

แผนเตรียมความพร้อมกรณีฉุกเฉิน

สำนักงานปลัดกระทรวงการพัฒนาสังคม

และความมั่นคงของมนุษย์

ประจำปีงบประมาณ พ.ศ. 2569



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



แผนเตรียมความพร้อมกรณีฉุกเฉิน

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ประจำปีงบประมาณ พ.ศ. 2569



สารบัญ

เรื่อง	หน้า
1. ความเป็นมา.....	1
2. วัตถุประสงค์.....	1
3. ขอบเขตการดำเนินงาน.....	2
4. ผลผลิต (Outputs).....	2
5. ผลลัพธ์ที่ต้องการ (Outcomes).....	2
6. ตัวชี้วัดและค่าเป้าหมาย.....	2
7. ผู้รับผิดชอบ.....	2
8. การเตรียมความพร้อม.....	3
9. การแก้ปัญหาจากภัยพิบัติ.....	7
10. การติดตามประเมินผล.....	12



1. ความเป็นมา

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของหน่วยงาน ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจ หน่วยงานจึงควรตระหนักและให้ความสำคัญในการดูแลรักษาข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศให้เกิดความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างต่อเนื่องและมีประสิทธิภาพ ซึ่งปัจจุบันอาจมีสถานการณ์หรือเหตุการณ์ที่ไม่ได้คาดการณ์ล่วงหน้าเกิดขึ้นทั้งจากปัจจัยภายในและปัจจัยภายนอกมากระทบกับการดำเนินงานของหน่วยงาน เช่น ไฟไหม้ การโจรกรรม กระแสไฟฟ้าดับ เป็นต้น ส่งผลให้การใช้ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ข้อมูลหรืออุปกรณ์ที่เกี่ยวข้องถูกทำลาย เกิดความเสียหายถึงขั้นร้ายแรงจนระบบสารสนเทศทั้งหมดไม่สามารถใช้งานต่อไปได้

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) มีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้สนับสนุนและเพิ่มประสิทธิภาพในการปฏิบัติงาน โดยระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้น มีส่วนประกอบสำคัญที่เป็นข้อมูลระบบสารสนเทศ และอุปกรณ์ต่างๆ เป็นจำนวนมาก ดังนั้น สป.พม. จึงมีความจำเป็นที่จะต้องมีการเตรียมความพร้อมกรณีฉุกเฉิน สำหรับเป็นแนวทางในการดำเนินงานเพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น ซึ่งจะช่วยลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อ สป.พม. ได้ ทำให้ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย และสามารถกลับมาดำเนินการได้อย่างปกติหรือตามระดับการให้บริการที่กำหนดไว้ในระยะเวลาที่เหมาะสม

2. วัตถุประสงค์

2.1 เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของ สป.พม.

2.2 เพื่อเป็นแนวทางในการดูแลรักษาข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของ สป.พม. ให้มีความมั่นคงปลอดภัยและมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อลดผลกระทบและความเสียหายที่จะเกิดขึ้นกับข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของ สป.พม. หากเกิดสถานการณ์ฉุกเฉินหรือภัยพิบัติขึ้น



3. ขอบเขตการดำเนินงาน

3.1 พิจารณาแนวทางเพื่อเตรียมความพร้อมรับภัยพิบัติที่เกิดขึ้นกับข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ โดยแนวทางที่กำหนดขึ้นเป็นการเตรียมความพร้อมก่อนเกิดเหตุการณ์ความเสียหายซึ่งมีเนื้อหาครอบคลุมภัยพิบัติที่เกิดจากอัคคีภัย กระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ การโจรกรรม อันส่งผลให้คอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบสารสนเทศ และเครือข่ายหลักเกิดความชำรุดหรือเสียหาย

3.2 พิจารณาแนวทางในการแก้ไขปัญหาเพื่อตอบสนองต่อภัยพิบัติที่เกิดขึ้น

3.3 กำหนดให้มีการทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

4. ผลผลิต (Outputs)

4.1 มีระบบเทคโนโลยีหรืออุปกรณ์ที่รองรับภัยพิบัติที่เกิดขึ้น

4.2 มีการบำรุงรักษาระบบเทคโนโลยีหรืออุปกรณ์ที่รองรับภัยพิบัติอย่างต่อเนื่อง

4.3 มีการแก้ไขปัญหาที่ได้รับผลกระทบจากภัยพิบัติ

5. ผลลัพธ์ที่ต้องการ (Outcomes)

