุรกิจขององค์กร โดยมีวัตถุประสงค์หลักเพื่อปรับปรุง ปกป้อง คุ้มครองรักษาความปลอดภัยของ

ทรัพยากรข้อมูลสารสนเทศขององค์กร แผนความปลอดภัยสารสนเทศจะได้ประสิทธิภาพนั้น ฝ่ายบริหารจะต้องมีการอนุมัติแผน เพื่อให้แผนสามารถดำเนินการได้ ซึ่งการอนุมัตินั้นอยู่บนพื้นฐานของการจัดการด้านการประเมินการสำรวจ และตรวจสอบ การวิเคราะห์ถึงความล่อแหลมของระบบสารสนเทศ รวมทั้งมีการควบคุมถึงด้านปฏิบัติการ ด้านเทคนิค และมีการตรวจสอบ ปรับเปลี่ยน ทบทวนแผนงาน

จุดประสงค์ในการทำแผนความปลอดภัยแบ่งเป็น 2 ประการคือ

1. เพื่อจัดหาภาพรวมความต้องการด้านระบบความปลอดภัยสารสนเทศ รวมถึงอธิบายการควบคุมให้ตรงตามความต้องการ
2. เพื่อจัดสรรหน้าที่ความรับผิดชอบ และความคาดหวังถึงพฤติกรรมของทุก ๆ บุคคลที่เกี่ยวข้องกับระบบสารสนเทศ แผนความปลอดภัยทุกแผนจะต้องได้รับการควบคุม ส่งต่อ ด้วยการกำหนดนโยบายความปลอดภัย

องค์กร The International Institute of Standard and Technology (NIST) ได้แนะนำว่าแผนความปลอดภัยควรจะแบ่งเป็น 2 ระบบ คือ

1. แผนแอพพลิเคชั่นหลัก (Major Application) เป็นการกำหนดแผนความปลอดภัยหลักให้แก่แอพพลิเคชั่นที่สำคัญของหน่วยงาน โดยที่แผนอาจเป็น โปรแกรมบุคคล (Individual Program) ฮาร์ดแวร์ ซอฟท์แวร์ โทรคมนาคม ซึ่งเป็นแอพพลิเคชั่นหลักที่ใช้สนับสนุนงานหลักของธุรกิจหรือหัวใจขององค์กร
2. แผนระบบสนับสนุนทั่วไป (General Support System) เป็นแผนที่จัดทำเพื่อสนับสนุนแอพพลิเคชั่นหลัก ได้แก่แผนเกี่ยวกับฮาร์ดแวร์ ซอฟท์แวร์ ข้อมูลสารสนเทศ ข้อมูลดิบ เครือข่าย อุปกรณ์อำนวยความสะดวกต่าง ๆ รวมทั้งบุคลากร

องค์ประกอบของแผนความปลอดภัยเทคโนโลยีสารสนเทศจะต้องประกอบไปด้วย ชื่อแผนงาน องค์กรที่รับผิดชอบ บุคคลที่รับผิดชอบ สถานะของแต่ละแผน วัตถุประสงค์ในการทำแผน สภาพแวดล้อมของระบบ ระบบอื่น ๆ ที่จะเข้ามาเกี่ยวข้อง กฎหมาย กฎเกณฑ์ ขั้นตอนการจัดการความเสี่ยงและผลกระทบต่าง ๆ

ขั้นตอนในการจัดทำแผนประกอบด้วย 4 ขั้นตอนคือ

1. ขั้นตอนเริ่มทำแผน (Initiation Phase) เป็นการประเมินเงื่อนไข ความเสี่ยง ความจำเป็นต่าง ๆ
2. ขั้นตอนการพัฒนาและการให้ได้มา (Development /Acquisition Phase) เป็นการจัดหาทดสอบเครื่องมือความปลอดภัยต่าง ๆ
3. ขั้นตอนการนำไปใช้ (Implementation Phase)

4. ขั้นตอนการดูแลและบำรุงรักษา (Operation and Maintenance)

เหตุผลและความจำเป็นในการสร้างแผนความปลอดภัยก็เพื่อเหตุผลต่าง ๆ คือ เพื่อตอบสนองต่อจุดประสงค์หลักของระบบรักษาความปลอดภัย เพื่อป้องกันการการถูกโจมตีอันเนื่องมาจากจุดอ่อนของระบบสารสนเทศ เพื่อป้องกันบุคคลจำพวกที่ก่อให้เกิดความไม่สงบในระบบสารสนเทศ และเพื่อป้องกันผลกระทบในแง่ลบต่าง ๆที่อาจเกิดขึ้นต่อองค์กร ตัวอย่างของแผนความปลอดภัยเทคโนโลยีสารสนเทศ เช่น แผนการวิเคราะห์ความเสี่ยงระบบสารสนเทศ แผนการดำเนินธุรกิจต่อเนื่อง (Business Continuity Plan) แผนการกู้ข้อมูลจากความเสียหาย (Disaster Recovery Plan) แผนปฏิบัติการฉุกเฉิน แผนบรรเทาปัญหา เป็นต้น

2.8 นโยบาย (Policy) มาตรฐาน (Standard) ข้อเสนอแนะ(Guideline) และขั้นตอนปฏิบัติงาน (Procedure) รักษาความปลอดภัยข้อมูลสารสนเทศ (Peltier. 2001 : 120)

นโยบาย (Policy) หมายถึงเจตจำนงเกี่ยวกับความเชื่อ จุดประสงค์ และเป้าหมายขององค์กร รวมทั้งความหมายอื่น ๆ สำหรับการบรรลุเรื่องใดเรื่องหนึ่งขององค์กร

มาตรฐาน (Standard) หมายถึงกิจกรรม การกระทำ กฎระเบียบ ที่ถูกจัดทำขึ้นเพื่อสนับสนุนนโยบาย ให้เกิดประสิทธิภาพและประสิทธิผล

ข้อแนะนำ (Guidelines) เป็นเจตจำนงทั่วไป ที่จัดทำให้บรรลุวัตประสงค์ตามนโยบายโดยการกำหนดกรอบ หรือขอบเขต เพื่อให้เกิดขั้นตอนการปฏิบัติงาน (Procedure) ต่อไป ซึ่งมาตรฐานจะเป็นข้อบังคับ ในขณะที่ข้อแนะนำจะเป็นการเสนอแนะให้ปฏิบัติตาม (Recommendations)

ขั้นตอนการปฏิบัติงาน (Procedures) เป็นการระบุเฉพาะเจาะจงว่า นโยบาย มาตรฐาน และข้อแนะนำ จะทำได้อย่างไรในการปฏิบัติงานจริง

ส่วนประกอบที่สำคัญในการจัดทำนโยบายความปลอดภัย (Policy Key Elements) คือการจัดทำนโยบายที่ดี ซึ่งควรมีลักษณะดังต่อไปนี้

1. สามารถเข้าใจได้ง่าย สำหรับทุกบุคคลในองค์กร (Be easy to understand)
2. นำไปใช้งานได้จริง (Be Applicable)
3. สามารถปฏิบัติได้จริง (Be Doable)
4. ต้องเป็นไปในเชิงบังคับ (Be Enforceable)
5. ต้องค่อยเป็นค่อยไป (Be Phased in)
6. ต้องพร้อมที่จะกระทำได้ก่อนเกิดปัญหา (Be Proactive)
7. หลีกเลี่ยงความเป็นที่สุด (Avoid Absolutes) ซึ่งจะทำให้เกิดการไม่ปฏิบัติตาม และการต่อต้าน

8. สอดคล้องกับวัตถุประสงค์ของธุรกิจ (Meet Business Objectives) เพื่อเป็นการลดความเสี่ยงให้กับองค์กร

ตัวอย่างของนโยบายรักษาความปลอดภัยข้อมูลสารสนเทศ เช่น นโยบายการใช้อินเตอร์เน็ต นโยบายการใช้ข้อมูลของคู่ค้า (Third Party Agreement) นโยบายการใช้เครือข่ายเสมือน (Virtual Private Network) นโยบายการกำหนดรหัสผ่าน นโยบายการเข้าถึงข้อมูลจากระยะไกล (Remote Access) นโยบายการส่งเมล์ออกนอกองค์กร นโยบายการใช้อุปกรณ์สื่อสารในองค์กร เป็นต้น

มาตรฐาน (Standard) เป็นสิ่งที่จัดทำขึ้นเพื่อสนับสนุนและเป็นแนวทางให้กับนโยบาย ซึ่งมาตรฐานจะเป็นสิ่งที่ต้องปฏิบัติตาม ได้แก่กิจกรรม การกระทำ กฎเกณฑ์ ข้อบังคับ ซึ่งทำให้เกิดประสิทธิภาพ และประสิทธิผลต่อนโยบาย

มาตรฐานระหว่างประเทศที่เกี่ยวกับความปลอดภัยของระบบมูลสารสนเทศมีอยู่ 2 มาตรฐานหลักคือ มาตรฐานของ BS7799 และมาตรฐาน ISO 17799 ซึ่งไม่แตกต่างกันมากนัก แต่ที่นี้ขอกล่าวถึงมาตรฐาน ISO 17799 ซึ่งคาดว่าจะนำมาใช้อย่างแพร่หลายสำหรับองค์กร

กฎหมายและพระราชบัญญัติต่าง ๆ ย่อมมีผลต่อการจัดทำแผนและนโยบายความปลอดภัยต่าง ๆ กฎหมายและพระราชบัญญัติของไทยที่สำคัญได้แก่ พระราชบัญญัติลิขสิทธิ์ พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติอาชญากรทางคอมพิวเตอร์และ พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น

ศีลธรรม จรรยาและจริยธรรม ถึงแม้ว่าจะมีเครื่องมือความปลอดภัยต่าง ๆ ได้แก่แผนความปลอดภัย นโยบายความปลอดภัย ข้อปฏิบัติงาน ข้อบังคับ มาตรฐาน กฎเกณฑ์ต่าง ๆ กฎหมายและพระราชบัญญัติต่าง ๆแล้วองค์กรจะต้องมีการพิจารณาเรื่องของการปลูกฝังศีลธรรม จรรยาและจริยธรรมให้แก่พนักงานในองค์กร เพราะเป็นเครื่องมืออันหนึ่งที่สามารถทำให้เกิดความปลอดภัยต่อระบบสารสนเทศขององค์กร เช่น การมีพฤติกรรมเป็นนักคอมพิวเตอร์ที่ดี การไม่ละเมิดความลับของผู้อื่น การใช้สารสนเทศเพื่อศึกษาหาความรู้ไม่ใช่เพื่อทำลายหรือทำร้ายผู้อื่น การไม่ละเมิดสิทธิผู้อื่น การไม่ละเมิดกฎหมาย เป็นต้น

บทที่ 3
สภาพการณ์ปัจจุบัน

3.1 ข้อมูลบริษัทเบื้องต้น

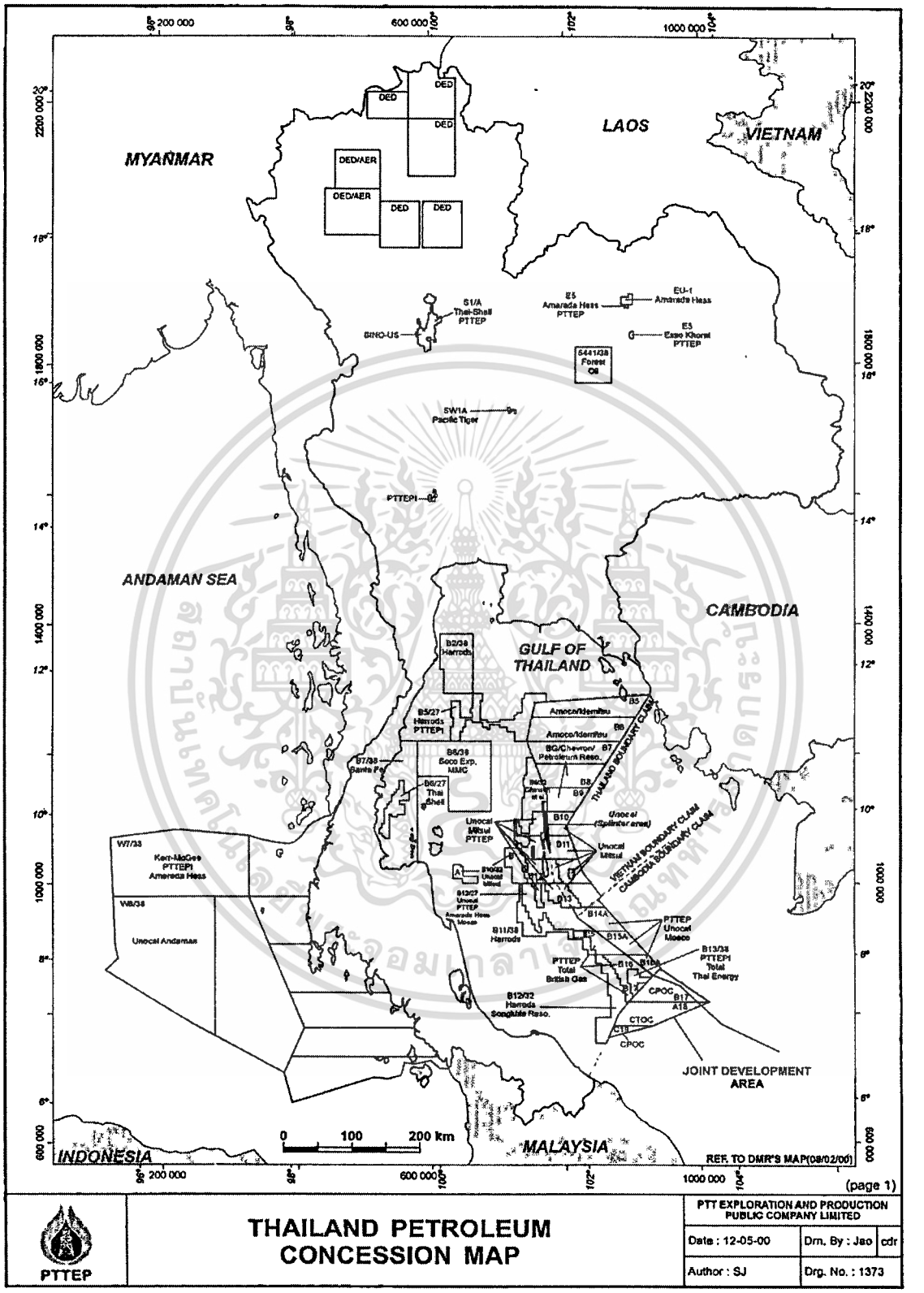
ปตท. สผ. จัดตั้งเป็นบริษัทขึ้นเมื่อวันที่ 20 มิถุนายน 2528 โดยเป็นไปตามเจตนารมณ์ของคณะรัฐมนตรี ที่ต้องการเสริมสร้างความมั่นคงด้านพลังงานให้กับประเทศ รวมทั้งลดการพึ่งพาการนำเข้าปิโตรเลียมจากต่างประเทศ คณะรัฐมนตรีจึงได้มอบหมายให้การปิโตรเลียมแห่งประเทศไทย (ปตท.) จัดตั้ง บริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด หรือ ปตท. สผ. ขึ้นโดยดำเนินธุรกิจหลัก คือ สำรวจ พัฒนา และผลิตปิโตรเลียมให้เกิดประโยชน์สูงสุดต่อประเทศ ต่อมาเพื่อเป็นการรองรับการขยายบทบาททางธุรกิจสำรวจและผลิตปิโตรเลียมทั้งภายในและต่างประเทศ และลดภาระของรัฐ ปตท. สผ. จึงได้ระดมทุนจากภาคเอกชนด้วยการนำหุ้นเข้าจดทะเบียนเป็นบริษัทมหาชนในปี พ. ศ. 2535 ปัจจุบัน ปตท. สผ. มีทุนจดทะเบียน 3,272 ล้านบาท และมี ปตท. เป็นผู้ถือหุ้นรายใหญ่ในสัดส่วนร้อยละ 60.97

นอกเหนือจากธุรกิจด้านสำรวจและผลิตปิโตรเลียมแล้ว ปตท. สผ. ยังได้ขยายการลงทุนไปสู่ธุรกิจแปรรูปพลังงานเพื่อเป็นการส่งเสริมการดำเนินงานของธุรกิจหลัก โดยได้ร่วมลงทุนกับบริษัท ไทยออยล์เพาเวอร์ จำกัด ดำเนินธุรกิจไฟฟ้าในโครงการผู้ผลิตไฟฟ้ารายเล็ก (SPP)

ในด้านการบริหาร ปตท. สผ. ในฐานะที่เป็นบริษัทจดทะเบียนชั้นนำของประเทศ ได้มีแนวทางการบริหารงานตามหลักการกำกับดูแลกิจการที่ดี สอดคล้องกับกฎหมายและข้อบังคับต่างๆ ที่เกี่ยวข้อง เพื่อให้เกิดความโปร่งใส มีระบบการจัดการที่มีประสิทธิภาพ และเพิ่มคุณค่าให้กับบริษัทฯ อย่างยั่งยืนในระยะยาว พร้อมกันนี้ ปตท. สผ. ได้พัฒนาการปฏิบัติงานภายในบริษัทฯ ให้เป็นองค์กรแห่งการเรียนรู้ ตามหลักการและแนวทางของ Society for Organizational Learning (SOL) เพื่อเพิ่มพูนศักยภาพและความก้าวหน้าในการดำเนินงานอันเป็นการเตรียมความพร้อมไปสู่การเป็นองค์กรระดับแนวหน้าดังวิสัยทัศน์ของบริษัทฯ

โครงการที่ ปตท. สผ. เป็นผู้ร่วมลงทุน และเป็นผู้ดำเนินการ ประกอบไปด้วย

1. โครงการบงกช แหล่งก๊าซธรรมชาติขนาดใหญ่ในอ่าวไทย
2. โครงการอาทิตย์ พื้นที่คาบเกี่ยวไทย – เวียดนาม
3. โครงการพีทีทีอีพี 1 ตั้งอยู่บริเวณ จังหวัดสุพรรณบุรี และนครปฐม
4. โครงการเจดีเอ ตั้งอยู่บริเวณพื้นที่คาบเกี่ยวไทย – มาเลเซีย
5. โครงการไพลิน แหล่งก๊าซขนาดใหญ่ในอ่าวไทย



รูปที่ 3.1 แสดงโครงการการลงทุนของ ปตท. สผ.

6. โครงการยาดานา ตั้งอยู่ในอ่าว เมาะตะมะ ในสหภาพพม่า
7. โครงการเอส 1 เป็นแหล่งน้ำมันสิริกิต์ จังหวัด สุโขทัย พิษณุโลก กำแพงเพชร
8. โครงการเยตะกุน ตั้งอยู่ในอ่าวเมาะตะมะ สหภาพพม่า
9. โครงการยูโนแคล 3 ในอ่าวไทย
10. โครงการอี 5 ตั้งอยู่บริเวณ จังหวัดขอนแก่น
11. โครงการดับเบิ้ลยู 7/38 ตั้งอยู่ในทะเลอันดามัน
12. โครงการแปลง 52/97 พื้นที่คาบเกี่ยวไทย – เวียดนาม
13. โครงการแปลงบี และ 48/95 ตั้งอยู่นอกชาน สาธารณรัฐสังคมนิยม เวียดนาม

3.2 ภารกิจขององค์กร

วิสัยทัศน์ (Vision)

เป็นบริษัทสำรวจและผลิตปิโตรเลียมชั้นนำที่มีความสามารถ วิถีทางในการดำเนินการและศักยภาพในการแข่งขันระดับแนวหน้าของโลก

พันธกิจ (Mission)

ประกอบธุรกิจหลักในการลงทุนและดำเนินการสำรวจพัฒนาและผลิตปิโตรเลียม รวมทั้งกิจการต่อเนื่องที่มีความสำคัญเชิงกลยุทธ์ทั้งในและนอกประเทศ

ค่านิยม (Corporate Values)

ปตท. สผ. ให้ความสำคัญกับบุคลากรที่มีความเชี่ยวชาญระดับมืออาชีพ ใฝ่หาความรู้ ถ่ายทอดแลกเปลี่ยนประสบการณ์ และทุ่มเทเพื่อผลงานที่เป็นเลิศ

3.3 หลักการกำกับดูแลกิจการที่ดี (Good Governance)

บริษัท ปตท.สำรวจและผลิตปิโตรเลียมจำกัด (มหาชน) หรือ ปตท.สผ.ตระหนักถึงความสำคัญของการกำกับดูแลกิจการที่ดีเป็นอย่างยิ่ง โดยยึดถือหลัก 6 ประการ ดังนี้

1. ความรับผิดชอบ (Accountability)
2. ความตระหนักในหน้าที่ (Responsibility)
3. ความยุติธรรมและซื่อสัตย์ (Faimess and Integrity)
4. การดำเนินงานที่โปร่งใส (Transparency)
5. การสร้างคุณค่าระยะยาวแก่ผู้มีผลประโยชน์ร่วมกัน (Creation of Long-term Value to all Stakeholders)
6. ส่งเสริมการปฏิบัติที่เป็นเลิศ (Promotion of Best Practices)

การกำกับดูแลที่ดีทั้ง 6 ประการนี้ บริษัทมีปัจจัยผลักดันภายในของ ปตท.ส.ผ. 3 ประการ คือ

1. ความเป็นมืออาชีพ (Professionalism) ของบุคลากรทุกระดับ อาทิเช่น
   (1) มีความรู้ ความสามารถ และความเชี่ยวชาญในหน้าที่ที่รับผิดชอบ
   (2) มีความซื่อสัตย์สุจริต
   (3) มีวินัย และมีความสำนึกในหน้าที่ความรับผิดชอบของตน
   (4) พร้อมที่จะปรับเปลี่ยนไปสู่สิ่งที่ดีขึ้น และรู้จักตอบสนองต่อการเปลี่ยนแปลง
2. ระบบการควบคุมภายในที่ดี (Good Internal Control System) โดยมีความโปร่งใสในการดำเนินงาน
3. การปฏิบัติอย่างเสมอภาคและเป็นที่เชื่อถือต่อผู้ที่มีผลประโยชน์ร่วมกัน (Fiduciary Duties towards Stakeholders) ดังนี้
   (1) ผู้ถือหุ้น (Shareholders) อันได้แก่ ปตท. นักลงทุนทั่วไป และผู้ถือหุ้นรายย่อย โดยจะต้องดูแลรักษาการลงทุนของผู้ถือหุ้นให้ได้ผลตอบแทนที่เหมาะสมและยุติธรรม ปกป้องรักษากองทุน ทรัพย์สิน และสถานภาพทางการเงิน ให้มีสภาวะมั่นคง พัฒนางานของบริษัทเพื่อประโยชน์ต่อความคงอยู่และความเจริญเติบโต
   (2) ลูกค้า (Customers) ด้วยการจัดหาผลิตภัณฑ์และการบริการต่างๆ ที่คุ้มค่าในด้านราคา คุณภาพ และความปลอดภัย โดยผ่านขั้นตอนวิเคราะห์จากผู้เชี่ยวชาญ ทั้งในด้านเทคโนโลยี การรักษาสิ่งแวดล้อม และการพาณิชย์
   (3) พนักงาน (Employees) ด้วยการส่งเสริมและพัฒนาความสามารถของพนักงานให้เกิดศักยภาพในการปฏิบัติงานสูงสุด โดยจัดให้มีสภาพการจ้างที่ยุติธรรมและมีโอกาสก้าวหน้าในบริษัทอย่างเป็นธรรม และจัดให้มีสภาพแวดล้อมในการทำงานที่ดีและปลอดภัย
   (4) รัฐบาล (Government) ด้วยการปฏิบัติตามนโยบายของรัฐ รวมทั้งการปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง
   (5) ผู้ร่วมทุน (Partners) ด้วยการปฏิบัติงานอย่างมืออาชีพและโปร่งใสเพื่อผลประโยชน์สูงสุดร่วมกัน
   (6) สังคมและสิ่งแวดล้อม (Public & Environment) ด้วยการดำเนินธุรกิจในฐานะพลเมืองที่ดี มีความรับผิดชอบต่อสังคม พัฒนานำทรัพยากรปิโตรเลียมมาใช้ให้ได้ประโยชน์สูงสุดอย่างยั่งยืน และตระหนักถึงการปฏิบัติตามมาตรฐานต่างๆ ที่เกี่ยวกับการรักษาสุขภาพอนามัย ความปลอดภัย และสิ่งแวดล้อมอย่างถูกต้องเหมาะสม เพื่อปกป้องผล

กระทบใดๆ ที่ก่อให้เกิดความสูญเสียต่อชีวิตและทรัพย์สินของบุคลากร ชุมชน และสิ่งแวดล้อม ตลอดจนเป็นแหล่งข้อมูลที่เกี่ยวกับปิโตรเลียมให้แก่ประเทศ และให้ความร่วมมือกับบริษัทอื่นๆ ในการพัฒนาทรัพยากรปิโตรเลียม

(7) ผู้ค้า/ผู้ขาย (Suppliers) ด้วยการปฏิบัติต่อผู้ค้า/ผู้ขายอย่างเสมอภาคและเป็นธรรม โดยคำนึงถึงประโยชน์ต่อบริษัทสูงสุด

(8) เจ้าหนี้ (Lenders) ด้วยการปฏิบัติตามพันธะสัญญา และให้ความเป็นธรรมแก่เจ้าหนี้ตามลำดับชั้นของหนี้ตามสัญญาที่ได้กระทำไว้

3.4 โครงสร้างองค์กรและการบริหารของบริษัท ปตท.สผ.

ปตท.สผ.มีโครงสร้างองค์กรและการบริหารแบ่งเป็นหลักๆ ได้แก่

1. คณะกรรมการบริษัท (Board of Directors) มีคณะกรรมการทั้งสิ้น 2 ชุด ได้แก่คณะกรรมการปตท.สผ. และคณะกรรมการตรวจสอบ คณะกรรมการมีอำนาจหน้าที่ในการกำหนดนโยบาย แผนกลยุทธ์ วิสัยทัศน์ แผนงาน งบประมาณในการดำเนินประจำปี การแต่งตั้งถอดถอนฝ่ายจัดการของ ปตท.สผ.รวมทั้งติดตามการดำเนินงานต่างๆ

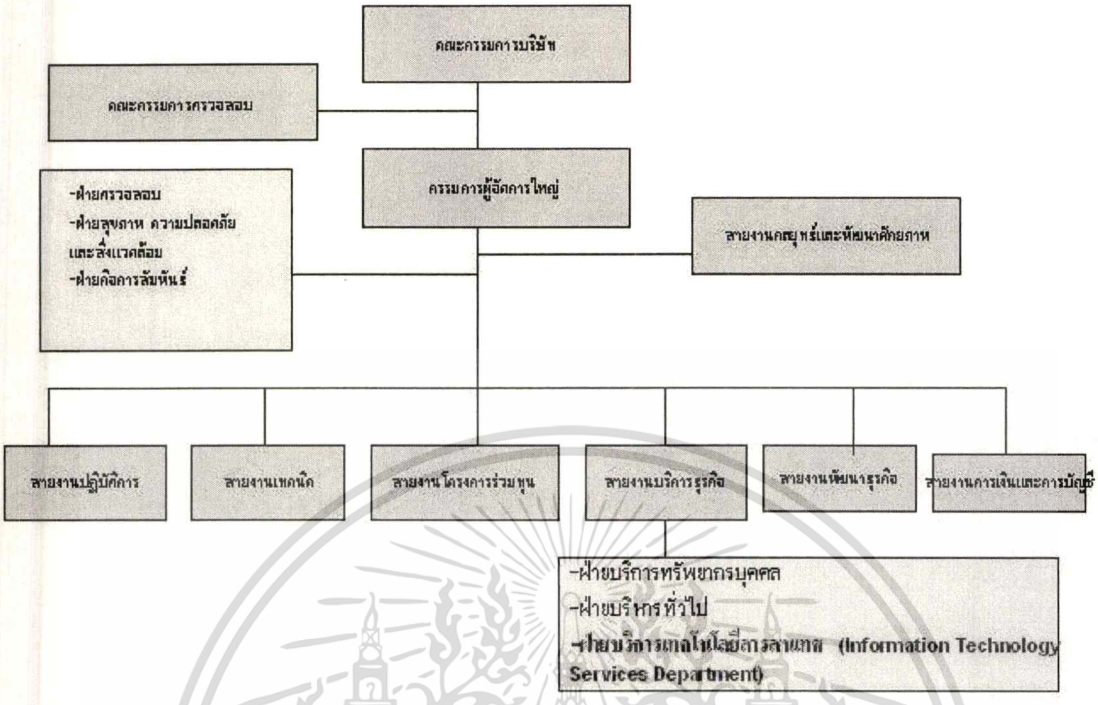
2. กรรมการผู้จัดการใหญ่ (President) มีหน้าที่ควบคุมจัดการดำเนินงานให้เป็นไปตามที่คณะกรรมการบริษัทเสนอแนะและให้ความเห็นชอบ

3. สายงานกลยุทธ์และพัฒนาศักยภาพ (Strategy & Capacity Development Division) มีหน้าที่สนับสนุนและวางแผนงานเพื่อดำเนินธุรกิจประกอบด้วย ฝ่ายแผนกลยุทธ์ ฝ่ายวิเคราะห์ธุรกิจ ฝ่ายนโยบายทรัพยากรบุคคล ฝ่ายพัฒนาองค์กร

4. สายงานปฏิบัติการ (Operation Division) มีหน้าที่ดำเนินงานตามโครงการต่างๆ

5. สายงานโครงการร่วมทุน (E & P Investment Division) มีหน้าที่ในการวิเคราะห์ ประเมิน ตรวจสอบโครงการและบริษัทที่จะร่วมทุนในการดำเนินโครงการต่างๆ

6. สายงานพัฒนาธุรกิจ (New Project Division) มีหน้าที่ในการพัฒนาธุรกิจต่อเนื่อง ศึกษาวิจัยพาณิชย์ปิโตรเลียม



รูปที่ 3.2 แสดงโครงสร้างองค์กร

7. สายงานเทคนิค (Technical Service Division) มีหน้าที่ในการสำรวจ ค้นคว้า ค้นหาแหล่งปิโตรเลียม รวมทั้งศึกษาขุดเจาะปิโตรเลียมโดยวิธีทางวิศวกรรมที่ดี

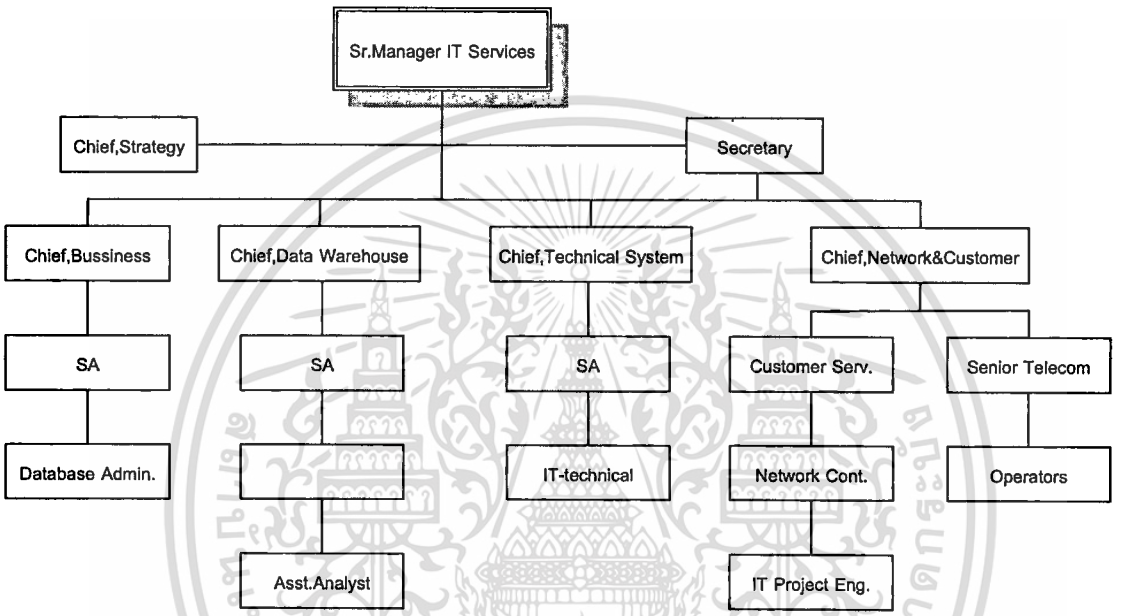
8. สายงานบริหารธุรกิจ (Business Service Division) มีหน้าที่ในการสนับสนุนงานธุรกิจได้แก่ งานบุคคล งานบริหารทั่วไป งานจัดซื้อจัดจ้าง งานกฎหมายข้อสัญญา งานบริการเทคโนโลยีสารสนเทศ

9. สายงานการเงินและบัญชี (Finance & Accounting Division) มีหน้าที่เกี่ยวกับงานบัญชีและงานการเงิน

3.5 โครงสร้างและหน้าที่แผนกเทคโนโลยีสารสนเทศ

แผนกบริการสารสนเทศ (Information Technology Department) เป็นแผนกที่สนับสนุนบริการธุรกิจขององค์กร ขึ้นตรงต่อฝ่ายบริการธุรกิจ แบ่งงานออกเป็น 5 หน่วยงานดังนี้

แผนกเทคโนโลยีสารสนเทศ



รูปที่ 3.3 แสดงโครงสร้างแผนกบริการเทคโนโลยีสารสนเทศ

3.5.1 หน้าที่ของแต่ละหน่วยงานของแผนกบริการเทคโนโลยีสารสนเทศ

1. หน่วยงานส่งเสริมและพัฒนากลยุทธ์ด้าน IT มีหน้าที่คือ
   - ศึกษา พัฒนา ออกแบบระบบซอฟท์แวร์และฮาร์ดแวร์ ที่เหมาะสมกับหน่วยปฏิบัติการและสำนักงานใหญ่
   - พัฒนาแผนกลยุทธ์และสร้างระบบการสำรองข้อมูล ในกรณีเกิดเหตุฉุกเฉิน (Disaster and Recovery System)
   - ประเมินผลและวิเคราะห์ความต้องการซอฟท์แวร์ขององค์กรให้สอดคล้องกับงบประมาณ และระยะเวลา
   - ประเมินผลและแนะนำเทคโนโลยีใหม่ๆ ที่จะนำมาปรับปรุงระบบเทคโนโลยี สารสนเทศในองค์กร
2. หน่วยงานสนับสนุนระบบงานด้านธุรกิจ (Business System Development) มีหน้าที่คือ

- ศึกษา ออกแบบและพัฒนาซอฟท์แวร์ที่เกี่ยวกับธุรกิจ เช่น งานบุคคล บัญชีการเงิน การจัดซื้อ การบริหารพัสดุ ประกอบกับช่วยสนับสนุนผู้ใช้ในการจัดหาซอฟท์แวร์และฮาร์ดแวร์ที่เหมาะสม
- ดูแล ตรวจสอบระบบการทำงาน เช่น การจัดการฐานข้อมูล เพื่อให้เกิดการทำงานที่มีประสิทธิภาพ
- ร่วมมือกับบริษัทที่ปรึกษาเพื่อการประยุกต์ใช้ซอฟท์แวร์ในองค์กร
- ให้ความช่วยเหลือฝึกอบรมพนักงานในองค์กร

3. หน่วยงานฐานข้อมูลองค์กร (Corporate Data Warehouse) มีหน้าที่คือ
   - ศึกษา ออกแบบพัฒนาข้อมูลสำหรับผู้บริหาร
   - ควบคุมระบบ Internet และ Intranet ขององค์กร
   - จัดออกแบบระบบสำนักงานอัตโนมัติและ Workflow System
   - จัดระบบงานห้องสมุดให้เกิดประสิทธิผล
   - จัดการระบบงานเกี่ยวกับงานฐานข้อมูลปิโตรเลียม
4. หน่วยงานสนับสนุนระบบงานด้านเทคนิค (Technical System Development) มีหน้าที่คือ
   - ศึกษา ออกแบบ วิเคราะห์ ซอฟท์แวร์ที่สนับสนุนงานด้านเทคนิค เช่น งานสำรวจน้ำมัน ผลิตน้ำมันหรือก๊าซ การขุดเจาะก๊าซ
   - วางแผน ออกแบบ ระบบเครือข่ายทางงานเทคนิค การทำสำรองข้อมูล และการรักษาความปลอดภัยข้อมูล
   - ศึกษา ประเมินผล วางแผน สำหรับการจัดซื้อ การดูแลรักษา การปรับสมรรถนะของฮาร์ดแวร์
5. หน่วยงานเครือข่ายและบริการผู้ใช้ (Network Control and Customer Service) มีหน้าที่คือ
   - พัฒนาและจัดทำคู่มือระบบงานคอมพิวเตอร์
   - ติดตั้งและพัฒนาซอฟท์แวร์มาตรฐาน สำหรับเครื่องคอมพิวเตอร์ทุกเครื่องในองค์กร รวมทั้งการฝึกอบรมแก่พนักงาน
   - จัดระบบความช่วยเหลือ (Help desk) เพื่อแก้ปัญหากับผู้ใช้งาน
   - ควบคุมและสั่งการงานประจำในศูนย์คอมพิวเตอร์ เช่น สำเนาข้อมูล การพิมพ์ ระบบแอร์ ระบบ UPS ระบบไฟ เป็นต้น
   - ควบคุมและพัฒนาคู่มือมาตรฐานที่เกี่ยวข้องกับเครือข่ายของบริษัท

- วางแผน ออกแบบ ติดตั้ง ระบบเครือข่ายขององค์กร รวมทั้งการแก้ปัญหาที่อาจเกิดขึ้นได้
- ตรวจสอบการทำงานของอุปกรณ์เครือข่ายทั้ง LAN และ WAN ให้มีประสิทธิภาพอยู่เสมอ
- ศึกษาเทคโนโลยี รวมทั้งกำหนดเทคโนโลยีที่เหมาะสมกับเครือข่ายขององค์กรทั้งฮาร์ดแวร์และซอฟท์แวร์
- ศึกษาและทดสอบซอฟท์แวร์ทั่วๆ ไปก่อนทำการติดตั้งใช้ในองค์กร
- ศึกษาและตรวจสอบระบบเครือข่ายการเข้าถึงระยะไกล (Remote Access)
- จัดการระบบอิเล็กทรอนิกส์เมล์ทั่วทั้งองค์กร (Electronic Mail System)
- จัดระบบ Telemetry System ของหน่วยปฏิบัติการ (Operation Unit)

3.5.2 ขอบเขตและความรับผิดชอบของแต่ละส่วนงาน

ปตท. สผ. ได้จัดแบ่งระบบสารสนเทศเป็นระบบย่อย ๆ (Sub system) และให้มีหัวหน้าส่วนเป็นผู้รับผิดชอบโดยแต่ละระบบย่อย ๆ ประกอบไปด้วยดังนี้

