คู่มือการรักษาความมั่นคงปลอดภัยICT

กระทรวงเทคโนโลยีสารสนเทศ
และการสื่อสาร

8 กุมภาพันธ์ 2550

สารบัญ

บทนำ

1. ความเป็นมา

คู่มือการรักษาความมั่นคงปลอดภัยฯ (พ.ศ. 2549 – 2551) ของ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นเอกสารที่จัดทำขึ้นเพื่อประกอบโครงการจัดทำแผนแม่บทการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งได้กำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของประเทศ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว ร่างแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติฯ จะช่วยจัดตั้งรูปแบบและลำดับความสำคัญในบริบทของ ความมั่นคงปลอดภัยด้านไอซีทีเมื่อคำนึงถึงสถานการณ์ปัจจุบันและการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องทั้งหลาย ทั้งที่จะเกิดต่อภาคประชาชน ภาคเอกชนและภาครัฐบาล หลังจากที่ประกาศใช้แผนแม่บท แล้วต้องการที่จะจัดให้มีกรอบการทำงานและเครื่องมือที่จำเป็นอย่างพอเพียง เพื่อที่จะสนับสนุนกิจกรรมต่างๆ ที่จะเกิดขึ้นของแผนฏิบัติการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับองค์กร ต่อไป

2. วัตถุประสงค์

1) เพื่อเป็นแนวทางในการจัดสร้างนโยบาย จุดประสงค์ กระบวนการ และขั้นตอนสำหรับ ISMS ซึ่งมีความสำคัญเป็นอย่างยิ่งในการจัดการแก้ไขปัญหาความเสี่ยงที่อาจเกิดขึ้น และยังมีความสำคัญต่อการพัฒนาศักยภาพของระบบรักษาความปลอดภัยของข้อมูล ส่งผลให้ตรงต่อนโยบายและจุดประสงค์หลักด้านเทคโนโลยีสารสนเทศขององค์กร
2) เพื่อเป็นแนวทางในการจัดสร้างและการปฏิบัติการระบบ ISMS ซึ่งจะเป็นการวางนโยบาย การควบคุม กำหนดขั้นตอนและกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล โดยสามารถริเริ่มได้จากการสร้างความมั่นคงปลอดภัยให้กับองค์กรในระดับพื้นฐาน ระดับกลางและระดับสูงตามลำดับ

3. นิยามและคำจำกัดความที่สำคัญ

การรักษาความมั่นคงปลอดภัยด้านไอซีที ประกอบด้วยการรักษาคุณค่าพื้นฐาน สามประการ ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมใช้งาน (Availability) ซึ่งมีคำจำกัดความที่สำคัญดังนี้

“เทคโนโลยีสารสนเทศ (IT)” หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

“ความลับ (Confidentiality)” คือ การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

“บูรณภาพ (Integrity)” คือการรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

“ความพร้อมใช้งาน (Availability)” คือการรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“การพิสูจน์ฝ่าย (Authentication)” คือการตรวจสอบและการพิสูจน์สิทธิของการขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิ สำหรับอุปกรณ์ไอที รวมถึงแอพพลิเคชันทั้งหลาย

“การพิสูจน์สิทธิ์ (Authorization)” หมายถึงการตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพพลิเคชัน นั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

“การเก็บสำรองข้อมูล (Data backup)” หมายถึง ในระหว่างการเก็บสำรอง สำเนาของชุดข้อมูลปัจจุบันจะถูกสร้างขึ้นมา เพื่อป้องกันการสูญหาย

“การปกป้องข้อมูล (Data protection)” หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

“การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)” หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้

“การประเมินความเสี่ยง หรือการวิเคราะห์ความเสี่ยง (Risk assessment or analysis)” ของระบบสารสนเทศ หมายถึง การตรวจสอบโอกาสของผลลัพธ์ใดๆ ที่ไม่พึงประสงค์ ต่อระบบฯ และผลเสียที่อาจจะเกิดขึ้นตามมาได้

“นโยบายด้านความมั่นคงปลอดภัย (Security policy)” หมายถึงนโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการขององค์กร รายละเอียดของวิธีการด้านความมั่นคงปลอดภัยมักจะอธิบายแยกไว้ในรายงานต่างหาก

การบริหารจัดการ/แผนปฏิบัติการด้านความมั่นคง

ในส่วนต่อไปนี้จะเป็นการนำเสนอข้อมูลทั่วไปเกี่ยวกับ วิธีการบริหารจัดการ การประยุกต์ใช้ และ การจัดทำเอกสาร ด้านความมั่นคงปลอดภัยระบบสารสนเทศ

1. บทบาทและหน้าที่สำคัญ

จะต้องมีการกำหนดบทบาทและหน้าที่ขององค์กร และเจ้าหน้าที่ประจำภายในแต่ละองค์กร ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านไอซีที อย่างเป็นทางการและเป็นลายลักษณ์อักษร เช่น

1) หน่วยงานกำกับดูแลด้านนโยบายความมั่นคงฯ ระดับชาติ
2) องค์กรอื่นๆ ที่เกี่ยวข้องในระดับกระทรวง ทบวง กรม เช่น ในกลุ่มงานที่เกี่ยวกับโครงสร้างพื้นฐานวิกฤต ได้แก่ กลุ่มไฟฟ้าและพลังงาน กลุ่มการเงิน ธนาคารและการประกันภัย กลุ่มการสื่อสาร โทรคมนาคมและขนส่ง กลุ่มความสงบสุขของสังคม เป็นต้น
3) ที่ปรึกษา หรือผู้เชี่ยวชาญด้านความมั่นคงฯ ขององค์กร
4) หัวหน้าเจ้าหน้าที่ด้านความมั่นคงระดับหน่วยงาน/องค์กร
5) หัวหน้างานการรักษาความมั่นคงฯ ขององค์กร
6) ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยฯ ทั้งหลายในองค์กร

2. เอกสารที่เกี่ยวข้อง

เพื่อใช้ในการบริหารจัดการ การสร้างและปรับปรุงเอกสารอย่างเป็นระบบ ให้ทันสมัยและกำหนดผู้ที่มีหน้าที่รับผิดชอบอย่างเป็นทางการ เอกสารสำคัญที่ต้องเตรียมการจะรวมถึง

1) กรอบความต้องการของเอกสารความมั่นคงฯ ไอซีที ของหน่วยงาน
2) กระบวนการผลิตเอกสาร/คู่มือ
3) ข้อกำหนดบัญชีเอกสาร/คู่มือด้านความมั่นคง

รายการเอกสารที่จำเป็น

หน่วยงานต้องจัดทำ แผน นโยบายและการประเมินความเสี่ยงด้านความมั่นคงฯ ซึ่งครอบคลุมภารกิจด้านระบบไอซีที เอกสารเหล่านี้จะต้องสอดคล้องกับเอกสารประกอบภารกิจหลักด้านความมั่นคงปลอดภัยฯ ขององค์กร ได้แก่

- นโยบายด้านความมั่นคงปลอดภัยระดับองค์กร

- การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยฯ ระดับองค์กร
- แผนด้านความมั่นคงปลอดภัย ระดับองค์กร

กระบวนการผลิตเอกสาร

ในระหว่างปฏิบัติงานอาจจำเป็นต้องสร้างเอกสารเพิ่มเติม ซึ่งจะรวมถึงเอกสาร ต่อไปนี้

- เอกสารประกอบการติดตั้งและตรวจรับระบบใหม่
- การเก็บรวบรวมเอกสารเป็นหมวดหมู่ภายใต้หัวข้อเดียว
- เอกสารแสดงปัญหา ข้อขัดข้องในระหว่างการใช้นโยบาย
- การพัฒนานโยบายใหม่ สำหรับเทคโนโลยีหรือการดำเนินงานที่เกิดขึ้นมาภายหลัง
- การพัฒนาคู่มือการปฏิบัติงานใหม่ เมื่อต้องการปรับฐานความรู้และฝึกอบรมเจ้าหน้าที่ตามความจำเป็น

ทั้งนี้ควรควบคุมเอกสาร โดยกำหนดผู้ลงนามเอกสารหลักเกี่ยวกับ ICT security และเอกสารที่เป็นนโยบายระดับสูง เป็นผู้บริหารสูงสุด หรือระดับหัวหน้าหน่วย ส่วนเอกสารที่เป็นงานระบบให้สามารถอนุมัติให้ใช้ได้โดยผู้ผลิตเอกสารเอง และ/หรือผู้บริหารระดับสูง

ข้อกำหนดบัญชีชั้นความลับของเอกสาร

เอกสารเกี่ยวกับการรักษาความมั่นคงปลอดภัยของหน่วยงานมักจะประกอบด้วยข้อมูลที่อาจก่อให้เกิดความเสี่ยงต่อการทำงาน ถ้ารั่วไหลออกไป หรือมีการลักลอบเข้ามาดู องค์กรจึงต้องออกระเบียบข้อกำหนดบัญชีเอกสารเหล่านี้

ในการกำหนดบัญชีเอกสารของระบบทั่วไป มักจะยึดถือแบบฉบับเดียวกับการจัดระดับของตัวระบบนั่นเอง ในการวิเคราะห์ความเสี่ยงของระบบโดยละเอียดอาจจะชี้ให้ชัดลงไปได้ว่า การจัดชั้นความลับของเอกสารนั้นๆ สูงกว่าหรือต่ำกว่าชั้นของระบบเช่น ข้อมูลการจัดรูปแบบของเซิร์ฟเวอร์สำหรับ Web server hosting ของหน่วยงานเพื่อเป็น Public website อาจจะต้องระบุชั้นว่า เป็น ลับเฉพาะ (“Security-In-Confident”) หรือ ผังการวางสายเคเบิ้ลสำหรับระบบสารสนเทศ “ลับมาก” (Secret) อาจระบุได้ว่าเป็น “ลับ” (Restrict) เป็นต้น

ตัวอย่างการจัดชั้นความลับเอกสาร เมื่อเทียบกับระบบงาน ได้แก่

การจัดชั้นของระบบงาน	**การจัดชั้นของเอกสาร**
สาธารณะ, เปิดเผย	เปิดเผย (Unclassified)
ปกปิด	ลับเฉพาะ
ลับ	ลับเฉพาะ, ลับ

3. การพัฒนาและกำหนดนโยบายด้านความมั่นคงฯ (ICT Security Policy)

เป็นการอธิบายนโยบายของ ICT Security รวมถึงมาตรฐานและความรับผิดชอบของหน่วยงานในส่วนที่เกี่ยวข้อง และเป็นการกำหนดความต้องการพื้นฐาน หรือความต้องการขั้นต่ำ และจะนำไปพัฒนาแผนบริหารความเสี่ยงของหน่วยงานต่อไป

กรอบการทำงานจะรวมถึง

1) กระบวนการตรวจสอบภายใน
2) หน้าที่ความรับผิดชอบขององค์กร
3) การควบคุมการกำหนดพารามิเตอร์
4) การควบคุมการเข้าถึงระบบฯ
5) การต่อเชื่อมและต่อเป็นเครือข่ายกับระบบอื่นๆ
6) การรักษาความมั่นคงฯ ทางกายภาพและการควบคุมสื่อหรือตัวกลางที่ใช้เก็บข้อมูล
7) ขั้นตอนฉุกเฉินและการจัดการเหตุการณ์
8) การบริหารความเปลี่ยนแปลง และการศึกษาอบรม