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศสามารถกลับมาใช้งานได้ตามปกติ หากเกิดปัญหาจากภัยพิบัติในเรื่องที่มีการกำหนดภายใต้แผนนี้

6. ตัวชี้วัดและค่าเป้าหมาย

6.1 มีการตรวจสอบความพร้อมของระบบเทคโนโลยีหรืออุปกรณ์ที่รองรับภัยพิบัติรวมทุกระบบ ไม่น้อยกว่าร้อยละ 95

6.2 มีการรายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขทุกครั้งที่เกิดภัยพิบัติ

6.3 มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับเตรียมพร้อมรับภัยพิบัติที่อาจเกิดขึ้นอย่างครบถ้วน

7. ผู้รับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีเจ้าหน้าที่ร่วมดำเนินการตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ประกอบด้วย



7.1 กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร (กทส.)

- | | |
|----------------------------|------------------------------------|
| 1) นายพูนพัฒน์ ชันธาโรจน์ | นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ |
| 2) จำสับเอกฤทธิเดช แสงแจ่ม | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| 3) นายภูวดล เกตุดี | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

7.2 กลุ่มการพัฒนาระบบสารสนเทศ (กพส.)

- | | |
|----------------------------|---------------------------------|
| 1) นางสาวทศวรรณ จันทร์อ่อน | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| 2) นายศรัณยู สวัสดิ์มงคล | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| 3) นายพลสิทธิ มีไปล์ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

7.3 กลุ่มการวิเคราะห์ข้อมูล (กวข.)

- | | |
|-------------------------|---------------------------------|
| 1) นางสาวยุภนันท์ สมปอง | นักพัฒนาสังคมชำนาญการพิเศษ |
| 2) นายปฏิพัทธ์ ก้อมมะณี | เจ้าพนักงานพัฒนาสังคมปฏิบัติงาน |

8. การเตรียมความพร้อม

8.1 การปฏิบัติเพื่อเตรียมรับสถานการณ์จากอัคคีภัย มีดังนี้

- ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร
- ศึกษาวิธีการและขั้นตอนการหนีไฟของอาคาร และถือปฏิบัติอย่างเคร่งครัด
- มีระบบดับเพลิงอัตโนมัติ ซึ่งประกอบด้วยอุปกรณ์ตรวจจับควันหรือความร้อนที่ผิดปกติ

ติดตั้งอยู่ในห้องปฏิบัติการศูนย์ข้อมูลสารสนเทศ (Data Center) สป.พม. หากเกิดเพลิงไหม้จะมี Alarm ซึ่งติดตั้งอยู่บริเวณประตูทางเข้าเป็นตัวส่งสัญญาณในลักษณะของแสงและเสียง มีการตรวจสอบความพร้อมของระบบอย่างน้อย 4 เดือน/ครั้ง

- มีคู่มือระบบดับเพลิงด้วยสารสะอาด (NOVEC1230) และปฏิบัติตามหากเกิดเพลิงไหม้
- มีระบบตรวจจับควันความไวสูงติดตั้งภายในห้อง Data Center สป.พม. หากตรวจพบ

การเปลี่ยนแปลงจะมีการแจ้งเตือนผ่าน SMS และ Line Notification

- มีเครื่องดับเพลิงแบบมือถือชนิดที่ใช้กับอุปกรณ์อิเล็กทรอนิกส์ติดตั้งภายในห้อง Data Center สป.พม. เพื่อการควบคุมเพลิงเบื้องต้น



8.2 การปฏิบัติเพื่อตรวจสอบสภาพแวดล้อมของห้อง Data Center สป.พม. มีดังนี้

- มีการตรวจสอบสภาพแวดล้อมภายในห้องและระบบควบคุมอุณหภูมิ/ความชื้น โดยอุณหภูมิภายในห้อง Data Center สป.พม. จะต้องประมาณ 20 - 25 องศาเซลเซียส และความชื้นประมาณ 40 - 50 เปอร์เซ็นต์ อย่างน้อยสัปดาห์ละ 1 ครั้ง
- มีการตรวจสอบระบบไฟฟ้าอย่างน้อยสัปดาห์ละ 1 ครั้ง

8.3 การปฏิบัติเพื่อเตรียมรับสถานการณ์ที่เกิดจากระบบไฟฟ้าขัดข้อง มีดังนี้

- มีการติดตั้งระบบสำรองและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ให้กับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ภายในห้อง Data Center สป.พม. ซึ่งระบบดังกล่าว ควรสำรองไฟฟ้าเพื่อใช้งานได้นานอย่างน้อย 1 ชั่วโมง และอยู่ในสภาพพร้อมใช้งานเสมอ
- เปิดเครื่องสำรองและปรับแรงดันไฟฟ้าอัตโนมัติตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ภายในห้อง Data Center สป.พม.
- มีการติดตั้งไฟฉุกเฉินเพื่อให้แสงสว่างเมื่อเกิดไฟดับ เพื่อเจ้าหน้าที่จะได้เข้าไปแก้ไขปัญหาได้สะดวก
- มีการตรวจสอบความพร้อมของระบบไฟฟ้าอย่างน้อย 6 เดือน/ครั้ง

8.4 การปฏิบัติเพื่อป้องกันการโจรกรรม มีดังนี้

- มีการติดตั้งระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ทั้งระบบ Access Control และ Access Alarm
- มีการบันทึกการเข้า - ออกห้อง Data Center สป.พม. โดยห้ามบุคคลที่ไม่มีหน้าที่เกี่ยวข้องเข้าไปในห้อง Data Center สป.พม. หรือหากมีความจำเป็น จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- มีการติดตั้งกล้องวงจรปิดที่ห้อง Data Center สป.พม.
- มีระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ในวันหยุดหรือนอกเวลาราชการ



8.5 การปฏิบัติเพื่อป้องกันการละเมิดระบบสารสนเทศ มีดังนี้

- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยของเครือข่าย เช่น Firewall ในส่วนต่าง ๆ ของเครือข่าย กำหนดค่าและดำเนินการตรวจสอบข้อมูลต่างๆ (Log) ของอุปกรณ์ Firewall และ IDS/IPS
- มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และลูกข่าย ที่มีการเข้าถึงเครือข่าย
- ดำเนินการตามนโยบายที่เกี่ยวข้อง ดังนี้
 - ประกาศสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง การใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต พ.ศ. 2553 (ประกาศ ณ วันที่ 21 กรกฎาคม 2553)
 - ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง นโยบายในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2557
 - แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวง การพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. 2569

8.6 การปฏิบัติเพื่อป้องกันการโจรกรรมข้อมูล มีดังนี้

- มีการรณรงค์ ส่งเสริมให้ความรู้กับผู้ใช้งานในการปฏิบัติตนเพื่อป้องกันการถูกโจรกรรมข้อมูล
- มีการติดตั้งโปรแกรมป้องกันไวรัส และ Patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต
- มีการติดตั้ง Patch ของระบบปฏิบัติการทุกสัปดาห์
- เปลี่ยนรหัสผ่านตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ หรือทุก 6 เดือน
- มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานอย่างสม่ำเสมอ
- ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคง ของมนุษย์
- ทำการสำรองข้อมูลระบบฐานข้อมูล ตามแผนการสำรองและทดสอบกู้คืนข้อมูล



8.7 การปฏิบัติเพื่อเตรียมความพร้อมสำหรับการกู้คืนระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์หลัก มีดังนี้

- ผู้รับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่เสนอแผนการสำรองและทดสอบกู้คืนข้อมูล ตลอดจนปฏิบัติงานตามแผนที่กำหนดไว้ โดยมีเจ้าหน้าที่ร่วมดำเนินการประกอบด้วย

1) กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร (กทส.)

- | | |
|----------------------------|------------------------------------|
| (1) นายพูนพัฒน์ ชันธาโรจน์ | นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ |
| (2) จ.ส.อ.ฤทธิเดช แสงแจ่ม | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| (3) นายภูวดล เกตุดี | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

2) กลุ่มการพัฒนาระบบสารสนเทศ (กพส.)

- | | |
|-------------------------------|---------------------------------|
| (1) นางสาวทัศนวรรณ จันทร์อ่อน | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| (2) นายศรัณยู สวัสดิ์มงคล | เจ้าพนักงานสื่อสารชำนาญงาน |
| (3) นายพลสิทธิ มีโป่ง | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

3) กลุ่มการวิเคราะห์ข้อมูล (กวข.)

- | | |
|--------------------------|---------------------------------|
| (1) นางสาวยุคนันท์ สมปาง | นักพัฒนาสังคมชำนาญการพิเศษ |
| (2) นายปฏิพัทธ์ ก้อมมะณี | เจ้าพนักงานพัฒนาสังคมปฏิบัติงาน |

- จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น สำหรับเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน ในกรณีระบบสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ เช่น

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานที่สำคัญ
- แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus
- แผ่น Driver อุปกรณ์ต่างๆ

- เอกสารที่เกี่ยวข้อง เช่น คู่มือในการติดตั้ง - กู้คืนระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์หลัก รายการซอฟต์แวร์และฮาร์ดแวร์ รายละเอียดการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น ผังเครือข่าย เป็นต้น ทั้งนี้ ให้เก็บแยกไว้ต่างหากจากห้อง Data Center สป.พม.



- กำหนดรายละเอียดการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนเครื่องเดิมที่เสียหาย ในกรณีที่มีเครื่องคอมพิวเตอร์/อุปกรณ์เสียหาย ให้ทำการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ใหม่มาทดแทนภายในระยะเวลา 15 วันทำการ โดยกำหนดให้มีคุณสมบัติของเครื่อง ให้เทียบเท่าหรือสูงกว่าเครื่องคอมพิวเตอร์/อุปกรณ์เดิมที่เสียหาย หลังจากนั้นให้ทำการติดตั้งซอฟต์แวร์ระบบสารสนเทศและระบบฐานข้อมูลให้เรียบร้อยภายในเวลา 3 วันทำการ

- หลังจากการกู้คืนระบบเสร็จสมบูรณ์แล้ว ให้ผู้มีหน้าที่ดูแลรับผิดชอบระบบงานสารสนเทศ ที่ได้กู้คืน ทำการตรวจสอบความถูกต้องอีกครั้ง

9. การแก้ปัญหาจากภัยพิบัติ

9.1 การปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์อัคคีภัย มีดังนี้

- ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว (ในกรณีที่ไม่ได้เป็นระบบอัตโนมัติ) เปิดสัญญาณเตือนภัย และปฏิบัติตามแผนการซักซ้อมการหนีไฟอย่างเคร่งครัด
- รับขนย้ายอุปกรณ์ที่จำเป็นไปไว้ในที่ปลอดภัย
- ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด หากพบว่ามีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง มาเปลี่ยนโดยเร็วที่สุด
- รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

9.2 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากระบบไฟฟ้าขัดข้อง มีดังนี้

- กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
- ประสานขอข้อมูลสาเหตุของไฟฟ้าดับ และระยะเวลาดำเนินการแก้ไข
- รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ



9.3 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากระบบควบคุมอุณหภูมิ/ความชื้นขัดข้อง มีดังนี้

- กรณีระบบควบคุมอุณหภูมิ/ความชื้นขัดข้อง จะต้องตัดการเชื่อมต่อระบบเครือข่าย โดยการปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายตามลำดับความสำคัญ
- จัดสถานที่และสภาพแวดล้อมให้มีการถ่ายเทอากาศ ให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถทำงานได้เป็นปกติ
- ติดต่อประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบควบคุมอุณหภูมิ/ความชื้น เพื่อดำเนินการแก้ไขโดยเร็วที่สุด
- รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

9.4 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากการละเมิดระบบสารสนเทศ มีดังนี้

- หากพบว่ามี การบุกรุกจากภายในระบบ ให้ตรวจสอบแหล่งกระทำผิด ระบุและปิดกั้นการเชื่อมต่อเครือข่าย หาผู้ละเมิด แจ้งเตือนให้ผู้รับผิดชอบระบบอื่นๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด ปรับแก้ไข รายงานผู้บังคับบัญชา และลงโทษตามประกาศสำนักงานปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เรื่อง การใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต พ.ศ. 2553 (ประกาศ ณ วันที่ 21 กรกฎาคม 2553) ในความผิดที่ไม่ร้ายแรง ส่วนกรณีที่เกิดความเสียหายร้ายแรงแก่ทางราชการ หรือเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ให้ลงโทษทางกฎหมาย
- หากพบว่ามี การบุกรุกจากภายนอก ระบบ ให้ประสานหน่วยงานที่เกี่ยวข้องหาแหล่งกระทำผิด ระบุและปิดกั้นการเข้าถึงระบบทุกกรณี โดยการกำหนดค่าที่อุปกรณ์ Router หรือ Firewall แจ้งเตือนให้ผู้รับผิดชอบระบบอื่นๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด แก้ไขจุดอ่อนที่เป็นสาเหตุ รายงานผู้บังคับบัญชา ดำเนินการตามกฎหมายกรณีที่เกิดความเสียหายร้ายแรงแก่ทางราชการ หรือเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ถ้าสามารถดำเนินการได้)
- หากพบการแพร่กระจายของไวรัสคอมพิวเตอร์ ให้ดำเนินการตรวจสอบและแยกแหล่งแพร่กระจายของไวรัสออกจากเครือข่ายหลัก โดยระบุการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่ตรวจพบ ดำเนินการตรวจสอบและแก้ไขข้อบกพร่องที่เป็นสาเหตุ เช่น การ Update Patch หรือ Service Pack ของระบบปฏิบัติการ การ Update Virus Signature และการ Scan Malware



9.5 กรณีที่ห้อง Data Center สป.พม. ไม่สามารถให้บริการได้ ต้องมีการเตรียมจัดหาระบบศูนย์สำรองระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Site : DR-Site) โดยต้องจัดหาครุภัณฑ์คอมพิวเตอร์ที่มีคุณลักษณะที่จำเป็น ประกอบด้วย

1) เครื่องคอมพิวเตอร์แม่ข่าย จำนวน 4 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีหน่วยประมวลผลกลาง (CPU) แบบ 14 แกนหลัก (14 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.2 GHz จำนวนไม่น้อยกว่า 2 หน่วย
- หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory ไม่น้อยกว่า 18 MB
- มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 192 GB
- สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5
- มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SCSI หรือ SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที หรือ ชนิด Solid State Drive หรือดีกว่า และมีความจุไม่น้อยกว่า 600 GB จำนวนไม่น้อยกว่า 4 หน่วย
- มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- มีจอภาพแบบ LED หรือดีกว่า ขนาดไม่น้อยกว่า 21 นิ้ว จำนวน 1 หน่วย
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

2) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลแบบภายนอก (External Storage) ซึ่งสามารถทำงานในระบบ SAN (Storage Area Network) ได้
- มีส่วนควบคุมอุปกรณ์ (Controller) แบบ Dual Controller มี Cache memory ของระบบรวมไม่น้อยกว่า 16 GB



- มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SATA หรือ SAS หรือดีกว่า ขนาดความจุไม่น้อยกว่า 900 GB และมีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อวินาที จำนวนไม่น้อยกว่า 24 หน่วย
- สามารถทำงาน แบบ Raid ไม่น้อยกว่า Raid 0, 1, 5

3) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
- มี Firewall Throughput ไม่น้อยกว่า 25 Gbps
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง
- สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment ได้เป็นอย่างดี
- สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- สามารถทำงานลักษณะ Transparent Mode ได้
- สามารถ Routing แบบ Static, Dynamic Routing ได้
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างดี
- สามารถเก็บและส่งรายละเอียด ตลอดจนตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

4) อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 24 ช่อง จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model
- สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้เป็นอย่างดี



- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10 Gbps (SFP/SFP+) จำนวนไม่น้อยกว่า 2 ช่อง
- มีสัญญาณไฟแสดงสถานะการทำงานของช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างดีน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

5) อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีสัญญาณไฟแสดงสถานะการทำงานของช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างดีน้อย
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

6) เช้าพื้นที่ตู้ Rack สำหรับวางระบบคอมพิวเตอร์ (Rack Data Center Co-location) ขนาด 42U โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีหมายเลข Public IP Address รุ่น 4 (IPv4) จำนวนไม่น้อยกว่า 4 หมายเลข
- มีหมายเลข Public IP Address รุ่น 6 (IPv6) จำนวนไม่น้อยกว่า 1,000 หมายเลข
- มีเต้าเสียบไฟฟ้าจำนวนไม่น้อยกว่า 16 เต้าเสียบ
- มีช่องเชื่อมต่อระบบเครือข่ายพร้อมใช้งานระบบอินเทอร์เน็ต แบบ 10/100 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง



- มีระบบกล้องวงจรปิด พร้อมระบบบันทึกภาพ ระบบควบคุมประตูเข้า - ออก (Access Control) ระบบไฟฟ้าสำรอง ระบบปรับอากาศและควบคุมความชื้น ระบบตรวจจับควันไฟ ระบบดับเพลิง และระบบตรวจจับน้ำรั่วซึม

10. การติดตามประเมินผล

10.1 ตรวจสอบจากเอกสารรายงานการบำรุงรักษาว่ามีการดำเนินงานครบถ้วนหรือไม่ ในกรณีที่มีปัญหาเกิดขึ้นจะต้องแสดงรายละเอียดเกี่ยวกับปัญหาและวิธีการแก้ปัญหา โดยที่เอกสารดังกล่าวจะต้องผ่านการตรวจสอบจากเจ้าหน้าที่ผู้รับผิดชอบ

10.2 ตรวจสอบอุปกรณ์ที่จำเป็นที่ได้จัดเตรียมไว้สำหรับเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นว่ามีความครบถ้วนหรือไม่ โดยจัดทำเป็นบันทึกผลการตรวจสอบ ซึ่งแสดงให้เห็นถึงผลการดำเนินงานในเรื่องดังกล่าว เช่น วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น

10.3 ตรวจสอบระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ในวันหยุดหรือนอกเวลาราชการ ว่าได้ดำเนินการครบถ้วนหรือไม่ หากพบว่าไม่เป็นไปตามแนวทางที่กำหนด ให้จัดทำเอกสารรายงานต่อผู้รับผิดชอบในเรื่องดังกล่าว เพื่อดำเนินการแก้ไขต่อไป

10.4 ในกรณีที่เกิดปัญหาดังกล่าวมาแล้วในข้อ 9 จะต้องตรวจสอบว่าได้ดำเนินการแก้ไขปัญหานั้นหรือไม่ โดยการตรวจสอบจากเอกสารรายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

10.5 สรุปผลการดำเนินงานรายปี โดยการวิเคราะห์ผลการปฏิบัติงานให้ผู้บังคับบัญชารับทราบ มีประเด็นต่างๆ อย่างน้อย ดังนี้

- สรุปผลการดำเนินงาน
- ปัญหาอุปสรรคและวิธีการแก้ไข (ถ้ามี)
- ข้อเสนอแนะ



ภาคผนวก

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

การสำรองและทดสอบกู้คืนข้อมูล

วัตถุประสงค์

เพื่อให้หน่วยงานมีระบบสำรองข้อมูลและสารสนเทศที่เหมาะสม และมีการเตรียมความพร้อมกรณีฉุกเฉิน หากไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้หน่วยงานสามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะทำงาน** หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. **เจ้าหน้าที่** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นประธาน
- 1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

2. การสำรองและทดสอบกู้คืนข้อมูล

- 2.1 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของ สป.พม.
- 2.2 พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นตามลำดับความสำคัญ เพื่อจัดทำระบบสำรอง
- 2.3 กำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง
- 2.4 กำหนดสื่อที่ใช้ในการเก็บข้อมูล และรูปแบบของการสำรองข้อมูล ซึ่งมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

2.5 รายการที่ต้องสำรองข้อมูลและความถี่อย่างน้อย 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

2.6 มีการสำรองข้อมูลเครื่องแม่ข่ายทั้งระบบ (Full System Backup) อย่างน้อยปีละ 1 ครั้ง

2.7 กำหนดขั้นตอนปฏิบัติและโปรแกรมในการสำรองข้อมูลและทดสอบกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง

2.8 กำหนดการเข้ารหัสข้อมูลในการสำรองข้อมูลที่สำคัญ โดยใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.9 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูลที่เหมาะสมกับสำคัญของแต่ละระบบสารสนเทศ

2.10 รายละเอียดที่ปรากฏในแผนการสำรองและทดสอบกู้คืนข้อมูล ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

- รายการที่ต้องสำรองข้อมูล
- การสำรองข้อมูล
- การทดสอบกู้คืนข้อมูล
- ปฏิทินการสำรองและทดสอบกู้คืนข้อมูล
- ผู้รับผิดชอบ
- การติดตามประเมินผล

2.11 มอบหมายเจ้าหน้าที่หลักเพื่อดำเนินงานตามแผนการสำรองและทดสอบกู้คืนข้อมูล และเจ้าหน้าที่สำรองเพื่อทำหน้าที่สำรองข้อมูลในกรณีที่เจ้าหน้าที่หลักไม่สามารถปฏิบัติงานได้ โดยเจ้าหน้าที่มีหน้าที่ ดังนี้

2.11.1 จัดทำคู่มือการสำรองและทดสอบกู้คืนข้อมูล

2.11.2 ดำเนินการตามปฏิทินการสำรองและทดสอบกู้คืนข้อมูล

2.11.3 บันทึกการสำรองข้อมูล (Operator Logs) และจัดทำรายงานผลการสำรองข้อมูลประจำเดือน โดยมีรายละเอียดอย่างน้อย ดังนี้ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

2.11.4 กรณีพบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปลผลการแก้ไขปัญหา และรายงานให้ผู้บังคับบัญชาทราบ

2.11.5 ตรวจสอบผลการสำรองข้อมูลว่าถูกต้องและสมบูรณ์ พร้อมทั้งบันทึกผลการตรวจสอบ

2.11.6 จัดเก็บสื่อบันทึกข้อมูลไว้ในที่ที่ปลอดภัย

2.11.7 มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล

2.11.8 มีการทดสอบกู้คืนข้อมูลจากข้อมูลที่สำรองเก็บไว้ อย่างน้อยปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

2.11.9 กรณีพบปัญหาที่สร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนทำให้ต้องกู้คืนระบบ เจ้าหน้าที่จะต้องดำเนินการแก้ไขปัญหา พร้อมทั้งสรุปรายงานการปฏิบัติงาน และการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

2.11.10 การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

2.11.11 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความก้าวหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

2.11.12 สรุปรผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงาน และรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปรผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

2.12 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล ปีละ 1 ครั้ง

3. การเตรียมความพร้อมกรณีฉุกเฉิน

3.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม.

3.2 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของ สป.พม. โดยมีสถานการณ์อย่างน้อย ดังนี้ อัคคีภัย ระบบไฟฟ้าขัดข้อง และระบบปรับอากาศผิดปกติ

3.3 รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

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

3.4 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติ เพื่อซักซ้อมแผนรับสถานการณ์ อย่างน้อยปีละ 1 กรณี

3.5 มอบหมายเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยเจ้าหน้าที่มีหน้าที่ ดังนี้

3.5.1 จัดเตรียมอุปกรณ์ที่จำเป็น เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่อาจจะเกิดขึ้น

3.5.2 ตรวจสอบและบันทึกผลการตรวจสอบความพร้อมของระบบและอุปกรณ์ตามระยะเวลา พร้อมทั้งจัดทำรายงานผลการดำเนินงาน โดยมีรายละเอียดอย่างน้อย ดังนี้ วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 5 : การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	แก้ไขล่าสุด : ต.ค. 68
	เรื่องที่ 1 : การสำรองและทดสอบกู้คืนข้อมูล	รหัสเอกสาร : IC-0501

3.5.3 กรณีชักซ้อมแผน/เกิดปัญหา เจ้าหน้าที่จะต้องรายงานข้อเท็จจริงและการแก้ไขปัญหา พร้อมทั้งสรุปผลการปฏิบัติงานและการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

3.5.4 บันทึกเหตุการณ์/สถานการณ์ฉุกเฉินที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อใช้ในการกรณีที่เหตุการณ์มีความเกี่ยวข้องกับทางกฎหมาย

3.5.5 สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้ สรุปผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไข และข้อเสนอแนะ

3.6 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง



ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗

โดยที่พระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ ได้กำหนดให้ หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับ หน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำมีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐดำเนินการ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานในสังกัด เป็นไปในทิศทางเดียวกัน กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ จึงเห็นควรกำหนดแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗”

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

หน่วยงาน หมายความว่า หน่วยงานในสังกัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับ ความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงานของรัฐนั้นๆ

(๓) กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๕ นโยบายการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๖ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และมีการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗ นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในกรณีที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสม เพื่อป้องกันการไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในกรณีที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๕๔

ข้อ ๘ นโยบายการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ที่ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ที่ใช้ที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๑ นโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๒ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อยดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๓ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบเทคโนโลยีสารสนเทศ

และการสื่อสารของหน่วยงานเกิดความเสียหาย หรือเป็นอันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตามแนวทางต่อไปนี้

(๑) ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

(๒) ผู้อำนวยการสำนัก/กอง/ศูนย์ หรือเทียบเท่า ที่รับผิดชอบการบริหารงานด้านสารสนเทศของหน่วยงาน มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยกำหนดมาตรการ และกำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานต้องจัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวง

ข้อ ๑๕ หน่วยงานต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๓ พฤศจิกายน พ.ศ. ๒๕๕๗



(นายวิเชียร ขวาลิต)

ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

สำนักงานปลัดกระทรวงการพัฒนาสังคม และความมั่นคงของมนุษย์

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร