ขั้นตอนปฏิบัติสำหรับการวิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศ

ผู้รับผิดชอบระบบสารสนเทศ กำหนดให้มีการวิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศที่ตนเองรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง และบริหารจัดการความเสี่ยงเหล่านั้นตามขั้นตอนดังนี้

(๑) จัดทำทะเบียนสินทรัพย์ตามขอบเขตของงานที่ตนรับผิดชอบ

(๒) วิเคราะห์และระบุเหตุการณ์ความเสี่ยงซึ่งอาจทำให้วัตถุประสงค์ด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้เกิดความเสียหายหรือไม่สอดคล้องได้

(๓) ประเมินค่าความเสี่ยงของเหตุการณ์ความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงที่ได้กำหนดไว้

(๔) จัดลำดับค่าความเสี่ยงของเหตุการณ์ความเสี่ยงต่างๆ เรียงตามลำดับจากมากไปน้อย

(๕) บันทึกผลการประเมินความเสี่ยงในข้างต้น

(๖) จัดทำแผนการลดความเสี่ยง โดยพิจารณาถึงลำดับการดำเนินการ ค่าใช้จ่าย ความคุ้มค่าหรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๗) นำเสนอแผนการลดความเสี่ยง ต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๘) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนการลดความเสี่ยง และรายงานให้ได้รับทราบเป็นระยะๆ จนกระทั่งเสร็จสิ้น

ขั้นตอนปฏิบัติสำหรับการพัฒนาหรือจัดหาระบบงานด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบที่ได้มีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) จัดให้มีการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษรข้อกำหนดดังกล่าวอย่างน้อยควรครอบคลุมประเด็นสำคัญต่างๆ ดังนี้

- คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัย
- การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย
- กรณีระบบงานมีข้อมูลที่มีความสำคัญ เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล และข้อมูลนั้นจะมีการส่งผ่านไปมาบนเครือข่ายระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์สำหรับให้บริการระบบงาน กำหนดให้มีการเข้ารหัสข้อมูลที่มีการรับส่งนั้น

(๒) กำหนดให้มีการจัดทำแผนการทดสอบระบบ นำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้บริหารดำเนินการทดสอบตามแผนการทดสอบระบบ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงหรือแก้ไขต่างๆ ตามความจำเป็น แผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

- แผนการทดสอบ UAT (User Acceptance Test)
- แผนการทดสอบ System Integration Test
- แผนการทดสอบข้อกำหนดด้านความมั่นคงปลอดภัย (Security Test)

ผู้พัฒนาระบบต้องนำเสนอแผนการทดสอบ UAT โดยอย่างน้อยให้แสดงเป็นหน้าจอต่างๆ ที่จะทำการทดสอบ และข้อมูลตัวอย่างที่จะใช้ในการทดสอบกับหน้าจอเหล่านั้น ทั้งข้อมูลที่คาดว่าระบบจะทำงานอย่างถูกต้องและที่คาดว่าระบบจะแสดงข้อผิดพลาดในการทำงาน

ขั้นตอนปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน

ผู้ใช้งาน กำหนดหรือใช้งานรหัสผ่านโดยปฏิบัติ ดังนี้

(๑) เก็บรักษารหัสผ่านที่ได้รับไว้เป็นความลับ

(๒) กำหนดรหัสผ่านที่มีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษร ตัวเลข และสัญลักษณ์ต่างๆ เข้าด้วยกัน

(๓) ใช้รหัสผ่านเพื่อป้องกันไฟล์ที่มีการใช้งานร่วมกับผู้อื่นทางเครือข่ายคอมพิวเตอร์

(๔) ไม่บันทึกรหัสผ่านไว้ในระบบเพื่อเป็นการช่วยจำและเพื่อให้สามารถย้อนกลับมาใช้ระบบโดยไม่ต้องใส่รหัสผ่านอีกครั้งหนึ่ง

(๕) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยผู้อื่น

(๖) เปลี่ยนรหัสผ่านตั้งต้นที่ได้รับโดยทันที หรือเมื่อเข้าใช้งานระบบเป็นครั้งแรก

(๗) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านของตนเองแก่ผู้อื่นเนื่องจากไม่สามารถมาปฏิบัติงานได้หรือความจำเป็นอื่นใดก็ตาม เมื่อกลับมาปฏิบัติงานได้ตามปกติ ให้ทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสิทธิการเข้าถึงระบบ

ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการสิทธิการเข้าถึงระบบของผู้ใช้งาน ดังนี้

(๑) กำหนดให้เฉพาะเจ้าหน้าที่หรือผู้ที่เกี่ยวข้องกับงานตามภารกิจเท่านั้นที่จะอนุญาตให้สามารถเข้าถึงระบบงานและข้อมูลได้

(๒) กำหนดให้เจ้าหน้าที่ใหม่ต้องขออนุมัติการใช้งานระบบ

(๓) กำหนดสิทธิการใช้ระบบของผู้ร้องขอโดยให้สิทธิให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ร้องขอ หรือความจำเป็นในการใช้งาน

(๔) กำหนดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบให้ถูกต้องและเหมาะสม เมื่อมีการเปลี่ยนแปลงโยกย้าย หรือพ้นหน้าที่จากการปฏิบัติราชการ

(๕) จัดเก็บข้อมูลหรือเอกสารการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้ในการอ้างอิงหรือตรวจสอบในภายหลัง

(๖) กำหนดให้มีการทบทวนบัญชีผู้ใช้งานของระบบต่างๆ อย่างสม่ำเสมอดังนี้

- พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายใน
- จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในเพื่อดำเนินการตรวจสอบว่ามีรายชื่อที่ออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้รับการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่
- ผู้บังคับบัญชาของหน่วยงานภายในแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง
- ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบ

เมื่อมีความจำเป็นต้องติดตั้ง เปลี่ยนแปลง แก้ไข หรือปรับปรุงระบบต่างๆ ขององค์กร ผู้รับผิดชอบระบบสารสนเทศปฏิบัติดังนี้

(๑) ดำเนินการบันทึกคำขออนุมัติและรายละเอียดที่เกี่ยวข้องของการเปลี่ยนแปลงระบบลงในแบบฟอร์ม FM-xx_Change form

(๒) หารือการเปลี่ยนแปลงนั้นกับผู้บังคับบัญชาและผู้ที่เกี่ยวข้อง

(๓) ระบุประเภทของการเปลี่ยนแปลง (Change Type)

(๔) พิจารณาระดับผลกระทบและความเร่งด่วนของการเปลี่ยนแปลงนั้น

(๕) พิจารณาและประเมินความเสี่ยงที่เกิดขึ้นจากการเปลี่ยนแปลงนั้น

(๖) จัดทำแผนดำเนินการเปลี่ยนแปลง (แผนดำเนินการเปลี่ยนแปลง (Rollout Plan) หมายถึง แผนการติดตั้ง แผนการทดสอบ และ/หรือ แผนการแจ้งกำหนดการต่างๆ ให้ผู้ที่เกี่ยวข้องได้รับทราบ)

(๗) จัดทำแผนถอยหลังกลับพร้อมทั้งสำรองข้อมูลต่างๆ ที่เกี่ยวข้องของระบบนั้นตามความจำเป็น (แผนการถอยหลังกลับ (Fallback Plan) หมายถึง แผนการย้อนกลับไปสู่สถานะก่อนดำเนินการเปลี่ยนแปลง โดยรวมแผนนี้จะหมายถึงการสำรองข้อมูลต่างๆ ที่จำเป็นก่อนดำเนินการเปลี่ยนแปลง ทั้งข้อมูลในฐานข้อมูล ข้อมูล Configuration ของระบบ ตัวซอฟต์แวร์ของระบบ และข้อมูลอื่นๆ ที่เกี่ยวข้องหากติดตั้งไม่สำเร็จ จะได้กลับไปใช้สถานะของระบบเดิมก่อนการเปลี่ยนแปลงได้)

(๘) ประกาศช่วงระยะเวลาการติดตั้งระบบให้ผู้ใช้งานได้รับทราบก่อนล่วงหน้า

(๙) ทดสอบการเปลี่ยนแปลงนั้นกับระบบทดสอบ รวมทั้งร่วมกับผู้ใช้งานและผู้ที่ (สำหรับกรณีที่สามารถทำได้) เกี่ยวข้องในการทดสอบจนกระทั่งมั่นใจว่าไม่มีปัญหาใดๆ

(๑๐) ติดตั้งบนระบบจริง

(๑๑) เปิดระบบใช้งาน

(๑๒) ประกาศแจ้งให้ผู้ใช้งานและผู้ที่เกี่ยวข้องได้รับทราบตามความจำเป็น

(๑๓) เฝ้าระวังว่าระบบมีปัญหาข้างเคียงใดๆ เกิดขึ้นหรือไม่

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการขีดความสามารถของระบบ

ผู้รับผิดชอบระบบสารสนเทศ บริหารจัดการขีดความสามารถของระบบ หรือ อุปกรณ์เครือข่ายที่มีการใช้งานในการให้บริการสารสนเทศ ดังนี้

(๑) จัดทำแผนการเฝ้าระวังทรัพยากรของระบบ โดยใช้แนวทาง ดังนี้

- กำหนดประเภทของข้อมูลที่ใช้ในการเฝ้าระวังปริมาณการใช้ทรัพยากรของระบบ เช่น ร้อยละของการใช้ทรัพยากรในการประมวลผลของ/สำหรับ
  - ซีพียู
  - หน่วยความจำ
  - ฮาร์ดดิสก์
  - การไหลของข้อมูลเข้า-ออกจากระบบ

เป็นต้น และกำหนดค่า Threshold ที่เหมาะสม

- กำหนดประเภทของข้อมูลที่ใช้ในการเฝ้าระวังปริมาณการใช้ระบบของผู้ใช้งาน เช่น
  - จำนวนธุรกรรมที่เกิดขึ้นในช่วงระยะเวลาหนึ่ง
  - จำนวนผู้ใช้งานที่เข้าถึงระบบในช่วงระยะเวลาหนึ่ง

  เป็นต้น และกำหนดค่า Threshold ที่เหมาะสม
- กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรของระบบ
- กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ระบบของผู้ใช้งาน
- กำหนด ผู้รับผิดชอบ ในการตรวจสอบ

แผนการเฝ้าระวังทรัพยากรของระบบ

ระบบ	ปริมาณการใช้ทรัพยากรของระบบปริมาณการ/ใช้ระบบ ที่ต้องตรวจสอบ	ความถี่ในการตรวจสอบ	ผู้รับผิดชอบในการตรวจสอบ
	ปริมาณการใช้ทรัพยากรของระบบ : ☐ CPU ค่า Threshold ที่ยอมรับได้..... ☐ หน่วยความจำ ค่า Threshold ที่ยอมรับได้..... ☐ ฮาร์ดดิสก์ ค่า Threshold ที่ยอมรับได้.....	☐ รายชั่วโมง ☑ รายวัน ☐ รายสัปดาห์ ☐ รายเดือน ☐ รายปี	
	ปริมาณการใช้ระบบ : ☐ จำนวนผู้ใช้งานในช่วงชั่วโมงทำงาน ค่า Threshold ที่ยอมรับได้..... ☐ ระยะเวลาการตอบสนองเฉลี่ยนับตั้งแต่เริ่มล็อกอินเข้าใช้งานจนกระทั่งระบบพร้อมใช้ ค่า Threshold ที่ยอมรับได้.....	☐ รายชั่วโมง ☑ รายวัน ☐ รายสัปดาห์ ☐ รายเดือน ☐ รายปี	

(๒) เมื่อถึงระยะเวลาการติดตามและเฝ้าระวัง ผู้รับผิดชอบ ดำเนินการการติดตามและตรวจสอบทรัพยากรของระบบตามแผนการเฝ้าระวังทรัพยากรของระบบที่ได้กำหนดไว้ โดยพิจารณาปริมาณการใช้ทรัพยากรของระบบว่าเป็นปกติหรือไม่ อยู่ในค่า Threshold ที่กำหนดไว้หรือไม่ และ/หรือ ติดตามและตรวจสอบปริมาณการใช้ระบบของผู้ใช้งานว่าเป็นปกติหรือไม่ อยู่ในค่า Threshold ที่กำหนดไว้หรือไม่

(๓) กรณีที่พบเหตุการณ์ผิดปกติของปริมาณการใช้ทรัพยากรหรือปริมาณการใช้ระบบของผู้ใช้งาน ผู้รับผิดชอบดำเนินการดังนี้

- วิเคราะห์เหตุการณ์และดำเนินการจัดการกับเหตุการณ์ที่พบนั้นตามความเหมาะสม
- บันทึกเหตุการณ์ที่ได้ดำเนินการแก้ไขและวิธีการแก้ไข
- รายงานให้ ผู้ให้บริการ ผู้บังคับบัญชา และผู้ที่เกี่ยวข้องได้รับทราบตามความจำเป็น