4. การบริหารความเสี่ยง

เป็นการแสดงคำอธิบายเกี่ยวกับการพัฒนาและการใช้แผนบริหารจัดการความเสี่ยง เพื่อที่จะจัดการความเสี่ยงที่มีผลต่อระบบไอซีที ในสิ่งแวดล้อมที่เป็นอยู่ ตามที่ได้กำหนดไว้ตามความต้องการของนโยบายความมั่นคงปลอดภัยด้านไอซีที โดยกำหนดขั้นตอนดังนี้

- ขั้นที่ 1 กำหนดสภาวะแวดล้อม (Stage 1: Establishing the Context)
- ขั้นที่ 2 บ่งชี้ปัจจัยความเสี่ยง (Stage 2: Identifying the Risks)
- ขั้นที่ 3 วิเคราะห์ความเสี่ยง (Stage 3: Analysing the Risks)
- ขั้นที่ 4 ระบุและจัดลำดับความเสี่ยง (Stage 4: Assessing and Prioritising Risks)
- ขั้นที่ 5 พัฒนาแผนรับมือ (Stage 5: Developing a Risk Treatment Plan)

ขั้นที่ 1 กำหนดสภาวะแวดล้อม

หน่วยงานควรจะดำเนินขั้นตอนดังต่อไปนี้

ลำดับ	สภาวะแวดล้อม	ประเด็นสำคัญ
1	การบริหารจัดการความเสี่ยง	ใครเป็นผู้ดำเนินงาน, เป้าหมายของกระบวนการเหล่านี้คืออะไร และ กรอบของกระบวนการบริหารจัดการคืออะไร
2	กลยุทธ์	อะไรคือจุดแข็งและจุดอ่อน, อะไรมีลำดับความสำคัญ, ใครคือผู้มีส่วนได้-เสีย, อะไรคือภัยคุกคามและโอกาส, และอะไรคือแรงผลักดันจากภายนอก
3	การจัดองค์การ	อะไรคือวัตถุประสงค์ที่ระบบไอซีทีถูกนำมาใช้งาน, อะไรเป็นแรงขับจากภายใน, อะไรเป็นปัจจัยแห่งความสำเร็จของระบบไอซีที, มีความเสี่ยงร่วมกับหน่วยงานอื่นๆ หรือไม่, มีทรัพยากรอะไรบ้างที่สามารถนำมาใช้ได้ และ ระบบไอซีทีสามารถช่วยให้เป้าหมายหลักและความสำคัญขององค์กรบรรลุผลได้อย่างไร
4	วิธีประเมินผล	เงื่อนไขตามกฎหมาย, มีอุปสรรคอะไรบ้างในด้าน งบประมาณ ทรัพยากรบุคคล และ/หรือการปฏิบัติงาน, อะไรคือ ”costs-benefits” ของกิจกรรม และระดับความเสี่ยงที่ยอมรับได้อยู่ที่ไหน
5	โครงสร้าง	มีทรัพย์สินที่เกี่ยวข้องอะไรบ้าง, ทรัพย์สินเหล่านี้ถูกใช้ไปอย่างไร, และ อะไรคือห้วงเวลา/เฟส หรือ องค์ประกอบทางโครงสร้างของกิจกรรมใดๆ

ขั้นที่ 2 บ่งชี้ปัจจัยความเสี่ยง

หลังจากดำเนินการในขั้นที่ 1 เรียบร้อยแล้ว จะต้องบ่งชี้ปัจจัยความเสี่ยง ซึ่งครอบคลุมความเสี่ยงให้มากที่สุดเท่าที่จะทำได้ มีประเด็นที่ต้องทำในแต่ละกรณี ได้แก่ เป็นความเสี่ยงของอะไร เกิดขึ้นได้อย่างไร และผลต่อเนื่องของความเสี่ยงที่จะเกิดขึ้น ขั้นตอนต่อไปจึงเป็นวิเคราะห์ความเสี่ยงเหล่านี้

ขั้นที่ 3 วิเคราะห์ความเสี่ยง

จุดประสงค์ของการวิเคราะห์ฯ คือเพื่อแยกความเสี่ยงที่ยอมรับได้ ออกมาจากความเสี่ยงที่ยอมรับไม่ได้ และจัดให้มีข้อมูลที่เพียงพอสำหรับการประเมินและจัดการกับความเสี่ยงเหล่านั้น

จากนั้นจึงทำรายการความเสี่ยงที่ระบุไว้ แยกเป็นแต่ละกรณี โดยมีรายละเอียดตามขั้นตอน ต่อไปนี้

ลำดับ	กิจกรรม
1	ระบุผลต่อเนื่องของความเสี่ยงนี้
2	ระบุสาเหตุของความเสี่ยงและบันทึกแหล่งข้อมูลหรือโลจิกของการค้นหาแหล่งที่มานั้นๆ
3	ระบุระดับความเสี่ยงในภาพรวม โดยใช้ตารางสัมพันธ์ (Matrix)

ตัวอย่างผลต่อเนื่องของความเสี่ยงและการจัดกลุ่ม แสดงในตาราง เช่น

ผลกระทบของความเสี่ยง ในประเด็นต่างๆ	การจัดระดับที่เหมาะสม
บาดเจ็บสาหัส หรือเสียชีวิต, สูญเสียทรัพย์ขั้นวิกฤต, การทำงานหลักของหน่วยงานหรือการให้บริการต้องชงักหรือล่าช้าไปเกินกว่าหนึ่งวัน, รัฐต้องปิดทำการหรือจะต้องปรับโครงสร้างของหน่วยงานใหม่อย่างที่เป็นสาระสำคัญ	ร้ายแรง
บาดเจ็บสาหัสต้องนำส่งโรงพยาบาล, ต้องสูญเสียทรัพย์สินมีค่าสูงมาก, การทำงานหลักของหน่วยงานหรือการให้บริการต้องชงักหรือล่าช้าไปไม่เกินกว่าหนึ่งวัน, การทำงานในระดับกระทรวงต้องหยุดชงักลงหรือต้องรายงานเจ้ากระทรวง	สำคัญ (Major)
บาดเจ็บ ต้องนำส่งโรงพยาบาล แต่กลับบ้านได้, ต้องสูญเสียทรัพย์สินมีค่าสูง, การทำงานหลักของหน่วยงานหรือการให้บริการต้องชงักหรือล่าช้าไปไม่เกินหนึ่งชั่วโมง, ต้องมีการจัดการโดยผู้บริหารระดับสูง	ปานกลาง (moderate)

ผลกระทบของความเสี่ยง ในประเด็นต่างๆ	การจัดระดับที่เหมาะสม
บาดเจ็บ ต้องปฐมพยาบาลในสถานที่เกิดเหตุ, ต้องสูญเสียทรัพย์สินมีค่าปานกลาง, การทำงานหลักของหน่วยงานหรือการให้บริการต้องชงักหรือล่าช้าไปไม่เกินครึ่งชั่วโมง, ต้องมีการทบทวนนโยบายและกระบวนการปัจุบันเพื่อลดปัญหานี้	เล็กน้อย (minor)
ไม่ได้รับบาดเจ็บ, สูญเสียทรัพย์สินจำนวนน้อย, ไม่มีผลต่อการดำเนินงาน, สามารถจัดการได้โดยกระบวนการและนโยบายที่มีอยู่แล้ว	ไม่มีผลกระทบ

การหาสาเหตุที่มาของความเสี่ยงอาจสร้างเป็นประเด็นในตารางตัวอย่างต่อไปนี้

ความเสี่ยง ถ้าเกิด	อัตราของความน่าจะเป็น
คาดว่าจะเกิดได้ในทุกกรณี	ค่อนข้างแน่นอน
น่าจะเกิดได้ในทุกกรณี	น่าจะเป็น
อาจจะเกิดได้บางครั้ง และอาจยากที่จะควบคุมเนื่องจากมีอิทธิพลจากปัจจัยภายนอก	เป็นไปได้
เกิดได้บางครั้ง	ไม่น่าจะเป็น
อาจเกิดได้ในบางกรณีเฉพาะ	ยาก

การกำหนดกลุ่มและคำอธิบายความเสี่ยงเพื่อสร้างตารางใช้วิเคราะห์ ดังตัวอย่างต่อไปนี้

ระดับ	ความหมาย	คำอธิบาย
E	Extreme	ต้องการค้นคว้าอย่างละเอียดเพิ่มเติมและการวางแผนการบริหารจัดการจากผู้บริหารระดับสูง
H	High	ต้องการให้ผู้บริหารระดับสูงรับทราบ
M	Moderate	สามารถจัดการได้โดยการเฝ้าระวังหรือกระบวนการตอบโต้เฉพาะ แต่ละกรณีได้
L	Low	สามารถจัดการได้โดยกระบวนการที่ปฏิบัติประจำ

ตัวอย่างการสร้างตาราง (Matrix) แสดงได้ดังนี้

	ผลต่อเนื่อง				
ความน่าจะเป็น	**ระดับความร้ายแรง**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost certain	E	E	E	H	H
Likely	E	E	H	H	M
Possible	E	E	H	M	L
Unlikely	E	H	M	L	L
Rare	H	H	M	L	L

ขั้นที่ 4 ระบุและจัดลำดับความเสี่ยง

จุดประสงค์ของการระบุและจัดลำดับความเสี่ยงเพื่อที่จะหาความเร่งด่วนของการบริหารจัดการความเสี่ยง โดยเปรียบเทียบระดับของความเสี่ยงกับ มาตรฐานที่เลือกไว้ เป้าหมายของระดับความเสี่ยงที่ตั้งไว้ และ มาตรการทางเลือกอื่น ถ้ามี

ตัวอย่างขั้นตอนในการระบุและจัดลำดับความเสี่ยงที่เลือกไว้ และสร้างทะเบียน แสดงในตารางต่อไปนี้

ลำดับ	กิจกรรม
1	จัดทำเอกสารแสดงทะเบียนความเสี่ยงแต่ละกรณี ควบคู่กับมาตรฐานที่เลือกไว้ เป้าหมายของระดับความเสี่ยงที่ตั้งไว้ และ มาตรการทางเลือกอื่น (ถ้ามี) เพื่อหาว่าอะไรเป็นความเสี่ยงที่ยอมรับได้
2	ระบุในแต่ละตารางเมื่อเทียบกับมาตรการที่บันทึกไว้ในลำดับที่ 1 เพื่อที่จะหาว่าความเสี่ยงนั้นยอมรับได้หรือไม่ ถ้ารับได้ให้ลงทะเบียนไว้
3	ใช้มาตรการในลำดับที่ 1 เพื่อที่จะกำหนดความเร่งด่วน ความเสี่ยงที่ยอมรับไม่ได้และบันทึกค่าไว้

ขั้นที่ 5 พัฒนาแผนรับมือ

แผนการรับมือกับความเสี่ยง (Risk Treatment Plan) จะแสดงวิธีการที่จะประยุกต์ใช้การควบคุมการรับมือกับความเสี่ยงอย่างเป็นระบบ ทั้งนี้เพื่อลดผลกระทบ ลดความน่าจะเป็น และ/หรือลดผลต่อเนื่องที่อาจจะเกิดขึ้นมาภายหลัง

โดยมีขั้นตอนควรดำเนินการดังนี้

ลำดับ	กิจกรรม
1	เขียนความเสี่ยงที่ระบุไว้ว่าเป็นกรณีที่ยอมรับไม่ได้ จากทะเบียนความเสี่ยงตามลำดับความสำคัญ
2	บันทึกการควบคุมที่เหมาะสมสำหรับความเสี่ยงแต่ละกรณีบนตารางความเสี่ยง อาจมีได้มากกว่าหนึ่งวิธี
3	วิเคราะห์ Cost/benefit แล้วบันทึกผลว่า ยอมรับได้หรือไม่ได้สำหรับวิธีควบคุมแต่ละวิธี
4	คำนวณผลกระทบข้างเคียง ถ้ามี จากการควบคุมที่ยอมรับได้
5	บันทึกผลจากข้อ 4 ในทะเบียนความเสี่ยง
6	บันทึกการควบคุมที่ยอมรับได้ในทะเบียนการควบคุม จากนั้นจึงพัฒนาแผนฯ โดยการกำหนดความรับผิดชอบ ตารางการทำงานและวิธีการเฝ้าระวังสำหรับการนำไปใช้ต่อไป

5. การพัฒนาแผนระบบรักษาความมั่นคงปลอดภัย (SSP -System Security Plan)

แผนระบบรักษาความมั่นคงปลอดภัยจะเป็นเอกสาร ซึ่งแสดงวิธีการนำนโยบาย ICT Security ไปใช้ และแสดงผลที่ได้จากแผนบริหารจัดการความเสี่ยง นอกจากนี้ยังจะแสดงสถาปัตยกรรมของการรักษาความมั่นคงฯ ในระดับสูงและเน้นนโยบายที่ต้องทำ

วัตถุประสงค์ของแผนระบบรักษาความมั่นคงปลอดภัยก็เพื่อที่จะแสดงให้เห็นได้ว่า จะดำเนินการตามนโยบายความมั่นคงฯ และการบริหารจัดการความเสี่ยงได้อย่างไร ถ้าพิจารณาร่วมกันกับระบบสารสนเทศของหน่วยงานนั้นๆ

ในการพัฒนาและบำรุงรักษาแผนฯ ต้องมอบหมายให้มีผู้จัดการระบบรับผิดชอบงานนี้โดยตรงในระดับสูงขึ้นไป เช่นในการบริหารจัดการซึ่งอาจประกอบไปด้วยแผนฯ หลายแผน อาจจำเป็นต้องมีที่ปรึกษาหรือผู้เชี่ยวชาญประจำหน่วยงานจะเป็นผู้รับผิดชอบในระดับองค์กรต่อไป

ตัวอย่างของผู้ที่มีส่วนได้-ส่วนเสียที่เกี่ยวข้องในการกำหนดแผนฯ จะรวมถึงตัวแทนในส่วนต่างๆ อาทิ เช่น

1) โครงการ อาจจะเป็นผู้รับจ้างก็ได้
2) เจ้าของสารสนเทศทั้งหลายที่ต้องการบริการจากระบบ
3) ผู้ใช้ต่างๆ ที่จะต้องพึ่งพาการพัฒนาความสามารถในการให้บริการของระบบ

4) ผู้ได้รับมอบหมายให้ตรวจสอบการบริหารจัดการระบบ
5) ส่วนงานวางแผนการบริหารจัดการสารสนเทศ
6) ผู้ที่ได้รับมอบหมายให้ประเมินและออกใบรับรอง (ถ้ามี)
7) ส่วนของการจัดการโครงสร้างพื้นฐาน (เช่น อาคาร และ/หรือโครงสร้างพื้นฐานของเครือข่าย)

6. การพัฒนาและดำเนินงานสำหรับกระบวนการปฏิบัติงานตามมาตรฐานความมั่นคงฯ

(Security Standard Operating Procedures -SOPs)

กระบวนการปฏิบัติงานตามมาตรฐานความมั่นคงฯ คือการกำหนดหน้าที่ของผู้ใช้ทั้งหมด รวมถึงผู้บริหารและระดับหัวหน้าหน่วยงาน ที่เกี่ยวกับกระบวนการต่างๆ ที่จำเป็นในการรับประกันว่าระบบไอซีทีจะสามารถดำเนินงานได้อย่างปลอดภัย

บทบาทของเจ้าหน้าที่ที่จะต้องกำหนดในกระบวนการ จะรวมถึง

- ที่ปรึกษา/ผู้เชี่ยวชาญประจำหน่วยงาน (ITSA)
- System Manager
- System Administrator
- ผู้ใช้ทั่วไป

ผู้จัดการระบบควรจะดำเนินการสร้างความเชื่อมั่นให้ได้ว่า SOPs จะได้รับการบำรุงรักษาและปรับปรุงให้ทันสมัย ได้แก่ การเตรียมการบริหารความเปลี่ยนแปลง และการจัดตารางเวลาสำหรับการทบทวนแผนฯ

ตัวอย่างรายละเอียดการจัดทำกระบวนการปฏิบัติงานตามมาตรฐานความมั่นคงฯ (SOPs) ในแต่ละระดับ แสดงไว้ในตารางต่อไปนี้

1) ที่ปรึกษา/ผู้เชี่ยวชาญประจำหน่วยงาน (ITSA)

ตารางต่อไปนี้จะแสดงกระบวนการขั้นต้นที่ควรระบุไว้ใน ITSA's SOPs

หัวข้อ	**กระบวนการที่ควรระบุไว้**
การให้ความรู้ผู้ใช้	เป็นการแนะนำผู้ใช้ใหม่ เพื่อที่จะใช้งานได้อย่างถูกต้องตามกฎความมั่นคงปลอดภัย
Audit logs	พิจารณาทบทวน system audit trail & manual logs โดยเฉพาะที่เกี่ยวกับผู้ใช้ที่ได้รับสิทธิพิเศษ
System integrity audit	● ตรวจทาน user accounts, system parameters, & access controls เพื่อตรวจสอบความมั่นคงปลอดภัย ● ตรวจสอบบูรณภาพของ System software ● ทดสอบ access controls □ตรวจสอบอุปกรณ์และการวางเคเบิ้ล
การรับส่งข้อมูล	● จัดการขั้นตอนการตรวจสอบการโยกย้ายข้อมูลบนสื่อที่เคลื่อนย้ายได้ โดยเฉพาะในส่วนที่ต้องส่งออกไปนอกที่ตั้งประจำ □จัดการขั้นตอนการตรวจสอบสื่อที่นำเข้ามา เพื่อเฝ้าระวังไวรัสและซอฟต์แวร์ที่ไม่พึงประสงค์
การเก็บทรัพย์สินไอที	การทำเครื่องหมาย ลงทะเบียน และเก็บรวบรวมทรัพย์สิน รวมถึงสื่อที่เคลื่อนย้ายได้
เหตุการณ์ด้านความมั่นคงฯ	การรายงานและจัดการเหตุฯ

2) System Manager SOPs

ตารางต่อไปนี้จะแสดงกระบวนการขั้นต้นที่ควรระบุไว้ใน System Manager's SOPs

หัวข้อ	**กระบวนการที่ควรระบุไว้**
System maintenance	การจัดการด้านความมั่นคงฯและการทำงานทั่วไปของระบบประจำวัน ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ รวมถึง ● การรักษาความตระหนักของ software vulnerabilities ● การทดสอบและติดตั้ง software patched/updates ● การติดตั้ง hardening techniques ที่เหมาะสม □การอัพเดท anti-virus software
การย้ายฮาร์ดแวร์ที่เลิกใช้ออกไปจากระบบ	การจัดการการกำจัดอุปกรณ์ที่เลิกใช้แล้ว รวมถึงสื่อที่ใช้บันทึกข้อมูล
การจัดการบัญชีผู้ใช้	การให้สิทธิผู้ใช้งานระบบที่เข้ามาใหม่
Configuration control	การอนุมัติและการยอมให้แก้ไข system software หรือ configuration
Access control	การให้สิทธิการเข้าถึงแอพพลิเคชั่นและข้อมูล
System backup and recovery	การฟื้นคืนระบบจากความล้มเหลว (recovering from system failures)

3) System Administrator SOPs

ตารางต่อไปนี้จะแสดงกระบวนการขั้นต้นที่ควรระบุไว้ใน System Administrator's SOPs

หัวข้อ	**กระบวนการที่ควรระบุไว้**
System closedown	การรักษาความมั่นคงปลอดภัยนอกเวลาทำการ
การควบคุมการเข้าถึง	การดำเนินการให้สิทธิการเข้าถึงแอพพลิเคชั่นและข้อมูล
การบริหารจัดการบัญชีผู้ใช้งาน	การเพิ่มและยกเลิกรายชื่อผู้ใช้จากระบบ, การให้สิทธิพิเศษ, Cleaning up directories & files เมื่อผู้ใช้ออกไปจากระบบแล้ว
System backup and recovery	การสำรองข้อมูล รวมถึง audit logs, การรักษาความมั่นคงฯ ของ backup tapes, recovering from system failures

4) System Users SOPs

ตารางต่อไปนี้จะแสดงกระบวนการขั้นต้นที่ควรระบุไว้ใน System User's SOPs

หัวข้อ	**กระบวนการที่ควรระบุไว้**
บทบาทและหน้าที่	ใครรับผิดชอบในส่วนไหนของมาตรการรักษาความมั่นคงฯ
การเตือน	ได้แก่ กิจกรรมของผู้ใช้อาจถูกตรวจสอบ และ ผู้ใช้อาจจะต้องรับผิดชอบต่อการกระทำที่เกิดขึ้นในระบบฯ
พาสเวิร์ด	แนวทางในการเลือกและการป้องกันพาสเวิร์ด
สิ่งที่ต้องรู้	แนวทางที่จะกำหนดเป็นระเบียบในสิ่งที่ต้องรู้ในระบบ
Security incidents	รายการสิ่งที่ต้องทำ หากเกิดเหตุฯ ที่น่าสงสัยหรือที่เกิดจริง
Classification	ระดับสูงสุดของ Classified material ซึ่งยอมให้ประมวลผลได้บนระบบ
การออกไปจากระบบชั่วขณะ (Temporary absence)	วิธีการที่ถูกต้องในการรักษาความมั่นคงฯ เมื่อจะลุกออกไปจากคอมพิวเตอร์ชั่วขณะ
เมื่อเลิกงาน	วิธีการที่ถูกต้องในการรักษาความมั่นคงฯ เมื่อเลิกงาน
Media control	กระบวนการสำหรับการควบคุมและกำจัดมีเดีย
Hardcopy	กระบวนการสำหรับทำเครื่องหมาย เก็บรักษาหรือกำจัดเอกสาร (hardcopy)
Visitors	การป้องกันผู้มาเยือนไม่ให้เข้ามาดูข้อมูลได้
การบำรุงรักษา	รายการสิ่งที่ต้องทำ สำหรับ hardware & software maintenance

ระเบียบข้อบังคับสำหรับผู้ใช้ทั่วไป

หน่วยงานต้องจัดให้มีแนวทางหรือคำแนะนำสำหรับผู้ใช้ทั่วไป โดยระบุความรับผิดชอบที่เกี่ยวกับความมั่นคงปลอดภัยฯ และผลที่จะตามมาถ้าไม่ปฏิบัติตามระเบียบ

คำแนะนำของหน่วยงานควรจะประกอบด้วย

- จำกัดการเข้าถึงข้อมูล สารสนเทศ และซอฟต์แวร์ที่ผู้ใช้มีสิทธิและเป็นสิ่งที่ต้องรู้
- รายงานเหตุการณ์ด้านความมั่นคง ภัยคุกคาม และช่องโหว่ทั้งหมดที่เกิดขึ้นทันทีที่พบ ต่อผู้รับผิดชอบโดยตรง
- ป้องกันการพิสูจน์ตัวตนที่ได้รับมอบ
- ให้ความมั่นใจได้ว่า system media & system output ได้รับการจัดชั้นความลับ ได้ทำเครื่องหมาย ควบคุม เก็บรักษาและกำจัดอย่างถูกต้อง
- ปกป้องเทอร์มินอลจากการเข้าถึงของผู้ที่ไม่เกี่ยวข้อง

นอกจากนี้ควรมีคำเตือนในเรื่องต่างๆ ที่ไม่ควรทำ ดังต่อไปนี้

- การนำเข้าของ malicious code มาสู่ระบบสารสนเทศ
- การก่อความเสียหายทางกายภาพต่อระบบ
- การนำมาใช้หรือใช้ unauthorized software, firmware, hardware ในระบบสารสนเทศ
- การอ้างสิทธิการเข้าถึงสารสนเทศแทนผู้อื่น
- ความพยายามเข้าถึงข้อมูลที่ไม่มีสิทธิ
- การโยกย้ายอุปกรณ์ในระบบฯ โดยไม่ได้รับอนุญาต

7. การตรวจสอบและการออกใบประเมินระบบสารสนเทศ

มีวัตถุประสงค์ที่จะแสดงข้อมูลเกี่ยวกับวิธีการรับรองและการออกใบรับรอง ความมั่นคงปลอดภัยของระบบไอซีที ทั้งนี้เพื่อสร้างความไว้วางใจให้กับฝ่ายบริหารของหน่วยงานและเจ้าของข้อมูล ตามที่กำหนดไว้ในแผนความมั่นคงฯของระบบงาน (จะเป็นหน้าที่ของหน่วยงานใหม่ที่จะดำเนินการต่อไป หลังจากอนุมัติใช้แผนแม่บทฯ แล้ว)

8. การดำเนินงานความมั่นคงด้านไอซีทีและการจัดการเหตุด้านความมั่นคงของหน่วยงาน

การดำเนินงานความมั่นคงด้านไอซีทีเป็นงานที่ต้องทำอย่างต่อเนื่อง ซึ่งประกอบด้วยขั้นตอนและวิธีการที่จะป้องกันแหล่งข้อมูลสารสนเทศและระบบงานทั้งหมด ได้แก่ Confidentiality, Integrity, Availability รวมถึง Authentication และ Access control

หน่วยงานควรระบุบทบาทและหน้าที่ในการบำรุงรักษา ICT Security อย่างชัดเจน และจัดให้มีทรัพยากรอย่างพอเพียงที่จะปฏิบัติหน้าที่ตามภารกิจที่เกี่ยวข้อง ได้แก่ การจัดการความเปลี่ยนแปลง กระบวนการจัดการที่เกิดขึ้น การดักจับเหตุการณ์ด้านความมั่นคงฯ และการจัดการในส่วนที่เกี่ยวข้อง การรายงานที่ต้องส่งออกไปนอกหน่วยงานเมื่อประสพเหตุฯ และการวางแผนโต้ตอบเหตุการณ์ เมื่อเกิดขึ้นมาแล้ว

1) การบริหารจัดการความเปลี่ยนแปลง

ความต้องการที่จะเปลี่ยนแปลง ระบุได้หลายวิธี เช่น

- การแจ้งเสียหรือความต้องการปรับปรุงระบบงานจากผู้ใช้
- ผู้จำหน่ายอุปกรณ์แจ้งการอัพเกรดซอฟต์แวร์หรือฮาร์ดแวร์
- ความก้าวหน้าในเทคโนโลยี
- การดำเนินงานของระบบใหม่ ซึ่งต้องเปลี่ยนระบบเดิม และ
- การระบุหน้าที่ใหม่ที่ต้องการปรับปรุงระบบหรือจัดหาระบบใหม่

ดังนั้นหน่วยงานจำเป็นต้องดำเนินการ ต่อไปนี้ ให้เกิดความมั่นใจว่า

- กระบวนการจัดการความเปลี่ยนแปลงได้ระบุไว้แล้วในเอกสารสำคัญของ ICT Security และจะได้รับการปฏิบัติตาม
- ข้อเสนอที่จะเปลี่ยนได้รับอนุมัติแล้ว โดยเจ้าหน้าที่
- การเปลี่ยนแปลงใดๆ ที่อาจมีผลต่อความมั่นคงปลอดภัยฯ จะต้องเสนอขออนุมัติก่อนเสมอ
- เอกสารที่เกี่ยวข้องกับระบบจะได้รับการปรับปรุงให้ทันสมัย เพื่อแสดงให้เห็นถึงส่วนที่เปลี่ยนไป

2) กระบวนการบริหารจัดการฯ (Change management process)

การเปลี่ยนแปลงสิ่งแวดล้อมของระบบจะต้องรวมถึง

- การอัพเกรด System hardware
- การอัพเกรด System or application software
- การเพิ่มจอเป็นกรณีพิเศษ
- การเปลี่ยนแปลงที่มีสาระสำคัญ ในส่วน system access controls

3) การดักจับ Security Incidents

นิยามของ Security incident คือ เหตุการณ์ ซึ่งมีผลกระทบต่อ Confidentiality, Integrity หรือ Availability ของระบบ ที่เกิดจาก การกระทำของ unauthorized access, disclosure, modification, misuse, damage, loss หรือ destruction

หน่วยงานต้องพัฒนา ดำเนินงานและรักษาเครื่องมือและกระบวนการที่ได้มาจาก การระบุความเสี่ยง การกู้คืนจากผลการดักจับเหตุด้านความมั่นคงฯ ประกอบด้วย

- Countermeasures against malicious code
- Intrusion detection strategies
- Audit analysis
- System integrity checking
- Vulnerability assessments

นอกจากนี้ภัยคุกคามที่จะเป็นเหตุด้านความมั่นคงมักจะถูกพบโดยพนักงาน มากกว่าที่จะพบโดย software tools ดังนั้นการฝึกอบรมเจ้าหน้าที่และพนักงานอย่างต่อเนื่องและมีความตระหนักในปัญหานี้จะช่วยบรรเทาภัยได้อย่างดี

เครื่องมือที่ใช้ดักจับ เป็นซอฟต์แวร์มีหลายชนิด เช่น Network and Host Intrusion Detection Systems, System Integrity Verification, Log Analysis, Intrusion Repulsion เป็นต้น

4) การจัดการ Security Incidents

หน่วยงานต้องจัดทำหน้าที่ความรับผิดชอบต่อเหตุด้านความมั่นคงฯ อย่างละเอียดรวมถึงกระบวนการสำหรับระบบของหน่วยงานแต่ละระบบ

ในการใช้มาตรฐานในหน่วยงาน ควรดำเนินการ

- สนับสนุนพนักงานให้บันทึกและรายงานข้อสังเกตที่เกิด หรือสงสัยว่าจะเป็นจุดอ่อนหรือภัยคุกคาม ต่อระบบหรือบริการ
- จัดทำและติดตามกระบวนการสำหรับรายงาน Software malfunctions
- ดำเนินจัดทำระบบงานในหน่วยงาน เพื่อจัดประเภท ปริมาณ และต้นทุนของเหตุและอาการเสียที่จะต้องประเมินและเฝ้าดู
- รับมือกับการละเมิดนโยบายองค์กรด้านความมั่นคงปลอดภัยในองค์กร

การบันทึกเหตุการณ์ควรดำเนินการอย่างเป็นรูปธรรม บันทึกเหล่านี้ควรเน้นวิธีการและความถี่ของการเกิดเหตุฯ และการละเมิด เพื่อที่จะดำเนินมาตรการแก้ไขต่อไป รายงานที่บันทึกข้อมูลควรประกอบด้วย

- วัน/เวลาที่เกิดเหตุ
- วัน/เวลาที่ค้นพบเหตุ
- คำอธิบายของเหตุ รวมถึงบุคคลและตำแหน่งที่เกี่ยวข้อง
- กิจกรรมที่ได้ใช้เพื่อรับมือเหตุ
- ได้รายงานเหตุให้ใครทราบแล้ว และ
- เอกสารอ้างอิง

5) การรายงานเหตุฯ ออกไปนอกองค์กร

การรายงาน Security incidents จัดให้มีวิธีการเพื่อที่จะวัดหรือประเมินความเสียหายรวม และดำเนินการแก้ไขขั้นต้น ครอบคลุมหน่วยราชการทั้งหมด รายงานเหตุฯเป็นเครื่องมือพื้นฐานสำหรับระบุแนวโน้มในการเกิดเหตุการณ์ และเพื่อที่จะพัฒนานโยบายใหม่ กระบวนการ เทคนิคและมาตรการฝึกอบรมเชิงป้องกัน

6) แผนตอบโต้เหตุการณ์ (Incident Response Plan)

หน่วยงานแต่ละหน่วยต้องพัฒนา Incident Response Plan ซึ่งอย่างน้อย ต้องครอบคลุม

- แนวทางกว้างๆ ว่าเหตุเกิดได้อย่างไร
- การฝึกอบรมขั้นต่ำของผู้ใช้และผู้บริหารจัดการระบบ
- เจ้าภาพที่รับผิดชอบในการตรวจสอบเหตุการณ์
- ขั้นตอนที่จำเป็นเพื่อรับประกันบูรณภาพของข้อมูลได้ว่าสนับสนุน “compromise”
- ขั้นตอนที่จำเป็นเพื่อรับประกันว่าระบบงานที่สำคัญยิ่งยังคงดำเนินไปได้อย่างต่อเนื่อง

- วิธีการรายงานเหตุการณ์อย่างเป็นทางการ

9. การติดตามและประเมินผล

มีวัตถุประสงค์เพื่อ

- ระบุการเปลี่ยนแปลงด้านการดำเนินงานขององค์กรที่จะต้องเกิดขึ้น และการติดตามและประเมินผล
- ระบุการเปลี่ยนแปลงต่อความเสี่ยงที่จะต้องติดตามและประเมินผลผล
- ประเมินประสิทธิผลของกระบวนการรักษาความมั่นคงฯ และระบุประเด็นที่ต้องการปรับปรุงต่อไป

การติดตามและประเมินด้าน Security ควรมีพื้นฐานบนข้อมูล ซึ่งจะ ละเอียด ทันสมัย และเชื่อถือได้

การรวบรวมสารสนเทศที่เป็นปัจจุบันเพื่อการทบทวนแผนฯ ควรครอบคลุม ส่วนงานต่อไปนี้

- ความเร่งด่วนของหน่วยงาน
- ความต้องการด้านการดำเนินงานประจำ
- ข้อมูลที่เกี่ยวกับภัยคุกคาม
- โอกาสที่จะเกิดและผลที่ตามมา ในแง่ที่จะประมาณการได้
- ผลสัมฤทธิ์ของวิธีการต่อต้านที่ใช้อยู่แล้ว
- การตอบโต้อื่นๆ ที่เป็นไปได้ และ
- วิธีปฏิบัติที่ดีที่สุด (Best practice)

เอกสารอ้างอิง

1. ACSI 33, Australian Government, Information and Communications Technology Security Manual, 31 March 2006
2. Information Security Guideline for NSW Government, June 2003
3. NIST SP800-53 Recommended Security Controls for Federal Information Systems
4. NIST SP800-53A, Guide for Assessing the Security Controls in Federal Information Systems
5. FIPS-199 Standards for Security Categorization of Federal Information and Information Systems
6. FIPS-200 Minimum Security Requirements for Federal Information and Information Systems
7. ISO/IEC 27001 ISMS33