1. ส่วนบริการลูกค้าและเครือข่าย (BIT/C) ดูแลรับผิดชอบในเรื่องของ
   (1) Phone and Fax
   (2) Local Area Network
   (3) Desktop Computer and Applications
   (4) File and Print Service
   (5) Wide Area Network
   (6) Mail System
2. ส่วนพัฒนาแอพพลิเคชั่น (BIT/D) ดูแลรับผิดชอบในเรื่องของ
   (1) Internet / Firewall
   (2) The Company's public web site
   (3) E&P Library and Information Center
3. ส่วนพัฒนาระบบแอพพลิเคชั่นธุรกิจ (BIT/B) ดูแลรับผิดชอบในเรื่องของ
   (1) SAP
   (2) Oracle Finance
   (3) Maximo (Maintenance Software)

4. ส่วนพัฒนาระบบแอพพลิเคชั่นทางเทคนิค (BIT/T) ดูแลรับผิดชอบในเรื่องของระบบสารสนเทศ Geological and Geophysical System

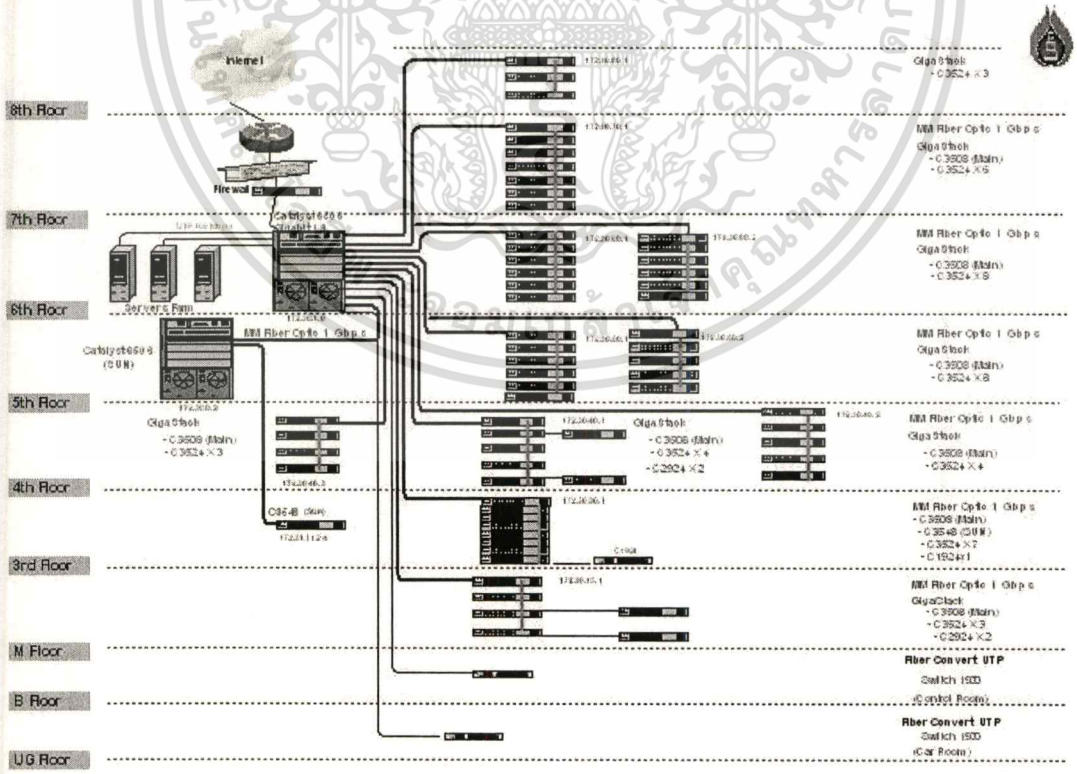
3.6 โครงสร้างสถาปัตยกรรมระบบสารสนเทศ

โครงสร้างสถาปัตยกรรมระบบสารสนเทศ ของ ปตท. สผ. แบ่งได้เป็น 4 กลุ่มใหญ่ ๆ คือ

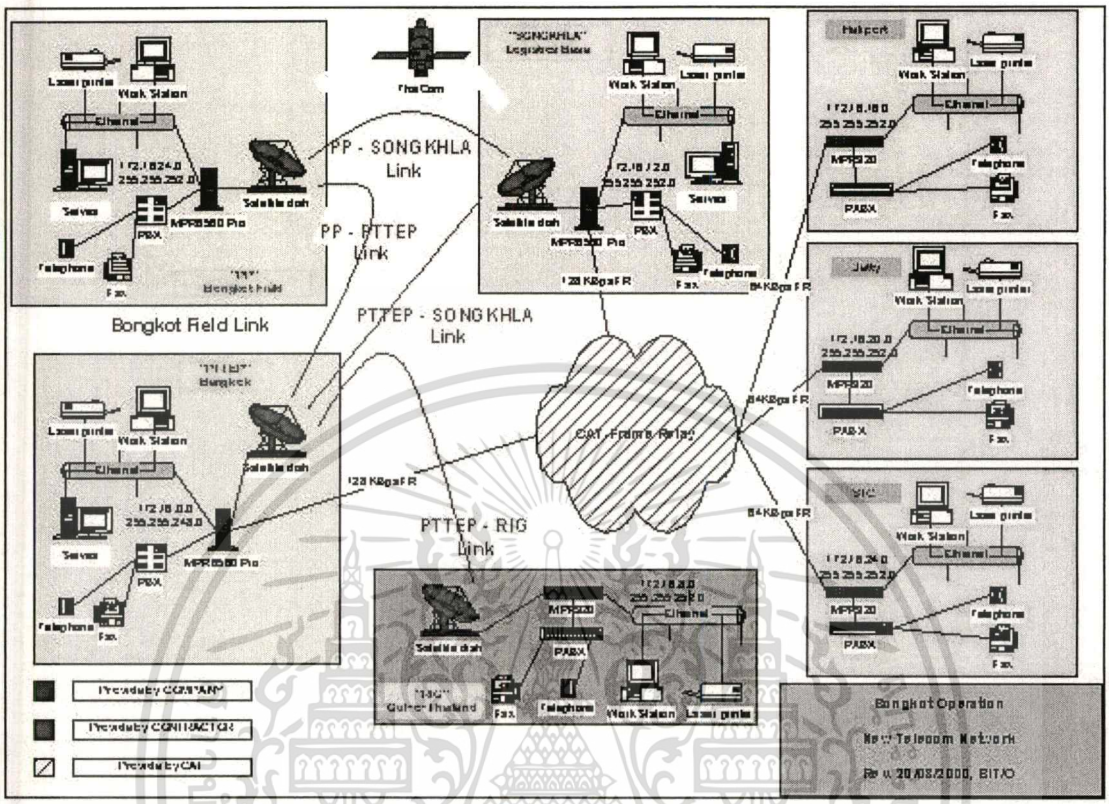
1. ระบบการสื่อสารและโทรคมนาคม (Communication System)
2. ระบบงานธุรกิจเบ็ดเสร็จ (PTTEP Integrate Business System (PIBS))
3. ระบบสารสนเทศงานธรณีวิทยาและธรณีฟิสิกส์ (Geological and Geophysical System หรือ G&G System)
4. ระบบงานเครื่องคอมพิวเตอร์ส่วนบุคคล (Desktop Computing System)

3.6.1 ระบบการสื่อสารและโทรคมนาคม (Communication System)

ระบบการสื่อสารและโทรคมนาคม แบ่งเป็น 2 ระบบ คือ ระบบ Local Area Network (LAN) และ Wild Area Network (WAN) เพื่อใช้ติดต่อสื่อสารหน่วยงานขององค์กรระหว่างสาขา



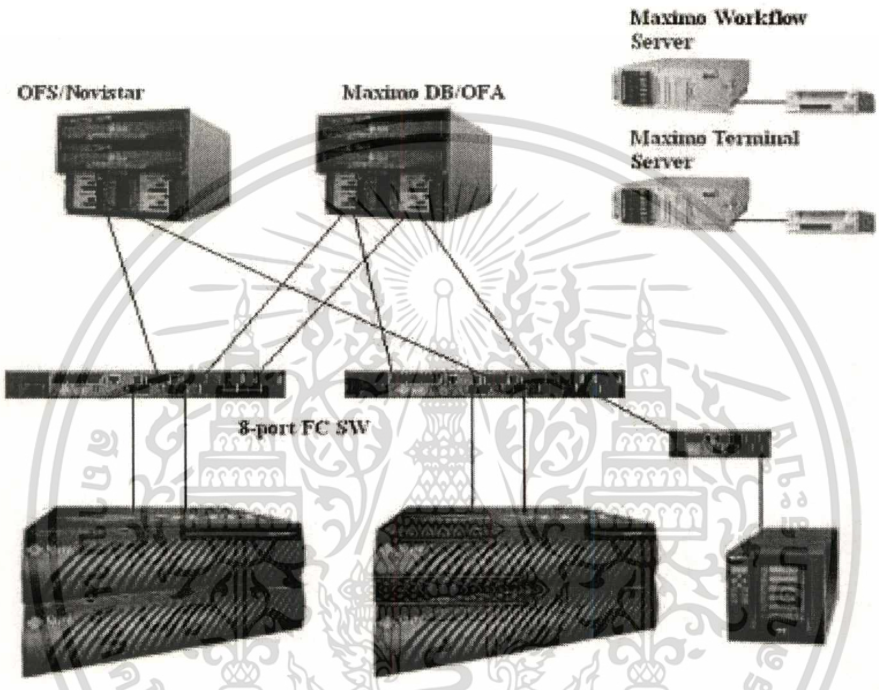
รูปที่ 3.4 แสดงระบบเครือข่ายท้องถิ่น



รูปที่ 3.5 แสดงระบบเครือข่ายระยะ ไกล (Wide Area Network)

3.6.2 ระบบงานธุรกิจเบ็ดเสร็จ (PTTEP Integrate Business System (PIBS)

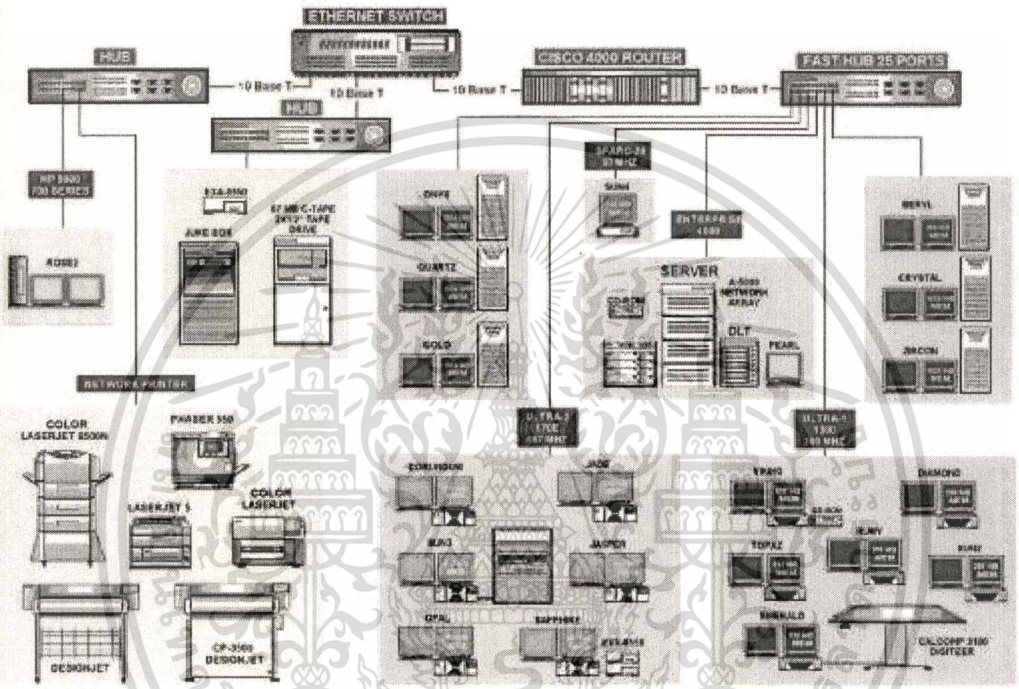
เป็นระบบสารสนเทศที่ทำงานด้านบัญชี การจัดซื้อจัดหาและการบำรุงรักษา โดยเป็นระบบฐานข้อมูลออราเคิล ทำงานในรูปแบบของสถาปัตยกรรมไคลเอ้นท์เซิฟเวอร์ โดยที่ข้อมูลถูกจัดเก็บในรูปแบบสื่อบันทึกที่เรียกว่า SAN (Storage Area Network) และ NAS (Network Area Storage)



รูปที่ 3.6 แสดงการเชื่อมต่อของระบบงานธุรกิจเบ็ดเสร็จ

3.6.3 ระบบสารสนเทศงานธรณีวิทยาและธรณีฟิสิกส์ (Geological and Geophysical System หรือ G&G System)

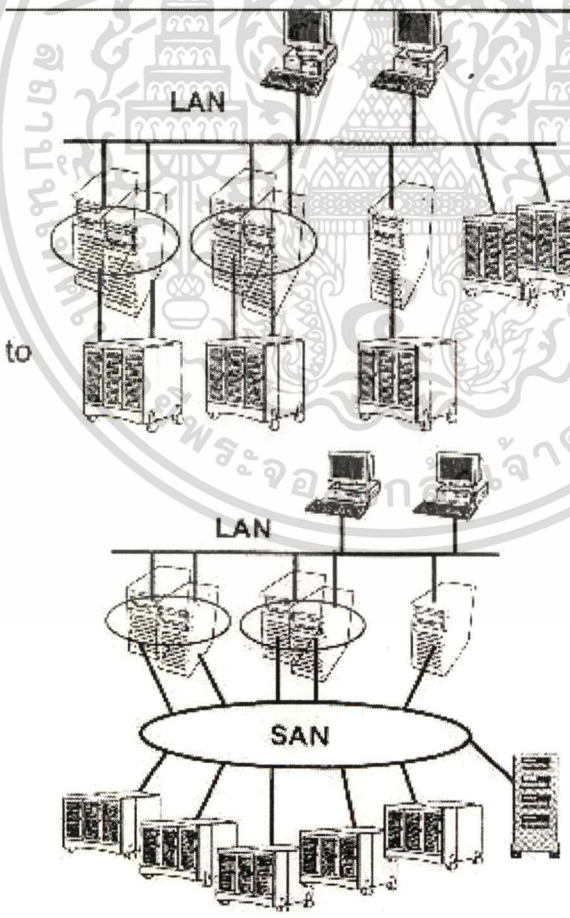
เป็นระบบงานสารสนเทศเพื่อการค้นหา สำรวจ วิเคราะห์ติดตามงานสำรวจก๊าซและแหล่งน้ำมันโดยใช้ระบบสารสนเทศแบบยูนิกซ์ทำงานทั้งส่วนแอพพลิเคชั่นและฐานข้อมูล



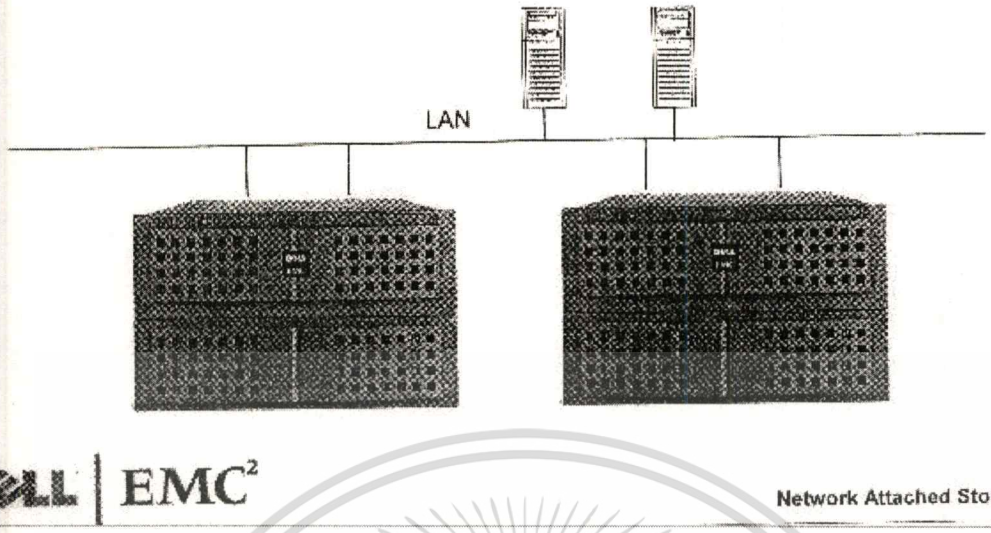
รูปที่ 3.7 แสดงระบบสารสนเทศงานธรณีวิทยาและธรณีฟิสิกส์

3.6.4 ระบบงานเครื่องคอมพิวเตอร์ส่วนบุคคล (Desktop Computing System) ประกอบด้วย

- เครื่องพีซี ประมาณ 700 เครื่อง มีคุณลักษณะเป็นเครื่องเพ็นเทียมโฟร์ระดับ 1.7 กิกะเฮิรต์ มีขนาดของฮาร์ดดิสก์ 20 กิกะไบต์ มีหน่วยความจำ 256 เมกกะไบต์
- สนับสนุนซอฟท์แวร์ที่ใช้ทั่วไป เช่น E-mail, Word Processing, Spreadsheet, Web Browser และซอฟท์แวร์ทางด้านเทคนิคอื่นๆ เช่น AutoCAD, MS Project, Primavera ฯลฯ
- แอพพลิเคชั่น เช่น Back-End Application เช่น Proxy Server, Firewall, Mail Gateway, Domain Server เป็นต้น
- ไฟล์เซิร์ฟเวอร์หรือไดร์เครือข่ายสำหรับเก็บแฟ้มข้อมูลส่วนบุคคลและแฟ้มข้อมูลของแผนกและการแบ่งปันแฟ้มข้อมูลระหว่างแผนกในองค์กร โดยเก็บในอุปกรณ์ที่เป็น SAN และ NAS



รูปที่ 3.8 แสดงการเชื่อมต่อของ SAN



รูปที่ 3.9 แสดงการเชื่อมต่อของ Network Attached Storage (NAS) ของ ปตท. สผ.

3.7 นโยบายเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ และการใช้การสื่อโทรคมนาคม

ปตท.สผ. ได้กำหนดนโยบายทั่วไปเกี่ยวกับการใช้อุปกรณ์และระบบเทคโนโลยีสารสนเทศในเชิงกว้างให้พนักงาน ลูกจ้างได้รับรู้และนำไปปฏิบัติ

3.7.1 วัตถุประสงค์ และความรับผิดชอบ

การใช้คอมพิวเตอร์และอุปกรณ์อื่นๆ ที่เกี่ยวข้อง กับการใช้บริการเทคโนโลยีสารสนเทศ หรืออุปกรณ์การสื่อสารโทรคมนาคม ถือเป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ ที่จะใช้ประโยชน์ให้ได้อย่างเหมาะสม เชื่อถือได้ตามมาตรฐานของการดำเนินธุรกิจ และสอดคล้องตามนโยบายและจรรยาบรรณของบริษัท

3.7.2 การใช้เทคโนโลยีสารสนเทศ

1. Internet
   - ปตท.สผ. สนับสนุนให้มีบริการ Internet เพื่อให้บุคลากรสามารถทำงานได้บรรลุเป้าหมายหรือวัตถุประสงค์อย่างมีประสิทธิภาพด้วยเทคโนโลยีที่ทันสมัย
   - ปตท. สผ. ส่งเสริมให้มีการใช้บริการ Internet เพื่อเป็นกลยุทธ์ในการดำเนินธุรกิจ และเป็นเครื่องมือแห่งการเรียนรู้ รวมถึงการใช้ในกิจกรรมส่วนตัวตามสมควร แต่ห้ามมิให้นำไปใช้ในธุรกิจส่วนตัว

- ตลอดเวลาที่ใช้บริการ Internet ทั้งในและนอกเวลาทำงานจะต้องรับผิดชอบที่จะหลีกเลี่ยง Internet Site ที่ ปตท. สผ. ถือว่าผิดกฎหมาย หรือ ละเมิดศีลธรรมอันดีงาม และผู้ใช้บริการจะต้องงดเว้นที่จะเผยแพร่ข้อมูลหรือข่าวสารของ Internet Site ดังกล่าวต่อผู้อื่น
- ปตท. สผ. มีสิทธิที่จะต้องตามดูแลการใช้บริการ Internet และปิดกั้นการเข้าถึง Internet Site ดังกล่าว และถ้าผู้ใช้ Internet มีข้อสงสัยว่า Internet Site ใดที่ ปตท. สผ. ถือว่าผิดกฎหมาย หรือละเมิดศีลธรรม ขอให้ปรึกษาฝ่ายกฎหมายของบริษัท
- กิจกรรมบน Internet ถือว่าเป็นกิจกรรมสาธารณะ ผู้ใช้จะต้องพิจารณาใช้อย่างระมัดระวัง การส่ง Internet E-mail สำหรับข้อมูลที่เป็นความลับจะต้องดำเนินการเข้ารหัสที่เหมาะสมด้วย

2. Electronic Mail (E-mail)
   - ปตท. สผ. ได้ดำเนินการให้มีระบบ Electronic mail (E-mail) เพื่อให้บุคลากรทุกระดับได้ใช้ในการสื่อสารโดยปกติในกิจกรรมของบริษัท สำหรับการใช้เพื่อกิจกรรมส่วนตัวสามารถทำได้ตามสมควร แต่บริษัทไม่อนุญาตให้นำไปใช้ในธุรกิจส่วนตัว
   - บุคลากรจะต้องหลีกเลี่ยงที่จะส่ง E-mail ที่จะเป็นอุปสรรคต่อการปฏิบัติงานของ ปตท. สผ. หรือสร้างความรำคาญต่อผู้อื่น หรือฝ่าฝืนนโยบายบริษัท หรือผิดกฎหมาย หรือละเมิดศีลธรรม
   - ผู้ใช้บริการ E-mail จะต้องรับทราบว่าเนื้อหาของ E-mail ซึ่งรวมถึง E-mail ส่วนตัวที่เก็บอยู่ในระบบ E-mail ของ ปตท. สผ. อาจจะถูกตรวจสอบด้วยเหตุผลที่เหมาะสมโดยผู้ที่ได้รับมอบหมายจาก ปตท. สผ.
   - พนักงานที่มีสิทธิพิเศษในการเข้าถึงเนื้อหา E-mail ของผู้อื่นจะกระทำการดังกล่าวก็ต่อเมื่อได้รับความเห็นชอบจากผู้มีอำนาจเท่านั้น ผู้ที่เข้าถึงเนื้อหาของ E-mail ของผู้อื่นโดยมิได้รับอนุญาตจะถือว่ามีความผิด

3. การเข้าถึงข้อมูล (Access)
   - บุคลากรที่ได้รับมอบหมายเท่านั้นที่มีสิทธิเข้าถึงแฟ้มข้อมูลหรือโปรแกรม ไม่ว่าจะเก็บในรูปของแฟ้มข้อมูลคอมพิวเตอร์หรือรูปแบบอื่นๆ
   - การพยายามเข้าถึงข้อมูลเพื่อดู ทำซ้ำ เผยแพร่ ลบทิ้ง หรือเปลี่ยนแปลงข้อมูล เปลี่ยนแปลงรหัสผ่าน หรือกระทำการอื่นใดที่ทำให้เกิดความเสียหายโดยผู้ที่ไม่ได้รับมอบหมาย ปตท. สผ. ถือว่ามีความผิด

4. การใช้อุปกรณ์การสื่อโทรคมนาคม

- อุปกรณ์การสื่อสารโทรคมนาคม ได้แก่ โทรศัพท์ โทรสาร โทรศัพท์มือถือ วิทยุติดตามตัว (Pager) วิทยุรับส่งอุปกรณ์รับสัญญาณดาวเทียม คู่สายเช่าต่างๆ เป็นต้น
- ปตท. สผ. ได้ดำเนินการให้มีระบบการสื่อสารโทรคมนาคมเพื่อให้บุคลากรใช้ในการสื่อสารเพื่อประโยชน์ทางธุรกิจของ ปตท. สผ. สำหรับการใช้เพื่อกิจกรรมส่วนตัวสามารถทำได้ตามสมควร แต่ไม่อนุญาตให้นำไปใช้ในธุรกิจส่วนตัว
- บุคลากรจะต้องหลีกเลี่ยงที่ใช้อุปกรณ์การสื่อสารโทรคมนาคมที่จะเป็นอุปสรรคต่อการปฏิบัติงานของ ปตท. สผ. หรือสร้างความรำคาญต่อผู้อื่นหรือฝ่าฝืนนโยบายบริษัท หรือใช้ในทางที่ผิดกฎหมาย
- อุปกรณ์การสื่อสารโทรคมนาคมบริษัทมีไว้ให้บุคลากรได้ใช้ตามความจำเป็นในการดำเนินธุรกิจตามหน้าที่ที่ได้รับมอบหมาย มิใช่ให้ตามตำแหน่งที่ได้รับแต่งตั้ง ดังนั้นการนำอุปกรณ์การสื่อสารโทรคมนาคมไปใช้ในธุรกิจส่วนตัวบริษัทไม่อนุญาตให้กระทำ
- การดักฟัง การบันทึกเทป ซึ่งเนื้อหาของการสื่อสาร เป็นสิ่งซึ่งมิให้กระทำ เว้นแต่การบันทึกเทป ซึ่งเนื้อหาของการสื่อสารที่ ปตท. สผ. ใช้ดำเนินการทางธุรกิจโดยปกติหรือการบันทึกเทปในกรณีพิเศษ ซึ่งจะต้องได้รับความเห็นชอบจากกรรมการผู้จัดการใหญ่ก่อน

3.7.3 สิทธิส่วนบุคคล (Privacy)

นโยบายของ ปตท. สผ. ยืนยันที่จะปฏิบัติตามกฎหมายที่เกี่ยวข้องกับสิทธิส่วนบุคคลของพนักงานในสถานที่ทำงาน แต่อย่างไรก็ตาม ปตท. สผ. สงวนสิทธิ์การเข้าถึงข้อมูลสารสนเทศใดๆ ซึ่งจะรวมถึง Voice Mail และ E-mail ที่เก็บอยู่ในระบบคอมพิวเตอร์ หรืออุปกรณ์อื่นๆ ที่เกี่ยวข้อง หรืออุปกรณ์โทรคมนาคม อันเป็นทรัพย์สินหรือสิทธิของ ปตท. สผ. หรืออยู่ในพื้นที่ของปตท. สผ. นอกจากนี้ บริษัทย่อมมีสิทธิที่จะเปลี่ยนรหัสผ่าน เพื่อประโยชน์ในการตรวจสอบ สอบสวน หรือค้นหาแฟ้มข้อมูลคอมพิวเตอร์ Voice Mail หรือ E-mail ดังกล่าว

3.7.4 การมอบหมายหรืออนุญาต

การมอบหมายหรืออนุญาตให้ผู้ปฏิบัติงานสมทบ พนักงานของผู้รับจ้าง หรือพนักงานจากบริษัทที่ปรึกษาใช้ระบบคอมพิวเตอร์ของ ปตท. สผ. หรืออุปกรณ์อื่นใดที่เกี่ยวข้อง ซึ่งรวมถึงลิขสิทธิ์ของซอฟท์แวร์ โปรแกรม และอุปกรณ์การสื่อสารโทรคมนาคม หน่วยงานต้นสังกัดจะต้องดูแลให้การ

ใช้ และการเข้าถึงระบบคอมพิวเตอร์และอุปกรณ์การสื่อสารโทรคมนาคม ดังกล่าวในขอบเขตที่จำกัดตามความจำเป็นที่จะใช้ทำงานเพื่อสนับสนุนธุรกิจของปตท. สผ.

3.8 นโยบายความปลอดภัยระบบสารสนเทศของ ปตท. สผ.[1]

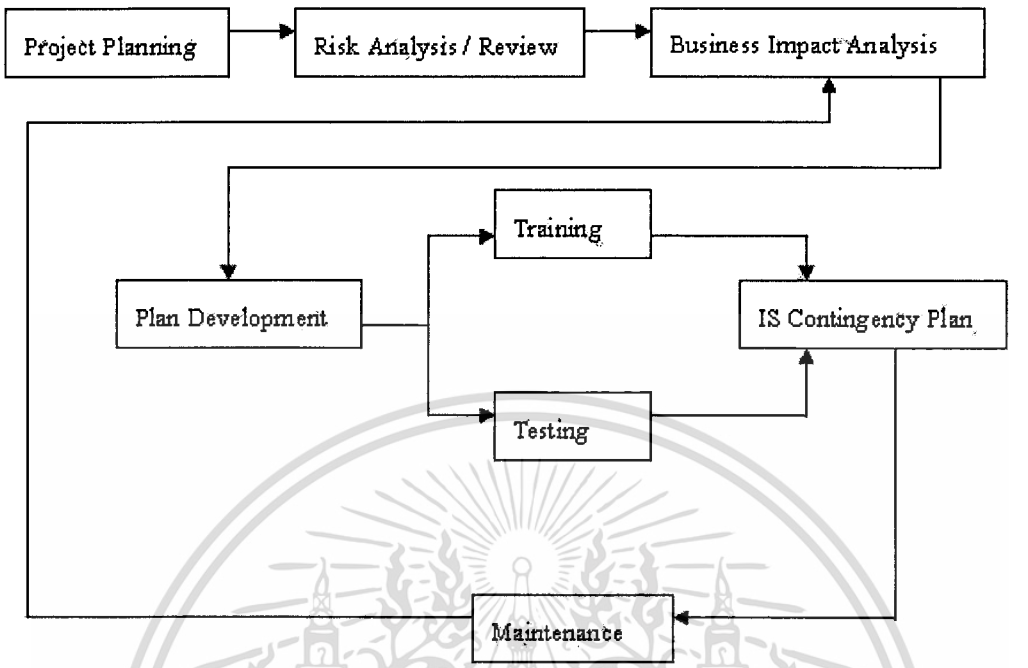
เนื่องจากการกำหนดนโยบายของ ปตท. สผ. จัดทำเป็นภาษาอังกฤษ ผู้ศึกษาจึงไม่ได้แปลข้อมูลให้เป็นภาษาไทย เนื่องจากการแปลเป็นภาษาไทยอาจทำให้ความหมายอาจคลาดเคลื่อนจากของเดิมที่ปตท. สผ. กำหนดไว้

3.9 แผนว่าด้วยการจัดการปัญหา (PTTEP Information System Contingency Plan)

เป็นแผนงานที่องค์กรจัดทำใช้เพื่อรองรับหรือจัดการปัญหาหรือความเสียหายที่อาจเกิดขึ้นกับองค์กรและระบบสารสนเทศ ซึ่งแผนจะประกอบด้วยแผนย่อย ๆ 4 แผนคือ

1. แผนบรรเทาความเสี่ยง (Risk Mitigation Plan)
2. แผนตอบสนองฉุกเฉิน (Emergency Response Plan)
3. แผนการดำเนินงานชั่วคราว (Interim Processing Plan)
4. แผนการกู้คืนสภาพเดิม (Recovery Plan)

[1] ภาคผนวก ก.



รูปที่ 3.10 แสดงขั้นตอนในการทำแผน (Planning Process)

3.9.1 แผนงานบรรเทาความเสี่ยง (Risk Mitigation Plan)

1. ประกอบด้วยขั้นตอนวิธีการที่เกี่ยวกับ
   - การออกนโยบายการจัดการปัญหา (IS Contingency Policy)
   - การจัดแบ่งระบบสารสนเทศของบริษัทเป็นระบบย่อย ๆ และจัดสรรผู้รับผิดชอบในแต่ละระบบ
   - ผู้รับผิดชอบแต่ละระบบจะรับผิดชอบเกี่ยวกับการจัดทำขั้นตอนวิธีการและแผนงานของระบบย่อยต่าง ๆ
   - การประชาสัมพันธ์ การตระหนักถึงแผน (The awareness of the plans)
   - การทดสอบแผนต่าง ๆ รวมทั้งขั้นตอนวิธีการต่าง ๆ
   - การบำรุงรักษาเอกสารให้ทันสมัยเสมอ โดยที่เอกสารต่าง ๆ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้รับผิดชอบในการประกาศใช้อย่างเป็นทางการ โดยที่แต่ละระบบย่อย ๆ จะมีแผนบรรเทาปัญหา ของตนเอง

2. Migration Plan จะมีเอกสารที่ประกอบด้วย
   (1) เวลากู้คืนตามประสงค์ (The Recovery Time Objective) (RTO) เป็นการกำหนดจุดหมายทางด้านเวลากู้คืนของแต่ละระบบย่อย ๆ หลังจากเกิดความสูญเสียหรือหายนะของแต่ละระบบย่อย ๆ โดยทั่ว ๆ ไปแต่ละหน่วยงานยอมรับผลกระทบว่าแต่ละระบบควรจะทำงานได้ หลังจากใช้เวลา 1 อาทิตย์
   (2) จุดเป้าหมายที่คาดจากการกู้คืน (The Recovery Point Objective (RPO)) หมายถึงการที่คาดว่าข้อมูลที่อาจจะสูญเสียไปจำนวนเท่าใดหลังจากกู้คืน ณ เวลาใดเวลาหนึ่ง และหน่วยงานทางธุรกิจต่าง ๆ สามารถยอมรับได้ ซึ่งหน่วยงานธุรกิจยอมรับว่าข้อมูลจะต้องไม่หายมากว่า 1 อัน และข้อมูลควรจะเก็บไว้นอกสถานที่ (off-site) แต่ก็ขึ้นอยู่กับความเหมาะสมของการพิจารณาจากหัวหน้าในฝ่ายต่าง ๆ ของระบบสารสนเทศ
   (3) ความยืดหยุ่นของระบบ (The System Resiliency) เกี่ยวข้องกับ RPO และ RTO ซึ่งหัวหน้าฝ่ายต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศจะต้องพิจารณาออกแบบระบบต่าง ๆ ให้มีความเหมาะสมทางวิศวกรรม
   (4) รายละเอียดขั้นตอนการกู้คืนของระบบย่อย ๆ (The Detail Recovery Procedures of The Subsystems) ขั้นตอนต่าง ๆ จะต้องมีการกำหนดบุคคลผู้รับผิดชอบโดยที่จะต้องมีผู้บริหารระบบเป็นผู้รับผิดชอบหลักและมีบุคคลอื่น ๆ สามารถทำตามได้กรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้
3. การจัดทำเอกสาร
   (1) การจัดทำเอกสารสำหรับการฝึกปฏิบัติต่าง ๆ รวมทั้งการทดสอบต่าง ๆ จะต้องมีเอกสารกำกับ โดยเอกสารนั้นอธิบายถึง
      - วันเวลาที่ฝึกปฏิบัติหรือทดสอบ
      - บุคคลที่เกี่ยวข้อง
      - วัสดุอุปกรณ์ที่ใช้รวมทั้งระบบที่ใช้
      - ขั้นตอนในการฝึกปฏิบัติ
      - ปัญหาที่เกิดขึ้น
   (2) รวมทั้งต้องมีการจัดทำรายการเอกสารดังต่อไปนี้ในฝ่ายเทคโนโลยีสารสนเทศ
      - จัดทำรายการซอฟท์แวร์ (Software Inventory Document)
      - จัดทำรายการฮาร์ดแวร์ (Hardware Inventory Document)
      - จัดทำเอกสารสัญญาการบำรุงรักษา (Maintenance Contract Document)

- จัดทำเอกสารที่อยู่ที่สามารถติดต่อได้ทันทีทันใด (BIT Emergency Contract Documents)

4. การฝึกปฏิบัติแผนงาน (IS Contingency Exercise)

(1) วัตถุประสงค์แผนงานเพื่อ

1. เพื่อกู้ช่วงระยะเวลาและลำดับความสำคัญของเหตุการณ์ต่าง ๆ
2. ทวนสอบแผนและเอกสารให้ง่ายและเข้าใจง่าย
3. ทวนซ้ำและอบรมแก่ผู้ดูแลระบบในขั้นตอนของการกู้คืนระบบ
4. ทวนซ้ำและอบรมผู้ใช้ให้สามารถทำงานได้ชั่วคราวตามวิธีการต่างๆ (Interim Procedures)

(2) การฝึกแผนปฏิบัติการจัดการปัญหาแบ่งเป็น 3 ชนิดประกอบด้วย

1. การฝึกปฏิบัติการร่วมฉุกเฉิน (Integrated Emergency Exercise) เป็นการฝึกการทำงานร่วมกับแผนกความปลอดภัยและสิ่งแวดล้อมร่วมกับแผนกประชาสัมพันธ์เป็นการฝึกการทำงานร่วมกันและการแจ้งเหตุปัญหา
2. การฝึกปฏิบัติตามกระบวนการกู้คืน (Recovery Procedures Exercise) โดยที่ผู้บริหารระบบจะต้องฝึกปฏิบัติอย่างน้อยปีละครั้ง
3. การฝึกปฏิบัติกระบวนการชั่วคราว (Interim Processing Exercise) เกี่ยวกับงานทางหน่วยธุรกิจหลักขององค์กรพนักงานต้องสามารถทำงานโดยตนเอง

3.9.2 แผนตอบสนองกรณีฉุกเฉิน (Emergency Response Plan) เป็นแผนงานและขั้นตอนการปฏิบัติงานที่อยู่ในหน่วยงานความปลอดภัยและสิ่งแวดล้อม

3.9.3 แผนปฏิบัติการชั่วคราว (Interim Processing Plan) เป็นแผนที่บ่งบอกถึงความรับผิดชอบของผู้ใช้งานที่สามารถทำงานได้ด้วยตนเอง (Manual Job) เพื่อรอการกู้คืนของระบบได้และบทบาทของพนักงานฝ่ายเทคโนโลยีสารสนเทศที่เกี่ยวข้องเช่นการสร้างระบบย่อย ๆ ขึ้นมารองรับให้พนักงานได้ทำงานต่อไปได้

1. ระบบสารสนเทศที่จัดการประกอบไปด้วย

1.1 ระบบ File and Print Servers

- ผลกระทบต่อธุรกิจองค์กร : ปานกลาง โดยกระทบต่อระบบต่างๆ คือ
  - ระบบการเงิน (Financial Impact)
  - การบริหารธุรกิจ (Business Service Impact) เช่นการจัดหาจัดซื้อ สวัสดิการ

- ระบบการสำรวจและผลิต (Exploration and Production Impact) ข้อมูลการลงทุน การสำรวจการขุดเจาะก๊าซต่าง ๆ

- การบรรเทาปัญหา (Mitigation Options) ทำได้โดย 1 ปีมีการสำรองข้อมูลไว้ต่างสถานที่เป็นเวลา 5 ปี และมีการตรวจสอบว่าการสำรองข้อมูลมีครบถ้วนสำหรับข้อมูลสำคัญ ๆ
- การให้ความรู้แก้ผู้ใช้เกี่ยวกับการเก็บข้อมูลที่ถูกต้องและเก็บไว้ในที่ปลอดภัย
  - การกู้คืน (Recovery Plan) ควรทำได้เสร็จสิ้นภายในหนึ่งสัปดาห์
  - กระบวนการทำงานชั่วคราว (Interim Processing Options) วิธีการโดยมีการเลือกกู้ข้อมูลที่มีความเร่งด่วนก่อนได้

1.2 ระบบ SAP มีผลกระทบต่องานบริหารทรัพยากรมนุษย์ (Human Resource Management Impact)

1.3 ระบบ Oracle Finance and Maximo มีความสำคัญสูงเกี่ยวกับ

- ระบบการเงินของสำนักงานใหญ่และสำนักงานสาขา
- Budgeting and Accounting
- Procurement and Logistic
- Flight Management
- Personal on Board (POB) report
- Manifesting and Stock
- Maintenance
- Joint Venture Accounting (JVA)
- Approve of Expenditure (AFE)
- Cash call

2. แนวทางเพื่อทุเลาปัญหา (Mitigation Options) ทำได้โดย

2.1 ให้มีการทำ off-line backup

- ข้อมูลและระบบมีการสำรองทุกวัน
- ข้อมูลที่สำรองในแต่ละวันต้องเก็บไว้เป็นเวลา 1 เดือน
- ข้อมูลสำรองประจำสัปดาห์ต้องเก็บไว้ 3 เดือน
- และเก็บสำรองข้อมูลไว้ประจำทุกเดือน

2.2 จัดทำสัญญาจ้าง (Maintenance Contract) โดย

- เกี่ยวกับฮาร์ดแวร์และซอฟท์แวร์
- เงื่อนไขในการบริการต้องภายใน 1 วัน

2.3 แผนการกู้คืน (Recovery Plan) โดยจะต้องประกอบด้วย

- Lead time about 45 days
- System Recovery about 4 hours
- Application recovery about 4 hours
- Total time to recovery about 8 hours (1 working day)

3. ระบบ G&G มีผลกระทบต่อองค์กรสูง ได้มีผลกระทบกับ

3.1 ลงทุนใหม่ New Venture Impact

3.2 Exploration and Production Investment Impact

วิธีการจัดการบรรเทาปัญหา (Mitigation Options) ได้แก่

- การสำรองข้อมูล
- การทำสำเนา (Hard Copy)
- การทำ Standardize Treatment and Flow of Data Asset

3.3 แผนการระหว่างช่วงเวลา (Interim Processing Options) ทำได้โดย

- ใช้อุปกรณ์ของผู้ค้าร่วม (Vendor's facilities)
- ใช้อุปกรณ์ของผู้ร่วมลงทุน (Partner's Facilities)
- ใช้การทำสัญญา (Quick Ship Contract)

4. E & P Library and Information Center งานด้านเอกสารที่เก็บไว้ในห้องสมุด ซึ่งมีผลกระทบโดยการจัดการปัญหาทำได้โดยเก็บไว้ในที่ทนความร้อนและความชื้น
5. ระบบโทรศัพท์และแฟ็กซ์ (Phone and Fax) ซึ่งมีผลกระทบต่อองค์กรปานกลาง การจัดการปัญหาอาจใช้โทรศัพท์เคลื่อนที่ (Mobile Phones) โทรศัพท์สาธารณะ จัดตัวระบบ PABX ใหม่
6. ระบบเครือข่ายท้องถิ่น (Local Area Network) มีผลกระทบต่อธุรกิจองค์กรปานกลาง
7. ระบบแอพพลิเคชั่น (Desktop Application) มีผลกระทบต่อองค์กรสูง การจัดการจะต้องมีการจัดทำระบบทรัพย์สินซอฟท์แวร์ ระบบการลงทะเบียน แอพพลิเคชั่นมาตรฐานจะต้องสามารถติดตั้งได้ทันทีโดยการทำ ghost หรือ clone ไว้
8. ระบบเครือข่ายระยะไกล (Wide Area Network) มีผลกระทบต่อองค์กรปานกลาง การจัดการทำได้โดยใช้การติดต่อสื่อสารทางอื่น ๆ ทดแทน

9. ระบบอินเทอร์เน็ต (Internet Access) มีความสำคัญในระดับต่ำสำหรับองค์กร การจัดการทำได้โดยใช้วิธีการอื่น ๆ แทน
10. ระบบอีเมล์ (E-mail) มีผลกระทบต่อองค์กรปานกลาง การจัดการปัญหาทำได้โดยให้ความรู้แก่พนักงานในการใช้ระบบอีเมล์ที่ถูกต้องไม่ได้ใช้เพื่อเก็บข้อมูล ให้ใช้วิธีการอื่นทดแทนในการสื่อสารติดต่อ

3.9.4 แผนการกู้คืนจากความเสียหายหรือการป้องกันความเสียหาย (Disaster Recovery Plan)

เนื่องจากปัจจุบันนี้ระบบสารสนเทศได้กลายเป็นปัจจัยหลักขององค์กรในการดำเนินธุรกิจปตท. สผ. เป็นองค์กรหนึ่งที่ใช้ระบบสารสนเทศเพื่อการธุรกิจด้านการสำรวจและผลิตปิโตรเลียม ซึ่งในต่างประเทศระบบสำรองข้อมูลเป็นเรื่องที่องค์กรให้ความสำคัญเพราะเป็นการประกันว่าธุรกิจจะไม่เกิดความเสียหายหรือเสียหายน้อยที่สุด หากเกิดเหตุการณ์ที่ไม่คาดคิด ปตท. สผ. จึงเล็งเห็นความสำคัญของการจัดตั้งหรือจัดหาศูนย์สำรองข้อมูลและระบบคอมพิวเตอร์ ขึ้นมารองรับความเสี่ยงของธุรกิจโดยการรับผิดชอบของแผนกเทคโนโลยีสารสนเทศ เนื่องจากข้อจำกัดด้านงบประมาณและทรัพยากร ทางแผนกสารสนเทศจึงพยายามแยกระบบที่มีความสำคัญหรือจัดทำระบบที่มีความสำคัญต่อองค์กรก่อนได้แก่ระบบงานด้านบัญชีและงบประมาณ ระบบเครือข่าย และระบบเมล์ โดยสถานที่ที่จะจัดทำนั้นได้พิจารณา อยู่ 3 แห่งได้แก่

- ที่ส่งกำลังบำรุง อำเภอสิงหนคร จังหวัดสงขลา
- สถานที่เก็บพัสดุ อำเภอโรจนะ วังน้อย จังหวัดพระนครศรีอยุธยา
- สถานที่ที่ของบริษัท ปตท. จำกัด (มหาชน) วังน้อย จังหวัดพระนครศรีอยุธยา

หลักการพิจารณาของแผนการกู้คืนจากความเสียหายและการป้องกันความเสียหายประกอบไปด้วย

1. Mind-set คือโอกาสที่จะเกิดความเสียหายอาจจะมีน้อยแต่ก็เป็นสิ่งจำเป็นที่จะต้องมีแผนการกู้คืนจากความเสียหาย รวมทั้งการทำแผนจะมีงบประมาณสูง นอกจากนี้แผนนี้ยังเป็นแผนเพื่อการกู้คืนมากกว่าแผนเพื่อการทำงานปกติ
2. เวลาในการกู้คืน (Recovery Time) จะต้องใช้เป็นหลักในการพิจารณาที่สำคัญซึ่งจะต้องตอบคำถามว่า ใช้เวลานานเท่าใดที่ทำให้ระบบสามารถกลับมาทำงานได้ปกติ เราสามารถกู้คืนได้ในระยะเวลาอันสั้นหรือไม่ ถ้าไม่มีแผนการกู้คืนจะมีวิธีการอื่นหรือไม่เพื่อให้ระบบสามารถกลับมาทำงานได้ปกติหลังจากเกิดความเสียหาย

3. ความสามารถยอมรับกับการสูญเสียข้อมูลได้หรือไม่ (Tolerable Data Lost) ถ้าองค์กรมีการสำรองข้อมูลไว้เมื่อเที่ยงคืนวันที่แล้วแต่ไฟไหม้ในช่วงบ่ายของอีกวันหนึ่งจะทำอย่างไรกับข้อมูลของช่วงเช้าที่ผ่านมา
4. เทคโนโลยีการสำรองข้อมูล (Backup Technology) เนื่องจากได้มีการพัฒนาเทคโนโลยีการทำสำรองข้อมูลอย่างมากได้แก่ความสามารถในการทำ
   - Remote Mirror เป็นการสำเนาข้อมูลทั้งหมด (entire data) จากเครื่องเก็บข้อมูลเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง เช่น SAN
   - Database Replication เป็นเทคนิคในการสำเนาเฉพาะฐานข้อมูลเท่านั้นไปยังอีกเครื่องหนึ่งในเครือข่าย
   - Log shipping เป็นเทคนิคในการทำสำเนาบันทึกรายการ (Log transaction) จากฐานข้อมูลหนึ่งไปยังอีกฐานข้อมูลหนึ่ง
   - Clustering เป็นเทคนิคในการสร้างระบบกลุ่มของคอมพิวเตอร์เพื่อช่วยกันทำงานหรือทำงานแทนอีกเครื่องหนึ่งที่เกิดความเสียหาย
   - Tape Backup เป็นเทคโนโลยีที่ใช้มานานเป็นการสำรองข้อมูลซึ่งต้องใช้เวลาในการกู้คืนข้อมูลซึ่งอาจมีความเสี่ยงในเรื่องของความทันสมัยข้อมูล

ระบบแผนการกู้คืนความเสียหายหรือการป้องกันระบบสารสนเทศประกอบไปด้วย 4 ระบบคือ

1. ระบบเครือข่ายและการติดต่อสื่อสาร รวมทั้งระบบเสียงและข้อมูล มีการจัดการให้ไปใช้ระบบเครือข่ายที่ศูนย์ส่งกำลังบำรุงที่จังหวัดสงขลาแทนหากเกิดความเสียหายที่สำนักงานใหญ่
2. ระบบธุรกิจเบ็ดเสร็จ (PTTEP Integrated Business System) เนื่องจากเป็นระบบงานด้านการเงิน การบัญชี การจัดซื้อจัดจ้าง และการบำรุงรักษาอุปกรณ์ที่ใช้ในการขุดเจาะและสำรวจปิโตรเลียมซึ่งมีความสำคัญขณะนี้กำลังศึกษาถึงความเป็นไปได้ในการสร้างศูนย์สำรองที่ศูนย์ส่งกำลังบำรุง จังหวัดสงขลา
3. ระบบสนับสนุนงานด้านเดส์กท็อป ได้แก่ไฟล์เซิฟเวอร์ ดีเอนเอสเซิฟเวอร์ เมล์เซิฟเวอร์ ได้มีการศึกษาในการสำเนาข้อมูลไปยังสถานที่เช่าของบริษัท ปตท. จำกัด (มหาชน) รวมทั้งมีการจัดเก็บข้อมูลแบคอัพที่ธนาคารต่าง ๆ เนื่องจากความล้มเหลวอาจเกิดขึ้นได้น้อยกับเซิฟเวอร์ต่าง ๆ เนื่องจากมีการใช้เทคโนโลยีในเรื่องของ Storage Area Network (SAN) และ Network Attach Storage (NAS),RAID 5 , Cluster จึงทำให้ลดความเสี่ยงในการทำงานล้มเหลวของระบบได้ดีในระดับหนึ่ง
4. ระบบ G&G ซึ่งกำลังศึกษาความเป็นไปได้และต้นทุนในการจัดทำ

บทที่ 4
การบริหารความเสี่ยง

การบริหารหรือการจัดการความเสี่ยงเป็นการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กรซึ่งมีความจำเป็นต้องมีการจัดการวิเคราะห์ความเสี่ยง Peltier (2001 : 14) ได้อธิบายว่าการวิเคราะห์ความเสี่ยงมีวัตถุประสงค์หลักประกอบด้วย

1. รักษาป้องกันข้อมูลวิกฤตขององค์กรได้แก่ ข้อมูลเงินเดือน ข้อมูลทางการเงิน การบัญชี เป็นต้น
2. เป็นการรักษาความเชื่อมั่นของกลุ่มลูกค้าและผู้ถือหุ้นต่าง ๆ
3. ป้องกันการเปิดเผยข้อมูลที่สำคัญ
4. เพื่อให้เกิดความมั่นใจว่าคอมพิวเตอร์ เครือข่ายและข้อมูลขององค์กรไม่ถูกนำไปใช้ในทางที่ผิดหรือสูญหายไป
5. เพื่อหลีกเลี่ยงความชุลมุนอลหม่านที่อาจเกิดขึ้นกับระบบสารสนเทศ
6. เพื่อหลีกเลี่ยงเหตุสุดวิสัยต่าง ๆ
7. เพื่อหลีกเลี่ยงการละเมิดกฎหมาย พระราชบัญญัติต่าง ๆ
8. เพื่อปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ
9. เพื่อหลีกเลี่ยงบรรยากาศการทำงานที่คัดค้านหรือไม่เห็นด้วย

4.1 วงจรชีวิตของการบริหารความเสี่ยง แบ่งได้ 4 ขั้นตอน (Peltier. 2001:18)

4.1.1 วงจรชีวิตขั้นที่ 1 เป็นการประเมินความเสี่ยงและการนิยามถึงความจำเป็น มีลักษณะคือ

1. เป็นการแยกแยะทรัพยากรสารสนเทศต่าง ๆ ที่เป็นทรัพย์สินขององค์กร
2. มีกระบวนการวิเคราะห์ความเสี่ยงที่สอดคล้องกับความจำเป็นทางธุรกิจ
3. จัดหาความร่วมมือจากผู้จัดการฝ่ายบริหารให้คำนึงถึงการป้องกันทรัพยากรสารสนเทศ
4. จัดการบริหารความเสี่ยงอย่างสม่ำเสมอ

4.1.2 วงจรชีวิตขั้นที่ 2 การนำนโยบายและเครื่องมือป้องกันที่เกี่ยวข้องเข้ามาใช้ (Implement Policies and Controls) มีลักษณะคือ

1. จัดทำนโยบายให้สอดคล้องกับความเสี่ยงที่เกิดกับธุรกิจ

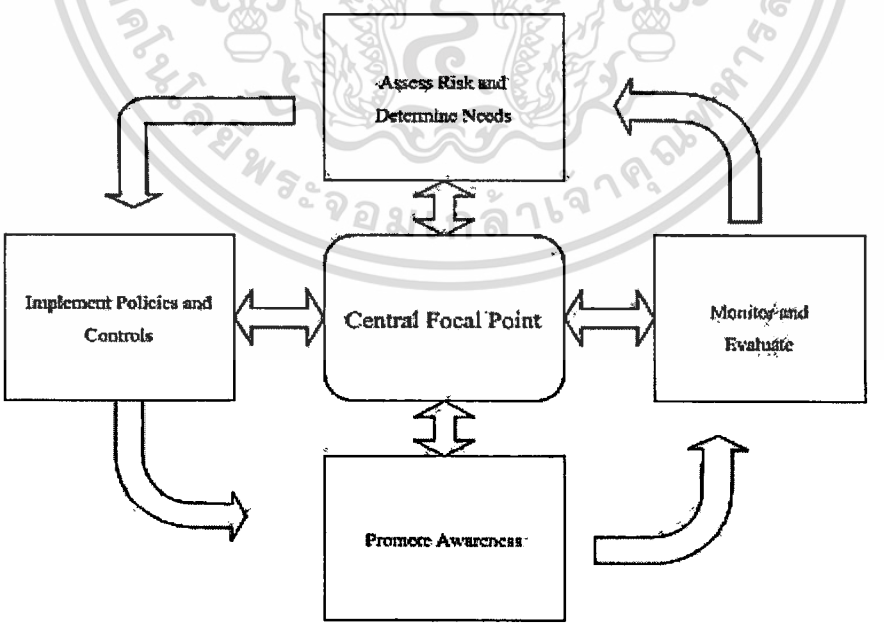
2. จัดทำมาตรฐานต่าง ๆ ที่สนับสนุนนโยบายข้างต้น
3. มีการแบ่งแยกระหว่างมาตรฐานและข้อแนะนำ
4. จัดทำนโยบายโดยให้ฝ่ายบริหารตรวจสอบทบทวนอีกครั้ง

4.1.3 วงจรชีวิตขั้นที่ 3 การประชาสัมพันธ์ข้อควรระวัง (Promote Awareness) เป็นขั้นตอนในการจัดทำที่มีลักษณะคือ

1. การให้ความรู้อย่างต่อเนื่องแก่ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับความเสี่ยง
2. จัดทำรายงานประจำปีไปยังฝ่ายบริหาร รวมถึงสถานะความเสี่ยงที่จะเกี่ยวข้องกับธุรกิจ

4.1.4 วงจรชีวิตขั้นที่ 4 การตรวจตราและการประเมินผลประสิทธิภาพของนโยบายและเครื่องมือควบคุมต่าง ๆ (Monitor and Evaluate) ประกอบไปด้วย

1. การตรวจตรางค์ประกอบต่าง ๆ ที่มีผลกระทบต่อความเสี่ยงและเป็นตัวบ่งบอกถึงประสิทธิภาพของความปลอดภัย
2. ชี้ให้เห็นผลดี ผลเสียแก่ผู้จัดการฝ่ายต่าง ๆ
3. ตระหนักถึงเครื่องมือใหม่ ๆ และเทคโนโลยีใหม่ ๆ ที่จะต้องใช้อยู่เสมอ



รูปที่ 4.1 แสดงวงจรชีวิตของการบริหารความเสี่ยง

4.2 ขั้นตอนในการวิเคราะห์ความเสี่ยง (Risk Analysis)

Peltier (2001:30) ได้กล่าวถึงแนวคิดในการวิเคราะห์ความเสี่ยงมีอยู่ 2 แนวคิดใหญ่ ๆ คือ

4.2.1 การวิเคราะห์เชิงปริมาณ (Quantitative Risk Analysis)

เป็นการวิเคราะห์เพื่อให้ได้มูลค่าหรือตัวเลขทางการเงิน ได้แก่การวิเคราะห์เกี่ยวกับมูลค่าของสินทรัพย์ จำนวนครั้งในการเกิดภัยคุกคาม ประสิทธิภาพของเครื่องมือป้องกัน ต้นทุนของการซื้อเครื่องมือป้องกัน ความไม่แน่นอนที่เกิดขึ้นและความน่าจะเป็นที่อาจเกิดขึ้นได้

4.2.2 การวิเคราะห์เชิงคุณภาพ (Qualitative Risk Analysis)

การวิเคราะห์เชิงคุณภาพเป็นเทคนิคที่ใช้เพื่อหาระดับของความต้องการในการป้องกันคุ้มครองแอพพลิเคชั่นและระบบต่าง ๆ เครื่องมืออำนวยความสะดวกต่าง ๆ รวมทั้งทรัพย์สินอื่น ๆ ขององค์กรซึ่งเป็นระบบในการตรวจสอบทรัพย์สิน ภัยคุกคามและจุดอ่อนต่าง ๆ ที่นำมาซึ่งความน่าจะเป็นในการเกิดภัยคุกคามต่างๆ ต้นทุนที่เสียไป รวมทั้งมูลค่าของเครื่องมือป้องกัน Smith (1994 : 65) ได้อธิบายว่าความเสี่ยงเชิงคุณภาพเป็นผลมาจากภัยคุกคาม(Threats) จุดอ่อนหรือช่องโหว่ (Vulnerability) และมูลค่าของทรัพย์สิน (Asset Value) Risk = Threats + Vulnerabilities + Asset Value

โดยที่ขั้นตอนในการวิเคราะห์เชิงคุณภาพประกอบไปด้วยขั้นตอนต่างๆ คือ

1. กำหนดนิยามหรือขอบเขต (Develop a scope statement) เป็นการกำหนดว่าสิ่งใดบ้างที่ต้องมีการวิเคราะห์ความเสี่ยง ซึ่งขอบเขตคือการตอบสนองต่อจุดประสงค์การป้องกันภัยคุกคามคือความมีบูรณภาพ ความลับข้อมูลและความพร้อมใช้ของข้อมูลในแอพพลิเคชั่นและระบบต่าง ๆ
2. จัดตั้งทีมงานที่มีความสามารถ ซึ่งทีมงานที่เข้ามาวิเคราะห์ความเสี่ยงควรมาจากผู้ที่เกี่ยวข้องได้แก่ผู้เป็นเจ้าของงาน ผู้ใช้ระบบ นักวิเคราะห์ระบบ นักโปรแกรมเมอร์ ผู้จัดการฐานข้อมูล ผู้ตรวจสอบระบบ ผู้ดูแลความปลอดภัยทางกายภาพ ผู้ดูแลระบบเครือข่าย นักกฎหมาย ผู้ดูแลงานประมวลผล ผู้ดูแลระบบปฏิบัติการต่าง ๆ เจ้าหน้าที่ความปลอดภัยสารสนเทศ
3. จัดการแยกประเภทความเสี่ยง (Identify threats) เป็นการวิเคราะห์ร่วมกันของกลุ่มเพื่อพิจารณาภัยคุกคามที่เป็นอันตรายต่อทรัพย์สิน
4. จัดลำดับความสำคัญของภัยคุกคาม (Prioritize threats) ซึ่งการจัดลำดับความสำคัญขึ้นกับความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น

ตารางที่ 4.1 ตารางจัดลำดับความสำคัญ

Low	Low to Medium	Medium	Medium to high	High
1	2	3	4	5

5. จัดลำดับความสำคัญของผลกระทบ (Impact Priority) เป็นการประเมินผลกระทบถึงความเสียหายกรณีถ้าเกิดภัยคุกคามใด ๆ ขึ้น โดยทีมงานจะร่วมกันศึกษาและจัดลำดับผลกระทบที่เกิดขึ้นเหมือนกับตารางข้อที่ 4
6. คำนวณผลรวมของความเสี่ยง (Calculate total threat impact) เป็นการรวมผลลัพธ์ของลำดับความสำคัญภัยคุกคามและผลกระทบที่เกิดขึ้น จะได้ผลลัพธ์ตัวเลขความเสี่ยง
7. เป็นขั้นตอนของการพิจารณาเครื่องมือป้องกันต่าง ๆ (Identify safeguards) โดยทีมงานจะแยกแยะจุดอ่อนและค้นหาเครื่องมือควบคุมทางเทคนิค เครื่องมือควบคุมทางกายภาพและเครื่องมือทางการจัดการ รวมทั้งระดับของการป้องกันที่ยอมรับได้ โดยรูปแบบที่ใช้สำหรับการป้องกันข้อมูลประกอบไปด้วย การหลีกเลี่ยง (Avoidance) การประกันความปลอดภัย (Assurance) การตรวจพบ (Detection) และการกู้คืน (Recovery) การหลีกเลี่ยงเป็นการป้องกันก่อนเกิดเหตุการณ์หรือเพื่อลดความเสี่ยงให้น้อยที่สุดหรือป้องกันการบุกรุก การประกันคือเป็นกลไกและกลยุทธ์ที่ประยุกต์ใช้เพื่อให้เกิดประสิทธิภาพต่อการควบคุมและป้องกัน การตรวจพบคือเทคนิคและโปรแกรมที่ใช้เพื่อตรวจสอบการแทรกแซงต่าง ๆและ การกู้คืนคือเป็นการวางแผนและบริการที่ตอบสนองต่อการกู้คืนระบบได้อย่างรวดเร็วและปลอดภัย
8. เป็นการวิเคราะห์ต้นทุนและประโยชน์ที่ได้ (Cost-Benefit Analysis) เครื่องมือความปลอดภัยต่าง ที่นำมาใช้ย่อมมีต้นทุน ดังนั้นต้องมีการวิเคราะห์ต้นทุนและประโยชน์ที่จะได้รับกับการประยุกต์ใช้และระดับที่พอเพียงต่อการนำมาใช้ปกป้องทรัพย์สิน
9. เป็นขั้นตอนของลำดับเครื่องมือความปลอดภัย (Rank safeguards in priority order) เมื่อวิเคราะห์ ต้นทุนและผลประโยชน์ที่ได้แล้วทีมงานควรเลือกเครื่องมือป้องกันตามลำดับความสำคัญโดยให้ผู้เป็นเจ้าของทรัพย์สินเป็นผู้เลือกโดยสอดคล้องกับวัตถุประสงค์ความปลอดภัย
10. เป็นขั้นตอนจัดทำรายงานผลการวิเคราะห์ความเสี่ยง เพื่อรายงานให้ฝ่ายบริหารได้ทราบถึงสิ่งที่ค้นพบและใช้เป็นเอกสารอ้างอิง ซึ่งรายงานจะช่วยให้ฝ่ายบริหารประยุกต์ใช้เครื่องมือควบคุมและป้องกันต่าง ๆ ที่สอดคล้องกับวัตถุประสงค์ทางธุรกิจขององค์กร โดยที่เนื้อหาของรายงานประกอบไปด้วย คำนำ ส่วนสรุปสำคัญ(Executive summary) ส่วนขั้นตอน

การแยกแยะภัยคุกคาม นิยามของความเสี่ยง การแยกแยะเครื่องมือป้องกัน ส่วนการวิเคราะห์ต้นทุนและประโยชน์ที่ได้ ข้อแนะนำในการใช้เครื่องมือความปลอดภัย และภาคผนวก

4.3 การวิเคราะห์ความเสี่ยงในกรณีของ บมจ. ปตท.สผ.

การวิเคราะห์ความเสี่ยงในกรณีของ บมจ. ปตท.สผ. นี้ผู้ศึกษาได้ยึดแนวในการวิเคราะห์ความเสี่ยงตามแบบของ Jakub A. Syta ซึ่งเป็นการวิเคราะห์เชิงคุณภาพ โดยมีขั้นตอนดังนี้คือ

1. แยกแยะชนิดของทรัพย์สินสารสนเทศ
2. กำหนดความสำคัญเชิงตัวเลขให้แก่ทรัพย์สินสารสนเทศนั้น
3. แยกแยะชนิดของภัยคุกคามที่อาจเกิดขึ้นกับทรัพย์สินนั้น
4. กำหนดความน่าจะเป็นในการเกิดภัยคุกคามหรือความเสี่ยงที่จะเกิดขึ้นกับทรัพย์สินสารสนเทศนั้น ๆ
5. คำนวณหาความเสี่ยงที่ได้

4.3.1 ขั้นตอนที่ 1 การแยกแยะชนิดของทรัพย์สินขององค์กรแยกได้เป็น 4 กลุ่มใหญ่ คือ

1. ทรัพยากรด้านข้อมูล (Information Assets)
2. ทรัพยากรด้านซอฟท์แวร์
3. ทรัพยากรด้านกายภาพ
4. ทรัพยากรอำนวยความสะดวกหรือบริการต่าง ๆ

4.3.2 ขั้นตอนที่ 2 การกำหนดความสำคัญเชิงตัวเลขให้แก่ทรัพย์สินสารสนเทศนั้นแบ่งไว้เป็น 5 ลำดับ ดังแสดงไว้ในตารางที่ 4.2

ตารางที่ 4.2 แสดงลำดับความสำคัญทรัพย์สินเชิงตัวเลข

ลำดับ	ความหมาย
0	ทรัพย์สินที่ไม่ได้เป็นส่วนหนึ่งของระบบที่ต้องจัดทำความปลอดภัย เช่นที่ทับกระดาษบนโต๊ะทำงาน
1	ทรัพย์สินที่ไม่ได้มีความสำคัญมากนักสำหรับการจัดการความปลอดภัยแต่เป็นเพียงส่วนหนึ่งที่ทำให้เกิดปัญหาที่ต้องมีการซ่อมแซม เช่น จอ คีย์บอร์ด
2	ทรัพย์สินที่มีบทบาทสำคัญและต้องมีการรักษาความปลอดภัยและต้องมีการซ่อมแซมหรือกู้คืนทันทีทันใด เช่นการ์ดเครือข่าย
3	ทรัพย์สินที่ใช้แบคอัพทรัพย์สินวิกฤต (Critical asset) ของระบบความปลอดภัยสารสนเทศ เช่น (Full Backup disk)
4	ทรัพย์สินที่วิกฤตที่ต้องการระบบความปลอดภัยสารสนเทศที่ดี เช่น เซิฟเวอร์ฐานข้อมูลการเงินการบัญชี เงินเดือน เป็นต้น

4.3.3 ขั้นตอนที่ 3 เป็นการแยกแยะชนิดของภัยคุกคามที่อาจเกิดขึ้นกับทรัพย์สินนั้น ๆ โดยอาศัยแนวคิดจาก IT Security Cookbook (http://www.boran.com/security/IT1X-2.html)

1. ภัยคุกคามทั่ว ๆ ไป
   - 1.1 ความผิดพลาดของมนุษย์ ได้แก่
     - การทำลายโดยประมาท การเปลี่ยนแปลง การเปิดเผย การลบข้อมูล
     - การละเลยได้แก่การไม่มีความระมัดระวัง การขาดข้อแนะนำ การขาดข้อมูลให้ความรู้ การคาดไม่ถึง
     - การทำงานหนักเกินไป
     - การติดตั้งระบบไม่ถูกต้อง
     - การไม่มีนโยบายความปลอดภัยที่บังคับใช้หรือไม่มีกำหนดขึ้นมาใช้
     - การละเลยในการวิเคราะห์ความเสี่ยง
   - 1.2 ความไม่ซื่อสัตย์ ได้แก่ การขโมย การนำข้อมูลไปขาย
   - 1.3 การโจมตีด้วยวิธีการทางสังคม เช่นแกล้งสอบถามข้อมูลต่าง อ้างเป็นบุคคลในองค์กรหรือแผนกสารสนเทศ การชักชวนให้กระทำอย่างใดอย่างหนึ่ง
   - 1.4 การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตของพนักงาน
   - 1.5 เจ้าหน้าที่คอมพิวเตอร์พัฒนาระบบโดยไม่แบ่งแยกระบบปฏิบัติงานจริงกับระบบทดสอบ

1.6 การนำซอฟท์แวร์และฮาร์ดแวร์ใหม่ ๆ มาใช้โดยไม่ได้ทดสอบ หรือรู้เท่าไม่ถึงการณ์และไม่ติดต่อเจ้าหน้าที่คอมพิวเตอร์

1.7 เกิดจากระเบิดเวลาของซอฟท์แวร์

1.8 การออกแบบระบบปฏิบัติการผิดพลาด โดยไม่ได้คำนึงถึงความปลอดภัยมากเท่าที่ควร

1.9 การนำโปรโตรคอลที่ไม่ได้ออกแบบโดยคำนึงถึงความปลอดภัยมาใช้

1.10 เกิดจากลอจิกบอมบ์ของซอฟท์แวร์

1.11 เกิดจากซอฟท์แวร์ประสงค์ร้าย เช่น ไวรัส วอร์ม ม้าโทรจัน แฟ้มแนบมากับเมล์

2. ภัยคุกคามต่อการพิสูจน์ตัวตนและสิทธิบุคคล (Identification /Authorization threats) ประกอบไปด้วย

2.1 การโจมตีโปรแกรมด้วยการปลอมตัวเป็นโปรแกรมปกติ เช่นม้าโทรจัน

2.2 การโจมตีฮาร์ดแวร์

2.3 ผู้โจมตีภายนอกปลอมตัวเป็นพนักงาน

2.4 ผู้โจมตีมาจากภายในโดยปลอมตัวเป็นพนักงานดูแลระบบหรือพนักงานคนอื่น

2.5 ผู้โจมตีปลอมตัวเป็นพนักงานสนับสนุนระบบ (Helpdesk)

3. ภัยคุกคามต่อความเชื่อมั่นในการให้บริการ (Reliability of services threats)

3.1 จากภัยธรรมชาติ เช่น ไฟไหม้ ควันไฟ น้ำท่าว พายุ ไฟนครหลวงดับ

3.2 ภัยจากมนุษย์ เช่น สงคราม โจรกรรม วางระเบิด สารเคมี อาวุธนิวเคลียร์

3.3 อุปกรณ์ไม่ทำงานเนื่องจากอะไหล่ สายเคเบิ้ล หรือการสื่อสารล้มเหลว

3.4 อุปกรณ์ไม่ทำงานเนื่องจากฝุ่นละออง แอร์ไม่ทำงาน คลื่นแม่เหล็ก กระแสไฟฟ้ากระชาก

3.5 การปฏิเสธการให้บริการ (Denial of services) เนื่องจาก

- ปัญหาจากเครือข่าย เช่นการใช้เร้าติ้ง
- อุปกรณ์ทำงานหนักเกินไป เช่น ซีพียูโหลด
- อีเมล์บอม์หรือเมล์ขยะ
- การดาวน์โหลดซอฟท์แวร์มาใช้โดยไม่รู้การทำงานที่ซ่อนอยู่ของโปรแกรม

3.6 เกิดจากการทำลายหรือประสงค์ร้ายต่อกระบวนการประมวลผลข้อมูลได้แก่

- การทำลายอุปกรณ์เชื่อมต่อสายเคเบิ้ล
- การทำลายอุปกรณ์คำนวณผลรวมทั้งสื่อต่าง ๆ
- การทำลายอุปกรณ์ไฟฟ้าที่จ่ายไฟ

- การขโมย
- การตัดไฟหรือใช้ไฟเกินกำลัง
- ไวรัสหรือหนอนเครือข่ายต่าง ๆ
- การลบแฟ้มวิกฤตของระบบ

4. ภัยคุกคามต่อความเป็นส่วนตัว (Privacy Threats) ได้แก่
   4.1 การดักฟัง (Eavesdropping) ได้แก่
   - Electromagnetic eavesdropping
   - การใช้โทรศัพท์ แฟกซ์ เคเบิ้ลโมเด็ม
   - เครือข่ายภายใน เช่นการแทรปสายสัญญาณ การดักจักข้อมูลภายในเครือข่าย หรือตู้ชุมสายโทรศัพท์
   - การโจมตีต่อ DNS
   - การเปลี่ยนเส้นทางเครือข่ายจากเร้าติ้งโปรโตคอล
   - การเข้าไปอ่านข้อมูลในแคชของระบบ
   - การดักจับสัญญาณวิทยุและสัญญาณแลนไร้สาย
   - การค้นหาจากของเหลือใช้หรือจากขยะ เช่นกระดาษรายงาน อุปกรณ์บันทึกที่ทิ้งไป

5. ภัยคุกคามต่อบูรณภาพและความถูกต้อง (Integrity/Accuracy threats) ได้แก่
   5.1 ซอฟท์แวร์ประสงค์ร้ายต่อข้อมูลและการประมวลผลที่เกิดจากปัจจัยภายนอก
   5.2 ซอฟท์แวร์ประสงค์ร้ายต่อข้อมูลและการประมวลผลที่เกิดจากปัจจัยภายใน
   5.3 การเปลี่ยนแปลงแก้ไขข้อมูล
   5.4 การขาดการเข้ารหัสกับข้อมูล

6. ภัยคุกคามสำหรับการควบคุมการเข้าถึง (Access Control threats) ได้แก่
   6.1 การแคร็กรหัสผ่านซึ่งเกิดจากการใช้รหัสผ่านที่ไม่ดี ใช้รหัสผ่านดีฟอลต์ ไม่ใส่รหัสผ่าน
   6.2 การเข้าถึงจากเครือข่ายภายนอกหรือการดักจับแพ็คเกตในเครือข่าย
   6.3 การโจมตีโปรแกรมโดยเข้ามาฝังตัวทำงานเบื้องหลัง (Backdoors) โดยใช้เครือข่ายภายใน
   6.4 การโจมตีโปรแกรมโดยเข้ามาฝังตัวทำงานเบื้องหลัง (Backdoors) โดยเข้าถึงเครือข่ายจากภายนอก
   6.5 การพัฒนาโปรแกรมที่ไม่ได้คำนึงถึงความปลอดภัย

6.6 การใช้โมเด็มเชื่อมต่อภายนอกตลอดเวลาหรือการปล่อยสัญญาณเครือข่ายไปยังทุกพอร์ตของเน็ตเวิร์ก

6.7 การมีบักในซอฟท์แวร์เครือข่าย (Network software) เช่น IOS, SNMP ที่อุปกรณ์ภายนอกเครือข่ายหรืออินเตอร์เน็ตสามารถสแกนตรวจสอบได้

6.8 การเข้าถึงทางกายภาพ เช่นเข้าถึงห้องคอมพิวเตอร์ ตู้แพ็ทสายเครือข่าย เป็นต้น

7. ภัยคุกคามต่อความมีชื่อเสียงขององค์กร (Repudiation threats) ได้แก่

7.1 เว็ปเซิฟเวอร์ถูกแคร็กหรือถูกเปลี่ยนหน้าเว็บเพจ

7.2 การถูกจับได้ว่าละเมิดสิขสิทธิ์ซอฟท์แวร์

7.3 การส่งข้อมูลผ่านไปยังจุดหมายปลายทางที่ผิด

8. ภัยคุกคามจากกฎหมายและพระราชบัญญัติ ได้แก่

8.1 พรบ. ว่าด้วยอาชญากรรมทางคอมพิวเตอร์

8.2 พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

8.3 พรบ. ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

8.4 กฎหมายลายมือชื่ออิเล็กทรอนิกส์

4.3.4 ขั้นตอนที่ 4 การแยกแยะความน่าจะเป็นการเกิดภัยคุกคามต่าง ๆ โดยจัดแยกชนิดของความน่าจะเป็นในการเกิดปัญหาด้านภัยคุกคามได้ 6 ลำดับคือ

ตารางที่ 4.3 แสดงความน่าจะเป็น (Probabilities) ในการเกิดภัยคุกคาม

ค่าความน่าจะเป็น	ความหมาย	โอกาสที่จะเกิดขึ้น
0	เป็นไม่ได้หรือแทบจะเป็นไปไม่ได้ (Impossible)	1 /20 ปี
1	ไม่น่าจะเป็นไปได้ (Unlikely)	1/5 ปี
2	มีความเป็นไปได้น้อย (Less probable)	1/1 ปี
3	มีความเป็นไปได้ (Probable)	1/1 เดือน
4	คือเกิดขึ้นได้บ่อย ๆ (Frequent)	1/วัน
5	คือเกิดขึ้นได้เสมอ ๆ (Continue)	มากกว่า 1 ครั้ง/วัน

4.3.5 ขั้นตอนที่ 5 เป็นวิธีการหามูลค่าความเสี่ยง (Assigning risk value) ซึ่งได้จากตัวเลขของการคูณกันระหว่างค่าที่กำหนดให้ทรัพย์สิน (Asset Value) จากขั้นตอนที่ 2 (ข้อ 4.3.2) กับค่าความน่าจะเป็น (Probabilities) จากขั้นตอนที่ 4 โดยนิยามว่า

- ถ้าค่าความเสี่ยงเท่ากับหรือน้อยกว่า 8 หรือค่าของสินทรัพย์เท่ากับ 4 และค่าความน่าจะเป็นเท่ากับ 4-5 จะต้องมีมาตรการในการป้องกันระบบสารสนเทศที่เข้มแข็งทันทีทันใด
- ถ้าค่าความเสี่ยงเท่ากับ 4-6 จำเป็นต้องมีความปลอดภัยของระบบแต่ลำดับความสำคัญน้อยกว่าข้างต้น
- ถ้าค่าความเสี่ยงน้อยกว่า 3 ความจำเป็นในการกำหนดมาตรการหรือการกระทำใด ๆ ไม่จำเป็นต้องมีเพิ่มเติมแต่ต้องมีการควบคุมเท่าที่จำเป็น

ตารางที่ 4.4 แสดงค่าความเสี่ยง

Asset Value	Probability 0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10
3	0	3	6	9	12	15
4	0	4	8	12	14	20

4.4 ผลการวิเคราะห์ความเสี่ยงในกรณีของ บมจ. ปตท.สผ.

จากการวิเคราะห์ความเสี่ยงระบบสารสนเทศของ ปตท.สผ โดยพิจารณาจากการให้ความสำคัญทรัพย์สินเชิงตัวเลข การวิเคราะห์ความน่าจะเป็นในการเกิดภัยคุกคาม และชนิดของภัยคุกคามที่อาจเกิดขึ้น ผู้ศึกษาได้จัดแยกชนิดของระบบสารสนเทศขององค์กรเป็น 8 กลุ่มใหญ่ ๆ คือ

4.4.1 กลุ่มของเซิฟเวอร์ (Hardware Asset Server) พบว่าเซิฟเวอร์หรือเครื่องที่ให้บริการที่มีมูลค่าความเสี่ยงสูงได้แก่

- เมล์เกตเวย์ เซิฟเวอร์ (Mail Gateway Server)
- เมล์เอกซ์เชน เซิฟเวอร์ (Mail Exchange Server)
- DNS and Active Directory Server
- WWW.PTTEP.COM Server

ตารางที่ 4.5 แสดงกลุ่มของเซิฟเวอร์ขององค์กร

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
1. Hardware Asset Server				
Mail Gateway Server	4	5	20	3.5,7.3,3.6.6
Mail Excchage Server	4	5	20	1.11,3.5,3.6.6,8.1
Windows2000 DNS and AD Server	4	5	20	1.1.2,4.1.4,1.1.6,1.8
HQ-FS4+5 NAS Server	4	4	16	1.4,1.11,3.6.7
HQ-FS1+2 SAN Server	4	4	16	1.4,1.11,3.6.7
www.pttep.com Server	4	5	20	5.3,6.5,7.1
Maebia Intranet Server	4	3	12	1.1.1,3.5,3.6.6,3.6.7,5.3,6.3,6.5
Poseidon Workflow Server	4	2	8	1.1.6,1.11,2.1,3.6.6,5.3
Reserve DC Server	3	3	9	1.1.2,4.1.4,1.1.6,1.8
Maximo Server	4	3	12	5,1.1.6
Orchird Database Server	4	3	12	5,1.1.6
BU4 Verita's Server	4	2	8	1.1.3,1.11,3.5,3.6.6
HQ-Portal Server	4	3	12	1.4,1.11,3.5
Tatooine Drivers Server	3	2	6	1.4,1.11,2.5,3.6.7,7.2,8
HQ-SWDP Appli. Server.	4	4	16	1.4,1.11,2.5,3.6.7
Unix Geology and Geophysic Server	4	4	16	1.1.3,1.1.6,1.14,2.1.3.5, 3.6.6,5.3,6.3

ปัจจัยหรือสาเหตุของความเสี่ยงสูงของอุปกรณ์เซิฟเวอร์เหล่านี้เกิดจากสาเหตุต่าง คือ

1. เป็นกลุ่มของเซิฟเวอร์ขององค์กรที่ติดต่อกับโลกภายนอก
2. โครงสร้างของระบบเครือข่ายไม่ได้มีการแบ่งแยกเครื่องเซิฟเวอร์ในรูปแบบของเขตปลอดทหาร (Demilitarized Zone) หรือ (DMZ)
3. ขาดเจ้าหน้าที่ที่มีความชำนาญในการควบคุมดูแลการติดตั้งและตรวจค่าระบบต่าง ๆ ที่เกี่ยวกับระบบความปลอดภัย รวมทั้งบริษัทผู้ขายขาดความรู้หรือประสบการณ์ด้านความปลอดภัยที่ดีพอ
4. ปัจจัยจากภัยคุกคามต่าง ๆ ได้แก่ การทำงานหนักของอุปกรณ์ เช่น เมล์เซิฟเวอร์ การติดตั้งระบบโดยไม่คำนึงถึงความปลอดภัย การละเลยในการวิเคราะห์ความเสี่ยง การ

เกิดการปฏิเสธการให้บริการ ไวรัสหรือหนอนเครือข่ายต่าง ๆ โอกาสเว็บเซิฟเวอร์ถูกเจาะระบบ การส่งผ่านข้อมูลไปยังจุดหมายปลายทางที่ผิด เป็นต้น

4.4.2 กลุ่มของอุปกรณ์เครือข่ายสื่อสารที่ใช้ในองค์กร (Network Communications Devices) อุปกรณ์ที่มีมูลค่าความเสี่ยงสูงได้แก่

- Cisco 4000 Router
- Motorolla Vanguard Router
- Firewall
- Netcache 1100 Server
- Contivity VPN box
- Cisco Catalyst 6500 Backbone Switch

ตารางที่ 4.6 แสดงกลุ่มของอุปกรณ์เครือข่ายสื่อสาร

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สิน เชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดช่องภัยคุกคามที่อาจเกิดขึ้น
2. Network Com.Devices				
Cisco 4000 Router	4	5	20	1.1.2,1.1.5,1.1.6,2.4,3.3,3.5,3.61, 4.1.5,6.2,6.7
Firewall Server	4	5	20	1.1.4,3.3,3.5,5.1,6.2
Motorolla Vanguard Router	4	5	20	1.1.2,1.1.5,1.1.6,2.4,3.3,3.5,3.61, 4.1.5,6.2,6.7
Netcache 1100 Server	4	5	20	1.1.3,1.1.4,1.8,3.5,3.6.6,4.1.6,6.1
Contivity VPN Box	4	5	20	1.1.4,1.1.5,1.1.6,1.11,3.5,6.1
Cisco 6500 Switch	4	5	20	3.5,3.1,4.1.5,6.7,6.2,6.1,6.8
Cisco Catalyst3508	4	2	8	3.5,3.1,2.2,3.3,4.1.5
Cisco Catlyst 3524	4	2	8	3.5,3.1,2.2,3.3,4.1.5
Cisco Catlyst 2948	4	2	8	3.5,3.1,2.2,3.3,4.1.5
Cisco Caalyst 1924	4	2	8	3.5,3.1,2.2,3.3,4.1.5
Cisco Catalyst 2950	4	2	8	3.5,3.1,2.2,3.3,4.1.5
D-link Wireless AP	4	2	8	3.5,3.1,2.2,3.3,4.1.5
Cisco Aironet AP	4	2	8	3.5,3.1,2.2,3.3,4.1.5

ปัจจัยหรือสาเหตุของมูลค่าความเสี่ยงสูงของอุปกรณ์เครือข่ายสื่อสารเกิดจากสาเหตุต่าง ๆ คือ

1. เป็นกลุ่มของอุปกรณ์ที่ใช้เชื่อมต่อกับการสื่อสารโลกภายนอกผ่านไปยังผู้ให้บริการอินเตอร์เน็ต (ISP)

2. โครงสร้างของระบบเครือข่ายขององค์กรเป็นปราการชั้นเดียวไม่ได้มีการแบ่งแยกเป็นเครือข่ายภายในและภายนอกอย่างชัดเจน
3. การติดตั้งค่าระบบกระทำโดยผู้ให้บริการซึ่งอาจขาดประสบการณ์และขาดผู้ตรวจสอบสำหรับค่าที่ใช้ในการติดตั้งระบบ รวมทั้งเจ้าหน้าที่ขององค์กรก็ขาดความรู้และประสบการณ์ที่ใช้ในการตรวจสอบความปลอดภัย
4. อุปกรณ์ที่ใช้มีหลายหน่วยงานดูแลและมีเจ้าหน้าที่หลายฝ่ายรับผิดชอบและขาดการประสานงานระหว่างกัน
5. ปัจจัยทางด้านภัยคุกคามอื่น ๆ ได้แก่
   - การที่อุปกรณ์ทำงานหนักเกินไป เช่นการตั้งค่าไฟร์วอลล์มากเกินไปมีผลต่อการโปรเซสที่ต้องทำการกรองแพ็คเกตมากเกินไป
   - การติดตั้งระบบไม่ถูกต้อง เช่นการตั้งค่าระบบไฟร์วอลล์ เร้าท์เตอร์ แคชหรือพร็อกซี่ เป็นต้น
   - การละเลยในการวิเคราะห์ความเสี่ยง
   - มีโอกาสเกิดการปฏิเสธการให้บริการ
   - ผู้โจมตีปลอมตัวเป็นพนักงานสนับสนุนระบบหรือผู้ดูแลระบบ
   - การดักจับสัญญาณในเครือข่ายภายนอก
   - การเข้าถึงจากเครือข่ายภายนอกหรือการดักจับแพ็คเกตในเครือข่าย

4.4.3 กลุ่มของอุปกรณ์ต่าง ๆ ของเครือข่าย (Network Accessories Equipments)

จากการวิเคราะห์ความเสี่ยงของอุปกรณ์ต่าง ๆ ของเครือข่ายพบว่าอุปกรณ์ที่มีความเสี่ยงสูงประกอบไปด้วยดังนี้

- 10/100/1000 Ethernet Card
- Fiber Optic Cable
- UTP 5E patch cable
- Converter UTP to Fiber

ตารางที่ 4.7 แสดงกลุ่มของอุปกรณ์ต่าง ๆ ของเครือข่าย

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
3. Network Accessories Equipments				
10/100/1000 Mbps Card	2	2	4	1.1.6,6.8,3.6.4
Fiber Optic cable	2	2	6	3.3,3.1,3.6.1
Network Patch Management	1	0	0	
Fiber Management Encl.	1	0	0	1.1.6,1.1.2
ST-ST Fiber patch cord	1	1	1	3.6.4
SC-SC Fiber patch cord	1	1	1	3.6.4,3.3
ST-SC Fiber patch cord	1	1	1	3.6.4,3.3
UTP 5E Cable	1	1	1	3.6.4,3.3
UTP 5E Patch Cable	1	1	1	3.6.4,3.3
UTP 5E Jack Connector	1	1	1	3.6.4
UTP Plug Connector	1	1	1	3.6.4
Patch Panel	1	1	1	3.6.4
Face Plate for RJ45	1	1	1	3.6.4
Cable Management panel	1	1	1	3.6.4
Line tester	1	1	1	3.6.4
Carbinet Rack	1	1	1	3.2,6.8
Wire Management Panel	1	1	1	3.6.4
Converter Utp-> Fiber	2	2	4	3.5,3.4,3.6,3,3.6.1

ปัจจัยหรือสาเหตุของมูลค่าความเสี่ยงสูงของอุปกรณ์ต่าง ๆ เกิดจากสาเหตุต่าง ๆ คือ

1. การเดินสายระหว่างสายไฟเบอร์และสายยูทีพีระหว่างชั้นต่าง ๆ ไม่ได้มีการแยกช่องทางเดินระหว่างกันและเนื่องจากมีการลากสายยูทีพีบ่อยครั้งทำให้โอกาสกระทบต่อสายไฟเบอร์มีค่อนข้างสูง
2. อุปกรณ์ไม่ทำงานเนื่องจากฝุ่นละออง คลื่นแม่เหล็กเนื่องจากอุปกรณ์เหล่านี้อยู่ในห้องไฟฟ้าแรงสูง
3. การติดตั้งระบบไม่ถูกต้องเนื่องจากมีการนำสายไฟเบอร์และสายยูทีพีไปรวมไว้ที่ตู้ชุมสายในห้องไฟฟ้าแรงสูง
4. การละเลยในการวิเคราะห์ความเสี่ยง เนื่องจากสายไฟเบอร์และสายยูทีพีอยู่ในห้องไฟฟ้าโอกาสที่จะเกิดการลากสายไฟฟ้าเพิ่มและผู้เดินสายรู้เท่าไม่ถึงการณ์และไม่ติดต่อเจ้าหน้าที่คอมพิวเตอร์
5. การแทรปสายสัญญาณทำได้ง่ายเนื่องจากมีจุดเชื่อมต่อเครือข่ายหรือแลนพอร์ตที่ล่อแหลมต่อเครือข่ายภายใน เช่น บริเวณพนักงานต้อนรับ บริเวณห้องประชุม บริเวณตู้ชุมสาย การดักจับสัญญาณแลนไร้สายในอาคาร

4.4.4 กลุ่มของอุปกรณ์โทรคมนาคม (Telecommunication Devices)

จากการวิเคราะห์ความเสี่ยงพบว่าอุปกรณ์โทรคมนาคมที่มีความเสี่ยงสูงประกอบไปด้วยดังนี้

- PBX
- Mobile Phone
- Sattelite Antena Disk
- Micom MUX

ตารางที่ 4.8 แสดงกลุ่มของอุปกรณ์โทรคมนาคม

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สิน เชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
4: Telecom Devices				
Mobile Phone	2	2	4	3.6.4
PABX Nec	4	1	4	3.1,1.1.6,2.2,3.3,4.1.3
Fax Canon	2	2	4	3.6.4,3.3
Sattelite Antena Disk	4	1	4	3.1,3.2,3.3,3.6.4
Micom Mux	3	2	6	3.6.4,3.3
Microwave radio terminal	2	2	4	3.1,3.2,3.3,3.6.4
Sattelite Modem Nec	2	2	4	3.3,3.6.4,4.1.1
SRX/5 Stat Mux	2	2	4	3.6.4,3.3
Alcatel PBX	4	1	4	3.1,1.1.6,2.2,3.3,4.1.3

สาเหตุหรือปัจจัยจากภัยคุกคามได้แก่

1. การขโมย
2. จากภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม พายุ
3. อุปกรณ์ไม่ทำงานเนื่องจากอะไหล่ สายเคเบิ้ลหรือการสื่อสารล้มเหลว
4. การละเลยในการวิเคราะห์ความเสี่ยงเมื่อมีการติดตั้งระบบ
5. การขาดการจัดเก็บข้อมูล(Inventory) ที่ถูกต้อง

4.4.5 กลุ่มของโครงสร้างพื้นฐานห้องคอมพิวเตอร์ (Computer Room Facilities)

จากการวิเคราะห์ความเสี่ยงพบว่าอุปกรณ์ที่มีความเสี่ยงสูงประกอบไปด้วยดังนี้

- ระบบเครื่องปรับอากาศ
- สารเคมีดับไฟ (FM 200)
- ระบบอุปกรณ์ฉีดแก๊ส (Gas cylinder)

- อุปกรณ์หัวฉีด Flexible Disharge Hose
- อุปกรณ์ดักจับควัน Photoelectric Smoke Detector
- อุปกรณ์สัญญาณควบคุม (FM200 Control Panel)
- ระบบประตูเข้าออก (Access Door)

ตารางที่ 4.9 แสดงอุปกรณ์โครงสร้างพื้นฐานห้องคอมพิวเตอร์ขององค์กร

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
5. Computer Room Facilities				
Air Conditioner	4	2	8	1.1.6,3.1,3.6,3.3,6.5
FM-200	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Gas Cylinder	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Flexible DishargeHose	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Electrical Solenoid Valve	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Disharge Nozzle	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Photoelcetric Smoke Detector	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Flashing Lamp and Horn	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Alarm Bell	2	2	4	1.1.6,3.1,3.6,3.3,6.5
Abort Station	2	2	4	1.1.6,3.1,3.6,3.3,6.5
Fm-200 Control Panel	3	2	6	1.1.6,3.1,3.6,3.3,6.5
Rised floor	1	2	2	1.1.3,1.1.6
Access Door	3	2	6	1.1.6,2.2,3.1
Humidity Control	2	2	4	1.1.2,1.1.6,3.1

ปัจจัยหรือสาเหตุของความเสี่ยงของอุปกรณ์เกิดจากสาเหตุต่าง ๆ คือ

1. การละเลยในการวิเคราะห์ความเสี่ยง
2. การขาดการทดสอบหรือมีความเป็นไปได้น้อยในการทดสอบระบบเนื่องจากมีข้อจำกัดของระบบเอง เช่นเนื่องจากข้อจำกัดที่ไม่สามารถทดลองฉีดน้ำยาดับเพลิงได้
3. การตัดไฟหรือใช้ไฟเกินกำลัง เช่น ระบบแอร์
4. อุปกรณ์ทำงานหนักเกินไป เช่นระบบแอร์ เป็นต้น

4.4.6 กลุ่มของทรัพย์สินฮาร์ดแวร์อื่น ๆ ของระบบคอมพิวเตอร์ (Hardware Assets)

จากการวิเคราะห์ความเสี่ยงพบว่าอุปกรณ์ขององค์กรที่น่าจะมีความเสี่ยงสูงประกอบไปด้วย ดังนี้

- เทปสำรองข้อมูล (SDLT, DLT tape backup)

- อุปกรณ์สำรองข้อมูล (ADIC Tape library Backup)
- โน้ตบุ๊ค (Notebook)
- เครื่องคอมพิวเตอร์ (Pc Pentium III,IV)

ตารางที่ 4.10 แสดงกลุ่มของทรัพย์สินฮาร์ดแวร์ของระบบคอมพิวเตอร์

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
6. Hardware Assets				
600 Pc Pentium IV	3	5	15	1.1.2,1.1.5,1.2,3.1,3.6.4
60 Notebook Dell	3	5	15	1.1.2,1.1.5,1.2,3.1,3.6.4
10 Notebook Toshiba	3	5	15	1.1.2,1.1.5,1.2,3.1,3.6.4
HP Printer 4000N	3	4	12	1.1.2,1.1.5,1.2,3.1,3.6.4
HP plotter3500C	3	4	12	1.1.2,1.1.5,1.2,3.1,3.6.4
HP pLotter650c	3	4	12	1.1.2,1.1.5,1.2,3.1,3.6.4
Diskette	3	2	6	3.4,4.1.1,3.6.4
Speaker	0	1	0	3.6.4,
Mouse	2	1	2	3.6.4,3.4,
Keyboard	2	1	2	3.4,1.1.2,3.3
Pad Mouse	0	0	0	3.6.4
Hp Scanner6400c	3	2	6	1.1.2,1.1.5,1.2,3.1,3.6.4
Fuji Scanner c400	3	2	6	1.1.2,1.1.5,1.2,3.1,3.6.4
HP Cd writer	3	3	9	3.3,3.4,3.6.4
ADIC tape libraryBackup	3	4	12	3.5,3.3,1.1.1
SDLT tape backup	3	4	12	3.5,3.3,1.1.1
DLT tape backup	3	4	12	3.5,3.3,1.1.1
Quantum Dlt tape backup	3	4	12	3.4,1.1.6,4.1.8
Hp-Cd tower	2	2	4	3.3,3.4,3.6.4
Sony Digital Camera	1	2	2	3.6.4
Cd-Rom	3	3	9	3.3,3.4
IoMega USB-HDD	3	2	6	1.1.1,3.6.4

ปัจจัยหรือสาเหตุของความเสี่ยงเกิดจากสาเหตุต่าง ๆ คือ

1 การละเลยในการวิเคราะห์ความเสี่ยง

2 การขโมยของพนักงาน

3 การไม่มีนโยบายความปลอดภัยที่บังคับใช้หรือไม่มีการกำหนดนโยบายขึ้นมาใช้ เช่น การนำโน้ตบุ๊คไปใช้นอกสถานที่ไม่ได้มีข้อแนะนำในการดูแลให้พนักงานปฏิบัติ เป็นต้น

4 ความไม่ซื่อสัตย์ของพนักงาน เช่น พนักงานรักษาความปลอดภัย แม่บ้าน เป็นต้น

5 อุปกรณ์ไม่ทำงานเนื่องจากฝุ่นละออง เครื่องปรับอากาศไม่ทำงาน คลื่นแม่เหล็กไฟฟ้า กระแสไฟฟ้าดับ ไม่มีอุปกรณ์สำรองไฟ

6 การเข้าถึงทางกายภาพ เช่นการเข้าห้องคอมพิวเตอร์ได้โดยการขาดการควบคุมหรือลงบันทึกของบุคคลภายนอก

4.4.7 กลุ่มของข้อมูลของหน่วยงานต่าง ๆ ในองค์กร (Information Asset)

จากการสัมภาษณ์ไปยังหน่วยงานต่าง ๆ ทุกหน่วยงานให้ความสำคัญกับข้อมูลสูง ผู้ศึกษาจึงใช้เกณฑ์ในการวิเคราะห์ความเสี่ยงสูงของข้อมูลของทุกหน่วยงาน ซึ่งข้อมูลทุกหน่วยงานมีความสำคัญต่อการปฏิบัติงานและหน่วยงานต่าง ๆไม่สามารถปฏิบัติงานได้อย่างดีถ้าขาดข้อมูลไปหรือระบบคอมพิวเตอร์หยุดทำงานไป

ตารางที่ 4.11 แสดงข้อมูลของหน่วยงานต่าง ๆ ตามโครงสร้างขององค์กร

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สิน เชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
7.Information Asset				
President Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Office of President Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Corporate Secretary Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Health, Safety and Environment Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
External Relations Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Internal Audit Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Strategy&Capacity Development Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Strategic Planning Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Economic&Commercial Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
HR Development Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Org & Process Development Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Operation Division Head Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Bongkot Asset Inforamtion	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Bongkot Petroleum Development Inforamation	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Bongkot Field Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Operation Arthit Asset Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
PTTEP1 Asset Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1
Operation Support Information	4	5	20	1.1.1,1.2,1.4,3.6,6.5,4.5,3.5,1

ตารางที่ 4.11 แสดงข้อมูลของหน่วยงานต่าง ๆ ตามโครงสร้างขององค์กร (ต่อ)

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
Operation Logistics Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Operation Maintenance & Inspection Infor.	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Operation Drilling Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Opeartion Well Engineering Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
E & P Investment Division Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
E& P Maynmar Project Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
E & P Project1 Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
E& P Proejct2 Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project Division Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project New venture1 Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project New venture2 Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project for New Bussiness Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project Petroleum Commercial Infor.	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
New Project Indonesia Projects	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Technical Services Division Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Geology Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Geophysics Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Reservior Engineering Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Production Development Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Facility Engineering Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Construction Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Business Services Division Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
HR Services & Relation Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Administration Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Procurement & Contract Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Legal Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
IT Services Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Finance & Accounting Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Finance Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1
Accounting Information	4	5	20	1.1.1,1.2,1.4,3.6.6,5.4,5.3,5.1

ปัจจัยหรือความเสี่ยงของข้อมูลของหน่วยงานต่าง ๆ เกิดจากภัยคุกคามต่อไปนี้

1. ความประมาทของพนักงาน เช่นการลบแฟ้มข้อมูลโดยรู้เท่าไม่ถึงการณ์ การเปลี่ยนแปลง การเปิดเผย การแชร์ข้อมูลโดยรู้เท่าไม่ถึงการณ์ เป็นต้น
2. การละเมิดสิทธิของผู้อื่นในการไปใช้เครื่องคอมพิวเตอร์และลบแฟ้มข้อมูลที่สำคัญทิ้งไป
3. การปลอมตัวเป็นพนักงานดูแลระบบเข้าไปลบแฟ้มข้อมูล

4. การละเลยของพนักงาน ไม่มีความระมัดระวัง การขาดข้อเสนอแนะ การขาดข้อมูลให้ความรู้หรือการคาดไม่ถึงเช่น เก็บข้อมูลที่สำคัญไว้ที่เครื่องส่วนตัว โดยไม่ได้เก็บไว้ที่เซิฟเวอร์หรือไดรฟ์ที่จัดไว้ให้และมีการสำรองข้อมูลไว้ให้
5. การโจมตีโปรแกรมด้วยการปลอมตัว เช่น ม้าโทรจัน เนื่องจากพนักงานทุกคนมีสิทธิ์เป็นผู้บริหารเครื่อง (Administrator) ทำให้สามารถติดตั้งซอฟท์แวร์ต่าง ๆ ได้อย่างอัตโนมัติและด้วยตนเองซึ่งทำให้มีความเสี่ยงสูง
6. เกิดจากไวรัสหรือหนอนเครือข่ายต่าง ๆ เนื่องจากผู้ใช้สามารถใช้เมล์ติดต่อโลกภายนอกมีการลงทะเบียนโดยใช้เมล์แอดเดรสขององค์กรจึงทำให้ได้รับเมล์พร้อมกับแฟ้มข้อมูลแนบมาจากบุคคลที่ไม่รู้จักและติดไวรัสหรือหนอนเครือข่ายต่าง ๆ ได้ รวมทั้งพนักงานไม่ได้ทำการสแกนไวรัสด้วยซอฟท์แวร์ที่ติดตั้งให้
7. การขาดการเข้ารหัสลับกับข้อมูล เนื่องจากองค์กรยังไม่ได้ลงทุนหรือศึกษาเกี่ยวกับการเข้ารหัสลับข้อมูลที่เพียงพอ
8. การใช้โมเด็มเชื่อมต่อโลกภายนอกตลอดเวลา เนื่องจากพนักงานบางคนใช้โมเด็มโดยไม่ได้ติดต่อหรือรับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ
9. การดาวน์โหลดซอฟท์แวร์มาใช้โดยไม่รู้การทำงานที่ซ่อนเร้นอยู่ของโปรแกรม เช่น การดาวน์โหลด Screen Saver หรือโปรแกรมเพลงต่าง ๆ มาใช้และขาดความรู้และความเข้าใจเกี่ยวกับความปลอดภัยที่เพียงพอ

4.4.8 กลุ่มของซอฟท์แวร์ที่ใช้ในองค์กร (Software Asset)

ในชนิดของกลุ่มซอฟท์แวร์ที่ใช้ในองค์กรนี้ผู้ศึกษาให้ความสำคัญของทรัพย์สินเชิงตัวเลขโดยพิจารณาจากจำนวนการใช้ซอฟท์แวร์และปริมาณของกลุ่มผู้ใช้หรือปริมาณผู้ใช้ที่จะได้รับผลกระทบจากการการชะงักงันของซอฟท์แวร์ กลุ่มของซอฟท์แวร์ที่มีมูลค่าความเสี่ยงสูงได้แก่

- MS Windows 2000 Professional
- MS Windows Office 2000 Professional
- Acrobat 4.5
- Arcserve 2000 Backup
- Veritas Backup
- Maximo
- Innoculate Virus Scan
- TimeWrite 2000

- WinZip 8.0
- Trend Micro Virus Mail Scan

ตารางที่ 4.12 แสดงกลุ่มของซอฟท์แวร์ที่ใช้ในองค์กร

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
8. Software Asset				
Acrobat 4.5	4	2	8	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Arcserve 2000 Backup	4	2	8	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
As$et 2.3	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Autocad 2000	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Babit	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Coreldraw 9.0	4	2	8	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
DeepE$T	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Docuwork 4.0	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
DocXPlo3:48a	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Dreamwaever 4	4	2	8	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Exceed 6.1	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Fast-Est2.23	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Flash 5	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Freelance 9.6	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Frontpage 2000	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3
Fujiscan 2.71	3	2	6	1.6,1.7,1.11,2.1,3.6.7,5.1,6.3

ตารางที่ 4.12 แสดงกลุ่มของซอฟท์แวร์ที่ใช้ในองค์กร (ต่อ)

ชนิดของทรัพย์สิน	ความสำคัญทรัพย์สินเชิงตัวเลข	ความน่าจะเป็นในการเกิดภัยคุกคาม	ค่าความเสี่ยงรวม	ชนิดของภัยคุกคามที่อาจเกิดขึ้น
Gem 2.14	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Grapher 2.04	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Hysys 2.4.1	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Inocultae Virus Scan	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Oracle 8I	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Oracle 7.3.2	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Oracle Financial Analyser	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Oracle application Desktop Integrator	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Oracle Discoverer	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Ociar3	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Microsoft Office2000	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Maximo	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Pathfind	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Petcom 2.41	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Photoshop 6	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Pipephase 7.41	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Predic 8.1	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Primevera 3.1	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Pro II 5.6	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Probe 4.0	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Production Report System	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Ms Porject 2000	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
PTTEP Petroleum Library	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Que$tor Onshore and Offshore 7.5a	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Reflection 6	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Risk 4	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Rxhighlight 97	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Rxview 5	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
SAP 4.6D	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Soralis 2.6	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Surfer 6.04	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Timewrite 2000	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Ms Visio 2000	3	2	6	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Interscan Virus Wall	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Webster Dictionary	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Winzip 8.0	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Windows2000 Server	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Windows 2000 Advanced Server	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Windows 2000 Professtional	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3
Veritas Backup	4	2	8	1.6,1.7,1.11,2.1,3.6,7,5.1,6.3

ปัจจัยหรือสาเหตุของภัยคุกคามที่ทำให้เกิดความเสี่ยงประกอบไปด้วยปัจจัยดังต่อไปนี้

1. การออกแบบซอฟท์แวร์โดยไม่ได้คำนึงถึงความปลอดภัยมากเท่าที่ควร
2. การโจมตีโปรแกรมด้วยไวรัส หรือวอร์มต่าง ๆ
3. เกิดจากระเบิดเวลาของซอฟท์แวร์
4. การโจมตีโปรแกรมด้วยการปลอมตัวเป็นโปรแกรมปกติ เช่นม้าโทรจันที่ส่งมากับเมล์เป็นแฟ้มแนบข้อมูลมา
5. เนื่องจากผู้ใช้ลบแฟ้มวิกฤตของโปรแกรม เนื่องจากผู้ใช้ในองค์กรมีสิทธิ์เป็นผู้บริหารระบบ (Administrator) ของเครื่อง
6. การโจมตีโปรแกรมโดยเข้ามาฝังตัวทำงานเบื้องหลัง โดยเข้าถึงจากเครือข่ายภายนอก
7. การมีบักในซอฟท์แวร์นั้น
8. การละเมิดลิขสิทธิ์ซอฟท์แวร์ เช่นจำนวนผู้ใช้มากกว่าจำนวนลิขสิทธ์ที่ถูกต้อง
9. การขาดการอัพเดตและการแก้ไข(Patch) ของซอฟท์แวร์นั้น ๆ ตามระยะเวลาที่เหมาะสม เช่น โปรแกรมป้องกันไวรัส เป็นต้น

ดังนั้นจากการวิเคราะห์ความเสี่ยงทรัพย์สินระบบสารสนเทศของ ปตท. สผ. นั้นทุกกลุ่มมีความเสี่ยงและโอกาสในการเกิดภัยคุกคามต่าง ๆ กัน ซึ่งการวิเคราะห์ความเสี่ยงย่อมทำให้องค์กรสามารถดำเนินการเกี่ยวกับการพัฒนาแผนความปลอดภัยสารสนเทศและเครื่องมือความปลอดภัยต่าง ๆ อย่างเหมาะสมต่อไป

บทที่ 5

การพัฒนาแผนความปลอดภัยระบบสารสนเทศ

เนื่องจาก ปตท. สผ. ยังไม่ได้มีการจัดทำแผนแม่บทความปลอดภัยระบบสารสนเทศเป็นลายลักษณ์อักษร ซึ่งจากการศึกษาสภาพการณ์ปัจจุบันพบว่าองค์กรได้มีการกำหนดนโยบายทั่ว ๆ ไปที่เกี่ยวเนื่องกับการใช้เทคโนโลยีสารสนเทศประกอบไปด้วยหัวข้อดังนี้

1. การใช้เทคโนโลยีสารสนเทศอินเตอร์เน็ต
2. การใช้เทคโนโลยีอิเล็กทรอนิกส์เมล์
3. การเข้าถึงข้อมูล
4. การใช้อุปกรณ์สื่อสารโทรคมนาคม
5. สิทธิส่วนบุคคล
6. ข้อกำหนดการใช้เทคโนโลยีสารสนเทศสำหรับผู้ปฏิบัติงานสมทบ พนักงานของผู้รับจ้างหรือพนักงานจากบริษัทที่ปรึกษา

ส่วนแผนงานความปลอดภัยอื่นๆ ได้มีการจัดทำเฉพาะแผนงานฉบับร่างได้แก่ แผนสำรองฉุกเฉิน (Contingency Plan) และแผนกู้คืนความเสียหาย (Disaster Recovery) แต่ก็ยังขาดความชัดเจนและการศึกษาที่ดีพอ นอกจากนี้ ในส่วนของนโยบายความปลอดภัยนั้น (ดูภาคผนวก ก) ถึงแม้ว่าจะมีการกำหนดขึ้นมาก็ขาดการทบทวน ขาดการสื่อสารกับพนักงานอย่างจริงจัง และขาดการกำหนดเพิ่มเติม รวมทั้งยังขาดการยึดมาตรฐานหรือแนวทางใดแนวทางหนึ่งขึ้นมาใช้สำหรับการรักษาความปลอดภัยระบบสารสนเทศขององค์กร ดังนั้นผู้ศึกษาจึงได้พัฒนาแผนความปลอดภัยระบบสารเทศโดยยึดแนวทางมาตรฐานระบบรักษาความปลอดภัยสากล ISO/IEC 17799 ซึ่งแผนความปลอดภัยระบบสารสนเทศขององค์กรมีลักษณะดังนี้

5.1 วัตถุประสงค์ (Purpose)

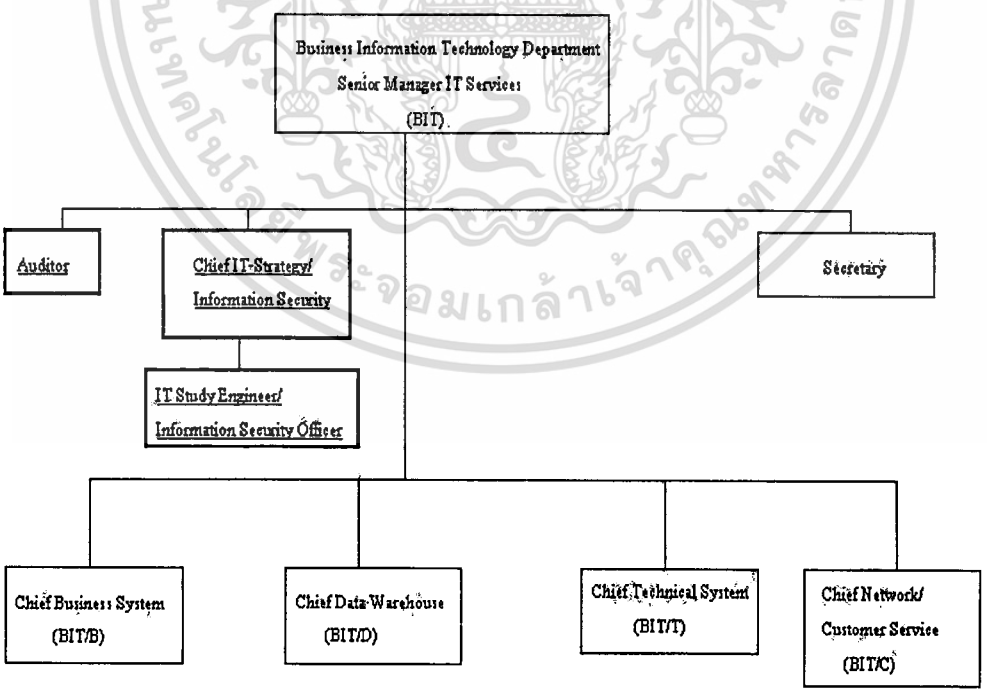
วัตถุประสงค์ของการจัดทำแผนแม่บทความปลอดภัยนี้เพื่อเป็นแนวทางสำหรับระบบรักษาความปลอดภัยสารสนเทศขององค์กร ปตท .สผ. ซึ่งความปลอดภัยระบบสารสนเทศครอบคลุมถึง

1. การรักษาความลับ (Confidentiality) คือการทำให้เกิดความเชื่อมั่นต่อพนักงาน ผู้บริหาร ผู้ว่าจ้าง ว่าสารสนเทศขององค์กรเป็นความลับเข้าถึงได้เฉพาะบุคคลที่เป็นเจ้าของหรือผู้ที่ได้รับอนุญาต
2. ความมีบูรณภาพ (Integrity) คือแผนกเทคโนโลยีสารสนเทศมีการป้องกันข้อมูลเพื่อความถูกต้องและความสมบูรณ์ของสารสนเทศและมีขั้นตอนการประมวลผลที่มีประสิทธิภาพ
3. ความพร้อมใช้งาน (Availability) คือการทำให้เกิดความมั่นใจว่า ผู้บริหาร พนักงาน ผู้ว่าจ้าง หรือที่ปรึกษาขององค์กรมีสิทธิเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องได้ตลอดเวลาตามสิทธิที่ได้รับ

5.2 ขอบเขตของการประยุกต์ใช้แผนความปลอดภัยและหน่วยงานที่รับผิดชอบ

ให้มีการใช้แผนความปลอดภัยและเครื่องมือความปลอดภัยภายในองค์กรสำนักงานใหญ่และสำนักงานสาขา โดยให้มีหน่วยงานสารสนเทศเข้ามีหน้าที่รับผิดชอบ และจัดโครงสร้างองค์กรภายในหน่วยงานและหน้าที่ความรับผิดชอบ ดังนี้

รูปแบบโครงสร้างองค์กรที่รวมงานด้านความปลอดภัยระบบสารสนเทศ



รูปที่ 5.1 แสดงโครงสร้างองค์กรแผนกเทคโนโลยีสารสนเทศที่ควรรวมงานด้านความปลอดภัยระบบสารสนเทศ

5.3 ความรับผิดชอบในเรื่องของระบบความปลอดภัยสารสนเทศ

ผู้จัดการอาวุโส (Senior Manager IT Services) หรือ BIT มีหน้าที่ในการกำหนดกลยุทธ์ ความปลอดภัย นำเสนอฝ่ายบริหาร และช่วยจัดหาทรัพยากรแรงสนับสนุนจากฝ่ายบริหาร นอกจากนี้ยังเป็นผู้สร้างวัฒนธรรมในเรื่องของความตระหนักเกี่ยวกับความปลอดภัย

หัวหน้าหน่วยสายงานกลยุทธ์และความปลอดภัย (Chief IT Strategy/ Information Security) มีหน้าที่ในการกำหนดกลยุทธ์ความปลอดภัยในองค์กร เป็นผู้กำหนดนิยาม ข้อเสนอแนะด้านความปลอดภัย ร่วมกับหน่วยงานต่าง ๆ เช่น ฝ่ายสุขภาพ อนามัยและสิ่งแวดล้อมและหน่วยงานต่าง ๆ ที่เป็นเจ้าของข้อมูลจัดทำร่างนโยบายและเครื่องมือความปลอดภัยต่าง ๆ เพื่อเสนอไปยังผู้จัดการอาวุโส รวมทั้งรับผิดชอบเกี่ยวกับข้อตระหนักด้านความปลอดภัยและเสนอแนะฝ่ายบริหารเกี่ยวกับประเด็นด้านความปลอดภัย รวมทั้งการมีทีมงานวิเคราะห์ความเสี่ยงและประสานงานกับหน่วยงานด้านความมั่นคงต่าง ๆ ของรัฐ

วิศวกรศึกษาและความปลอดภัย (IT Study Engineer/ Information Security Officer) มีหน้าที่รับผิดชอบเกี่ยวกับการศึกษา การจัดทำ การตรวจสอบวิเคราะห์ความปลอดภัยหรือภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นร่วมกับเจ้าหน้าที่ หน่วยงานสนับสนุนงานด้านเทคนิค (BIT/T) หน่วยงานสนับสนุนด้านธุรกิจ (BIT/B) หน่วยงานสนับสนุนด้านฐานข้อมูลองค์กร (BIT/D) หน่วยงานสนับสนุนด้านเครือข่ายและบริการ (BIT/C) จัดทำรายงานรวมทั้งกลยุทธ์วิเคราะห์ความเสี่ยงต่าง ๆ รายงานไปยังหัวหน้าและจัดทำรายงานเหตุสุดวิสัย (Incident Report) สำเนาไปยังฝ่ายสุขภาพ ความปลอดภัยและสิ่งแวดล้อม (BHS)

ผู้ตรวจสอบ (Auditor) เจ้าหน้าที่ตรวจสอบระบบความปลอดภัย มีหน้าที่ตรวจสอบความปลอดภัยของระบบสารสนเทศ รวมทั้งทดลองแคร็กเข้ามาในระบบสารสนเทศขององค์กร โดยอาจว่าจ้างบุคคลภายนอกหรือองค์กรอิสระ

5.4 เป้าหมาย (Goals) ของการทำแผนความปลอดภัยระบบสารสนเทศ

เป้าหมายของการวางแผนระบบความปลอดภัยสารสนเทศนี้เพื่อ

1. เป็นแนวทางให้องค์กรได้ยึดถือเป็นแนวปฏิบัติ
2. เพื่อปรับปรุงการปกป้องคุ้มครองทรัพยากรสารสนเทศให้ได้รับการป้องกันและการคุ้มครองจากความเสี่ยงหรือเหตุสุดวิสัยที่อาจเกิดขึ้น
3. เพื่อปกป้องคุ้มครองผู้บริหาร พนักงาน และผู้ว่าจ้างขององค์กรให้สอดคล้องกับกฎหมายและพระราชบัญญัติข้อบังคับต่าง ๆ

5.5 การทบทวน การปรับปรุง และการประยุกต์ใช้แผน

ผู้จัดการอาวุโสแผนกเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบสูงสุดเกี่ยวกับระบบความปลอดภัยสารสนเทศขององค์กร ปตท. สผ. โดยมีหน่วยงานส่งเสริมและพัฒนากลยุทธ์และความปลอดภัยมีหน้าที่รับผิดชอบในการจัดเตรียมแผน การออกแบบ การประยุกต์ใช้ โดยวางแผนความปลอดภัยรวมทั้งเครื่องมือความปลอดภัยต่าง ๆ ควรมีการทบทวนแผน นโยบาย ทุก 1-2 ปี เนื่องจากองค์กรจะมีการเปลี่ยนแปลงเทคโนโลยีหรือระบบปฏิบัติการทุก 2 ปี นอกจากนี้หน่วยงานในแผนกเทคโนโลยีสารสนเทศทุกหน่วยมีหน้าที่รับผิดชอบในการประยุกต์ใช้แผนความปลอดภัย สำหรับการติดตั้ง การประมวลผลคอมพิวเตอร์และการสื่อสารเครือข่ายทุกระบบในแผนกเทคโนโลยีสารสนเทศ และมีการตรวจสอบความปลอดภัยจากเจ้าหน้าที่ตรวจสอบภายนอกหรือองค์กรอิสระเป็นประจำ

5.6 แผนความปลอดภัยสารสนเทศจัดแบ่งเป็น 3 ระดับในการควบคุมหรือป้องกันคือ

5.6.1 การจัดการควบคุมเชิงบริหาร เป็นการจัดการแผนในเรื่องของการบริหารทั่ว ๆ ไป เกี่ยวกับระบบสารสนเทศได้แก่

1. การประเมินความเสี่ยง การจัดการความเสี่ยงเป็นการวิเคราะห์ภัยคุกคาม ความเสี่ยงที่อาจเกิดขึ้นกับ ปตท. สผ. โดยให้มีหัวหน้าหน่วยงานสายกลยุทธ์ร่วมทำงานกับตัวแทนของแผนกหรือหน่วยงานต่าง ๆ ในองค์กรในการจัดแยก จัดทำบัญชี ชนิดของทรัพย์สิน ของสำนักงานใหญ่ หน่วยงานโครงการปฏิบัติการบงกชและอาทิตย์ (Bongkot Asset, Arthit Asset) สำนักงานจัดส่งบำรุงกำลัง (Songkhla Logistic Base) โครงการไทย- มาเลเซีย (JDA) โครงการเมียนมาร์ โครงการสุพรรณ โครงการโอมาน โครงการเวียดนาม รวมทั้งวิเคราะห์ภัยคุกคามผลกระทบของแต่ละโครงการที่จะเกิดขึ้นกับโครงการและระบบสารสนเทศและเสนอแนะแนวทางป้องกันทรัพย์สินข้อมูลสารสนเทศของแต่ละหน่วยงานหรือโครงการนั้น ๆ (ตัวอย่างของการวิเคราะห์และประเมินความเสี่ยงในบทที่ 4 ผู้ศึกษาศึกษาเฉพาะสำนักงานใหญ่)

ตัวอย่างการดำเนินงานวิเคราะห์ความเสี่ยง

- **ขั้นตอนวิธีการเกี่ยวกับการจัดตั้งทีมงานวิเคราะห์ความเสี่ยงซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานต่าง ๆ คือ**
  - **ผู้จัดการใหญ่**
  - **ผู้จัดการอาวุโสแผนกเทคโนโลยีสารสนเทศ**
  - **หัวหน้าหน่วยงานส่งเสริมและพัฒนากลยุทธ์แผนกเทคโนโลยีสารสนเทศ**
  - **หัวหน้าหน่วยงานฐานข้อมูลองค์กรแผนกเทคโนโลยีสารสนเทศ**
  - **หัวหน้าหน่วยงานสนับสนุนระบบงานด้านเทคนิคแผนกเทคโนโลยีสารสนเทศ**

- หัวหน้าหน่วยงานเครือข่ายและบริการผู้ใช้
- หัวหน้าหน่วยงานสนับสนุนระบบธุรกิจ
- ตัวแทนจากสายงานกลยุทธ์และพัฒนาศักยภาพ
- ตัวแทนจากฝ่ายตรวจสอบ
- ตัวแทนจากฝ่ายสุขภาพ ความปลอดภัยและสิ่งแวดล้อม
- ตัวแทนจากฝ่ายกิจการสัมพันธ์
- ตัวแทนจากสายงานปฏิบัติการ
- ตัวแทนจากสายงานเทคนิค
- ตัวแทนจากสายงาน โครงการร่วมทุน
- ตัวแทนจากสายงานบริการธุรกิจ
- ตัวแทนจากสายงานพัฒนาธุรกิจ
- ตัวแทนจากสายงานการเงินและการบัญชี

❑ ขั้นตอนในการดำเนินการวิเคราะห์ความเสี่ยง ประกอบด้วย

- ทีมงานประเมินความเสี่ยงทำการวิเคราะห์ จัดแยก ชนิดของทรัพย์สินด้านระบบสารสนเทศที่มีความสำคัญของแต่ละหน่วยงาน
- วิเคราะห์โอกาสหรือความเสี่ยงที่ข้อมูลสารสนเทศนั้นจะสูญหายไปหรือถูกทำลายไป
- วิเคราะห์ภัยคุกคามที่จะเกิดขึ้นกับแต่ละสายงานหรือหน่วยงานนั้น ๆ ทั้งสำนักงานใหญ่ โครงการต่าง ๆ
- จัดลำดับความสำคัญของทรัพย์สินข้อมูลสารสนเทศที่ต้องมีการปกป้องคุ้มครองเป็นพิเศษ
- เสนอแนะแนวทางป้องกันหรือเครื่องมือป้องกันที่เหมาะสม

❑ ขั้นตอนการนำไปประยุกต์ใช้

- แต่ละหน่วยงานหรือสายงานแจ้งไปยังแผนกเทคโนโลยีสารสนเทศถึงความต้องการให้มีการคุ้มครองชนิดและประเภทของข้อมูลที่ต้องการ
- แผนกเทคโนโลยีสารสนเทศจัดหา จัดทำเครื่องมือในการป้องกันและหรือวิธีการในการป้องกันความสูญหายของข้อมูล
- แผนกเทคโนโลยีสารสนเทศจัดทำงบประมาณเสนอไปยังคณะกรรมการและผู้บริหารเพื่อจัดซื้อ จัดสร้างเครื่องมือในการลดความเสี่ยง

❑ การติดตามและการประเมินผล

- แต่ละสายงานต้องมีการประเมินผลถึงผลดีผลเสียจากการวิเคราะห์ความเสี่ยงและเหตุสุดวิสัยที่เกิดเหนือความคาดหมาย
- รายงานสรุปผลไปยังคณะทีมงานประเมินความเสี่ยงเพื่อหาแนวทางหรือแผนงานอื่นเพื่อสนับสนุนต่อไป
- ทีมงานประเมินความเสี่ยงมีการจัดการประชุม วิเคราะห์ความเสี่ยงอย่างเป็นประจำทุก 6 เดือน

2. ให้แผนกเทคโนโลยีสารสนเทศจัดทำแผนในลักษณะของวงจรชีวิตของการบริหารระบบสารสนเทศ 5 แนวทางคือ
   - ขั้นตอนเริ่มต้น(Initiation Phase) คือเมื่อหน่วยงานเทคโนโลยีสารสนเทศขององค์กรได้แก่ BIT/B BIT/C BIT/D BIT/T ต้องการพัฒนาระบบสารสนเทศจะต้องมีการจัดการประเมินความเสี่ยงที่อาจเกิดขึ้นต่อระบบงานปัจจุบันและให้จัดทำแผนแสดงรายละเอียดเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นและแนวทางป้องกันและแก้ไข
   - ขั้นตอนการพัฒนาและการจัดหา (Development/ Acquisition Phase) หน่วยงานต่าง ๆ ของแผนกเทคโนโลยีสารสนเทศจะต้องมีกลไกในการกำจัดหรือลดความเสี่ยงในขั้นตอนของการจัดหาและพัฒนาโดยมีวิธีการคือ
     - การออกแบบจะต้องกำหนดความต้องการเรื่องความปลอดภัย
     - ควรมีขั้นตอนทดสอบและประเมินความปลอดภัยในการจัดซื้อจัดหา
     - ต้องมีการจัดส่งเอกสารร้องขอ (Request for proposals) ที่กำหนดความต้องการความปลอดภัย การทดสอบความปลอดภัยไปยังคู่ค้าหรือบริษัทที่จัดซื้อจัดหา จัดจ้าง
     - การจัดซื้อจัดหาแอพพลิเคชั่นสำเร็จ จะต้องมีการกำหนดคุณสมบัติในความปลอดภัยของแอพพลิเคชั่นนั้น ไว้ด้วย
   - ขั้นตอนการประยุกต์ใช้ (Implementation Phase) ในการประยุกต์ใช้หรือติดตั้งระบบสารสนเทศของหน่วยงานต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศนั้นฟังก์ชันหรือคุณลักษณะด้านความปลอดภัยจะต้องมีการติดตั้ง (Configured) และให้ทำงาน และมีการทดสอบความปลอดภัยและมีการทบทวนความปลอดภัยตามสมควร โดยให้สอดคล้องกับนโยบาย กฎระเบียบ กฎหมาย มาตรฐานและข้อแนะนำขององค์กรที่ยึดถือปฏิบัติ
   - ขั้นตอนการดำเนินงานและการบำรุงรักษา (Operation/Maintenance Phase) เมื่อระบบสารสนเทศของหน่วยงานต่าง ๆ ภายในแผนกเทคโนโลยีสารสนเทศได้ดำเนินงาน

ในช่วงระยะเวลาหนึ่งอาจมีการเพิ่มเติมในส่วนของฮาร์ดแวร์และซอฟท์แวร์ การเปลี่ยนแปลงใด ๆ จะต้องมีการกำหนดแผนงานด้านต่าง ๆ คือ

- การจัดการความปลอดภัยและการบริหาร ให้มีการทำสำรองข้อมูล มีการฝึกอบรมแจ้งกล่าวพนักงานและปรับปรุงฟังก์ชันของความปลอดภัยให้สอดคล้องกับการเปลี่ยนแปลงด้วย
- มีการประกันการปฏิบัติงาน คือหน่วยงานต่าง ๆ จะต้องมีการตรวจสอบการทำงานของระบบหลังจากเปลี่ยนแปลงปรับปรุงฮาร์ดแวร์และซอฟท์แวร์
- มีการตรวจสอบและติดตาม โดยต้องมีมาตรการในการตรวจสอบแผนความปลอดภัยอย่างเหมาะสม

- ขั้นตอนการทำลาย (Disposal Phase) เป็นหน้าที่ความรับผิดชอบของหน่วยงานต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศที่จะต้องจัดทำบัญชีอุปกรณ์หรือทรัพยากรทางคอมพิวเตอร์ที่ต้องทำลายหรือบริจาคอันเนื่องมาจากเสีย หมดอายุการใช้งาน หรือหมดอายุทางการบัญชี และจะต้องมีการรับรองและตรวจสอบจากฝ่ายต่าง ๆ อย่างเหมาะสมเป็นลายลักษณ์อักษรและต้องจัดทำแผนในการทำลายวัสดุหรืออุปกรณ์ต่าง ๆ เหล่านั้น

ตัวอย่างการวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีสารสนเทศในแผนกเทคโนโลยีสารสนเทศ

- การแบ่งแยกชนิดและทรัพย์สินของระบบสารสนเทศที่มีความสำคัญและความเสี่ยง

1. ระบบเซิฟเวอร์ที่จัดเก็บแฟ้มข้อมูลและจัดการการพิมพ์ ได้แก่
   - HQ-FS4 ที่สำนักงานใหญ่
   - HQ-FS5 ที่สำนักงานใหญ่
   - HQ-FS1 ที่สำนักงานใหญ่
   - BQP-DC1 ที่สำนักงานบงกช ในทะเลอ่าวไทย
   - BQP-SKL1 ที่สำนักงานบำรุงเสบียง จังหวัดสงขลา
   - OM-DC1 ที่สำนักงาน ประเทศโอมาน
2. เซิฟเวอร์ Geology and Geophysic
3. เซิฟเวอร์ฐานข้อมูลสำหรับระบบงานสนับสนุนธุรกิจ
4. เซิฟเวอร์เมล์อิเล็กทรอนิกส์
5. เซิฟเวอร์ที่เป็นอินทราเน็ตและ Data warehouse

- แนวทางหรือเครื่องมือป้องกัน ได้แก่
  - มีการจัดทำ Off-line Backup โดยเก็บข้อมูลทุกวันลักษณะของ Differential Backup , Weekly full Backup, Monthly full Backup
  - ทุกหน่วยงานเก็บสำรองข้อมูลไว้ที่ธนาคารหรือที่ที่มีความปลอดภัยเทียบเท่า
  - ทุกหน่วยงานสร้างคู่มือขั้นตอนในการทำสำรองข้อมูลและขั้นตอนในการกู้คืนข้อมูล
  - มีการจัดทำสัญญาจ้างหรือเช่าอุปกรณ์ฮาร์ดแวร์และซอฟท์แวร์จากผู้ค้ารายอื่นในกรณีที่อุปกรณ์สำรองข้อมูลเสียหายหรือนำไปซ่อม
  - ให้มีการจัดทำรายการ ชนิดของข้อมูลที่สำรอง ฐานข้อมูล ชื่อเซิฟเวอร์ วันเวลาที่มีการทำสำรองข้อมูลและชื่อสื่อที่ใช้ในการสำรอง

5.6.2 การควบคุมเชิงปฏิบัติการ (Operational Control) เป็นการวางแผนที่เกี่ยวกับงานด้านความปลอดภัยระบบสารสนเทศขององค์กรที่จะเกิดจากการกระทำของบุคคลหรือเกี่ยวข้องกับบุคคลากรในองค์กรซึ่งประกอบไปด้วย

1. ความปลอดภัยของระบบสารสนเทศจากบุคคลในองค์กร (Personal Security) เพื่อลดความเสี่ยงจากการกระทำผิดพลาด การขโมย การฉ้อโกง และการใช้งานระบบสารสนเทศในทางที่ผิด โดยให้ฝ่ายบุคคล (BHS) มีอำนาจหน้าที่ในการทำงานขั้นต้นเกี่ยวกับการรับสมัคร เพื่อดูคุณลักษณะและคุณสมบัติที่ตระหนักในความปลอดภัย โดยมีการทำข้อตกลงในสัญญาจ้างงานเกี่ยวกับเงื่อนไขและนิยามความรับผิดชอบของพนักงานในเรื่องความปลอดภัยระบบสารสนเทศ

ตัวอย่างขั้นตอนในการดำเนินงาน

- ฝ่ายบุคคลพิจารณาประวัติของพนักงานในขั้นตอนการรับสมัครงานและการสัมภาษณ์
- ฝ่ายบุคคลจัดทำข้อตกลงในสัญญาจ้างงานเกี่ยวกับเงื่อนไขและความรับผิดชอบและความผิดในการทำลายหรือละเมิดความปลอดภัยข้อมูลขององค์กร
- หัวหน้าหน่วยงานหรือผู้บังคับบัญชาของแต่ละหน่วยงานจัดส่งรายชื่อพนักงานเพื่อขอบัญชีชื่อผู้ใช้และบัญชีเมล์ต่อแผนกเทคโนโลยีสารสนเทศ
- หัวหน้าหน่วยงานหรือแต่ละสายงานพิจารณาในการกำหนดสิทธิ์ในการเข้าถึงชนิดและประเภทของข้อมูลหรือไดร์ฟที่ต้องการให้กับพนักงานในสายงาน
- แผนกเทคโนโลยีจัดทำรายละเอียดเกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลของพนักงาน
- ฝ่ายกฎหมายร่วมกับฝ่ายบุคคลกำหนดมาตรการ การลงโทษสำหรับพนักงานที่ละเมิดข้อบังคับของเปิดเผยความลับข้อมูลขององค์กร การล่วงละเมิดทรัพยากรข้อมูลของผู้อื่น การดัดแปร การแก้ไข

- ฝ่ายบุคคลแจ้งข้อกฎหมายอื่น ๆ เช่นพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ที่มีผลต่อพนักงานในการใช้สารสนเทศ

2. ให้มีการจัดการความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) ให้เป็นอำนาจหน้าที่ของฝ่ายบริหารอาคาร (BAM) ดำเนินงานร่วมกับเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ (BIT) จัดทำวางแผนการจัดการความปลอดภัยของอาคารเพื่อป้องกันการเข้าถึง การแทรกแซง การทำลายข้อมูล ศูนย์คอมพิวเตอร์ และอุปกรณ์ระบบสารสนเทศทุกชนิดขององค์กร เช่นการกำหนดพื้นที่ทางกายภาพของอาคารให้ชัดเจน พื้นที่ทำงานของพนักงาน พื้นที่ติดตั้งระบบสารสนเทศ การติดตั้งอุปกรณ์สำรองไฟฟ้า การแยกพื้นที่ทางเดินของสายไฟและสายสัญญาณที่ใช้เชื่อมโยงระบบสารสนเทศ

ตัวอย่างการดำเนินงานสำหรับห้องคอมพิวเตอร์

- ฝ่ายอาคารติดตั้งกล้องวงจรปิดบริเวณทางเข้าห้องคอมพิวเตอร์
- ฝ่ายอาคารติดตั้งอุปกรณ์ปั่นไฟฟ้าเพื่อใช้ในยามที่ไฟฟ้านครหลวงดับ
- มีพนักงานรักษาความปลอดภัยตรวจตราทุก 4 ชั่วโมง
- มีระบบไฟสำรองฉุกเฉิน
- มีระบบแอร์ที่แยกจากอาคารและมีการแบ่งกันทำงานตัวละ 12 ชั่วโมง
- มีอุปกรณ์วัดความชื้นและอุณหภูมิของห้อง
- ห้ามการนำอาหารเครื่องดื่มเข้าห้องคอมพิวเตอร์
- มีอุปกรณ์ดักจับควันไฟ และดับไฟ
- มีการยกพื้นเพื่อสามารถจัดเก็บสายไฟฟ้าและสายเครือข่ายต่าง ๆ
- มีระบบ Access Control
- มีปุ่มเปิดอัตโนมัติภายในห้องคอมพิวเตอร์บริเวณประตูทางออก
- มีการจดบันทึกผู้ที่เข้ามาใช้บริการศูนย์คอมพิวเตอร์

3. ให้มีการจัดการระบบการติดต่อสื่อสารเครือข่ายและการปฏิบัติการ (Communicational and Operations Management) ให้เป็นหน้าที่ของแผนกเทคโนโลยีสารสนเทศดำเนินการเกี่ยวกับ

- จัดทำขั้นตอนคู่มือการปฏิบัติงานเกี่ยวกับความปลอดภัยของระบบเครือข่าย รวมทั้งจัดอำนาจหน้าที่ความรับผิดชอบเพื่อทำให้เกิดความถูกต้องและปลอดภัยต่อการดำเนินการกับอุปกรณ์ประมวลผลข้อมูล

- มีการจัดทำแผนระบบและเงื่อนไขในการยอมรับระบบสารสนเทศที่มีการเปลี่ยนแปลง การปรับปรุงหรือเวอร์ชั่นใหม่ ควรมีการทำแผนทดสอบที่เหมาะสมก่อนที่จะยอมรับนำมาใช้งาน

ตัวอย่างขั้นตอนในการดำเนินงาน

- มีการจัดทำแผนผังแสดงการจัดการเครือข่ายท้องถิ่นและระยะไกลสำหรับสำนักงานกรุงเทพ สงขลา ชายฝั่ง สำนักงานที่พม่าและที่สำนักงานโอมาน
- มีการตรวจสอบอุปกรณ์ที่ติดตั้งว่าตรงกับแผนผัง
- มีการตรวจสอบการทำงานของอุปกรณ์หรือตรวจสอบ log ต่าง ๆ ของระบบ
- มีการกำหนดผู้รับผิดชอบด้านระบบเครือข่าย
- มีการกำหนดสิทธิ์ในการเข้าใช้งานตามหน้าที่ที่รับผิดชอบ
- มีการ Encrypt รหัสผ่านที่อุปกรณ์ต่าง ๆ
- ผู้ดูแลต้องหมั่นตรวจสอบความปลอดภัยของระบบเสมอ
- ผู้ดูแลต้องตรวจสอบประสิทธิภาพการใช้งานของอุปกรณ์อยู่เสมอ
- ให้จัดทำมาตรการวิธีการป้องกัน ต่อต้าน ซอฟท์แวร์ประสงค์ร้าย ที่อาจเกิดขึ้นได้กับองค์กร และกับพนักงานโดยให้แผนกเทคโนโลยีสารสนเทศ จัดหาเครื่องมือป้องกันและควบคุมซอฟท์แวร์เหล่านั้นและจัดทำแผนภูมิกู้คืนความเสียหายและแผนงานให้สามารถทำงานต่อเนื่องได้ยามเกิดปัญหา

ตัวอย่างการดำเนินงาน

- ติดตั้งซอฟท์แวร์ป้องกันไวรัสที่เครื่องไคลเอ้นท์ทุกเครื่อง
- ต้องมีการปรับปรุงซอฟท์แวร์ป้องกันไวรัสอยู่เสมอ ๆ
- มีการอบรมแก่พนักงานในการได้รับแฟ้มข้อมูลที่ผิดปกติจากภายนอก
- มีการอบรมการใช้โปรแกรมป้องกันไวรัสกับพนักงาน
- มีการติดตั้งซอฟท์แวร์ป้องกันไวรัสสำหรับเมล์เกตเวย์เซิฟเวอร์
- มีการติดตามข่าวสารข้อมูลและอันตรายของไวรัสที่เกิดขึ้นในแต่ละวัน
- มีการสำรองข้อมูลอยู่เสมอ ๆ
- มีการตรวจสอบไวรัสสำหรับแอพพลิเคชั่นทางอินเตอร์เน็ต

เลขที่ .....

วันที่ .....

หน่วยงานของพนักงาน .....

เพื่อให้เป็นไปตามแผนนโยบาย มาตรฐาน และขั้นตอนเกี่ยวกับความปลอดภัยในระบบสารสนเทศของบริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน) ข้าพเจ้ายินยอมตกลงกับข้อกำหนดดังต่อไปนี้

1. ข้าพเจ้าได้รับคู่มือพนักงานขององค์กร
2. ข้าพเจ้ายอมรับเงื่อนไขในการกำหนดสิทธิในการเข้าถึงข้อมูลระบบสารสนเทศขององค์กรและจะไม่พยายามในการละเมิดสิทธิในการเข้าถึงข้อมูลผู้อื่นและจะใช้ทรัพยากรสารสนเทศเพื่อประโยชน์องค์กรเท่านั้น
3. ข้าพเจ้าจะรักษารหัสผู้ใช้ประจำตัวและรหัสผ่านไว้เป็นความลับที่สุด
4. ข้าพเจ้าจะทำการล็อคหรือปิดเครื่องทุกครั้งเมื่อข้าพเจ้าไม่ได้นั่งปฏิบัติงานที่เครื่องคอมพิวเตอร์
5. ข้าพเจ้าจะไม่นำทรัพย์สินข้อมูลขององค์กรไปเผยแพร่ให้บุคคลภายนอกทราบหรือให้พนักงานที่ไม่เกี่ยวข้องทราบ
6. ข้าพเจ้าจะทำลายข้อมูลความลับขององค์กรที่ไม่ได้ใช้งานแล้วจนเกิดความมั่นใจว่าไม่สามารถนำข้อมูลไปเผยแพร่ได้
7. ข้าพเจ้าตระหนักถึงการใช้ทรัพยากรระบบสารสนเทศขององค์กรและจะคำนึงถึงความเสียหาย การถูกลักขโมยหรือการสูญหายเป็นต้น
8. หากว่าข้าพเจ้าพบการกระทำของบุคคลภายนอกหรือบริษัทที่ว่าจ้างเกี่ยวกับข้อมูลขององค์กร ข้าพเจ้าจะรายงานให้ผู้บังคับบัญชาทราบทันที
9. ข้าพเจ้ายอมรับการถูกลงโทษและการถูกออกจากงานในกรณีที่ละเมิดข้อตกลงข้างต้น

ข้าพเจ้าได้อ่านและเข้าใจข้อความข้างต้นทุกประการ

ลงชื่อ .....

(.....)

วันที่ .....

พยาน .....

รูปที่ 5.2 แสดงตัวอย่างสัญญาจ้างงานที่รวมประเด็นด้านความปลอดภัยระบบสารสนเทศ

- มีการใช้ซอฟท์แวร์ป้องกันไวรัสที่แตกต่างกันระหว่างเครื่องไคลเอ้นท์และเครื่องเซิฟเวอร์
- ให้แผนกเทคโนโลยีสารสนเทศมีการจัดการงานในลักษณะงานแม่บ้าน เพื่อรักษาไว้ซึ่งความมีบูรณภาพและความพร้อมใช้งานของการประมวลผลข้อมูลและบริการติดต่อสื่อสารเครือข่าย โดยให้มีการทำสำรองข้อมูลขององค์กรเป็นประจำและมีการจัดเก็บไว้ในสถานที่ที่ต่างกัน มีการจัดทำบันทึกการปฏิบัติงานเกี่ยวกับระบบต่าง ๆ เก็บรายงานข้อผิดพลาดที่เกิดขึ้นกับระบบ
- ให้มีการจัดการงานทางด้านเครือข่ายเพื่อให้เกิดความมั่นใจว่ามีการป้องกันข้อมูลจากเครือข่ายและปกป้องโครงสร้างพื้นฐานต่าง ๆ โดยผู้จัดการหรือหัวหน้าหน่วยงานเครือข่ายและบริการ (BIT/C) ต้องประยุกต์ใช้เครื่องมือป้องกันข้อมูลในเครือข่ายรวมทั้งป้องกันการเชื่อมต่อจากการเข้าถึงที่ไม่ได้รับอนุญาต

4. ให้มีการจัดการเก็บสื่อบันทึกและมีวิธีการป้องกัน สื่อบันทึกได้แก่ เทป ดิสก์ วีดีโอ ซีดี กระดาษ รายงาน คาสเซ็ท และอื่น ๆ โดยหน่วยงานต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศควรมีการจัดเก็บดูแลสื่อบันทึกเหล่านี้ในที่ที่ปลอดภัย มีการจัดทำรายการ ติดแถบฉลาก และมีการทำลายอย่างถูกต้องและปลอดภัยและจัดทำเอกสารขั้นตอนในการเคลื่อนย้ายอย่างเหมาะสม
5. ให้มีการจัดการความปลอดภัยในการแลกเปลี่ยนข้อมูลและซอฟท์แวร์ระหว่างองค์กรเพื่อป้องกันการสูญหาย การดัดแปร การใช้ข้อมูลในทางที่ผิดซึ่งเกิดจากการแลกเปลี่ยนระหว่างองค์กร ให้หน่วยงานต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศมีเอกสารข้อตกลงระหว่างบริษัทต่างๆ สำหรับการค้าผ่านอิเลกทรอนิกส์จะต้องมีรายละเอียดการอนุญาตเข้าถึงข้อมูลและซอฟท์แวร์ระหว่างกันในเครือข่ายสาธารณะ นอกจากนี้ให้หน่วยงานต่าง ๆ ที่มีการจัดส่งพัสดุ ข้อมูล ขององค์กรในทางกายภาพ โดยผ่านผู้ให้บริการจัดส่งพัสดุ จะต้องคำนึงถึงความปลอดภัย โดยเลือกผู้ให้บริการที่เชื่อถือได้ และมีการบรรจุที่ดี มีการยืนยันการรับส่งพัสดุนั้น ๆ
6. ให้มีการจัดการความปลอดภัยของอิเล็กทรอนิกส์เมล์ เนื่องจากการสื่อสารผ่านอิเล็กทรอนิกส์เมล์มีบทบาทมากขึ้นสำหรับการติดต่อสื่อสารขององค์กร ให้แผนกเทคโนโลยีสารสนเทศมีการจัดการประเมินความเสี่ยง จุดอ่อน การดัดแปลง ข้อบกพร่อง การตีความ การควบคุมผู้ใช้ เกี่ยวกับอิเล็กทรอนิกส์เมล์ ผู้จัดการอาวุโสแผนกเทคโนโลยีสารสนเทศจัดทำนโยบาย การใช้อิเล็กทรอนิกส์เมล์ เพื่อปกป้องคุ้มครองแฟ้มข้อมูล การโจมตีจากไวรัส วอร์ม ม้าโทรจันต่าง ๆ มีข้อเสนอแนะสำหรับพนักงานในการใช้เมล์ มีการระบุความรับผิดชอบของพนักงานต่อการใช้เมล์ ข้อบังคับทางกฎหมายที่ต้องทราบ และให้มีการเลือกใช้เทคโนโลยีการเข้ารหัสและการพิสูจน์ตัวตนที่เหมาะสม

ตัวอย่างการดำเนินการเกี่ยวกับความปลอดภัยอิเล็กทรอนิกส์เมล์

- รายการเซิฟเวอร์ที่ให้บริการ ได้แก่
  - Mail Node 1
  - Mail Node2
  - SKL-DC1
  - BKT-DC1
  - OM-DC1
  - HQ-OWA
- แนวทางในการป้องกัน
  - ติดตั้งระบบในแบบ Clustering/Mirroring
  - จัดทำสำรองข้อมูล Online Backup
  - จัดทำสำรองข้อมูล MailBox , Public Folder
  - มีการทดสอบการกู้คืนข้อมูล
  - มีการติดตั้งซอฟท์แวร์ต่อต้านไวรัสสำหรับเมล์เข้าและออก
  - ให้มีการติดตั้งซอฟท์แวร์สำหรับการเตือน(Alert) เหตุการณ์ผิดปกติของระบบ

7. ให้มีการพัฒนาแผนการดำเนินธุรกิจให้ต่อเนื่อง (Business Continuity Management) ให้แผนกเทคโนโลยีสารสนเทศร่วมกับแผนกหรือหน่วยงานต่าง ๆ ในองค์กรจัดทำแผนต่าง ๆ เพื่อป้องกันการชะงักงันของธุรกิจอันเกิดจากผลกระทบจากความล้มเหลวหรือความเสียหายของระบบสารสนเทศ โดยให้มีการเขียนแผนงานต่อเนื่อง โครงแบบของแผนงาน การประยุกต์ใช้ และการทดสอบแผนต่าง ๆ การบำรุงรักษาและการทบทวนปรับปรุงแผนอย่างต่อเนื่อง
8. ให้มีการจัดทำแผนกรณีฉุกเฉิน (Contingency Plan) เนื่องจากระบบสารสนเทศขององค์กรอาจได้รับความเสียหายจากปัจจัยเสี่ยงต่าง ๆ ที่อาจทำให้เกิดการชะงักงันหรือหยุดบริการแก่พนักงาน ดังนั้นหน่วยงานต่าง ๆ ของแผนกเทคโนโลยีสารสนเทศควรมีกระบวนการขั้นตอนอื่น ๆ หรือทำแผนขึ้นมารองรับเพื่อให้พนักงานสามารถทำงานต่อไปได้โดยให้มีการจัดทำแผนกรณีฉุกเฉินเช่น
   - การกู้คืนข้อมูล
   - จัดทำข้อตกลงเกี่ยวกับการทำสำรองข้อมูล เช่นเซิฟเวอร์ใดที่ทำสำรองข้อมูลและมีปริมาณฮาร์ดดิสก์เท่าใด

- จัดทำคู่มือการทำสำรองข้อมูลในลักษณะที่แสดงรายละเอียดประจำวัน ประจำสัปดาห์ ประจำเดือน ประจำปีและแสดงประเภทของการทำสำรองข้อมูลคือเป็นลักษณะการสำรองข้อมูลแบบสมบูรณ์หรือเฉพาะส่วนที่แตกต่าง
- สถานที่ที่จัดเก็บให้การมีการจัดเก็บที่ธนาคารหรือที่ที่ปลอดภัย
- ระยะเวลาในการจัดเก็บอย่างน้อย 5 ปี
- ให้มีการจัดทำคู่มือขั้นตอนการสำรองข้อมูลและการกู้คืนข้อมูล

9. ให้มีการจัดทำแผนฟื้นฟูความเสียหาย (Disaster Recovery Plan) เนื่องจากระบบสารสนเทศขององค์กรอาจได้รับผลกระทบจากภัยธรรมชาติ การก่อวินาศกรรมต่าง ๆ ได้ ให้แผนกเทคโนโลยีสารสนเทศจัดทำแผนฟื้นฟูความเสียหาย ลักษณะของเครือข่ายการเชื่อมต่อและประเภทหรือชนิดของเซิฟเวอร์และแอพพลิเคชั่นที่ต้องจัดให้มีขึ้น ณ ที่ศูนย์ฟื้นฟูความเสียหายนั้น ๆ รวมทั้งศึกษาต้นทุนและงบประมาณที่ต้องใช้จัดทำ
10. ให้มีการจัดทำโปรแกรมข้อตระหนักเกี่ยวกับความปลอดภัย (Security Awareness Program) ให้แผนกเทคโนโลยีสารสนเทศ (BIT) ร่วมกับแผนกบุคคล (BHS) จัดทำเครื่องมือหรือโปรแกรมข้อตระหนักเกี่ยวกับความปลอดภัยให้กับพนักงานและพนักงานที่เข้าใหม่ เพื่อให้พนักงานได้ตระหนักถึงความปลอดภัยของข้อมูลสารสนเทศขององค์กร รวมทั้งก่อให้เกิดประสิทธิภาพต่อแผน นโยบาย มาตรฐาน กฎระเบียบ ด้านความปลอดภัยขององค์กร โดยลักษณะโปรแกรมคือ
    - ให้มีการจัดทำนโยบายความปลอดภัย มาตรฐาน ข้อบังคับ ข้อปฏิบัติเกี่ยวกับความปลอดภัยด้านสารสนเทศอยู่ในคู่มือพนักงาน
    - ให้มีการจัดทำหรือนำเสนอในการปฐมนิเทศพนักงานที่เข้ามาใหม่เสมอ ๆ
    - ให้มีการจัดการติดต่อสื่อสารในรูปแบบต่าง ๆ เพื่อให้พนักงานได้รับรู้เช่น การประกาศให้ทราบ แผ่นพับ การจัดทำวีดีโอ
    - ให้มีการฝึกอบรมออนไลน์ไปยังสำนักงานสาขาต่าง ๆ
11. ให้มีการจัดทำการบริหารเหตุสุดวิสัย (Incident Response Plan) เหตุสุดวิสัยคือเหตุการณ์ความไม่ปลอดภัยหรือภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศขององค์กรโดยไม่คาดคิด ให้แผนกเทคโนโลยีสารสนเทศ (BIT) ทำงานร่วมกับแผนกสุขภาพ ความปลอดภัยและสิ่งแวดล้อม ดำเนินการจัดตั้งทีมงานที่รับผิดชอบตอบสนองต่อเหตุสุดวิสัย มีการจัดทำคู่มือเอกสารเกี่ยวกับระบบต่าง ๆ เช่น ระบบเครือข่ายองค์กร ระบบฐานข้อมูล ระบบการจัดเก็บแฟ้มข้อมูลวิกฤต ระบบเมล์ รายละเอียดบริษัทที่ว่าจ้าง

- จัดทำขั้นตอนในการตอบสนองต่อเหตุสุดวิสัย ได้แก่การตรวจพบเหตุการณ์ การจัดทำรายงานไปยังผู้บริหารหรือผู้จัดการอาวุโสแผนกเทคโนโลยีสารสนเทศ และขั้นตอนในการแก้ไขปัญหา
- จัดทำรูปแบบในการบันทึกเหตุการณ์และแก้ไขปัญหาเหตุสุดวิสัยให้พนักงานและแนวทางแก้ไขปัญหาเพื่อเก็บไว้เป็นหลักฐานในการวิเคราะห์เลือกเครื่องมือ นโยบาย วิธีการต่าง ๆ ขึ้นมาใช้ควบคุมความปลอดภัยต่อไป

5.6.3 การควบคุมทางเทคนิค (PTTEP Technical Control)

ให้เป็นหน้าที่และความรับผิดชอบของแผนกเทคโนโลยีสารสนเทศในการสร้าง วิเคราะห์ จัดหา ทดสอบ ประยุกต์ใช้ระบบความปลอดภัยเชิงเทคนิคหรือการควบคุมเชิงเทคนิค ซึ่งการควบคุมเชิงเทคนิคเกี่ยวข้องกับฟังก์ชันระบบความปลอดภัยของคอมพิวเตอร์ เช่น สามารถควบคุมการเข้าถึงโดยไม่ได้รับอนุญาต การสามารถรับรู้ถึงการละเมิดความปลอดภัย สามารถควบคุมแอพพลิเคชั่นและฐานข้อมูลขององค์กรได้ โดยฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมทางเทคนิคประกอบไปด้วย

1. ความสามารถในการจำแนกบุคคลและการพิสูจน์ตัวตน

การใช้ระบบสารสนเทศขององค์กรนั้นให้ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่สร้างระบบการพิสูจน์ ตัวตนของพนักงาน พนักงานว่าจ้าง พนักงานสมทบ คู่ค้า คู่สัญญา ผู้จัดซื้อจัดหา ที่เข้ามาใช้ระบบสารสนเทศขององค์กรทุกระบบโดยใช้รหัสเฉพาะบุคคลเดียวกันและให้ศึกษาการนำเทคโนโลยีต่าง ๆ มาใช้อย่างเหมาะสมในการพิสูจน์ตัวตน

ตัวอย่างขั้นตอนในการดำเนินงาน

- จัดให้มีการกำหนดระเบียบหรือขั้นตอนในการขออนุญาตใช้งานระบบสารสนเทศ
- การเปลี่ยนแปลงสถานภาพผู้ใช้จะต้องแจ้งให้ System Administrator รับทราบ
- การให้อำนาจใช้งานต้องให้ตามความจำเป็นและความเหมาะสมกับงานที่รับผิดชอบ
- ผู้ใช้งานต้องมีสถานะเป็นผู้ใช้ (User) เท่านั้นไม่ใช่ ผู้ดูแลระบบ (Administrator)
- มีการสอบทานบันทึกผู้ใช้อย่างสม่ำเสมอ
- จัดทำรายงานการใช้งานจำนวนข้อมูลที่มีโดยผู้ดูแลระบบ (System Administrator)

วันที่ …….. หมายเลขเหตุการณ์ ……..

(เฉพาะเจ้าหน้าที่แผนก BIT)

ชื่อพนักงานผู้รายงานเหตุการณ์ ……

แผนก/ฝ่าย …….. สถานที่ที่เกิดเหตุ ……

ลักษณะเหตุการณ์ผิดปกติที่เกิดขึ้น

……

……

……

……

……

……

……

เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศผู้ตรวจสอบ ……

ความรุนแรงของปัญหา น้อย ปานกลาง มาก

วิธีการแก้ไขปัญหา

……

……

ความสำเร็จในการแก้ไขปัญหา ประสบความสำเร็จ ล้มเหลว

ลงบันทึกโดย ……(เจ้าหน้าที่ความปลอดภัยระบบสารสนเทศ)

รูปที่ 5.3 แสดงตัวอย่างแบบรายงานเหตุสุดวิสัย

2. การควบคุมการเข้าถึง (Access Control)

ให้แผนกเทคโนโลยีสารสนเทศจัดทำนโยบายสำหรับการควบคุมการเข้าถึงและจัดทำเป็นเอกสารให้ชัดเจนสำหรับพนักงาน ผู้ว่าจ้าง พนักงานสมทบ คู่ค้า คู่สัญญา ผู้จัดซื้อจัดหา เพื่อควบคุมการเข้าถึงการใช้แอพพลิเคชั่น ไฟล์เซิฟเวอร์ ดาต้าเบสเซิฟเวอร์ กรุปแวร์เซิฟเวอร์ และระบบเครือข่ายสื่อสารต่าง ๆ ขององค์กรโดยให้มีลักษณะคือ

- ขั้นตอนการลงทะเบียนและการถอนการลงทะเบียนต้องเป็นลายลักษณ์อักษร
- มีการจัดการสิทธิส่วนบุคคล
- มีการจัดการรหัสผ่านผู้ใช้
- มีการตรวจสอบและตรวจตราการเข้าถึงและการใช้ระบบ
- มีการควบคุมเส้นทางการสื่อสารของเครือข่ายอย่างถูกต้อง
- มีการแบ่งแยกเครือข่ายภายใน เครือข่ายสำนักงานสาขา และเครือข่ายภายนอก
- มีการจัดการ การทำงานระยะไกลหรือเทเลเวิคกิ้ง (Teleworking)

3. การพัฒนาระบบและการบำรุงรักษา (System Development and Maintenance)

ให้หน่วยงานต่าง ๆ ในแผนกเทคโนโลยีสารสนเทศจัดการความปลอดภัยเกี่ยวกับโครงสร้างพื้นฐาน แอพพลิเคชั่นทางธุรกิจและแอพพลิเคชั่นที่พัฒนาโดยผู้ใช้ โดยมีการตรวจสอบในเรื่องของการอินพุตและเอ้าท์พุตที่ถูกต้อง รวมทั้งให้มีการควบคุมโดยการใช้เทคโนโลยีการเข้ารหัส ลายเซ็นดิจิตัล และการห้ามปฏิเสธความรับผิดชอบ โดยคำนึงถึงมาตรฐาน จำนวนของกุญแจที่เลือกใช้ การเลือกผู้ให้ใบรับรอง CA ซึ่งจะต้องให้เกิดความปลอดภัยกับข้อมูลขององค์กรมากที่สุด นอกจากนี้การปรับปรุงแอพพลิเคชั่นต่าง ๆ ต้องมีขั้นตอนการเปลี่ยนแปลง มีการทดสอบ มีการป้องกันไลบรารี่และซอร์สโค้ดของโปรแกรมอย่างเหมาะสม

5.7 การพัฒนานโยบายความปลอดภัย

จากการพิจารณานโยบายความปลอดภัยในปัจจุบันขององค์กรในบทที่ 3 นั้น แผนกเทคโนโลยีสารสนเทศยังไม่ได้มีการปรับปรุงให้ทันสมัยกับเทคโนโลยีต่าง ๆ ที่นำมาใช้ในองค์กรและให้สอดคล้องกับระบบความปลอดภัยสารสนเทศ ดังนั้นผู้ศึกษาจึงได้นำเสนอนโยบายบางส่วนที่พิจารณาจากความเสี่ยงที่อาจเกิดขึ้นและเพื่อป้องกันภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นกับองค์กร โดยนโยบายที่ควรจัดทำเพิ่มเติมได้แก่

5.7.1 นโยบายการตรวจสอบ (Auditor Policy)

วัตถุประสงค์ เพื่อให้อำนาจแก่เจ้าหน้าที่ความปลอดภัยระบบสารสนเทศ (Information Security Officer) และทีมงานตรวจสอบความปลอดภัยของระบบใด ๆ ในองค์กร ปตท. สผ.

เหตุผลการตรวจสอบ

- เพื่อให้เกิดความมั่นใจว่าระบบสารสนเทศมีบูรณภาพ ความลับและพร้อมใช้งานตลอดเวลา
- เพื่อตรวจสอบความเป็นไปได้ในการเกิดเหตุสุดวิสัยที่อาจเกิดขึ้นกับองค์กร
- เพื่อตรวจตราผู้ใช้และระบบการทำงานของเทคโนโลยีสารสนเทศ

ขอบเขต นโยบายนี้ครอบคลุมถึงอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารโทรคมนาคมของบริษัท ปตท สผ และสำนักงานสาขา

นโยบาย เมื่อมีการร้องขอการตรวจสอบตามวัตถุประสงค์ข้างต้นของเจ้าหน้าที่ความปลอดภัยสารสนเทศและทีมงานหน่วยงานต่าง ๆ ต้องมีการอนุญาตให้เข้าถึงตามคำร้องขอตามที่ต้องการ ได้แก่ การเข้าถึงเครือข่าย แอพพลิเคชั่นเซิฟเวอร์ ดาต้าเบสเซิฟเวอร์ กรุ๊ปแวร์เซิฟเวอร์ และอื่น ๆ รวมทั้งสถานที่ทำงาน เป็นต้น

บทลงโทษ พนักงานผู้ใดฝ่าฝืนให้มีความผิดและถูกลงโทษถึงขั้นไล่ออกจากงาน

5.7.2 นโยบายการส่งต่ออิเล็กทรอนิกส์เมล์ (Automatically Forwarded Email Policy)

วัตถุประสงค์ เพื่อป้องกันการเปิดเผยข้อมูลวิกฤตขององค์กร

ขอบเขต นโยบายนี้ครอบคลุมถึงการส่งเมล์ข้อมูลเกี่ยวกับ ปตท. สผ. ออกนอกองค์กร ไปให้พนักงาน บุคคลภายนอก องค์กรภายนอก พนักงานว่าจ้าง คู่ค้า คู่สัญญา องค์กรอิสระ หน่วยงานรัฐและอื่น ๆ

นโยบาย พนักงานทุกคนต้องมีความระมัดระวังในการส่งข้อมูลเมล์ใด ๆ ก็ตามจากภายในองค์กร ปตท. สผ. ไปยังโลกเครือข่ายภายนอก การส่งข้อมูลวิกฤตใด ๆ ต้องได้รับอนุญาตจากผู้บังคับบัญชาหรือสำเนาให้ทราบและได้รับอนุญาตจากผู้ส่งมาให้ และการส่งข้อมูลใด ๆ ต้องคำนึงถึงจริยธรรม ศีลธรรมและขนบธรรมเนียมต่าง ๆ

บทลงโทษ พนักงานใด ๆ ฝ่าฝืนจะมีบทลงโทษถึงขั้นไล่ออกจากงาน

นิยาม อีเมล์หมายถึงการส่งข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์โดยใช้ภาษาสื่อสาร (Protocol) ทางคอมพิวเตอร์ เช่น SMTP POP3 เป็นต้น โดยใช้ซอฟท์แวร์ต่าง ๆ เช่น Microsoft Outlook , Lotus Notes, Eudora เป็นต้น

การส่งต่อเมล์ (Forwarded Mail) หมายถึงการนำข้อความในรูปอิเล็กทรอนิกส์จากผู้หนึ่งส่งต่อไปยังอีกผู้หนึ่ง

ข้อมูลวิกฤต คือข้อมูลที่ไม่ต้องการให้เปิดเผยหรือการเปิดเผยต้องได้รับอนุญาตจากผู้บังคับบัญชา

5.7.3 นโยบายการเข้าถึงเครือข่ายโดยผ่านโทรศัพท์ (Dial in Access Policy)

วัตถุประสงค์ เพื่อป้องกันข้อมูลอิเล็กทรอนิกส์ของ ปตท. สผ. จากการเข้าถึงของบุคคลที่ได้รับอนุญาตให้เข้าถึงจากการหมุนโทรศัพท์เข้ามายังเครือข่าย (Dial in connection)

ขอบเขต นโยบายนี้กำหนดขึ้นสำหรับผู้ที่หมุนโทรศัพท์เข้ามายังเครือข่ายของ ปตท. สผ. และสำนักงานสาขา

นโยบาย พนักงานขององค์กร พนักงานผู้ว่าจ้าง คู่ค้า คู่สัญญาที่ได้รับอนุญาตให้หมุนโทรศัพท์เข้ามายังในเครือข่ายจะต้องไม่นำรหัสผ่าน หมายเลขประจำตัวผู้ใช้ให้ผู้อื่นได้รับทราบ การขออนุญาตเพื่อเข้ามายังองค์กรจะต้องได้รับอนุญาตจากผู้บัญชาตามสายงานและหัวหน้าหน่วยงานสนับสนุนแผนกเทคโนโลยีสารสนเทศ โดยผู้ใช้งานจะต้องแจ้งหมายเลขโทรศัพท์ที่ใช้หมุนเข้ามายังเครือข่ายขององค์กร

บทลงโทษ พนักงานใดละเมิด ฝ่าฝืน ให้มีความผิดและถูกลงโทษ คู่ค้า คู่สัญญา ผู้ว่าจ้างใดฝ่าฝืนถือว่ามีความผิดทางกฎหมายว่าด้วยพระราชบัญญัติอาชญากรรมทางคอมพิวเตอร์

5.7.4 นโยบายการสร้างรหัสผ่าน (Password Policy)

วัตถุประสงค์ เพื่อสร้างมาตรฐานรูปแบบในการสร้างรหัสผ่าน การป้องกัน แนะนำระยะเวลาในการเปลี่ยนรหัสผ่านของพนักงาน พนักงานว่าจ้าง ของบริษัท ปตท. สผ.

ขอบเขต นโยบายนี้ให้เป็นแนวทางปฏิบัติสำหรับผู้ใช้ระบบเทคโนโลยีสารสนเทศขององค์กร

1. นโยบายทั่วไป
    1. รหัสผ่านของ System Level เช่น root, enable,Windows2000 Admin, Application administration account, etc) ควรมีการเปลี่ยนแปลงทุก 4 เดือนหรือเมื่อพบว่าไม่ปลอดภัย
    2. รหัสผ่านผู้ใช้ (User Level password) เช่น System account, email, web, desktop computer และอื่น ๆ ควรมีการเปลี่ยนแปลงทุก 4-6 เดือน หรือเมื่อพบว่าไม่ปลอดภัย
    3. บัญชีของผู้ใช้ควรเป็นชื่อบัญชีผู้ใช้ที่เหมือนกันทุกระบบและการเปลี่ยนรหัสผ่านควรมีผลต่อทุกระบบหรือทุกแอพพลิเคชั่น เช่นเดียวกัน

4. รหัสผ่านจะต้องไม่มีการส่งผ่านทางอีเมล์หรือในรูปแบบของอิเล็กทรอนิกส์หรือจัดเก็บไว้ในรูปแบบของแฟ้มข้อมูล

2. ข้อแนะนำในการสร้างรหัสผ่าน
   1. ลักษณะรหัสผ่านที่ไม่ดี
      - เป็นรหัสผ่านที่มีอักขระน้อยกว่า 8 ตัว
      - เป็นรหัสผ่านที่ปรากฏอยู่ในศัพท์ดิกชันนารี
      - เป็นรหัสผ่านที่ใช้คำต่อไปนี้เช่น ชื่อของครอบครัว สัตว์เลี้ยง เพื่อน ชื่อบริษัท องค์กร ชื่อเมือง ถนน วันเกิด ตัวเลขเรียง หรือตัวหนังสือเรียงกัน
   2. ลักษณะรหัสผ่านที่ดี
      - ประกอบด้วยตัวอักษรใหญ่ และตัวอักษรเล็กผสมกัน
      - ประกอบไปด้วยตัวอักษร ตัวเลข สัญลักษณ์ สัญลักษณ์พิเศษต่าง ๆ ผสมกัน
      - มีความยาวเกินกว่า 8 ตัว
      - เป็นลักษณะของคำที่ตรงข้ามกับลักษณะรหัสผ่านที่ไม่ดี
3. การปกป้องรหัสผ่าน
   1. ไม่เปิดเผยรหัสผ่านแก่บุคคลใด ๆ ทั้งสิ้นไม่ว่าด้วยเหตุผลใด ๆ ก็ตามหรือวิธีการใด ๆ ก็ตาม
   2. ไม่เปิดเผยรหัสผ่านแก่ผู้บังคับบัญชา
   3. ไม่ควรกากบาทในช่องจำรหัสผ่าน (Remember Password) สำหรับแอพพลิเคชั่นใด ๆ ก็ตาม
   4. ควรมีการร้องขอให้แผนกเทคโนโลยีสารสนเทศทดสอบการตั้งรหัสผ่าน (Password Cracking)

5.7.5 นโยบายความปลอดภัยของเร้าท์เตอร์ (Router Policy)

<u>วัตถุประสงค์</u> เพื่อกำหนดความต้องการเบื้องต้นในการกำหนดค่าให้กับเร้าท์เตอร์และสวิตซ์ต่าง ๆ ที่เชื่อมต่อในองค์กรและนอกองค์กร ปตท.สผ.

<u>ขอบเขต</u> เพื่อกำหนดนโยบายการติดตั้งและตั้งค่าให้กับเร้าท์เตอร์และสวิตซ์ของ ปตท.สผ. สำนักงานใหญ่ และสำนักงานสาขา

<u>นโยบาย</u> เร้าท์เตอร์ทุกตัวจะต้องมีการกำหนดค่าพื้นฐานต่าง ๆ คือ

- มีการเข้ารหัสลับรหัสผ่าน (Encrypted password)
- มีการกำหนดเส้นทาง (Routing table) ที่ถูกต้อง

- มีการเลือกโปรโตรคอลเส้นทางที่ปลอดภัย
- มีการกรองข้อมูลหรือแพ็คเกตที่เหมาะสม (Packet Filtering)
- มีการกำหนดมาตรฐาน SNMP Community String
- ป้องกันการเข้าถึงทางกายภาพ (Console Port) ของอุปกรณ์เร้าท์เตอร์และสวิตซ์

5.7.6 นโยบายการเชื่อมต่อเครือข่ายเสมือน (Virtual Private Network) (VPN) Policy

วัตถุประสงค์ เพื่อกำหนดข้อแนะนำในการใช้ VPN ผ่าน IPSec เพื่อเชื่อมต่อมายังเครือข่ายของ ปตท.สผ. สำนักงานใหญ่

ขอบเขต นโยบายนี้ใช้บังคับแก่พนักงาน พนักงานว่าจ้าง ที่ปรึกษา พนักงานชั่วคราว คู่ค้าและคู่สัญญาที่ใช้ VPN เข้ามายังเครือข่าย ปตท. สผ .

นโยบาย พนักงาน ปตท.สผ. และผู้ได้รับอนุญาตเท่านั้นจะได้รับการเชื่อมต่อมายังเครือข่ายขององค์กร ผู้ใช้จะต้องรับผิดชอบในการเลือกซื้อชั่วโมงอินเตอร์เน็ตจากผู้ให้บริการอินเตอร์เน็ต (ISP) การติดตั้งบัญชีและซอฟท์แวร์ VPN Client ให้ติดต่อกับเจ้าหน้าที่สนับสนุนในหน่วยงานเทคโนโลยีสารสนเทศ

- เป็นความรับผิดชอบของพนักงานในการเก็บรักษาบัญชีผู้ใช้ให้เป็นความลับเพื่อใช้ในการพิสูจน์ตัวตนของพนักงาน
- VPN Gateway จะถูกจัดสร้างและดำเนินการโดยผ่านไปยังเครือข่ายของแผนกเทคโนโลยีสารสนเทศ
- เครื่องทุกเครื่องที่ใช้บริการ VPN เข้ามายังองค์กรจะต้องติดตั้งซอฟท์แวร์ต่อต้านไวรัสโดยบริษัทเป็นผู้จัดหาให้
- การใช้อุปกรณ์คอมพิวเตอร์ที่ไม่ใช่ขององค์กรเพื่อสร้างการเชื่อมต่อมายังองค์กร จะต้องมีการติดตั้งอุปกรณ์ตามที่แผนกเทคโนโลยีสารสนเทศเป็นผู้กำหนดให้

บทลงโทษ พนักงานผู้ใดฝ่าฝืนหรือละเมิดนโยบายให้มีความผิดและถูกลงโทษ

5.7.7 นโยบายการใช้เครือข่ายไร้สาย (Wireless Communication Policy)

วัตถุประสงค์ นโยบายนี้ไม่อนุญาตให้มีการใช้เครือข่ายไร้สายที่ไม่ปลอดภัยเข้ามาเชื่อมต่อเครือข่ายในองค์กรยกเว้นเครือข่ายไร้สายที่จัดหาโดยแผนกเทคโนโลยีสารสนเทศ

ขอบเขต นโยบายนี้ครอบคลุมถึงอุปกรณ์เครือข่ายไร้สาย เช่นเครื่องคอมพิวเตอร์ Access Point, PDA, Wireless Network Card, Mobile Phone และอุปกรณ์ไร้สายอื่น ๆ เพื่อเชื่อมต่อเข้ามายังเครือข่ายของ ปตท. สผ.

นโยบาย การประยุกต์ใช้อุปกรณ์ไร้สายในองค์กรต้องได้รับอนุญาต ความเห็นชอบจากแผนกเทคโนโลยีสารสนเทศโดยจะต้องมีการกำหนดเทคโนโลยีการเข้ารหัสลับข้อมูล การสามารถตรวจสอบและบันทึกหมายเลขประจำเครื่องของอุปกรณ์ (MAC Address)และ การพิสูจน์สิทธิ์ผู้ใช้ที่ดี

บทลงโทษ พนักงานผู้ใดจัดซื้อ จัดหาอุปกรณ์ไร้สายมาเชื่อมต่อเครือข่ายภายในองค์กรโดยไม่ได้รับอนุญาตถือว่ามีความผิดและถูกลงโทษถึงขั้นไล่ออกจากงาน

5.7.8 นโยบายการใช้ศูนย์คอมพิวเตอร์ (Computer Center Policy)

วัตถุประสงค์ เพื่อปกป้องศูนย์คอมพิวเตอร์และอุปกรณ์อำนวยความสะดวกต่าง ๆ ในศูนย์คอมพิวเตอร์

ขอบเขต นโยบายครอบคลุมถึงศูนย์คอมพิวเตอร์สำนักงานใหญ่และสำนักงานสาขาต่าง ๆ

นโยบาย การเข้าใช้ศูนย์คอมพิวเตอร์ต้องได้รับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ ผู้เข้าใช้จะต้องลงบันทึกไว้เป็นลายลักษณ์อักษร ไม่อนุญาตให้นำอาหารและเครื่องดื่มเข้าไปในห้องคอมพิวเตอร์ กรณีของผู้เข้ามาบริการจะต้องมีเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศดูแลและรับผิดชอบ

บทลงโทษ พนักงาน บริษัทว่าจ้าง บริษัทที่ปรึกษาใด ฝ่าฝืนหรือละเมิดให้มีความผิด

5.7.9 นโยบายการเข้าถึงขององค์กรภายนอก (Third Party Access Policy)

วัตถุประสงค์ เพื่อให้เกิดความเชื่อมั่นว่าการเข้าถึงทรัพยากรสารสนเทศของ ปตท. สผ.โดยองค์กรภายนอก ได้แก่ คู่ค้า ผู้จัดซื้อจัดหา และองค์กรต่าง ๆ เป็นไปอย่างเหมาะสมและปลอดภัย

ขอบเขต นโยบายนี้เป็นแนวทางปฏิบัติสำหรับการเข้าถึงของบุคคลภายนอกต่อเครือข่ายองค์กรทั้งสำนักงานใหญ่และสำนักงานสาขา

นโยบาย การเข้าถึงทรัพยากรระบบสารสนเทศของ ปตท.สผ. จากองค์กรภายนอกนั้นให้หัวหน้าหน่วยงานหรือแผนกนั้น ๆ ทำเรื่องร้องขอไปยังผู้จัดการอาวุโสแผนกเทคโนโลยีสารสนเทศ โดยจะต้องประเมินความเสี่ยงของข้อมูลที่อาจเกิดจากการเข้าถึงขององค์กรภายนอกจากแผนกเทคโนโลยีสารสนเทศ ให้แผนกเทคโนโลยีสารสนเทศทำสัญญาข้อตกลงกับองค์กรต่าง ๆ เหล่านั้นเกี่ยวกับความปลอดภัยของข้อมูลและการใช้ทรัพยากรต่าง ๆ ขององค์กร ต้องมีการจัดเก็บบันทึกและตรวจตราการเข้าถึงขององค์กรภายนอกอยู่เป็นประจำ

บทลงโทษ องค์กรใด ๆ ละเมิดข้อตกลงทำให้ไม่เกิดความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศของ ปตท.สผ. ให้มีความผิดตามสัญญาว่าจ้างงานและความผิดทางกฎหมาย

บทที่ 6
สรุปและข้อเสนอแนะ

6.1 ผลการศึกษาการวางแผนระบบความปลอดภัยสารสนเทศ

จากการศึกษาสภาพการณ์ปัจจุบันของ ปตท.สผ. เกี่ยวกับระบบความปลอดภัยสารสนเทศนั้น พบว่ายังขาดการกำหนดแผนแม่บทเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศ มีแต่แผนงานย่อย ฉบับร่างคือแผนการตอบสนองเหตุสุดวิสัย (IS Contingency Plan) และแผนการกู้คืนความเสียหาย (Disaster Recovery Plan) ซึ่งยังไม่ได้มีการนำมาปฏิบัติหรือประยุกต์ใช้จริง ในส่วนของนโยบายที่กำหนดขึ้นมาใช้เกี่ยวกับนโยบายสารสนเทศนั้นก็เป็นนโยบายทั่ว ๆ เกี่ยวกับการใช้เทคโนโลยีสารสนเทศทั่ว ๆ ไป ไม่ได้มุ่งเน้นในเรื่องของความปลอดภัย อีกทั้งนโยบายที่เกี่ยวกับนโยบายสารสนเทศก็ไม่ได้มีการนำมาปฏิบัติอย่างจริงจังหรือทำให้ผู้ใช้เกิดข้อตระหนักเกี่ยวกับความปลอดภัยสารสนเทศ ซึ่งเมื่อนำมาตรฐานความปลอดภัยของ ISO/IEC 17799 มาศึกษาเพื่อกำหนดในแผนแม่บทของ ปตท.สผ. แล้วผู้ศึกษาเห็นว่าเป็นมาตรฐานที่สามารถนำมาประยุกต์ใช้ได้กับองค์กรทุกมาตรา

มาตราต่าง ๆ ของ ISO/IEC 17799 :2000(E) จะกล่าวถึงเรื่องต่าง ๆ คือ (ดูภาคผนวก ข เพิ่มเติม)

1. ขอบเขตซึ่งกล่าวถึงประเด็นและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. กล่าวถึงนิยาม และความหมายต่าง ๆ ด้านความปลอดภัย
3. กล่าวถึงนโยบายความปลอดภัย (Security Policy) ซึ่งเป็นเครื่องมือที่กำหนดขึ้นมาโดยฝ่ายบริหารเพื่อใช้กับความปลอดภัยของข้อมูล
4. กล่าวถึงการจัดโครงสร้างองค์กรเทคโนโลยีสารสนเทศ (Organization Security)
5. กล่าวถึงการจัดแบ่งประเภทของทรัพย์สินและการควบคุม (Asset Classification and Control)
6. กล่าวถึงการจัดการความปลอดภัยส่วนบุคคล (Personnel Security)
7. กล่าวถึงการจัดการความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
8. กล่าวถึงการจัดการติดต่อสื่อสารและการปฏิบัติการต่าง ๆ (Communications and Operations Management)
9. กล่าวถึงการจัดการความปลอดภัยในส่วนของการควบคุมการเข้าถึง (Access Control)

10. กล่าวถึงการจัดการความปลอดภัยเมื่อมีการพัฒนาระบบและการบำรุงรักษาระบบ (System Development and Maintenance)
11. กล่าวถึงการจัดการความปลอดภัยในประเด็นของการต้องสร้างแผนการดำเนินธุรกิจให้ต่อเนื่อง (Business Continuity Management)
12. กล่าวถึงการจัดการความปลอดภัยในส่วนของสิ่งประยุกต์อื่น ๆ (Compliance) ในประเด็นเรื่องกฎหมาย ศีลธรรม และการจัดให้มีการตรวจสอบความปลอดภัยในองค์กร

โครงการวิเคราะห์ระบบงานผู้ศึกษาได้พัฒนาแผนความปลอดภัยระบบสารสนเทศองค์กรขึ้นโดยอาศัยแนวคิดของมาตรฐาน ISO/IEC 17799:2000 (E) ซึ่งเป็นมาตรฐานที่คาดว่าจะนำมาใช้กับทุกองค์กรในอนาคตเหมือนกับมาตรฐาน ISO ตัวอื่น ๆ เช่นมาตรฐานสิ่งแวดล้อม ในส่วนของนโยบายความปลอดภัยที่กำหนดขึ้นนั้นผู้ศึกษานำเสนอเฉพาะนโยบายที่ควรกำหนดขึ้นมาใช้ก่อนสำหรับองค์กรในปัจจุบัน

6.2 ประโยชน์ที่คาดว่าได้รับ

สิ่งที่คาดว่าได้รับจากการพัฒนาแผนความปลอดภัยสารสนเทศนี้คือ สามารถจัดทำแผนสารสนเทศที่สอดคล้องกับมาตรฐานสากลสำหรับให้องค์กร รวมทั้งสามารถแยกประเภทของทรัพย์สินขององค์กรได้ และสามารถวิเคราะห์ความเสี่ยงและภัยคุกคามที่คาดว่าจะเกิดกับระบบสารสนเทศขององค์กรเพื่อเป็นแนวทางให้องค์กรต่อไป นอกจากนี้องค์กรยังได้นำไปกำหนดเครื่องมือความปลอดภัยอื่น ๆ เช่น กฎ ระเบียบ ข้อเสนอแนะอื่น ๆ ขึ้นมาใช้เสริมซึ่งกันและกันเพื่อรักษาไว้ซึ่งความลับ ความมีบูรณภาพและความพร้อมใช้งาน

นอกจากนี้แผนงานนี้ยังเป็นแนวทางมาตรฐานให้องค์กรอื่น ๆ ได้ศึกษาและเป็นแนวทางในการประยุกต์ใช้สำหรับแต่ละองค์กรเพื่อที่จะขอรับมาตรฐาน ISO/IEC 17799 ที่จะนำมาใช้ในอนาคตต่อไป

6.3 ข้อเสนอแนะ

การป้องกันความปลอดภัยสารสนเทศเป็นการลงทุนที่ค่อนข้างสูงดังนั้นผู้บริหารจะต้องมองเห็นความสำคัญของการปกป้องข้อมูลและจะต้องตระหนักถึงผลกระทบต่าง ๆ ที่จะตามมากับระบบสารสนเทศขององค์กร นอกจากนี้ประเด็นความปลอดภัยเทคโนโลยีสารสนเทศเป็นประเด็นที่ได้รับความสนใจและเติบโตอย่างมาก ในปัจจุบันประเทศต่าง ๆ รวมทั้งองค์กรต่าง ๆ เริ่มตื่นตัวเกี่ยวกับความปลอดภัยของระบบสารสนเทศมากขึ้น ซึ่งการศึกษาและการจัดทำเครื่องมือความปลอดภัยต่าง ๆ เป็นเรื่องที่ต้องมีการศึกษาอย่างกว้างขวาง เพราะมีหลายหัวข้อและหลายประเด็น ซึ่งผู้ที่ต้องการศึกษาอย่างลึกซึ้งเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศควรที่จะศึกษาจากองค์ความรู้ต้นแบบหรือ Common

Body of Knowledge (CBK) ของมาตรฐานความปลอดภัยสารสนเทศของประเทศอังกฤษ BS7799 ซึ่งแบ่งองค์ความรู้เป็น 10 ขอบเขต (Domains) และนอกจากนี้มาตรฐาน ISO/IEC17799 ก็ได้รับแนวทางมาจากมาตรฐานนี้เช่นกัน

บรรณานุกรม

เรืองไกร รังสิพล. 2545. **เปิดโลก Firewall และ Internet Security**. กรุงเทพฯ: โปรวิชั่น.

Julia, H. Allen. 2002. **The CERT Guide to System and Network Security Practices**. New York: Addison-Wesley.

Desman, B. Mark. 2002. **Building an Information Security Awareness Program**. New York: Auerbach.

Peltier, R. Thomas. 2001. **Information Security Policies ,Procedures, and Standards**. New York: Auerbach.

Peltier, R. Thomas. 2001. **Information Security Risk Analysis.** New York: Auerbach.

Tipton, F. Harold, and Krause, Micki. Editors. 2000. **Information Security Management Handbook**. Fourth Edition ed. New York.

Swanson, Marianne. 1998. **"Guide for Developing Security Plans for Information Technology System"**. [online]. Available: Http://www.csrc.nist.gov.

ISO. 2000. **"ISO/IEC 17799:2000(E)".** [online]. Available: Http://www.iso.ch.

ภาคผนวก ก.

PTT Exploration and Production PCL
IT Policy

Subject	**Security, backup, ownership of files, protection of the group's intellectual property**	Reference	ITP- 02101
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Since vital information is stored on computers, loss of data can be catastrophic.

Electronically stored files containing business information have to be kept safe and remain the property of the company at all times. Given the fact that individuals can, with simple procedures, copy complex information (e.g. Exploration and Production data bases) or intellectual property (e.g. seismic interpretation Maps), there is a need that employees sign legally binding documents protecting the company from abuses.

Critical IT systems should not depend on one expert alone.

Therefore:

1. **Important data, operating and application systems shall be protected with backup routines in accordance with written instructions issued by the Information Technology Services Department's Manager. These backup routines shall follow best practices contained in the technical literature. A daily backup for data is considered the minimum.**

   Policies regarding on-site / off-site storage of the back-up media issued by the IT Manager be strictly adhered to.

   Files residing on PCs, laptops and other mobile devices which are not connected to servers shall be regularly backed up by the users in accordance with instructions issued by the IS Manager.

2. **Employees are to be made aware that electronically stored business files remain the property of the company. The employer must have access to them at all times. The files must be surrendered to the company before an employee leaves our service.**

   Employment agreements should contain paragraphs protecting the company from wrongful doings with electronically stored information and intellectual property belonging to the company.

3. **Critical IT systems must be mastered by more than one IT expert.**

PTT Exploration and Production PCL

IT Policy

Subject	**Security, asset register, documentation**	Reference	ITP- 02103
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Over the past years, computers and software became critical business tools. Often this equipment is linked via interface cards, modems, cables and software to servers and networks. Without proper documentation of the above infrastructures, control, maintenance and disaster recovery becomes difficult if not impossible.

Network architecture is a complex and know-how intensive aspect of IT.

Therefore:

1. **The Operating projects will keep an itemized register of all hardware and software bought or leased. The Accounting and Budgeting Department will decide on the degree of details to be contained in the register, taking into account time / effort and benefits. As a guide line, the register should contain the following information:**

   - **Inventory code of asset / software**
   - **Date of purchase / original lease**
   - **Duration of lease, if applicable**
   - **Type of asset (hardware / software)**
   - **Detailed technical description**
   - **Purchase / lease value**
   - **Location**
   - **Name of person responsible for asset**

   Software bought together with the hardware is also contained in the software register.

2. **The Operating Projects shall maintain a proper network documentation.**
   The IT topologies and network architectures existing within the Operating Projects are regularly exchanged and discussed among the IS manager and IT coordinators of the Operating Projects.

PTT Exploration and Production PCL
IT Policy

Subject	**Security, physical and logical access to computers, transfer of e-mail files**	Reference	ITP- 02105
Applicability	As per ITP- 03007	Page(s)	1 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Vital and/or confidential data is stored on computers. It has to be protected from being altered, read or copied by unauthorized persons.

Therefore:

1. **Common sense and prudence apply when using and storing data. It is kept under "lock and key". Confidential / sensitive data shall be accessible via secret passwords.**

2. **Physical and logical access to computers and data**

2.1. **The location of important computer rooms is carefully planned. Access to computer rooms is restricted to authorized persons.**

2.2. **Logical access to computer files shall be given via log-on names and passwords which are properly administrated. The use of Windows NT offers good protection. Where necessary and/or technically feasible, log-on registers shall be maintained.**

2.3. **All access to the Operating Projects and HO computers and computer networks from outside shall be channeled through "firewalls" with the possible exception of "remote support" which, however, has to be controlled. The Operating Projects shall charge a person with administrating the firewall. Electronic mail should, wherever possible, be stored on an in-house server and not on servers of service providers.**

3. **Security levels for transmitting data via e-mail**

3.1. **Software and methods of transmission and encryption which affect the communication among Projects and Partners are decided by HO after consultation with the Operating Projects and experts on this technical matter.**

3.2. **Routine information on daily business is e-mailed normally.**

3.3. **Confidential files are protected by passwords known to sender and recipient or with encryption methods to be defined later.**

PTT Exploration and Production PCL
IT Policy

Subject	**Security, physical and logical access to computers, transfer of e-mail files**	Reference	ITP- 02105
Applicability	As per ITP- 03007	Page(s)	2 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Remark(s)			

3.4. Classified information shall be sent via fax or courier mail. Classified information is defined as any information which contains:

a) Our intentions (e.g. plans and strategies regarding the future of individual Projects / activities, major investments).

b) Information on competitors, market participants which is not commonly known.

c) Highly condensed information which would give the reader a complete overview over the company and Projects's structure, assets and activities.

4. Please also refer to ITP- 2101 regarding the confidentiality aspect of information and intellectual property contained in electronic files.

ภาคผนวก ก.

PTT Exploration and Production PCL
IT Policy

Subject	**Security, backup, ownership of files, protection of the group's intellectual property**	Reference	ITP- 02101
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Since vital information is stored on computers, loss of data can be catastrophic.

Electronically stored files containing business information have to be kept safe and remain the property of the company at all times. Given the fact that individuals can, with simple procedures, copy complex information (e.g. Exploration and Production data bases) or intellectual property (e.g. seismic interpretation Maps), there is a need that employees sign legally binding documents protecting the company from abuses.

Critical IT systems should not depend on one expert alone.

Therefore:

1. **Important data, operating and application systems shall be protected with backup routines in accordance with written instructions issued by the Information Technology Services Department's Manager. These backup routines shall follow best practices contained in the technical literature. A daily backup for data is considered the minimum.**

   Policies regarding on-site / off-site storage of the back-up media issued by the IT Manager be strictly adhered to.

   Files residing on PCs, laptops and other mobile devices which are not connected to servers shall be regularly backed up by the users in accordance with instructions issued by the IS Manager.

2. **Employees are to be made aware that electronically stored business files remain the property of the company. The employer must have access to them at all times. The files must be surrendered to the company before an employee leaves our service.**

   Employment agreements should contain paragraphs protecting the company from wrongful doings with electronically stored information and intellectual property belonging to the company.

3. **Critical IT systems must be mastered by more than one IT expert.**

PTT Exploration and Production PCL
IT Policy

Subject	**Security, disaster management**	Reference	ITP- 02109
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

1. **All Operating Projects shall have plans in place for coping with major system failures of mission critical proportions where loss of information would threaten the integrity of the Projects' operation.**

   A manual for disaster management has to be created and updated. Simulation of system failures and testing of the adequacy of the disaster management procedures shall be done once a year.

2. **The IT Coordinators of the Projects are responsible for the implementation of this policy.**

PTT Exploration and Production PCL
IT Policy

Subject	**Compliance with copyright laws**	Reference	ITP- 02111
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st Sept 1999
Authorized by		Revision(s)	1st Sept 1999
Signed			
Remark(s)			

1. **The employees of PTTEP only use original software and comply with all aspects of the copyright laws.**

2. **Users have to be formally advised not to install unlicensed software on company owned PCs, laptops and other portable devices.**

PTT Exploration and Production PCL
IT Policy

Subject	**Language of communication on IT matters**	Reference	ITP- 02201
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

The business world is fast becoming integrated. English is the language of choice when doing business internationally. IT programming languages and technical reference manuals are mostly published in English.

The Projects must be able to share expertise.

Therefore:

1. **The language of communication on IT matters are English/Thai.**

2. **All new technical IT documentation, network architecture charts, procedure manuals issued within the Projects shall be written in English.**

PTT Exploration and Production PCL
IT Policy

Subject	**Communication, Internet, General**	Reference	ITP- 02203
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Internet and its technologies will have a tremendous impact on our Business.

Therefore:

All our executives shall keep in mind the following when making business decisions:

1 **"Disintermediation"**

The internet is positioned to facilitate the trend of "cutting out the middleman", especially in routine activities such as the on-going supply of goods to customers.

2. **Information Delivery**

Global, instantaneous delivery of customized information in the form of data, images, graphics, video and audio will become a key competitive differentiator in the 21st century.

3. **Customer - Vendor Relationships**

The internet will be a critical data collection tool where customers and vendors will e-mail their complaints about products and services. If used correctly, this will help to customize products and improve customer service.

The customer - vendor relationship will often be reversed. The customers' advertised needs on the internet will be met by vendors' offers on the internet.

PTT Exploration and Production PCL
IT Policy

Subject	**Communication, web pages, advertising on the web**	Reference	ITP- 02205
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Research (USA) shows that 10 % of small businesses advertise on the net. This figure is expected to triple within a short period of time. Two thirds of the companies maintaining web sites claim that web-advertising works.

The best Web sites are not depositories for static corporate publications. This type of information adds little value to the company.

Therefore:

1. **Efforts to publish the company news releases on the web are encouraged.**

2. **In future it will be considered if "links" among the project's different web pages should be introduced.**

3. **Publishing company's major activities on the net can make us vulnerable to legal liabilities and obligations. Standard clauses regarding disclaiming responsibility for errors or omissions are mentioned on all web pages of the projects.**

4. **The project's manager will decide on the rights of individual employee groups for web browsing.**

PTT Exploration and Production PCL
IT Policy

Subject	**Communication, e-mail, bulletin boards**	Reference	ITP- 02207
Applicability	As per ITP- 03007	Page(s)	1 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

E-mail is a cost efficient and a fast way to communicate, provided certain procedures are followed.

Confidential e-mail could easily be sent to a wrong party by mistake.

Therefore:

1. **The use of e-mail in internal and external communication shall be encouraged. A proper e-mail etiquette will be maintained. An ethical and considerate manner in compliance with applicable laws is essential.**

   The indiscriminate dissemination of e-mail copies, the careless drafting of incomplete or too hasty comments must be avoided. E-mail is no substitute for face-to-face communication.

   All users of e-mail are to be made aware that: e-mail remains stored in electronic files for indefinite periods of time and might be used for purposes other than the one envisaged by the sender. Public records may be defined to include all e-mail sent or received by a person. The reported sender may not be the real sender of the message.

2. **Copies of important e-mail messages should be sent via normal mail. Hard copies to be filed separately.**

   The Managers will decide if e-mails should carry a message which could read as follows: "The integrity of this message cannot be guaranteed on the internet. If you are not the intended recipient of this message, then please delete it and notify the sender" or "This document contains privileged information. If you are not the intended recipient of the e-mail, you may not disseminate, copy or take any action in reliance on it. If you have received this e-mail in error, please notify ..... by return e-mail.

PTT Exploration and Production PCL
IT Policy

Subject	**Communication, e-mail, bulletin boards**	Reference	ITP- 02207
Applicability	As per ITP- 03007	Page(s)	2 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Remark(s)			

3. **The company respects the rights of its staff using computers and networks for valid purposes. However, where there is abuse, or suspected abuse of the facilities and services, the company has – within the limits of applicable law – the right to inspect individual machines and servers, along with all files, messages and logs contained on those installations, and make whatever correlation is required to investigate such abuse or suspected abuse.**

1.

The authority to inspect the machines, servers and files – always within the applicable laws – will reside with the President.

4. **Company e-mail services may be used for incidental personal purposes provided that such use does not interfere with the company's computing facilities and/or interfere with the e-mail users' employment obligations. The use may not violate any applicable law including copyright violations or illegal activities.**

Suspected or known violations of law or this policy shall be confidentially reported to the appropriate supervisory level of the operational unit in which the violation occurs.

5. **The possibility to use group internal bulletin boards (for discussions, dialogues and possibly even the publication of staff letters and policies such as this IT POLICY) should be studied and eventually encouraged.**

PTT Exploration and Production PCL
IT Policy

Subject	**Electronic Data Interchange (EDI)**	Reference	ITP- 02209
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

In our businesses, EDI is making only small inroads so far.

US surveys in the banking industry show that EDI greatly reduces transaction cost, e.g. from US$ 1.40 for a traditional transaction to US$ 0.08 by using electronic bank to bank transfer.

In some countries this technology is already relevant.

Therefore:

1. **The IS department will continue to actively monitor the trend.**

   Provided that our business partners (e.g. customers) adopt this technology as well, it can help us to take a leading role in actively managing the trade relationship, resolve trade disputes, reduce overdue debtors, monitor key performance indicators, etc.

2. **If interest is shown by important business partners we shall support and implement EDI solutions.**

PTT Exploration and Production PCL
IT Policy

Subject	**IT know-how to be shared within the group**	Reference	ITP- 02211
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

There is a vast yet decentralized IT know-how available within the PTT group. This know-how is to be shared among all group companies.

Eventually we intend to have some form of competency centers in place, whose roles will be defined later on.

Therefore:

1. **Before additional hardware and software for major applications is budgeted or purchased, the IT Committee, Finance Manager, IT manager and IT coordinator responsible for the investment will consult their counterparts in the other projects.**

   Major applications are mission critical computing activities such as large-scale applications for technical database, inventory management systems, integrated commercial software packages such as SAP, JDE and ORACAL.

2. **Information and know-how on projects of a strategic nature will be shared among the IT managers, IT coordinators and IT committee.**

3. **Strategic projects are those which are intended to give the company or the projects a competitive advantage.**

4. **To facilitate the dissemination of IT knowledge, an address list of the group's IT experts shall be maintained and distributed. The enclosed address list also shows the area(s) of expertise of the IT professionals.**

5. **A periodically published, simple yet informative group IT newsletter shall be introduced. Please also refer to the comments contained in ITP- 02207 regarding bulletin boards.**

PTT Exploration and Production PCL
IT Policy

Subject	**Vendors of hardware, software and services, telephone systems**	Reference	ITP- 02303
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st August 2000
Authorized by		Revision(s)	1st August 2000
Signed	:		
Remark(s)			

Quality IT installation are the most cost effective.

Many vendors will succumb to industry consolidation.

IT, voice, video, fax, teleconferencing, modems will become more and more integrated. Appropriate cables, switches, interface cards etc. will soon be an issue.

Therefore:

1. **For important, company wide IT hardware infrastructures, software applications and other services, vendors are chosen with a good track-record able to support the hardware and software locally on a long-term basis with well documented product libraries.**

   We assess the "longevity" of vendors. For key installations the financial health of vendors is monitored. Specialized vendors with strong balance sheets are favored.

   Vendors have to provide the companies with the source codes of the application programs and regular updates of these source codes. If this is not possible, the source codes and regular updates thereof have to be deposited with and independent 3rd party.

2. **For key IT hardware infrastructures and software applications, we avoid the less known products even it they seem to be cheaper.**

   Downloading of programs from the internet can be a source of problems. The IT managers of the operating assets might want to issue policies on this subject.

3. **We request for written commitments from vendors regarding crucial aspects of their services before signing purchase orders.**

4. **The concept of "Total Cost of Ownership" to be applied when deciding on vendors and products.**

5. **When new telephone systems are evaluated, a co-operation between the person(s) in charge of the telephone system (e.g. property manager) and the IT expert(s) is required to ensure compatibility.**

PTT Exploration and Production PCL
IT Policy

Subject	**Standardization of hardware and software**	Reference	ITP- 02305
Applicability	As per ITP- 03007	Page(s)	1 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

By using standardization to streamline processes and increase productivity, our businesses can reduce costs and secure a competitive advantage. Standardization will make information systems easier to use, less expensive to operate and maintain.

Our businesses depend on the exchange of information. Our staff must remain flexible and able to fill vacancies or new positions.

Once standardization (platforms & connectivity) is achieved, the exchange of IT expertise is easier, the maintenance of the systems more economical and the group's image will be enhanced.

Therefore:

1. Future purchases of hardware and software will be as per below list:

Hardware

No standardization is planned. However, it is recommended that the projects concentrate on "open systems" with two to three reputable suppliers / brands. This will result in negotiating and purchasing power.

2. Operating Systems

2.1. Minis, Mainframes

No standardization is planned. However, it is recommended that the projects concentrate on "open systems".

2.2. PC / Networks

Microsoft Windows NT
Microsoft Windows NT Server
Microsoft Terminal Server / MetaFrame (to be considered)
Microsoft Exchange Server (preferred)
Protocol (main): TCP/IP

PTT Exploration and Production PCL
IT Policy

Subject	**Standardization of hardware and software**	Reference	ITP- 02305
Applicability	As per ITP- 03007	Page(s)	2 of 2
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Remark(s)			

3. Application Software

3.1. Minis, Mainframes

No standardization is planned. However, it is recommended that the projects concentrate on "open systems".

3.2. PC / Networks

Word Processing	**MS Word 97**
Spread Sheet Calculation	**MS Excel 97**
Presentation Software	**MS Powerpoint 97**
PC Databases	**MS Access 97**
Accounts Consolidation	**Hyperion Enterprise**
Mail Software	**MS Outlook (preferred)**
PC Programming	**Visual Basic**
Web Browser	**No standard**
Antivirus Software	**No standard but must be certified**

4. **Together with the PTT group we are participating in the "Microsoft Select D Program" since 1st Nov 1998 committing to a certain number of MS products to be purchased within two years. With this scheme, the group companies receive sizable discounts.**

PTT has been appointed to administrate the above program for the PTT group.

An itemized list of planned purchases of MS products will be drawn up periodically by PTTEP's IS department and submitted to the person in charge of administrating the program.

PTT Exploration and Production PCL
IT Policy

Subject	**Software development / implementation, general**	Reference	ITP- 02401
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective Date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

The aim of IT is to have reliable applications which improve business support services, systems integration and knowledge management.

This can only be achieved by providing quality solutions to the intermediaries between service departments or projects and IT. These intermediaries (= users) are, for instance, PTTEP's executives, technical and support staffs.

The users who represent support departments and Projects must take ownership of the IT solutions, and they must be willing to head project teams. This is the best way to prevent costly failures and delays in the introduction of computer systems.

The final decision regarding software implementation rests with the business managers.

Therefore:

1. **Hardware's and software's only purpose is to make our businesses stand out from the competition by offering more responsive customer service, faster delivery and greater reliability.**

2. **Decisions on IT investments and solutions are business driven and not only technology driven.**

3. **High quality project teams will be formed for important projects. These project teams shall consist of both, experienced users with a good understanding of the capabilities and limitations of IT and experienced system people.**

4. **IT experts shall guide the users, help them to think their requirements through, define their wishes and translate them into computer language.**

5. **Users are the "owners" of IT solutions.**

PTT Exploration and Production PCL
IT Policy

Subject	**Software development, buy vs. build**	Reference	ITP- 02403
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

Studies show that there is an intense drive to buy instead of developing software packages to handle company wide, day-to-day transactions and operations. Given that change is the norm, companies seek solutions that are flexible and nimble.

Projects that take years to install make short payback periods impossible. If it takes three years to fully implement an "own" application and our needs change after two, it is impossible to commercially justify tailor-made solutions.

Own experiences show that custom-built applications take a long time to program and are difficult to maintain.

Therefore:

1. **We seek out flexible technology and policies that can evolve rapidly. We shall always consider solutions that can swiftly adjust to business processes and exploit advancements in technology. We aim for IT solutions which can rapidly and cost effectively improve applications for the benefit of our company share holders and partners.**

   This cannot be done if our applications are so structured that a new technology or upgraded software version requires major investments in time and money.

2. **Wherever possible, "off-the-shelf application packages" shall be bought from reputable suppliers. Such packages must be of proven quality and well documented.**

3. **In order to allow for upgrading of these packages without undue delay and cost, modification is to be avoided.**

   It is the duty of the IT committee and IS manager to warn the users of the dangers and cost of modification wherever applicable.

PTT Exploration and Production PCL
IT Policy

Subject	**IT effectiveness**	Reference	ITP- 02405
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

IT is a service function. More and more users are taking advantage of computers and software.

It is important to get feed-back from the users to fine-tune the computer programs.

Therefore:

1. **The user satisfaction shall be periodically and objectively measured in a systematic way.**

   With the installation of computer networks a "help desk" function or a bulletin board managed by a team of IT professionals and experienced users could be implemented.

   The projects will decide on a structured, regular dialogue between business units and IT coordinators. This will lead to better understanding of issues and to an improved operational efficiency.

2. **The usefulness and necessity of hard copy printouts shall be periodically verified.**

3. **Managers are encouraged to use computers, e.g. by having written for them simple but meaningful and attractive log-on pages containing useful and updated information.**

PTT Exploration and Production PCL
IT Policy

Subject	**Implementation, maintenance and control of the GROUP IT POLICY**	Reference	ITP- 03001
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

The IT POLICY must remain relevant at all times. It shall be regularly reviewed and updated to allow for adjustments to the company's changing businesses needs and to new technologies.

The implementation of and the adherence of the projects and business support departments to this policy must be monitored.

Therefore:

1. The VPs are responsible for the implementation of the IT POLICY. They may delegate this responsibility but the VPs have to communicate the vision expressed in this IT POLICY to their subordinates.

2.1. Each project will have an IT coordinator who is informed on all important IT issues within the project and who coordinates IT matters with his/her counterparts in other project groups. The IT coordinator can be any IT professional of the project groups. The names of the project IT coordinators are shown on ITP- 03007.

2.2. There shall be a group IT coordinator for IT matters within the group. The group IT coordinator is shown on ITP- 03007.

3. The business support department managers, the IS manager and the IT coordinators of the projects will regularly discuss deletions, additions and amendments of the IT POLICY. Proposals will be sent to the IT coordinator and IT committee for review / approval.

4. "IT POLICY" is a permanent agenda point for IT committee meetings.

5.1. Internal and/or external auditors shall periodically verify that the group projects as per ITP- 03007 comply with the IT POLICY.

5.2. Internal and/or external specialists periodically review the adequacy of the technical aspects contained in this IT POLICY either on their own initiative or on specific instructions.

PTT Exploration and Production PCL
IT Policy

Subject	**Cost of IT services, accounting for IT**	Reference	ITP- 03003
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

The cost associated with IT is high. At present there is no uniform standard to compile and compare these expenses. Cost for IT is a major factor to remain competitive, and it must be properly monitored.

Therefore:

1. **Charts of accounts and accounting manuals must define IT cost.**

2. **IT cost must be fairly and consistently allocated to the operations to allow for a realistic assessment of the operations' performance and to permit a correct calculation of the prices for products and services.**

3. **The cost associated with IT (input) must be compared with the results produced (output) e.g. IT cost per invoice.**

4. **The allocation of IT cost shall be based on measurable, pre-determined and controllable parameters. This gives the users / operating units the possibility to reduce IT cost associated with their business.**

PTT Exploration and Production PCL
IT Policy

Subject	**Training, Employment of Staff**	Reference	ITP- 03005
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

IT is here to stay and will play an ever increasing role in business. Companies and employees who do not make good use of new technologies will not progress and, eventually, fail to remain competitive in the market place.

We want to be a "learning organization". Formal training is a part of this.

Therefore:

1. **We continue to employ staff who are willing and able to constantly learn about practical applications of IT in their day to day activities. IT training is a life long process.**

2. **We encourage staff to upgrade their skills by taking up relevant IT courses. Such courses must be in line with the staff's present or future job function. We promote knowledge transfer throughout the group's organization. Experimentation with new approaches is part of this IT training policy.**

   The initiative and motivation for learning and taking up training courses must come from the staff itself because results from "mandatory" training courses are short lived.

3. **Amounts for IT training shall be contained in the yearly budgets.**

4. **The company's IT professionals will regularly organize workshops for employees, informing them on trends in the industry, explaining terms often used and answering questions on general IT issues.**

5. **Managers need to keep abreast with the latest IT knowledge and development by being trained on IT aspects.**

PTT Exploration and Production PCL
IT Policy

Subject	**Applicability of IT policies, Projects specific IT policies**	Reference	ITP- 03007
		Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

The IT POLICY should cover as many as possible of the projects associated or managed by the Information System Dept..

Therefore:

1. **The projects shall have their own IT policies generally in line with the IT POLICY.**

2. **The projects will use the general indexing method / structure of the IT POLICY for their own IT policies.**

3. **Project IT policies shall be made available to Head Office and the other projects.**

PTT Exploration and Production PCL
IT Policy

Subject	**Table of definitions**	Reference	ITP- 03011
Applicability	As per ITP- 03007	Page(s)	1 of 1
Distribution	As per ITP- 03009	Effective date	1st July 2000
Authorized by		Revision(s)	1st July 2000
Signed			
Remark(s)			

CFO(s) Chief Financial Officer(s) reporting to the

Country(ies) The countries / markets for which the above CEOs are responsible and accountable for.

Group group of companies

IT Policy The suite of documents contained or referred to in this book and any future amendments and additions thereof.

HO Head Office

IT The application of information technology in computers and communication systems for the storage, processing and transmission of information with the objective of improving internal and external communication in the group's businesses.

IT Manager(s) Employee(s) responsible for the IT operations within the country(ies) or a company(ies) e.g.

OCR Optical Character Reading, a computer program able to read scanned text and store it in a document / text file.

OS Operating System (Software like UNIX, DOS, Windows NT, etc.)

ภาคผนวก ข.

มาตรฐานสากล ISO/IEC 17799
ว่าด้วยเทคโนโลยีสารสนเทศ – แนวปฏิบัติการบริหารความปลอดภัยสารสนเทศ

1. ขอบเขต

มาตรฐานนี้เป็นการให้คำแนะนำสำหรับการบริหารความปลอดภัยข้อมูลสารสนเทศสำหรับการจัดทำ การประยุกต์ใช้และการบำรุงรักษาระบบความปลอดภัยสารสนเทศในองค์กร โดยมีวัตถุประสงค์เพื่อเป็นแนวทางขั้นต้นในการพัฒนามาตรฐานความปลอดภัยในองค์กรและนำไปใช้ให้เกิดประสิทธิผลรวมทั้งทำให้เกิดความมั่นใจระหว่างองค์กร ข้อแนะนำในมาตรฐานนี้ต้องมีการเลือกนำไปใช้ให้สอดคล้องกับกฎหมายและกฎระเบียบต่าง ๆ

2. นิยามและความหมาย

2.1 ความปลอดภัยสารสนเทศ (Information security) ครอบคลุมถึง

2.1.1 ความลับ (Confidentiality) คือการทำให้เกิดความมั่นใจว่าสารสนเทศเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาต

2.1.2 ความมีบูรณภาพ (Integrity) คือการป้องกันเพื่อความถูกต้องและความสมบูรณ์ของสารสนเทศและขั้นตอนการประมวลผล

2.1.3 ความพร้อมใช้งาน (Availability) หมายถึงการทำให้เกิดความมั่นใจว่าผู้ที่ได้รับอนุญาตมีสิทธิ์เข้าถึงเข้ามูลและทรัพย์สินที่เกี่ยวข้องได้ตลอดเวลาที่ต้องการ

2.2 การประเมินความเสี่ยง (Risk Assessment) คือ การประเมินภัยคุกคาม ผลกระทบ จุดอ่อนของสารสนเทศและสิ่งอำนวยความสะดวกสำหรับการประมวลผลข้อมูลที่อาจเกิดขึ้นได้

2.3 การบริหารความเสี่ยง (Risk management) คือกระบวนการในการแยกแยะ การควบคุม การทำให้เหลือน้อยที่สุด หรือการกำจัดความเสี่ยงที่อาจส่งผลต่อความปลอดภัยระบบสารสนเทศและมีต้นทุนที่ยอมรับได้

3. นโยบายความปลอดภัย (Security Policy)

นโยบายความปลอดภัยสารสนเทศ มีวัตถุประสงค์เพื่อจัดหาแนวทางในการบริหารและการสนับสนุนความปลอดภัยสารสนเทศ โดยที่ฝ่ายบริหารต้องมีทิศทางนโยบายที่ชัดเจนและมีการ

สนับสนุนและมีพันธะสัญญาเกี่ยวกับความปลอดภัยสารสนเทศโดยจัดทำเป็นประเด็นและบำรุงรักษานโยบายความปลอดภัยสารสนเทศทั่วทั้งองค์กร

3.1 จัดทำเอกสารนโยบายความปลอดภัย โดยที่นโยบายมีการอนุมัติจากฝ่ายบริหารและมีการตีพิมพ์รวมทั้งแจ้งให้พนักงานทุกคนทราบ

3.2 จัดทำการทบทวนและการประเมินผล คือนโยบายต่าง ๆ ต้องมีผู้รับผิดชอบในการบำรุงรักษาและมีการทบทวนตามช่วงเวลา

4. องค์กรความปลอดภัย (Organizational security)

4.1 มีโครงสร้างพื้นฐานของความปลอดภัยสารสนเทศ เพื่อบริหารความปลอดภัยสารสนเทศในองค์กร โดยจัดให้มีการประชุมปรึกษาหารือกับหน่วยงานต่าง ๆ เพื่อกำหนด ประยุกต์ใช้สารสนเทศ การจัดสรรหน้าที่ความรับผิดชอบ การมีที่ปรึกษาด้านความปลอดภัยสารสนเทศ การกำหนดความปลอดภัยแก่บริษัทคู่ค้า ผู้รับเหมาและบริษัทที่ปรึกษาต่าง ๆ

4.1.1 มีการจัดการประชุมทางด้านการบริหารการจัดการความปลอดภัยข้อมูลโดยทีมงานผู้บริหารมีส่วนร่วมที่กำหนดหาแนวทางและวิสัยทัศน์ด้านความปลอดภัย

4.1.2 จัดความร่วมมือด้านความปลอดภัยข้อมูลโดยจัดให้มีแผนกงานหรือฝ่ายต่าง ๆ เข้ามามีส่วนร่วมประชุมหรือกำหนดบทบาทเกี่ยวกับการควบคุมความปลอดภัยสารสนเทศ

4.1.3 มีการจัดสรรอำนาจหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศ

4.1.4 มีขั้นตอนในการให้อำนาจเกี่ยวกับอุปกรณ์อำนวยความสะดวกต่างด้านสารสนเทศ เช่นการนำอุปกรณ์ใหม่ ๆ เข้ามาใช้ด้านสารสนเทศต้องได้รับการอนุมัติ อนุญาตจากบุคคลที่รับผิดชอบด้านความปลอดภัย

4.1.5 มีผู้เชี่ยวชาญด้านความปลอดภัยให้คำแนะนำเกี่ยวกับความปลอดภัยของข้อมูลสารสนเทศ

4.2 การจัดการความปลอดภัย การเข้าถึงข้อมูลของบุคคลที่สามเพื่อรักษาความปลอดภัยต่อสิ่งอำนวยความสะดวก การประมวลผลข้อมูลรวมทั้งทรัพย์สินข้อมูล ประกอบไปด้วย ขั้นตอนคือ จำแนกแยกแยะความเสี่ยงที่เกิดจากการเข้าถึงของบุคคลที่สาม ได้แก่ การเข้าถึง

4.2.1 จำแนกแยกแยะความเสี่ยงที่อาจเกิดขึ้นจากการเข้าถึงของบุคคลที่สามที่เกี่ยวข้อง ได้แก่ชนิดของการเข้าถึงทางกายภาพและลอจิคัล เหตุผลและความจำเป็นในการเข้าถึง บริษัทที่เข้ามาให้บริการ พนักงานรักษาความปลอดภัย แม่บ้าน พนักงานทำความสะอาด นักศึกษาฝึกงาน ผู้ให้คำปรึกษา

4.2.2 กำหนดสัญญาความต้องการด้านความปลอดภัยกับบริษัทร่วมค้าให้ปฏิบัติตามนโยบายความปลอดภัยต่างๆ ซึ่งสัญญาควรประกอบไปด้วย นโยบายความปลอดภัยข้อมูลทั่วๆไป การค้าครองทรัพย์สินต่าง ๆ การอธิบายลักษณะของการให้บริการแต่ละอย่าง ระดับของการได้รับบริการ การคุ้มครองทรัพย์สินทางปัญญา ข้อตกลงในการเข้าถึงข้อมูลหรือสิ่งอำนวยความสะดวกทางการประมวลผล

4.3 การทำเอ้าท์ซอสซิ่ง (Outsourcing) เพื่อรักษาความปลอดภัยข้อมูลในกรณีที่การประมวลผลข้อมูลอยู่ในความรับผิดชอบโดยองค์กรใดองค์กรหนึ่งประกอบด้วย

4.3.1 มีการกำหนดสนธิสัญญาเกี่ยวกับความต้องการด้านความปลอดภัยกับบุคคลภายนอก เช่นสิทธิในการตรวจสอบได้ ระดับการเข้าถึงทางกายภาพที่อนุญาตได้ เป็นต้น

5. การจัดการแยกชนิดของทรัพย์สินและการจัดการควบคุม (Asset classification and control) มีวัตถุประสงค์เพื่อคงไว้ซึ่งการปกป้องคุ้มครองทรัพย์สินขององค์กรอย่างเหมาะสม

5.1 มีการจัดทำบัญชีทรัพย์สิน เพื่อบำรุงรักษาป้องกันทรัพย์สินขององค์กรอย่างเหมาะสม ทรัพย์สินที่สำคัญต้องมีการจัดทำบัญชีและแต่งตั้งผู้รับผิดชอบ ประกอบด้วย

5.1.1 จัดทำทรัพย์สินคงคลัง ประกอบไปด้วยทรัพย์สินทางข้อมูล ได้แก่ฐานข้อมูล แฟ้มข้อมูล เอกสาร แผนงานต่อเนื่อง ซอฟท์แวร์ ทรัพย์สินทางกายภาพ

5.2 จัดทำการแบ่งแยกชนิดของสารสนเทศ มีวัตถุประสงค์เพื่อ ทำให้เกิดความมั่นใจว่าทรัพย์สินข้อมูลได้รับการคุ้มครองในระดับที่เหมาะสม

5.2.1 มีการจัดทำข้อแนะนำในการแบ่งแยกประเภทและการจัดเก็บ

5.2.2 มีการจัดทำประทับตราและการส่งมอบจัดเก็บ โดยกำหนดขั้นตอนกระบวนการต่าง ๆ ประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร การทำลาย

6. มีการจัดการความปลอดภัยของบุคคล (Personnel Security) เพื่อลดความเสี่ยงจากการกระทำผิดพลาดของมนุษย์ การขโมย การฉ้อโกง การใช้งานในทางที่ผิด

6.1 ความปลอดภัยในงานและทรัพยากร เพื่อลดความเสี่ยงจากการผิดพลาดของมนุษย์ การขโมย การฉ้อโกง โดยกำหนดความปลอดภัยในหน้าที่งาน มีนโยบายและการตรวจสอบพนักงานทั้งในขั้นตอนการรับสมัครรวมถึงพนักงานลูกจ้างชั่วคราว มีการทำข้อตกลงเกี่ยวกับความลับของข้อมูลกับบุคลากรในสัญญาจ้างงาน กำหนดความปลอดภัยข้อมูลเป็นเงื่อนไขและนิยามหนึ่งของความรับผิดชอบของพนักงานในการจ้างงาน

6.2 การฝึกอบรมพนักงาน เพื่อเกิดความมั่นใจว่าพนักงานตระหนักและใส่ใจในภัยคุกคามที่เกิดกับความปลอดภัยข้อมูล รวมทั้งการสร้างความสนับสนุนในนโยบายความปลอดภัยข้อมูลขององค์กร พนักงานต้องได้รับการฝึกอบรมเกี่ยวกับขั้นตอนความปลอดภัยรวมทั้งการใช้งานข้อมูลได้อย่างถูกต้องเพื่อลดความเสี่ยงให้น้อยที่สุด โดยให้การศึกษาและการฝึกอบรมเกี่ยวกับความปลอดภัยของข้อมูลแก่พนักงานทุกระดับในการใช้งานการประมวลผลข้อมูลเช่นขั้นตอนการล็อกออนการใช้ซอฟท์แวร์

6.3 มีการจัดการการตอบสนองต่อเหตุสุดวิสัยและการทำงานที่ผิดปกติ (Responding to security incidents and malfunctions) เพื่อ ลดความเสียหายของข้อมูลจากเหตุสุดวิสัยและการทำงานที่ผิดปกติรวมทั้งเพื่อการตรวจสอบและเรียนรู้จากเหตุสุดวิสัยที่เกิดขึ้น โดยจะต้องประกอบไปด้วย คือ มีการรายงานเหตุสุดวิสัยไปยังบุคคลหรือฝ่ายจัดการได้ทราบทันทีทันใด มีการจัดทำรายงานจุดอ่อนของความปลอดภัย มีการจัดทำรายงานการทำงานที่ผิดปกติของซอฟท์แวร์ จัดทำนโยบายจากประสบการณ์ที่ได้รับจากเหตุสุดวิสัย จัดสร้างกฎระเบียบลงโทษพนักงาน

7. การจัดการความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

7.1 มีการจัดการที่ปลอดภัย (Secure area) เพื่อป้องกันการเข้าถึง การแทรกแซง การทำลายข้อมูลทุกชนิดขององค์กรโดยมีการจัดแยกพื้นที่ให้ชัดเจน มีขั้นตอนคือ

7.1.1 กำหนดขอบเขตพื้นที่ทางกายภาพขึ้นมาให้ชัดเจน

7.1.2 กำหนดทางเข้าทางกายภาพที่มีการควบคุมอย่างชัดเจนเพื่อให้บุคคลที่มีสิทธิเท่านั้นที่สามารถเข้าไปยังพื้นที่ได้

7.1.3 กำหนดพื้นที่ของออฟฟิศ ห้องทำงานและห้องอำนวยความสะดวกต่าง ๆ ซึ่งต้องมีการล็อคอย่างดีเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

7.1.4 มีการจัดการการทำงานในพื้นที่ที่ปลอดภัย โดยมีการจัดการควบคุมทำข้อเสนอแนะสำหรับพนักงานและลูกจ้าง

7.1.5 มีการจัดการพื้นที่สำหรับการรับส่งพัสดุและพื้นที่ใช้บรรจุพัสดุ ซึ่งถ้าเป็นไปได้จะต้องมีการจัดการแยกจากพื้นที่ที่มีอุปกรณ์ในการประมวลผลข้อมูล มีการตรวจสอบพัสดุอุปกรณ์ก่อนนำไปใช้ มีการจัดทำการลงทะเบียน มีประตูกั้นทางภายในและภายนอก

7.2 มีการจัดการความปลอดภัยของอุปกรณ์ (Equipment Security) เพื่อป้องกันการสูญหาย การทำลายทรัพย์สินและทำให้การดำเนินธุรกิจชะงักงัน โดยมีการจัดการประเด็นต่าง ๆ คือ

7.2.1 จัดการสถานที่ตั้งของอุปกรณ์และมีการป้องกันให้ปลอดภัย เพื่อหลีกเลี่ยงความเสี่ยงจากการถูกขโมย ไฟไหม้ การระเบิด ควัน น้ำท่วม ฝุ่น แรงสั่นสะเทือน สารเคมี คลื่นไฟฟ้า คลื่นแม่เหล็ก มีการกำหนดนโยบายการรับประทานอาหาร การสูบบุหรี่ในพื้นที่ที่มีอุปกรณ์สำหรับการประมวลผลข้อมูล

7.2.2 มีการจัดการอุปกรณ์สำรองไฟฟ้า (Power supplies) อุปกรณ์ควรได้รับการป้องกันจากการขาดกระแสไฟฟ้าโดยการจัดหาไฟสำรองรวมทั้งอุปกรณ์สำรองปั่นไฟ

7.2.3 ความปลอดภัยของสายเคเบิ้ล คือสายไฟและสายสัญญาณที่ใช้เชื่อมโยงข้อมูลควรป้องการจากการถูกขัดจังหวะหรือการทำลาย

7.2.4 การบำรุงรักษาอุปกรณ์ ควรมีการตรวจสอบเป็นประจำเพื่อความพร้อมใช้งานและความมีบูรณภาพ

7.2.5 การจัดการกับอุปกรณ์ส่วนตัวของพนักงานที่นำเข้ามาใช้ควรได้รับการอนุญาต

7.2.6 มีการจัดการความปลอดภัยอุปกรณ์ที่ทิ้งทำลายหรือการนำกลับมาใช้ใหม่ เช่น อุปกรณ์สื่อบันทึกข้อมูลต่างต้องมีการทำลายมากกว่าการลบหรือการเขียนทับ

7.3 การควบคุมทั่ว ๆ ไป เพื่อป้องกันการขโมยข้อมูลและอุปกรณ์ต่างๆ ที่ใช้ในการประมวลผลข้อมูล

7.3.1 การจัดการโต๊ะทำงานให้สะอาดและมีหน้าจอคอมพิวเตอร์ที่ปลอดภัย

7.3.2 การเคลื่อนย้ายทรัพย์สิน อุปกรณ์ ข้อมูล ฮาร์ดแวร์ ซอฟท์แวร์ การเคลื่อนย้ายต้องมีการทำเป็นบันทึกและได้รับอนุญาตอย่างถูกต้อง

8. การบริหารการติดต่อสื่อสารและการปฏิบัติการ (Communications and operations management)

8.1 จัดสรรความรับผิดชอบและมีขั้นตอนปฏิบัติงาน เพื่อทำให้เกิดความถูกต้องและปลอดภัยต่อการดำเนินการกับอุปกรณ์ประมวลผลข้อมูล

8.1.1 มีเอกสารขั้นตอนการปฏิบัติงาน ที่มีคำแนะนำในด้านต่าง ๆ เช่น การจัดเก็บ การดำเนินการเกี่ยวกับข้อมูล

8.1.2 การเปลี่ยนแปลงขั้นตอนการปฏิบัติงานต้องมีเอกสารควบคุม โดยมีการจัดทำบันทึกแยกแยะสิ่งที่เปลี่ยนแปลง มีการประเมินผลถึงผลกระทบจากการเปลี่ยนแปลง มีขั้นตอนการอนุมัติเป็นทางการ จัดทำความรับผิดชอบในกรณียกเลิกหรือล้มเหลวที่อาจเกิดขึ้น

8.1.3 มีขั้นตอนปฏิบัติกรณีมีเหตุสุดวิสัยเกิดขึ้น ขั้นตอนการปฏิบัติงานและการจัดการเหตุสุดวิสัยต้องจัดทำขึ้นเพื่อให้เกิดประสิทธิภาพและความรวดเร็วอันอาจเกิดจาก ความล้มเหลวของระบบ การสูญเสียบริการ การปฏิเสธการให้บริการ ผลลัพธ์ที่ผิดพลาด

จากข้อมูลที่ไม่สมบูรณ์ มีคู่มือการปฏิบัติสำหรับแผนบรรเทาปัญหา (Contingency plan) มีการตรวจสอบและหาหลักฐานเพื่อใช้ในการวิเคราะห์ปัญหา มีการปฏิบัติการกู้คืนระบบ

8.1.4 มีการจัดแยกหน้าที่หรือกิจกรรม ซึ่งเป็นวิธีการในการลดความเสี่ยงในกรณีที่ระบบถูกนำไปใช้ในทางที่ผิด

8.1.5 จัดการแยกอุปกรณ์ที่ใช้ในการพัฒนาระบบและอุปกรณ์ที่ใช้ปฏิบัติงานจริง โดยมีการกำหนดกฎเกณฑ์อย่างชัดเจนและเป็นลายลักษณ์อักษรในการเคลื่อนย้ายซอฟท์แวร์จากระบบที่พัฒนาไปสู่ระบบปฏิบัติงานจริง

8.1.6 มีการจัดอุปกรณ์สิ่งอำนวยความสะดวกต่าง ๆ ซึ่งการจัดสิ่งอำนวยความสะดวกต่าง ๆ เช่นการใช้คู่สัญญาจากภายนอกต้องมีการพิจารณาความเสี่ยงและต้องมีการควบคุมกำหนดกฎเกณฑ์ข้อตกลงในสัญญา

8.2 การวางแผนและการยอมรับระบบ (System planning and acceptances)

8.2.1 มีวัตถุประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบให้น้อยลง การวางแผนล่วงหน้าที่ชัดเจนและการเตรียมการเป็นสิ่งจำเป็นเพื่อตอบสนองต่อความพร้อมใช้งานในทรัพยากรรวมทั้งสามารถมีข้อกำหนดการปฏิบัติงานที่เกี่ยวกับระบบใหม่ มีการจัดทำเป็นเอกสารและมีการทดสอบก่อนที่จะยอมรับและนำมาใช้งานจริง

8.2.2 ความสามารถในการวางแผน โดยผู้จัดการต้องตรวจสอบความสามารถของระบบและใช้ข้อมูลเพื่อแยกแยะและเพื่อหลีกเลี่ยงปัญหาคอขวดที่อาจเกิดขึ้น

8.2.3 การยอมรับระบบ เงื่อนไขการยอมรับระบบสารสนเทศที่จัดทำขึ้นใหม่ การอัพเกรดรวมทั้งเวอร์ชั่นใหม่ ควรจะมีการจัดทำการทดสอบที่เหมาะสมก่อนที่จะเป็นที่ยอมรับ ซึ่งเงื่อนไขยอมรับควรประกอบไปด้วย ประสิทธิภาพและความสามารถ การกู้คืนข้อผิดพลาด มีแผนบรรเทาปัญหา การจัดเตรียมและการทดสอบมีขั้นตอนการปฏิบัติเป็นประจำ มีข้อตกลงเกี่ยวกับความปลอดภัย มีคู่มือการปฏิบัติงานที่มีประสิทธิภาพ มีการจัดการฝึกอบรม มีหลักเกณฑ์การยืนยันการติดตั้งระบบใหม่ไม่ส่งผลกระทบกับระบบเก่า

8.3 มีการจัดการป้องกันต่อซอฟท์แวร์ประสงค์ร้าย (Malicious software) เพื่อปกป้องความมีบูรณภาพของซอฟท์แวร์และข้อมูล ซอฟท์แวร์ประสงค์ร้ายได้แก่ ไวรัสคอมพิวเตอร์ หนอนเครือข่าย ม้าโทรจัน และลอจิกบอมบ์

8.3.1 มีการจัดการควบคุมเพื่อต่อต้านซอฟท์แวร์ประสงค์ร้าย ควรมีคู่มือปฏิบัติงานให้ผู้ใช้งานคอมพิวเตอร์ระมัดระวังต่อซอฟท์แวร์ประสงค์ร้าย การควบคุมต้องมีประเด็นด้าน

เหล่านี้คือ มีนโยบายเกี่ยวกับซอฟท์แวร์ลิขสิทธิ์และการห้ามใช้ซอฟท์แวร์ที่ไม่ได้รับอนุญาต มีนโยบายเกี่ยวกับการป้องกันความเสี่ยงเกี่ยวกับการได้รับแฟ้มข้อมูลจากเครือข่ายภายนอกหรือจากสื่อต่าง ๆ มีการติดตั้งและอัพเดตซอฟท์แวร์ต่อต้านไวรัสเป็นประจำ มีการตรวจสอบไฟล์ที่แนบมากับเมล์ มีการจัดสรรความรับผิดชอบในการกู้คืน มีการจัดทำสำรองข้อมูลและซอฟท์แวร์ มีขั้นตอนตรวจสอบข้อมูลสารสนเทศเกี่ยวกับซอฟท์แวร์ประสงค์ร้ายและการแจ้งเตือน

8.4 มีการจัดการลักษณะงานแบบแม่บ้าน (Housekeeping) วัตถุประสงค์เพื่อรักษาไว้ซึ่งความมีบูรณภาพและความพร้อมใช้งานของการประมวลผลข้อมูลและบริการติดต่อสื่อสารเครือข่าย ได้แก่ งานที่เกี่ยวกับ

8.4.1 การทำสำรองข้อมูล (Information back-up) การสำรองข้อมูลทางธุรกิจที่สำคัญและการทำสำรองซอฟท์แวร์ควรทำเป็นปกติประจำและมีการเก็บไว้สถานที่ที่แยกจากกัน

8.4.2 การจัดการบันทึกงานปฏิบัติการ (Operator logs) พนักงานปฏิบัติการควรเก็บบันทึกกิจกรรมต่าง ๆ ที่ประกอบไปด้วย เวลาในการเริ่มสตาร์ดและเสร็จสิ้นของระบบ การทำงานผิดพลาดและการแก้ไข ผู้รับผิดชอบในการจัดทำบันทึก

8.4.3 การเก็บรายงานบันทึกความผิดพลาด (Fault logging) ความผิดพลาดที่เกิดขึ้นควรมีการจัดทำรายงานบันทึกและแก้ไขที่ถูกต้อง โดยมีการตรวจสอบความผิดพลาด รวมทั้งทบทวนเครื่องมือที่ใช้ในการแก้ไขข้อผิดพลาด

8.5 การจัดการเครือข่าย (Network management) วัตถุประสงค์เพื่อทำให้เกิดความมั่นใจถึงวิธีการป้องกันข้อมูลในเครือข่ายและการปกป้องโครงสร้างพื้นฐานต่าง ๆ

8.5.1 การควบคุมเครือข่าย ผู้จัดการเครือข่ายต้องประยุกต์ใช้เครื่องมือป้องกันข้อมูลในเครือข่ายรวมทั้งป้องกันการเชื่อมต่อจากการเข้าถึงที่ไม่ได้รับอนุญาตโดยพิจารณาจากมีการจัดความรับผิดชอบและขั้นตอนการจัดการอุปกรณ์ระยะไกล มีการควบคุมเป็นพิเศษกับข้อมูลที่เคลื่อนย้ายในเครือข่ายสาธารณะเพื่อคงไว้ซึ่งความลับ ความมีบูรณภาพของข้อมูล มีการจัดการกิจกรรมและบริการต่าง ๆ ทางธุรกิจให้สอดคล้องกับโครงสร้างพื้นฐานของการประมวลผลข้อมูล

8.6 การจัดการจัดเก็บสื่อบันทึกและความปลอดภัยของสื่อบันทึก (Media handling and security) เพื่อป้องกันทรัพย์สินเสียหายและการชะงักงันทางกิจกรรมของธุรกิจ ต้องมีการควบคุมและป้องกันทางกายภาพและมีขั้นตอนการปฏิบัติงานที่เหมาะสมเพื่อปกป้องสื่อบันทึกคอมพิวเตอร์ได้แก่ เทป ดิสก์ คาสเซ็ท ข้อมูลนำเข้าและนำออก เอกสารระบบ

8.6.1 การจัดการเกี่ยวกับการเคลื่อนย้ายสื่อบันทึกคอมพิวเตอร์ ควรมีขั้นรอนจากฝ่ายบริหาร เช่น มีการทำลาย มีการอนุญาตเป็นทางการสำหรับการเคลื่อนย้าย มีการจัดเก็บในที่ที่ปลอดภัยและมีสภาพแวดล้อมที่ปลอดภัย

8.6.2 การกำจัดสื่อบันทึก (Disposal of media) สื่อบันทึกที่ไม่ต้องการต้องมีการกำจัดอย่างปลอดภัย ควรมีขั้นตอนการปฏิบัติเพื่อลดความเสี่ยงโดยพิจารณาจากประเด็นต่อไปนี้ สื่อบันทึกได้แก่ กระดาษเอกสาร เทปบันทึก กระดาษพิมพ์เขียว กระดาษรายงาน กระดาษผงหมึก เทปแม่เหล็ก แผ่นดิสก์ คาสเซ็ท ออฟติคัลดิสก์ โปรแกรมต่าง ๆ ข้อมูลทดสอบ เอกสารระบบ เป็นต้น มีการจัดทำบันทึกเป็นลายลักษณ์อักษร

8.6.3 จัดทำขั้นตอนในการจัดเก็บข้อมูล เพื่อป้องกันการเปิดเผยข้อมูลและการใช้ในทางที่ผิด ขั้นตอนการปฏิบัติควรแยกสำหรับเอกสาร ระบบคอมพิวเตอร์ เครือข่าย โมบายเมล์ เสียง มัลติมีเดีย อุปกรณ์ไปรษณีย์ แฟกซ์ มีขั้นตอนการปฏิบัติคือ มีการจัดทำและมีสัญลักษณ์สำหรับสื่อบันทึกทุกรายการ จำกัดบุคคลและการอนุญาตการเข้าถึง จัดทำบันทึกรายการสำหรับผู้รับข้อมูล

8.6.4 การจัดการความปลอดภัยกับเอกสารของระบบ เอกสารของระบบได้แก่ข้อมูลที่มีความสำคัญ เช่นคำบรรยายการทำงานของแอพพลิเคชั่น ขั้นตอนการทำงาน โครงสร้างข้อมูล ซึ่งต้องมีการจัดเก็บอย่างปลอดภัยและอนุญาตเฉพาะผู้เป็นเจ้าของแอพพลิเคชั่น เมื่อมีการแลกเปลี่ยนในเครือข่ายสาธารณะต้องปกป้องคุ้มครองด้วย

8.7 การแลกเปลี่ยนข้อมูลและซอฟท์แวร์

เพื่อป้องกันการสูญหาย การดัดแปร การใช้ในทางที่ผิดของข้อมูลซึ่งเกิดการแลกเปลี่ยนระหว่างองค์กร

8.7.1 ทำการค้าร่วมกันต้องมีเอกสารข้อตกลงระหว่างกันในการทำการค้าผ่านอิเล็กทรอนิกส์รวมทั้งมีรายละเอียดการอนุญาตการเข้าถึงข้อมูล

8.7.2 มีการทำข้อตกลงว่าด้วยการแลกเปลี่ยนข้อมูลและซอฟท์แวร์ ข้อตกลงอย่างเป็นทางการควรจัดทำขึ้นสำหรับการแลกเปลี่ยนข้อมูลหรือซอฟท์แวร์ระหว่างองค์กร ซึ่งข้อตกลงรวมถึงการจัดส่ง ความรับผิดชอบของผู้ส่ง มีมาตรฐานฉลากติดระหว่างองค์กรในเรื่องของลิขสิทธิ์และมีการจัดทำการเข้ารหัส

8.7.3 มีการจัดการความปลอดภัยสื่อบันทึกระหว่างจัดส่ง เนื่องจากการขนส่งข้อมูลอาจเกิดการเข้าถึงโดยไม่ได้รับอนุญาต มีการขัดจังหวะในขณะส่งทางกายภาพ การจัดส่งทางกายภาพต่าง ๆ ต้องใช้การจัดส่งที่เชื่อถือได้จากผู้ให้บริการจัดส่งพัสดุ มีการบรรจุที่ดี

มีการจัดการความปลอดภัยสำหรับการค้าอิเล็กทรอนิกส์ ซึ่งเกี่ยวข้องกับการใช้ EDI เมล์ และการประมวลผลข้อมูลผ่านเครือข่ายสาธารณะเช่นอินเตอร์เน็ต ซึ่งการค้าอิเล็กทรอนิกส์มีจุดอ่อนสำหรับการถูกโจมตีในเครือข่าย การควบคุมจะต้องมีการพิสูจน์ตัวตน มีการอนุญาต มีสัญญาและข้อผูกมัด มีรายการราคาข้อมูล มีลำดับที่ของการประมวลผลข้อมูล เงื่อนไขการชำระเงิน การจัดส่ง การยืนยันการรับของ สำหรับองค์กรที่

8.7.4 มีการจัดการความปลอดภัยอิเล็กทรอนิกส์เมล์

(1) การจัดการความเสี่ยง พิจารณาจากประเด็นต่าง ๆ เช่นประเด็นจุดอ่อนของการเข้าถึง ประเด็นการดัดแปลงและการปฏิเสธการให้บริการ ประเด็นจุดอ่อนในเรื่องข้อบกพร่อง เช่น สถานที่ผู้รับ ประเด็นของผลกระทบต่อการติดต่อสื่อสารของขั้นตอนทางธุรกิจ ประเด็นด้านกฎหมาย ประเด็นด้านการตีความ ประเด็นด้านการควบคุมผู้ใช้การเข้าถึงจากระยะไกล

(2) มีการจัดทำนโยบายอิเล็กทรอนิกส์เมล์ ประกอบไปด้วย การโจมตีเมล์จากไวรัส การคุ้มครองแฟ้มข้อมูลแนบ ข้อแนะนำในกรณีห้ามใช้เมล์ การระบุความรับผิดชอบของลูกจ้างต่อการใช้เมล์ มีการเข้ารหัสข้อความ และการควบคุมด้านการพิสูจน์ตัวตน

8.7.5 การจัดการความปลอดภัยระบบสำนักงานอิเล็กทรอนิกส์ โดยมีการจัดทำนโยบายและข้อแนะนำสำหรับการลดความเสี่ยงต่อความปลอดภัยของระบบสำนักงานอิเล็กทรอนิกส์ ได้แก่เอกสาร คอมพิวเตอร์ โมบายเมล์ เสียง มัลติมีเดีย แฟกซ์และอุปกรณ์สื่อสารอื่น ๆ

8.7.6 ระบบการเผยแพร่ต่อสาธารณะ (Public available systems) ความเอาใจใส่ต่อการป้องกันบูรณภาพ ข้อมูลเผยแพร่ตีพิมพ์ในรูปอิเล็กทรอนิกส์ต้องมีการป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตซึ่งอาจนำมาซึ่งความเสื่อมเสียชื่อเสียงต่อสาธารณะขององค์กร เช่นข้อมูลในเว็บเซิฟเวอร์ที่เข้าถึงได้ทางอินเตอร์เน็ตจะต้อมีข้อมูลที่สอดคล้องกับกฎหมาย กฎเกณฑ์ ข้อบังคับ จะต้องได้รับอนุญาตอย่างเป็นทางการก่อนเผยแพร่สู่สาธารณะ ซอฟท์แวร์ ข้อมูล สารสนเทศอื่น ๆ ที่ต้องการความมีบูรณภาพอย่างสูงแต่ถูกนำไปเผยแพร่ในที่สาธารณะจะต้องได้รับการปกป้องโดยกลไกที่เหมาะสม เช่น ลายเซ็นดิจิทัล รวมทั้งข้อมูลแบบสอบถามตอบกลับจะต้องได้รับการคุ้มครองตามกฎหมาย

8.7.7 การแลกเปลี่ยนข้อมูลสารสนเทศในรูปแบบอื่น ๆ ต้องมีขั้นตอนการปฏิบัติงานและเครื่องมือควบคุมต่าง ๆ ที่จัดทำขึ้นเพื่อป้องกันการแลกเปลี่ยนข้อมูลที่ส่งผ่านด้วย

เสียง โทรสาร วีดีโอ รวมทั้งมีการกำหนดนโยบายสำหรับการปฏิบัติงานแก่ผู้ใช้งานซึ่งเกี่ยวข้องประเด็น เช่น การเตือนให้พนักงานระมัดระวังในการไม่เปิดเผยข้อมูล วิกฤต การถูกดักฟัง การแทร็บสายข้อมูล ส่งถึงผู้รับปลายทางที่ถูกต้อง การเตือนพนักงานไม่ให้เปิดเผยข้อมูลที่เป็นความลับต่อสาธารณะ การใช้โทรสารติดต่อปลายทางที่ถูกต้อง

9. การควบคุมการเข้าถึง (Access Control)

9.1 การกำหนดความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง โดยมีวัตถุประสงค์เพื่อควบคุมการเข้าถึงข้อมูล

การควบคุมการเข้าถึงข้อมูลและขั้นตอนการทำงานของธุรกิจควรได้รับการควบคุมโดยเป็นไปตามความต้องการทางธุรกิจและความปลอดภัยโดยต้องมีการกำหนดนโยบายสำหรับการอนุญาตและการเผยแพร่ข้อมูลให้รับรู้

9.1.1 นโยบายควบคุมการเข้าถึง

(1) การจัดทำนโยบายและความต้องการทางธุรกิจ คือความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึงควรกำหนดและจัดทำเป็นเอกสารให้ชัดเจน การควบคุมการเข้าถึงต้องมีกำและสิทธิ์สำหรับพนักงานหรือกลุ่มพนักงานที่ชัดเจนในนโยบาย โดยที่นโยบายควรเกี่ยวข้องกับเช่น การกำหนดความต้องการของแต่ละบุคคลสำหรับแอพพลิเคชั่น จัดแยกชนิดของข้อมูลที่เกี่ยวกับแอพพลิเคชั่นธุรกิจ ความสอดคล้องระหว่างการควบคุมการเข้าถึงกับชนิดของข้อมูลที่จัดแยก กฎหมาย ข้อบังคับที่สอดคล้อง เป็นต้น

(2) มีการจัดทำกฎในการควบคุมการเข้าถึงโดยมีกฎเกณฑ์ในการบังคับใช้

9.2 มีการจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตในระบบสารสนเทศ ขั้นตอนการปฏิบัติที่เป็นทางการต้องจัดทำขึ้นเพื่อจัดสรรสิทธิ์ในการเข้าถึงในระบบสารสนเทศและบริการสารสนเทศ โดยขั้นตอนจะต้องควบคุมตั้งแต่การลงทะเบียนของผู้ใช้ใหม่จนถึงการถอนการลงทะเบียน

9.2.1 การลงทะเบียนผู้ใช้ (User registration) ต้องมีขั้นตอนปฏิบัติที่เป็นทางการเกี่ยวกับการลงทะเบียนและการถอนการลงทะเบียนเพื่อประกาศการใช้สิทธิ์ของผู้ใช้ต่าง ๆ เช่นมีการใช้ชื่อผู้ใช้ที่เป็นรหัสประจำตัวเฉพาะ (Unique ID) ต้องมีการแบ่งระดับในการเข้าถึง ให้ผู้ใช้มีลายลักษณ์อักษรในการเข้าถึงข้อมูล จัดทำบันทึกและมีการตรวจสอบ

9.2.2 มีการจัดการสิทธิ์ส่วนบุคคล โดยต้องมีการควบคุมสำหรับการจัดสรรและการใช้สิทธิ์ส่วนบุคคลในการเขียนทับกับระบบและแอพพลิเคชั่น ฐานข้อมูล สำหรับระบบที่มีผู้ใช้หลายฝ่าย

9.2.3 การจัดการรหัสผ่านผู้ใช้ (User password management) การจัดการรหัสผ่านมีแนวคิดคือ

(1) ให้พนักงานเก็บรหัสผ่านของตนเองและของกลุ่มเป็นความลับโดยมีการระบุไว้ในสัญญาจ้างงาน

(2) ให้พนักงานเก็บรหัสผ่านของตนเองเป็นความลับ รหัสผ่านชั่วคราวที่สร้างขึ้นสำหรับผู้ใช้ที่ลืมรหัสผ่านจะต้องบังคับให้เปลี่ยนแปลง

(3) รหัสผ่านชั่วคราวที่สร้างให้ผู้ใช้ควรส่งผ่านด้วยวิธีการที่ปลอดภัยไม่ควรอยู่ในรูปข้อมูลกระจ่าง

(4) รหัสผ่านไม่ควรเก็บในคอมพิวเตอร์ที่ไม่ได้ถูกป้องกัน ควรใช้เทคโนโลยีในการระบุตัวตนและการพิสูจน์ตัวตน

9.2.4 มีการตรวจสอบการให้สิทธิ์ผู้ใช้ ควรมีการตรวจสอบเป็นช่วงระยะเวลาทุก ๆ 6 เดือน และทุก 3 เดือนสำหรับการขออนุญาตสำหรับสิทธิพิเศษ

9.3 ความรับผิดชอบผู้ใช้ (User responsibilities) เพื่อป้องกันการเข้าถึงของผู้ใช้ที่ไม่ได้รับอนุญาต ความร่วมมือของผู้ใช้ที่ได้รับอนุญาตมีความจำเป็นต่อความปลอดภัยที่มีประสิทธิภาพ

9.3.1 การใช้รหัสผ่าน (Password use) ต้องเก็บรหัสผ่านเป็นความลับ หลีกเลี่ยงการใช้กระดาษจดรหัสผ่าน เปลี่ยนรหัสผ่านเมื่อมีสิ่งชี้บอกว่าเกิดความไม่ปลอดภัย เลือกใช้รหัสผ่านที่มีคุณภาพอย่างต่ำ 6 ตัวอักษร จำได้ง่าย บุคคลอื่นเดาไม่ได้ หรือไม่เกี่ยวข้องกับชื่อ เบอร์โทรศัพท์ วันเกิดเป็นต้น ไม่เป็นตัวเลขหรือตัวหนังสือล้วน มีการเปลี่ยนรหัสผ่านเป็นช่วงและไม่ใช้รหัสผ่านที่ใช้มาแล้ว เปลี่ยนรหัสผ่านชั่วคราวเมื่อล็อกออนครั้งแรก ไม่ให้มีการแบ่งกันใช้รหัสผ่าน

9.3.2 การจัดการอุปกรณ์อื่น ๆ ของพนักงาน ผู้ใช้งานต้องมั่นใจว่าอุปกรณ์ต่าง ๆ ต้องได้รับการป้องกันเช่นเมื่อเสร็จงานให้ปิดเซสชั่น มีการล็อกออฟ ติดกุญแจเป็นต้น

9.4 การควบคุมการเข้าถึงเครือข่าย (Network access control) มีวัตถุประสงค์เพื่อป้องกันคุ้มครองบริการเครือข่าย คือการเข้าถึงบริการเครือข่ายทั้งจากภายในและภายนอกต้องมีการควบคุม เพื่อที่ว่าผู้ใช้ ผู้มีสิทธิ์ในเครือข่ายและบริการเครือข่ายทำให้เกิดความไม่ปลอดภัยกับเครือข่าย ทั้งนี้เพื่อก่อให้เกิดสิ่งต่อไปนี้

- มีการติดต่ออย่างเหมาะสมระหว่างเครือข่ายองค์กรและเครือข่ายขององค์กรอื่น ๆ หรือเครือข่ายสาธารณะ
- เพื่อกลไกการพิสูจน์ตัวตนที่เหมาะสมสำหรับผู้ใช้และอุปกรณ์
- ควบคุมผู้ใช้ในการเข้าถึงบริการข้อมูล

9.4.1 นโยบายการใช้บริการเครือข่าย โดยนโยบายจะต้องกล่าวถึงสิ่งต่อไปนี้

- เครือข่ายและบริการใดที่ให้บริการการเข้าถึง
- ขั้นตอนการปฏิบัติสำหรับการอนุญาตว่าบุคคลใดที่ได้รับอนุญาตให้เข้าถึงเครือข่ายและบริการเครือข่าย
- มีการจัดการควบคุมและขั้นตอนในการปกป้องคุ้มครองการเข้าถึงการเชื่อมต่อเครือข่ายและบริการเครือข่าย

9.4.2 มีการควบคุมเส้นทางการสื่อสารในเครือข่าย คือเส้นทางจากเครื่องผู้ใช้ไปยังเครื่องบริการต้องมีการควบคุม เครือข่ายต้องมีการออกแบบให้มีการแบ่งปันทรัพยากรและมีความยืดหยุ่นเรื่องเร้าท์ติ้ง มีการควบคุมเพื่อลดความเสี่ยง เพื่อป้องกันผู้ใช้เลือกเส้นทางภายนอกอื่น ๆ

9.4.3 มีการพิสูจน์ตัวตนสำหรับการเชื่อมต่อภายนอก เช่นการเข้าถึงจากระยะไกลควรมีการเข้ารหัสในการพิสูจน์ตัวตน

9.4.4 มีการพิสูจน์ตัวตนในโหมดต่าง ๆ

9.4.5 มีการควบคุมพอร์ตต่างๆ ที่เข้าถึงระยะไกล สำหรับเครื่องคอมพิวเตอร์และระบบโทรคมนาคม

9.4.6 มีการแบ่งแยกเครือข่ายสำหรับเครือข่ายในองค์กรและเครือข่ายภายนอกที่ใช้ติดต่อกัน

9.4.7 มีการควบคุมการเชื่อมต่อเครือข่าย มีการกำหนดค่าเกตเวย์ ทราฟฟิก เครื่องเมล์เซิฟเวอร์ การโอนถ่ายข้อมูลให้เป็นทางเดียวหรือสองทาง

9.4.8 มีการควบคุมเส้นทางเครือข่าย (Network routing control) ควรมีการกำหนดตรวจสอบต้นทางและปลายทางให้ถูกต้อง

9.4.9 มีการจัดการความปลอดภัยของบริการเครือข่ายอื่น ๆ ให้มีความปลอดภัย

9.5 การจัดการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) โดยเพื่อป้องกันการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาต

9.5.1 ต้องมีการแยกแยะตัวบุคคลอย่างอัตโนมัติที่เทอร์มินัลโดยมีการพิสูจน์ตัวตนสำหรับการเข้าถึง

9.5.2 มีขั้นตอนวิธีการล็อกออนสู่เทอร์มินัล จำนวนครั้งที่อนุญาต มีข้อความแสดงถึงความสำเร็จหรือล้มเหลว เป็นต้น

9.5.3 มีการแยกแยะผู้ใช้และการพิสูจน์ตัวตนคือผู้ใช้ทุกคนต้องมีรหัสประจำตัวที่เป็นเลขประจำตัวผู้ใช้

9.5.4 มีการจัดการรหัสผ่านที่ป้องกันความปลอดภัย เช่น ผู้ใช้สามารถเปลี่ยนได้ มีทางเลือกสำหรับการเลือกใช้ สามารถบังคับผู้ใช้เปลี่ยนรหัสผ่านได้

9.5.5 มีการจัดการเรื่องการใช้โปรแกรมอรรถประโยชน์ที่สามารถทำลายระบบปฏิบัติการได้

9.5.6 มีการจัดการระบบเตือนภัยหรือความเสี่ยงให้ผู้ใช้ได้รับรู้อันตรายที่อาจเกิดขึ้น

9.5.7 มีการกำหนดช่วงเวลาปิดตัวของระบบเมื่อไม่มีการทำกิจกรรมใด ๆ

9.5.8 มีความสามารถในการกำหนดเวลาในการเชื่อมต่อได้

9.6 มีการจัดการการควบคุมการเข้าถึงแอพพลิเคชั่น (Application access control) เพื่อป้องกันการถึงข้อมูลในระบบสารสนเทศโดยไม่ได้รับอนุญาต อุปกรณ์ความปลอดภัยต้องนำมาใช้จำกัดการเข้าถึงระบบแอพพลิเคชั่น การเข้าถึงซอฟท์แวร์และข้อมูลทางดิจิทัลต้องมีการกำหนดเพื่อผู้ใช้งานที่มีสิทธิ์เท่านั้น

9.7 การตรวจตราการเข้าถึงและการใช้ระบบ (Monitoring System access and use) เพื่อตรวจสอบกิจกรรมที่ไม่ได้รับอนุญาต ระบบควรจะมีการเฝ้าระวังตรวจตราการเข้าถึงและมีการจัดเก็บบันทึกเพื่อเป็นหลักฐานในกรณีเกิดเหตุสุดวิสัย โดยมีการบันทึกเหตุการณ์ มีการตรวจตราการใช้ระบบ มีขั้นตอนการปฏิบัติงานและขอบเขตความเสี่ยงเพื่อตรวจสอบผู้ใช้งาน มีการเข้าจังหวะสัญญานนาฬิกาเพื่อเป็นหลักฐานในการตรวจตามวันและเวลาที่เกิดเหตุการณ์

9.8 การจัดการอุปกรณ์โมบายและการทำงานจากบ้าน (Mobile computing and teleworking) เพื่อเกิดความมั่นใจในความปลอดภัยของข้อมูลเมื่อใช้โมบายและอุปกรณ์ทำงานจากบ้านระยะไกล โดยอุปกรณ์โมบายได้แก่ โน้ตบุ๊ค ปาล์ม แลปท้อปและมือถือต้องมั่นใจว่าข้อมูลทางธุรกิจไม่เสียหาย มีการสำรองข้อมูล การทำงานจากบ้านระยะไกลจะต้องมีการใช้เทคโนโลยีสื่อสารต่าง ๆ เพื่อให้พนักงานทำงานจากนอกสถานที่ที่เป็นหลักแหล่งภายนอกองค์กรและต้องมีการจัดการป้องกันที่เหมาะสม

10. การพัฒนาระบบและการบำรุงรักษา (System development and Maintenance)

10.1 มีการกำหนดความต้องการด้านความปลอดภัยในระบบที่สร้างขึ้น

วัตถุประสงค์เพื่อเกิดความมั่นใจว่าได้มีการสร้างการรักษาความปลอดภัยขึ้นในระบบสารสนเทศ ขั้นตอนนี้รวมถึงโครงสร้างพื้นฐาน แอพพลิเคชั่นทางธุรกิจ และแอพพลิเคชั่นที่สามารถพัฒนาโดยผู้ใช้ การออกแบบและการประยุกต์ใช้ต้องคำนึงถึงความปลอดภัย เงื่อนไขความปลอดภัยต้องมีการแยกแยะและเป็นข้อตกลงเบื้องต้นก่อนพัฒนาระบบขึ้นมา ข้อต้องการด้านความปลอดภัยต้องมีการจัดการ กำหนดขั้นตอนในขั้นตอนของความต้องการ

10.2 มีการกำหนดความปลอดภัยในระบบแอพพลิเคชั่น วัตถุประสงค์เพื่อป้องกันข้อมูลของผู้ใช้งานสูญหาย มีการดัดแปลงและนำไปใช้ในทางที่ผิดในระบบแอพพลิเคชั่น

10.3.1 มีการตรวจสอบการนำเข้าข้อมูล (Input data validation) การนำข้อมูลเข้าระบบแอพพลิเคชั่นต้องมีการตรวจสอบให้เกิดความมั่นใจว่าถูกต้องและเหมาะสม การตรวจสอบต้องเกิดขึ้นในขั้นตอนการนำข้อมูลเข้าในการประมวลผลและมีการตรวจสอบข้อผิดพลาดอื่นๆ เช่น ค่าตัวเลขที่เกินจากช่วงที่กำหนด

10.3.2 มีการควบคุมการประมวลผลภายใน (Internal processing) ได้แก่มีการจัดขอบเขตของความเสี่ยงที่อาจเกิดขึ้นในโปรแกรม มีการตรวจสอบและการควบคุมต่อผลกระทบที่อาจเกิดกับข้อมูล มีการพิสูจน์ตัวตนข้อความ (Message authentication) ต้องมีการจัดทำขึ้นในแอพพลิเคชั่นที่ต้องการความปลอดภัยในเรื่องของความมีบูรณภาพของเนื้อหาของข้อความ

10.3 มีการควบคุมโดยการเข้ารหัส (Cryptographic controls) เพื่อก่อให้เกิดความลับ การพิสูจน์ตัวตนและความมีบูรณภาพของข้อมูล ระบบการเข้ารหัสและเทคนิคการเข้ารหัสควรนำมาใช้เพื่อปกป้องข้อมูลที่พิจารณาแล้วว่ามีความเสี่ยงและเนื่องจากเครื่องมือปกป้องอื่น ๆ ไม่สามารถทำได้

10.3.1 นโยบายในการกำหนดใช้การเข้ารหัส ขึ้นอยู่กับการประเมินผลความเสี่ยงที่เกิดขึ้นว่ามีความเหมาะสมนำมาใช้ในองค์กรมากน้อยเพียงใด การกำหนดนโยบายพิจารณาโดยความสำคัญของข้อมูลทางธุรกิจ แนวคิดของการจัดการกุญแจเข้ารหัส บทบาทและบุคคลรับผิดชอบ ระดับในการคุ้มครองการเข้ารหัส มาตรฐานที่จะนำมาใช้ในองค์กร

10.3.2 การเข้ารหัส (Encryption) เป็นเทคนิคที่ใช้ปกป้องความลับของข้อมูลและข้อมูลวิกฤต

10.3.3 ลายเซ็นดิจิทัล (Digital signatures) เป็นการป้องกันโดยใช้วิธีพิสูจน์ตัวตนและความมีบูรณภาพของเอกสารอิเล็กทรอนิกส์ เช่นใช้ในการค้าอิเล็กทรอนิกส์ โดยมีข้อพึงระวังในการรักษากุญแจส่วนตัว

10.3.4 บริการการห้ามปฏิเสธความรับผิดชอบ (Non-repudiation services) บริการการห้ามปฏิเสธความรับผิดควรพิจารณานำมาใช้เพื่อแก้ปัญหาการโต้แย้งเกี่ยวกับเหตุการณ์ที่อาจเกิดขึ้นหรืออาจไม่เกิดขึ้นเกี่ยวกับการกระทำต่าง ๆ

10.3.5 การจัดการกุญแจ (Key management) ต้องคำนึงถึงการคุ้มครองกุญแจเข้ารหัส การจัดการกับกุญแจเข้ารหัสเป็นสิ่งสำคัญและการสูญหายหรือเปิดเผยมีผลต่อความลับ การพิสูจน์ตัวตนและความมีบูรณภาพของข้อมูล ต้องมีมาตรฐาน ขั้นตอนการปฏิบัติและวิธีการใช้กุญแจ การสร้างกุญแจ ใบรับรองกุญแจสาธารณะ การแจกจ่ายกุญแจไปยังผู้รับกุญแจ การแลกเปลี่ยนและการอัพเดตกุญแจ การทำลายกุญแจ การกู้คืนกุญแจ ต้องมีการพิจารณาเป็นอย่างดี

10.4 การจัดการความปลอดภัยระบบแฟ้มข้อมูล (Security of system files) เพื่อให้เกิดความมั่นใจว่าโครงการด้านไอทีและกิจกรรมเกี่ยวข้องต่าง ๆ มีความปลอดภัยและการเข้าถึงแฟ้มข้อมูลได้รับการควบคุมที่ถูกต้อง

10.4.1 การควบคุมซอฟท์แวร์ที่ใช้งานอยู่ (Operational software) การควบคุมต้องมีการจัดทำอย่างเหมาะสมเพื่อมีการประยุกต์ใช้ซอฟท์แวร์ในระบบปฏิบัติงานที่ใช้อยู่เพื่อลดความเสี่ยงในการขัดจังหวะของระบบที่ทำงานอยู่

10.4.2 การปกป้องข้อมูลที่ใช้ทดสอบระบบ ข้อมูลทดสอบต้องได้รับการควบคุม ต้องมีการแยกฐานข้อมูลที่ใช้งานอยู่กับข้อมูลที่ใช้ทดสอบ

10.4.3 การควบคุมการเข้าถึงไลบรารี่ของโปรแกรม (Program source library) เพื่อที่จะลดโอกาสในการขัดจังหวะของโปรแกรมคอมพิวเตอร์

10.5 การจัดการความปลอดภัยในขั้นตอนการพัฒนาและการสนับสนุนระบบ (Development and support process) เพื่อคงไว้ซึ่งความปลอดภัยในระบบแอพพลิเคชั่นและข้อมูลสารสนเทศ โดยมีขั้นตอนการปฏิบัติเกี่ยวกับการควบคุมการเปลี่ยนแปลงระบบซึ่งต้องมีขั้นตอนที่บังคับใช้อย่างเป็นทางการ การการทบทวนเชิงเทคนิคสำหรับการเปลี่ยนแปลงกับระบบที่ใช้งานอยู่ จะต้องมีการทวนสอบและการทดลองก่อนนำไปใช้กับระบบงานจริงสำหรับการลงแพ็ท การติดตั้งโค้ดใหม่ มีการจำกัดการเปลี่ยนแปลงสำหรับซอฟท์แวร์แพคเกจซึ่งเป็นซอฟท์แวร์ที่พัฒนามาจากผู้ค้าซึ่งการเปลี่ยนแปลงต้องพิจารณาในเรื่องของความเสี่ยงของการควบคุมและความมีบูรณภาพของการประมวลผล และมีการระมัดระวังเรื่องการทำงานที่ผิดปกติของโค้ดต่าง หรือโค้ดโทรจัน นอกจากนี้การจ้างเอ๊าซอสเพื่อพัฒนาโปรแกรมต้องมีข้อตกลงเกี่ยวกับสิทธิทางปัญญา ใบรับรองคุณภาพและความถูกต้อง การจัดการความล้มเหลวที่อาจเกิดขึ้น ข้อตกลงทางสัญญาเกี่ยวกับคุณภาพของโค้ด มีการทดสอบก่อนติดตั้งเพื่อตรวจดูโค้ดโทรจัน เป็นต้น

11. การจัดการธุรกิจให้ธุรกิจดำเนินงานต่อเนื่อง (Business continuity management)

11.1 คุณลักษณะของการจัดการธุรกิจให้ดำเนินงานต่อเนื่อง มีวัตถุประสงค์เพื่อตอบสนองต่อการชะงักงันของธุรกิจและป้องกันกระบวนการวิกฤตทางเศรษฐกิจอันเกิดจากผลกระทบของความล้มเหลวหรือความเสียหายของระบบสารสนเทศ ต้องมีการวิเคราะห์ผลกระทบของความเสียหาย ความล้มเหลวของความปลอดภัย และการสูญเสียการให้บริการต่าง ๆ และมีการจัดทำแผนบรรเทาปัญหา (Contingency plan) เพื่อทำให้ขั้นตอนการทำงานทางธุรกิจสามารถกู้คืนกลับมาทำงานได้ตามปกติ

11.1.1 มีขั้นตอนการจัดการดำเนินงานให้ต่อเนื่อง ควรมีขั้นตอนการจัดการในการพัฒนาและการคงไว้ซึ่งการดำเนินงานต่อเนื่องทั่วทั้งองค์กร โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้น โดยทำการแยกแยะและจัดลำดับสำคัญของหน่วยงานที่วิกฤต เข้าใจผลกระทบที่เกิดจากการทำให้ธุรกิจชะงักงัน พิจารณาซื้อประกันภัยที่เหมาะสม จัดทำกลยุทธ์และเอกสารการทำงานต่อเนื่อง ทดสอบและปรับปรุงแผนงานเป็นประจำและแผนงานต้องสอดคล้องกับขั้นตอนการทำงานและโครงสร้างองค์กร

11.1.2 การดำเนินงานต่อเนื่องของธุรกิจและการวิเคราะห์ผลกระทบ คือการดำเนินงานต่อเนื่องของธุรกิจควรจะมีการจำแนกแยกแยะเหตุการณ์ต่าง ๆ ที่อาจทำให้ขั้นตอนการทำงานของธุรกิจชะงักงัน เช่นอุปกรณ์ไม่ทำงาน ไฟไหม้ และต้องจัดการทำการประเมินความเสี่ยงเพื่อหาผลกระทบที่ทำให้เกิดการชะงักงันได้ โดยจะต้องให้ผู้เป็นเจ้าของขั้นตอนการทำงานนั้น ๆ เข้ามามีส่วนร่วมทำงาน เพื่อให้ได้ผลประเมินความเสี่ยงแล้วต้องมีการจัดทำแผนกลยุทธ์โดยฝ่ายบริหารประกาศใช้ในองค์กร

11.1.3 การเขียนแผนงานต่อเนื่องและการประยุกต์ใช้ แผนงานควรจะพัฒนาขึ้นมาเพื่อคงไว้หรือกู้คืนการทำงานของธุรกิจให้กลับคงเดิมในช่วงระยะเวลาที่ต้องการได้ โดยขั้นตอนการทำแผนพิจารณาประเด็นต่าง ๆ คือ ทำการจำแนกแยกแยะและทำข้อตกลงในส่วนของความรับผิดชอบและขั้นตอนปฏิบัติงานฉุกเฉิน และมีการจัดการประยุกต์ใช้ขั้นตอนการทำงานฉุกเฉิน มีเอกสารเกี่ยวกับข้อตกลงด้านการทำงานและขั้นตอนการปฏิบัติงาน ให้ความรู้แก่พนักงาน จัดทำการทดสอบและปรับปรุงแผนอยู่เสมอ

11.1.4 โครงแบบของแผนงานต่อเนื่อง (Business continuity planning framework) โครงแบบของแผนงานต่อเนื่องต้องพิจารณาในประเด็นในเรื่องต่าง ๆคือ แผนงานการอพยพ ขั้นตอนปฏิบัติกรณีฉุกเฉิน ขั้นตอนในการกลับคืน ขั้นตอนปฏิบัติการกลับสภาพเดิม การจัดตารางการบำรุงรักษา มีกิจกรรมให้ความรู้และการระมัดระวัง มีการจัดสรรความรับผิดชอบให้แก่บุคคล

11.1.5 การทดสอบ การบำรุงรักษาและการประเมินใหม่สำหรับแผนการดำเนินงานให้ต่อเนื่อง

(1) การทดสอบแผน การทดสอบอาจล้มเหลวได้เนื่องจากกำหนดสมมุติฐานของเหตุการณ์ผิดพลาดหรือเกิดจากการมองข้ามเหตุการณ์ไป การเปลี่ยนอุปกรณ์หรือบุคลากร จึงต้องมีการทดสอบเป็นประจำเพื่อเกิดความมั่นใจในประสิทธิผล การทดสอบควรทำเป็นหลาย ๆ เหตุการณ์ การทำเป็นทางเลือกต่าง การทดสอบการกู้คืน การทำสอบการจัดหาอุปกรณ์ของซัพพลายเออร์

(2) การบำรุงรักษาและการประเมินแผนงานใหม่ คือแผนงานต้องทบทวนอย่างต่อเนื่องและปรับปรุงอย่างต่อเนื่อง เช่นบุคคลรับผิดชอบ ที่อยู่ที่ติดต่อได้ กลยุทธ์ทางธุรกิจ ผู้จัดหาอุปกรณ์ ความเสี่ยงที่อาจเกิดขึ้น

12. ข้อบังคับอื่น ๆ (Compliance) มีวัตถุประสงค์เพื่อหลีกเลี่ยงอาชญากรรม กฎหมายแพ่งและพาณิชย์ กฎเกณฑ์ และข้อสัญญาต่าง ๆ มีลักษณะคือ

12.1 มีการกำหนดนิยามพระราชบัญญัติต่างและมีการจัดทำเป็นเอกสารสำหรับระบบสารสนเทศในแต่ละระบบและกำหนดบุคคลที่รับผิดชอบดูแล ข้อคำนึงด้านลิขสิทธิ์ทางปัญญา ได้แก่ copyright ,software copyright การป้องกันเอกสารบันทึกต่าง ๆ ที่สมควรต้องป้องกัน การปกป้องข้อมูลและข้อมูลส่วนบุคคล การป้องกันการใช้อุปกรณ์ต่างทางสารสนเทศในทางที่ผิด มีกฎเกณฑ์การควบคุมการการเข้ารหัส มีการจัดการการรวบรวมหลักฐานในกรณีมีการละเมิดหรือทำผิดต่าง ๆ

12.2 มีการทบทวนนโยบายความปลอดภัยและสิ่งประยุกต์ทางเทคนิคอื่น ๆ เพื่อทำให้เกิดความเหมาะสมของนโยบายความปลอดภัยขององค์กรและตรงตามมาตรฐาน

12.3 4.12.3 มีการทวนสอบระบบ (System audit consideration) เพื่อก่อให้เกิดประสิทธิภาพสูงสุดและป้องกันการแทรกแซงให้น้อยที่สุด โดยมีกระบวนการทวนสอบหรือเจาะระบบ

ประวัติผู้เขียน

ชื่อผู้เขียน	นายญาณพัฒน์ ช้างโต
วันเดือนปีเกิด	19 มกราคม พ.ศ. 2512
วุฒิการศึกษา	ปริญญาตรี มหาวิทยาลัยศิลปากร
	ปริญญาตรี มหาวิทยาลัยรามคำแหง
	ปริญญาโท มหาวิทยาลัยธรรมศาสตร์
ตำแหน่งงาน	Officer, Network Control
สถานที่ทำงาน	บริษัท ปตท สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน)