



ข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.)

ตามประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2557 ประกาศใช้เมื่อวันที่ 7 พฤศจิกายน พ.ศ. 2557 กำหนดในข้อ 11 นโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศ โดยให้หน่วยงานพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง มีการกำหนดบุคลากรเพื่อทำหน้าที่ดูแลรับผิดชอบ และต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ โดยมีความถี่ของการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ผู้ปฏิบัติ

1. คณะทำงาน หมายถึง คณะทำงานจัดทำระบบสำรองข้อมูลและสารสนเทศของ สป.พม.
2. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)

ข้อปฏิบัติ

1. ข้อตกลงและเงื่อนไข

1.1 คณะทำงานจัดทำระบบสำรองข้อมูลและสารสนเทศของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการพัฒนาระบบคลังข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธาน

1.2 ระบบสำรองข้อมูลและสารสนเทศของ สป.พม. ประกอบด้วย การสำรองและทดสอบกู้คืนข้อมูล และการเตรียมความพร้อมกรณีฉุกเฉิน

2. ขั้นตอน/กระบวนการ

2.1 แต่งตั้งคณะทำงานจัดทำระบบสำรองข้อมูลและสารสนเทศของ สป.พม.

2.2 ประชุมคณะทำงานจัดทำระบบสำรองข้อมูลและสารสนเทศของ สป.พม. เพื่อจัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.3 นำเสนอร่างแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อขอความเห็นชอบต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกรม (สป.พม.)

2.4 ดำเนินงานตามแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.5 ทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

3. หน้าที่/ความรับผิดชอบ

3.1 การสำรองและทดสอบกู้คืนข้อมูล

3.1.1 หน้าที่ของคณะทำงาน มีข้อปฏิบัติ ดังนี้

- (1) พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรอง ตามลำดับความสำคัญ
- (2) กำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง
- (3) กำหนดสื่อที่ใช้ในการเก็บข้อมูล และรูปแบบของการสำรองข้อมูล ซึ่งมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- (4) รายการที่ต้องสำรองข้อมูล และความถี่อย่างน้อย ดังนี้
 - เว็บไซต์หน่วยงาน : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/สัปดาห์
 - Web Application servers : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/เดือน
 - Database servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ทุกวัน
 - Firewall server : สำรองข้อมูล Rule ของ Firewall 1 ครั้ง/สัปดาห์
 - Server อื่นๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ 1 ครั้ง/เดือน
- (5) มีการสำรองข้อมูลเครื่องแม่ข่ายทั้งระบบ (Full System Backup) อย่างน้อยปีละ 1 ครั้ง
- (6) กำหนดขั้นตอนปฏิบัติและโปรแกรมในการสำรองข้อมูลและทดสอบกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง
- (7) กำหนดการเข้ารหัสข้อมูลในการสำรองข้อมูลที่สำคัญ โดยใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
- (8) มอบหมายเจ้าหน้าที่หลัก เพื่อดำเนินงานตามแผนการสำรองและทดสอบกู้คืนข้อมูล
- (9) มอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูล ในกรณีที่เจ้าหน้าที่หลักไม่สามารถปฏิบัติงานได้
- (10) จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูลที่เหมาะสมกับสำคัญของแต่ละระบบสารสนเทศ
- (11) รายละเอียดที่ปรากฏในแผนการสำรองและทดสอบกู้คืนข้อมูล ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้
 - รายการที่ต้องสำรองข้อมูล
 - การสำรองข้อมูล
 - การทดสอบกู้คืนข้อมูล
 - ปฏิทินการสำรองและทดสอบกู้คืนข้อมูล
 - ผู้รับผิดชอบ
 - การติดตามประเมินผล
- (12) ติดตามประเมินผล และทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล ปีละ 1 ครั้ง

3.1.2 หน้าที่ของเจ้าหน้าที่ มีข้อปฏิบัติ ดังนี้

- (1) จัดทำคู่มือการสำรองและทดสอบกู้คืนข้อมูลแต่ละระบบ
- (2) ดำเนินการตามปฏิทินการสำรองและทดสอบกู้คืนข้อมูล

(3) บันทึกการสำรองข้อมูล (Operator logs) ลงในแบบฟอร์ม โดยมีรายละเอียดอย่างน้อย ดังนี้ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก และรายงานผลการดำเนินงานต่อคณะทำงานเป็นประจำทุกเดือน

(4) กรณีพบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานให้ผู้บังคับบัญชาทราบ

(5) ตรวจสอบผลการสำรองข้อมูลว่าถูกต้องและสมบูรณ์ พร้อมทั้งบันทึกผลการตรวจสอบลงในแบบฟอร์ม

(6) มีการจัดเก็บสื่อบันทึกข้อมูลไว้ในที่ที่ปลอดภัย

(7) มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

(8) มีการทดสอบกู้คืนข้อมูล จากข้อมูลที่สำรองเก็บไว้ อย่างน้อยปีละ 1 ครั้ง

(9) กรณีพบปัญหาที่สร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนทำให้ต้องกู้คืนระบบ เจ้าหน้าที่จะต้องดำเนินการแก้ไขปัญหา พร้อมทั้งสรุปรายงานการปฏิบัติงานและการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

(10) การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

(11) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความก้าวหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

(12) สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

3.2 การเตรียมความพร้อมกรณีฉุกเฉิน

3.2.1 หน้าที่ของคณะทำงาน มีข้อปฏิบัติ ดังนี้

(1) พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม. โดยมีสถานการณ์อย่างน้อย ดังนี้ อัคคีภัย ระบบไฟฟ้าขัดข้อง และระบบปรับอากาศผิดปกติ

(2) มอบหมายเจ้าหน้าที่ผู้รับผิดชอบ เพื่อดำเนินงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน

(3) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม.

(4) รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

- ประเภทของสถานการณ์ฉุกเฉินหรือภัยพิบัติ
- การเตรียมความพร้อม
- การแก้ปัญหา
- ขั้นตอนการปฏิบัติ
- ผู้รับผิดชอบ
- การติดตามประเมินผล

(5) พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติ เพื่อชักซ้อมแผนรับสถานการณ์ อย่างน้อยปีละ 1 กรณี

(6) ติดตามประเมินผล และทบทวน/ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

3.2.2 หน้าที่ของเจ้าหน้าที่ มีข้อปฏิบัติ ดังนี้

- (1) จัดเตรียมอุปกรณ์ที่จำเป็น เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น
- (2) ตรวจสอบความพร้อมของระบบและอุปกรณ์ตามระยะเวลา พร้อมทั้งบันทึกผลการตรวจสอบลงในแบบฟอร์ม โดยมีรายละเอียดอย่างน้อย ดังนี้ วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น และรายงานผลการดำเนินงานต่อคณะทำงาน
- (3) กรณีชักซ้อมแผน/เกิดปัญหา เจ้าหน้าที่จะต้องรายงานข้อเท็จจริงและการแก้ไขปัญหา พร้อมทั้งสรุปผลการปฏิบัติงานและการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ
- (4) บันทึกเหตุการณ์/สถานการณ์ฉุกเฉินที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับกฎหมาย
- (5) สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

