ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.)

ตามประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2557 ประกาศใช้เมื่อวันที่ 7 พฤศจิกายน พ.ศ. 2557 กำหนดในข้อ 12 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยหน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง และในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ผู้ปฏิบัติ

1. ผู้รับการตรวจประเมิน หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)

2. ผู้ตรวจสอบและประเมินความเสี่ยง หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายของกองตรวจสอบภายใน สป.พม.

ข้อปฏิบัติ

1. ข้อตกลงและเงื่อนไข

1.1 การตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม. ดำเนินการตรวจสอบให้สอดคล้องตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สป.พม.

1.2 การตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม. ดำเนินการโดยผู้ตรวจสอบภายในหน่วยงาน สป.พม. (Internal IT Auditor)

2. ขั้นตอน/กระบวนการ

2.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม. ปีละ 1 ครั้ง ระหว่างผู้ตรวจสอบและประเมินความเสี่ยง และผู้รับการตรวจประเมิน

2.2 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม. ระหว่างผู้ตรวจสอบและประเมินความเสี่ยง และผู้รับการตรวจประเมิน

2.3 การตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศที่มีความสำคัญหรือเป็นข้อมูลส่วนบุคคล มีข้อจำกัดดังนี้

(1) ผู้ตรวจสอบและประเมินความเสี่ยง สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบในลักษณะที่อ่านได้เพียงอย่างเดียว

(2) สำหรับการอนุญาตให้ผู้ตรวจสอบและประเมินความเสี่ยงสามารถเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้ จะต้องใช้วิธีการที่ปลอดภัย

(3) มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบและประเมินความเสี่ยงทำงานบนข้อมูลสำเนา

(4) มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

(5) มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

3. หน้าที่/ความรับผิดชอบ

3.1 ผู้รับการตรวจประเมิน

(1) ศทส. แต่งตั้งคณะทำงานจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สป.พม.

(2) ประชุมคณะทำงานจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ ศทส. เพื่อจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สป.พม.

(3) นำเสนอร่างแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สป.พม. เพื่อขอความเห็นชอบต่อปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (ปพม.)

(4) ดำเนินงานตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สป.พม.

(5) มอบหมายเจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้รับการตรวจประเมิน สำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม.

(6) รายงานผลการดำเนินงานตามแบบรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สป.พม.

(7) เตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม.

(8) ทบทวน/ปรับปรุงแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สป.พม. ปีละ 1 ครั้ง

3.2 ผู้ตรวจสอบและประเมินความเสี่ยง

(1) จัดทำแบบรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สป.พม. ตามขอบเขตและขั้นตอนปฏิบัติที่กำหนด สำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม.

(2) ดำเนินการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม.

(3) รายงานผลการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม. ให้ ปพม. และผู้รับการตรวจประเมินทราบ

(4) ติดตามผลการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สป.พม.