
# แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
# (Business Continuity Plan : BCP)
# สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
# ประจำปีงบประมาณ พ.ศ. ๒๕๖๘


# แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
# (Business Continuity Plan : BCP)
# สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
# ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

**สารบัญ**

## ๑. บทนำ

ในยุคที่องค์กรต้องขับเคลื่อนภารกิจสำคัญและพึ่งพาการใช้ระบบเทคโนโลยีสารสนเทศเป็นอย่างสูง ความต่อเนื่องในการดำเนินการตามภารกิจจึงมีความสำคัญอย่างยิ่ง สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้มีการพัฒนาระบบเทคโนโลยีสารสนเทศที่ทันสมัยเพื่อสนับสนุนการปฏิบัติงานแก่บุคลากร สคร. เพื่อให้ สคร. บรรลุภารกิจในการ “บริหารและพัฒนารัฐวิสาหกิจและหลักทรัพย์ของรัฐ โดยการเสนอแนะนโยบายและมาตรการกำกับดูแลการประเมินผล และการพัฒนารัฐวิสาหกิจ เพื่อเพิ่มประสิทธิภาพรัฐวิสาหกิจและสร้างมูลค่าเพิ่มให้แก่ทรัพย์สินของรัฐ พร้อมทั้งส่งเสริมและสนับสนุนการให้เอกชนร่วมลงทุนในกิจการของรัฐ” อีกทั้งให้การสนับสนุนการบริหารจัดการภายในของ สคร. ทั้งนี้ เพื่อรับมือกับความเสี่ยงจากเหตุการณ์ที่ไม่อาจคาดการณ์ได้ เช่น โรคระบาด ภัยจากมนุษย์ เช่น การโจมตีทางไซเบอร์ หรือภัยธรรมชาติ เช่น อุทกภัย วาตภัย หรือแผ่นดินไหว ซึ่งอาจส่งผลกระทบโดยตรงต่อโครงสร้างพื้นฐานด้านสารสนเทศ รวมถึงข้อมูลสารสนเทศของ สคร. ให้ไม่สามารถให้บริการได้อย่างต่อเนื่อง ประกอบกับประกาศ สคร. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ สามารถให้บริการแก่ผู้ใช้งาน (User) ได้อย่างต่อเนื่องและมีประสิทธิภาพ ตลอดจนสามารถปฏิบัติงานตามภารกิจของ สคร. ได้ตามเป้าหมายที่กำหนดไว้

ดังนั้น ศทส. จึงได้วิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ โดยพิจารณาจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) ภัยพิบัติ หรือสถานการณ์อื่นๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต การสำรองและกู้คืนข้อมูลสารสนเทศ (Diaster Recovery Plan) กระบวนการบริหารจัดการเหตุการณ์ (Incident Management Process) เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. (Business Continuity Plan) สำหรับใช้เป็นแนวทางในการปฏิบัติงาน ดำเนินการซักซ้อมและให้ความรู้แก่บุคลากร สคร. ในส่วนที่เกี่ยวข้องต่อไป

แผนบริหารความต่อเนื่องด้านสารสนเทศฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางในการเตรียมพร้อมรับมือ และฟื้นฟูระบบสารสนเทศในกรณีเกิดเหตุฉุกเฉิน โดยมีเป้าหมายเพื่อให้ภารกิจของ สคร. สามารถดำเนินต่อไปได้อย่างราบรื่น หรือกลับสู่สภาวะปกติในระยะเวลาที่สั้นที่สุด เพื่อลดความเสียหายที่อาจเกิดขึ้น ศทส. หวังเป็นอย่างยิ่งว่าแผนฉบับนี้จะช่วยเสริมสร้างความมั่นใจในความพร้อมด้านสารสนเทศของ สคร. ในการเผชิญกับทุกสถานการณ์ ทั้งจากเหตุสุดวิสัยและภัยธรรมชาติที่อาจเกิดขึ้นในอนาคต และเพื่อให้หน่วยงานที่เกี่ยวข้อง ประชาชน เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของระบบสารสนเทศ ของ สคร.

## ๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศของ สคร.

๒.๒ เพื่อให้สามารถเตรียมความพร้อมในการรับมือในสภาวะวิกฤตที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศได้อย่างเป็นระบบ รวมถึงมีแนวปฏิบัติในการบริหารจัดการ กำกับ ตรวจสอบ และดูแลรักษาระบบคอมพิวเตอร์และระบบสารสนเทศ ให้มีความมั่นคง ปลอดภัย มีเสถียรภาพ และพร้อมใช้งานตลอดเวลา

๒.๓ เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือให้บริการ เพื่อให้มีแนวทางในการสำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

๒.๔ เพื่อกำหนดแนวปฏิบัติงานเมื่อเกิดสถานการณ์วิกฤตจากเหตุการณ์ที่ไม่อาจคาดการณ์ได้ เช่น โรคระบาด ภัยจากมนุษย์ เช่น การโจมตีทางไซเบอร์ หรือภัยธรรมชาติ เช่น อุทกภัย วาตภัย หรือแผ่นดินไหว ซึ่งอาจส่งผลกระทบโดยตรงต่อโครงสร้างพื้นฐานด้านสารสนเทศ และเป็นการบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้

๒.๕ เพื่อให้หน่วยงานที่เกี่ยวข้อง ประชาชน เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของระบบสารสนเทศ ของ สคร. แม้จะต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

## ๓. สมมติฐานของแผนบริหารความต่อเนื่อง

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. ฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

๓.๑ เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่างๆ แต่มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้

๓.๒ ศทส. รับผิดชอบการประสานงานเพื่อสำรองระบบสารสนเทศต่างๆ โดยระบบสำรองสารสนเทศมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก

๓.๓ เหตุการณฉุกเฉินที่เกิดขึ้นไมไดสงผลกระทบตอสถานที่พำนักของบุคลากร สคร.

๓.๔ บุคลากร ที่ระบุในเอกสารฉบับนี้ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว

**หมายเหตุ:** สคร. ติดตั้งระบบสำรองข้อมูลเพื่อการสำรองข้อมูลสารสนเทศไว้ที่ห้องศูนย์ข้อมูล (Data Center) ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง (สป.กค.) จ. ปทุมธานี ซึ่งมีระบบรักษาความปลอดภัยที่มีมาตรฐาน มีการควบคุมการเข้าถึงอย่างเข้มงวด และมีการสำรองข้อมูลแบบอัตโนมัติเฉพาะส่วนที่มีการเพิ่มขึ้น (Incremental Backup) และส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน และสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ซึ่งหากระบบเกิดเหตุฉุกเฉิน ขัดข้อง หรือข้อมูลเกิดการสูญหาย ยังสามารถกู้คืนให้นำกลับมาใช้งานได้โดยเร็ว และผู้ดูแลระบบ (Administrator) ของ ศทส. สคร. จะต้องประสานงานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ในกรณีฉุกเฉินต่างๆ ต่อไป

**๔. ขอบเขต**

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของ สคร. ฉบับนี้ เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤตในพื้นที่ สคร. ณ อาคาร ๑๕๐ ปี กระทรวงการคลัง และ ณ ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี ดังนี้

๔.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.

๔.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี

๔.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)*

๔.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค*

๔.๕ เหตุการณ์ไฟฟ้าดับ*

๔.๖ เหตุการณ์อัคคีภัย*

๔.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย แผ่นดินไหว และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง*

๔.๘ เหตุการณ์ที่เกิดจากโรคระบาดต่อเนื่อง

**หมายเหตุ *** เหตุเกิด ณ ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี

**๕. การทบทวนแผนบริหารความต่อเนื่อง**

แผนบริหารความต่อเนื่องฉบับนี้ ต้องได้รับการทบทวนและซ้อมแผนอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าแผนสอดคล้องกับสถานการณ์ปัจจุบัน และสามารถนำมาใช้ได้อย่างมีประสิทธิภาพ

**๖. การวิเคราะห์ทรัพยากรที่สำคัญ**

เพื่อให้ ศทส. สามารถบริหารจัดการการดำเนินงานให้มีความต่อเนื่อง จึงได้พิจารณาจากผลกระทบต่อทรัพยากร ๕ ด้าน ดังนี้

๖.๑ ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว

๖.๒ ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้น ทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญหรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้

๖.๓ ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยีหรือระบบสารสนเทศหรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

๖.๔ ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

๖.๕ ผลกระทบด้านคู่ค้า/ ผู้ให้บริการที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

ตารางสรุปการวิเคราะห์ผลกระทบของทรัพยากรต่อเหตุการณ์สภาวะวิกฤต

| เหตุการณ์สภาวะวิกฤต | | ผลกระทบ | | | | |
|---|---|---|---|---|---|---|
| | | ด้านอาคาร/สถานที่ปฏิบัติงาน | ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาวัสดุอุปกรณ์ที่สำคัญ | ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ | ด้านบุคลากรหลัก | คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย |
| ๑ | เหตุการณ์อุทกภัย/วาตภัย | ✓ | ✓ | ✓ | ✓ | ✓ |
| ๒ | เหตุการณ์อัคคีภัย | ✓ | ✓ | ✓ | ✓ | ✓ |
| ๓ | เหตุการณ์ไฟฟ้าดับในวงกว้าง | ✓ | ✓ | ✓ | ✓ | ✓ |
| ๔ | เหตุการณ์ชุมนุมประท้วง/จลาจล/เหตุการณ์ก่อการร้าย | ✓ | ✓ | ✓ | ✓ | ✓ |
| ๕ | เหตุการณ์อาชญากรรมไซเบอร์ (Cybercrime) | | ✓ | ✓ | ✓ | ✓ |
| ๖ | เหตุการณ์โรคระบาดต่อเนื่อง | | | | ✓ | ✓ |
| ๗ | เหตุการณ์แผ่นดินไหว | ✓ | ✓ | ✓ | ✓ | ✓ |

แผนความต่อเนื่อง (BCP) ฉบับนี้ไม่รองรับการปฏิบัติงาน ในกรณีที่เหตุขัดข้องเกิดขึ้นจากการดำเนินงานปกติและเหตุขัดข้อง ดังกล่าว ไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของ สคร. เนื่องจาก ศทส. ยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้อำนวยการ ศทส. และผู้บริหารของแต่ละกลุ่มงาน/ฝ่าย สามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

## ๗. การวิเคราะห์ความเสี่ยงด้านสารสนเทศ

เนื่องจาก สคร. มีภารกิจในการบริหารและพัฒนารัฐวิสาหกิจและหลักทรัพย์ของรัฐ โดยการเสนอแนะนโยบายและมาตรการการกำกับดูแล การประเมินผลและการพัฒนารัฐวิสาหกิจ เพื่อเพิ่มประสิทธิภาพรัฐวิสาหกิจและสร้างมูลค่าเพิ่มให้แก่ทรัพย์สินของรัฐ พร้อมทั้งส่งเสริมและสนับสนุนการให้เอกชนร่วมลงทุนในกิจการของรัฐ สคร. จึงได้นำระบบคอมพิวเตอร์และระบบสารสนเทศเข้ามาสนับสนุนและอำนวยความสะดวกในการปฏิบัติงาน ซึ่งระบบดังกล่าวจำเป็นต้องมีการวิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ รวมถึงมีแผนการบริหารความต่อเนื่อง เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤต ลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น อันจะส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีความมั่นคงปลอดภัย และเกิดประโยชน์สูงสุดแก่การปฏิบัติราชการ

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีดังนี้

๗.๑ ความเสี่ยงที่เกิดจากบุคคล ดังนี้

๗.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. หมายถึง บุคลากรของ สคร. ขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ด้านซอฟต์แวร์ และด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ไม่เหมาะสม

๗.๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี หมายถึง ผู้ที่ก่อกวน เจาะทำลายระบบเพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ หากไม่ได้รับการป้องกันด้วยเครื่องมือหรืออุปกรณ์ที่มีมาตรฐานและอัพเดทให้ทันสมัย เช่น Firewall ระบบ IPS และระบบป้องกันไวรัส

๗.๑.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) หมายถึง ผู้ที่ลักลอบเข้าไปโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) หากศูนย์ข้อมูลดังกล่าวไม่ได้รับการป้องกันที่ดี เช่น มาตรการในการเข้าถึงห้องศูนย์ข้อมูล (Data Center) กล้องวงจรปิด และเจ้าหน้าที่รักษาความปลอดภัย เป็นต้น

๗.๒ ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ในห้องศูนย์ข้อมูล (Data Center) ทำงานไม่เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูล (Process Device) ชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบปรับอากาศชำรุดส่งผลให้อุณภูมิห้องศูนย์ข้อมูล (Data Center) สูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ที่ให้บริการหยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้ หรืออาจได้รับความเสียหาย หรือเกิดเหตุให้สาย fiber optic ขาด หรือ switch ในการรับสัญญาณเสียหาย บุคลากร สคร. ก็จะไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศรวมถึงระบบอินเทอร์เน็ตได้

๗.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

๗.๓.๑ เหตุการณ์ไฟฟ้าดับ หมายถึง ภัยที่เกิดจากไฟฟ้าดับ ซึ่งอาจส่งผลให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี ไม่มีแหล่งจ่ายพลังงานอื่นๆ ที่ใช้ในการเปิดระบบคอมพิวเตอร์เพื่อให้ผู้ดูแลระบบสารสนเทศเปิดใช้งานระบบ และให้บริการระบบสารสนเทศได้เป็นปกติ เช่น สายไฟฟ้าขาด ไฟฟ้าช็อต หม้อแปลงไฟฟ้าระเบิดจนเกิดความเสียหาย

๗.๓.๒ เหตุการณ์อัคคีภัย หมายถึง ภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้างความเสียหายร้ายแรงที่สุด ทำให้อาคารห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ถูกไฟไหม้จนทำให้ไม่สามารถปฏิบัติงานได้ ซึ่งเกิดได้หลายสาเหตุ เช่น ไฟฟ้าลัดวงจร หรือไฟไหม้บริเวณอื่นแล้วไหม้ลุกลามมาที่ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี

๗.๓.๓ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย เหตุการณ์ที่เกิดจากแผ่นดินไหว และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง ซึ่งอาจเกิดผลกระทบโดยตรงต่อการเข้าปฏิบัติงานภายในพื้นที่ สคร.

๗.๔ เหตุการณ์ที่เกิดจากโรคระบาดต่อเนื่อง ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่จะเกิดผลกระทบต่อการเข้าไปปฏิบัติงานภายในพื้นที่ สคร.

**๘. การประเมินความเสี่ยงด้านสารสนเทศ**

ศทส. ได้ประเมินความเสี่ยงด้านสารสนเทศจากความเสี่ยงที่เกิดจากบุคคล จากด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ในข้อ ๔ และ ๗ มาเป็นแนวทางในการดำเนินงาน โดยผู้ดูแลระบบ (Administrator) ของ ศทส. จะเป็นผู้ประสานงานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ซึ่งได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของ สคร. แล้ว ปรากฏดังนี้

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๑. เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. | - ระบบคอมพิวเตอร์ติดไวรัส ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผลข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้<br>- ข้อมูลเกิดการรั่วไหล | ๕ | ๑ | ๕ | ค่อนข้างต่ำ | - ผู้ดูแลระบบ (Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่ายภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว<br>- หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)<br>- จัดให้มีการซักซ้อมความเข้าใจและดำเนินการให้ความรู้แก่บุคลากร สคร.<br>- จัดให้มีการซักซ้อมสถาณการณ์เสมือนจริง |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๒. เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี | - ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบ หน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศล่มได้ | ๓ | ๔ | ๑๒ | ค่อนข้างสูง | - ผู้ดูแลระบบ (Administrator) พบเหตุ และตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อ จากนั้นให้ปิดพอร์ตที่ไม่ได้ใช้งานโดยทันทีรวมถึงปิดบัญชีหรือเปลี่ยนรหัสผ่านผู้ใช้งานที่ถูกละเมิด<br>- ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหายและรายงานให้ผู้อำนวยการ ศทส. ทราบและรายงานตามลำดับชั้นเพื่อสั่งการต่อไป<br>- ผู้ดูแลระบบ (Administrator) ทำการกู้คืนระบบตรวจสอบผลการกู้คืนข้อมูล และรายงานความสำเร็จให้ผู้อำนวยการ ศทส. ทราบต่อไป<br>- ผู้ดูแลระบบ (administrator) ตรวจสอบการรั่วไหลหรือข้อมูลส่วนบุคคลสูญหายว่ามีหรือไม่ หากพบว่ามี ให้แจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ รวมถึงสรุปความเสียหายและผลกระทบที่อาจจะเกิดขึ้นภายใน ๗๒ ชั่วโมง ซึ่งแนวทางให้เป็นไปตามกฎหมาย PDPA |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๓. เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) | - อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ สคร. โดยเฉพาะข้อมูลที่เป็นความลับ<br>- ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถให้บริการได้เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | - เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. พบเหตุและแจ้งให้ผู้ดูแลระบบ (Administrator) ของ ศทส. ทราบ เพื่อรายงานให้ผู้อำนวยการ ศทส. ทราบและรายงานตามลำดับชั้นและสั่งการต่อไป<br>- ผู้ดูแลระบบ (Administrator) ของ ศทส. ร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ร่วมกันตรวจสอบความครบถ้วนและความเสียหายของอุปกรณ์ประมวลผลข้อมูล (Process Device) และผลกระทบต่อระบบคอมพิวเตอร์ระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ และดำเนินการติดต่อบริษัทฯ หรือ Vender ที่รับผิดชอบเพื่อจัดหาอุปกรณ์ทดแทนหรือกู้คืนระบบสารสนเทศต่อไป |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๔. เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค | - ระบบหรือบริการออนไลน์ไม่สามารถเข้าถึงได้ (Downtime)<br>- สคร. ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติ<br>- ความเสียหายต่อระบบปฏิบัติการ เซิร์ฟเวอร์ ฐานข้อมูล เช่น ซอฟต์แวร์สำคัญล่มหรือทำงานผิดปกติ ไฟล์ข้อมูลเสียหายหรือถูกเปลี่ยนแปลง<br>- ข้อมูลสำรองไม่สามารถกู้คืนได้<br>- เกิดเหตุให้สาย fiber optic ขาด หรือ switch ในการรับสัญญาณเสียหาย | ๒ | ๒ | ๔ | ค่อนข้างต่ำ | - แยกระบบที่ผิดปกติออกจากเครือข่าย เพื่อป้องกันความเสียหายแพร่กระจายไปยังส่วนอื่นของระบบ จากนั้น ปิดการเชื่อมต่อภายนอกที่ไม่จำเป็น เช่น VPN หรือเซิร์ฟเวอร์ที่ถูกเจาะ เพื่อจำกัดช่องทางที่ผู้ไม่หวังดีอาจใช้ในการเข้าถึงระบบเพิ่มเติม<br>- กู้คืนระบบและข้อมูล (System & Data Recovery) โดยการนำข้อมูลจาก Backup ที่ปลอดภัยมาใช้เพื่อฟื้นฟูระบบให้กลับมาอยู่ในสถานะปกติ อัปเดตแพตช์ความปลอดภัยทั้งหมด (Patch Management) เพื่ออุดช่องโหว่ที่อาจถูกใช้ในการโจมตี และทดสอบระบบให้แน่ใจว่าปลอดภัยก่อนนำกลับมาออนไลน์<br>- เพิ่มระบบสำรองข้อมูล (Backup) และทดสอบกระบวนการกู้คืนข้อมูลเป็นประจำ เพื่อให้มั่นใจได้ว่าสามารถกู้ระบบได้อย่างรวดเร็วหากเกิดเหตุการณ์ซ้ำอีกครั้ง<br>- สาเหตุที่ทำให้สาย fiber optic ขาด หากเสียหายเล็กน้อยให้ดำเนินการแก้ไข/จัดหาทดแทน |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๕. เหตุการณ์ไฟฟ้าดับ | - อุปกรณ์ประมวลผลข้อมูล (Process Device) บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศได้ไม่เต็มประสิทธิภาพ<br>- ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูล (Data Center) สูงขึ้น หรือไฟดับทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย<br>- การปฏิบัติงานเกิดความล่าช้า เนื่องจากต้องรอการซ่อมแซมแก้ไข | ๒ | ๒ | ๔ | ค่อนข้างต่ำ | - เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. พบเหตุและแจ้งให้ผู้ดูแลระบบ (Administrator) ของ ศทส. ทราบ เพื่อรายงานให้ผู้อำนวยการ ศทส. ทราบและรายงานตามลำดับชั้น และสั่งการต่อไป<br>- ผู้ดูแลระบบ (Administrator) ของ ศทส. ร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ร่วมกันตรวจสอบความเสียหาย ประเมินผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) หรือระบบปรับอากาศที่ได้รับความเสียหาย หรือ |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๖. เหตุการณ์อัคคีภัย | - สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้<br>- อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ไม่สามารถให้บริการได้ | ๑ | ๕ | ๕ | ค่อนข้างต่ำ | <u>กรณีที่ ๑ ไฟเริ่มไหม้หรือสามารถดับไฟได้</u><br>- ผู้ดูแลระบบ (Administrator) ประเมินสถานการณ์ร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ในเบื้องต้นว่าควรหยุดให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศหรือไม่<br>- กรณีถ้าหยุดให้บริการ ศทส. ประชาสัมพันธ์ ให้บุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากเหตุไฟไหม้<br>- ผู้ดูแลระบบ (Administrator) ประสานงานเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. เพื่อตรวจสอบความเสียหาย ประเมินผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| | | | | | | (Process Device) ระบบปรับอากาศและสภาพภายในห้องศูนย์ข้อมูล (Data Center) ร่วมกัน พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบเพื่อรายงานตามลำดับชั้นและสั่งการต่อไป<br>- หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (Administrator) ดำเนินการแก้ไขและเปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ<br>- ศทส. ประชาสัมพันธ์ให้บุคลากร สคร. ได้รับทราบว่าระบบสามารถกลับมาใช้งานได้แล้ว<br>- หากเสียหายมาก ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบเพื่อรายงานตามลำดับชั้นและสั่งการต่อไป |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| | | | | | | <u>กรณีที่ ๒ ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง</u><br>- ศทส. ประชาสัมพันธ์ให้บุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการเนื่องจากเหตุไฟไหม้<br>- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์ข้อมูล (Data Center) ร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| | | | | | | - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้น และสั่งการต่อไป |
| ๗. เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย แผ่นดินไหว และการชุมนุมประท้วง หรือความไม่สงบทางการเมือง | อาจถูกปิดกั้นการเข้าออก หรือไม่สามารถเข้าปฏิบัติงานยังพื้นที่ปฏิบัติงานบริเวณอาคาร ๑๕๐ ปี กระทรวงการคลัง หรือกรณีเกิดขึ้นที่ศูนย์ Data Center ณ จังหวัดปทุมธานี | ๒ | ๒ | ๔ | ค่อนข้างต่ำ | กรณีที่ไม่สามารถเข้าพื้นที่ปฏิบัติงาน ณ สคร. ได้ ให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ สคร. กำหนด |

| ความเสี่ยง | ความสูญเสียที่คาดว่าจะเกิดขึ้น | โอกาสที่เกิด | ผลกระทบ | ระดับความเสี่ยง | ผลประเมินระดับความเสี่ยง | แนวทางการแก้ไข |
|---|---|---|---|---|---|---|
| ๘. เหตุการณ์ที่เกิดจากโรคระบาดต่อเนื่อง | เมื่อบุคลากรไม่สามารถเข้าปฏิบัติงานในพื้นที่ได้ แม้อาจจะมีโอกาสเกิดหรือไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่อาจจะเกิดผลกระทบในส่วนของการเข้าไปปฏิบัติงานภายในพื้นที่ สคร. | ๒ | ๑ | ๒ | ต่ำ | - สคร. มีการเตรียมระบบสารสนเทศเพื่อรองรับการเข้าถึงระบบได้จากทุกที่ทุกเวลาผ่านเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing)<br>- การลงนามแบบ E-signature<br>- การจัดหาอุปกรณ์คอมพิวเตอร์ให้เพียงพอต่อจำนวนบุคลากร |

**หมายเหตุ** เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

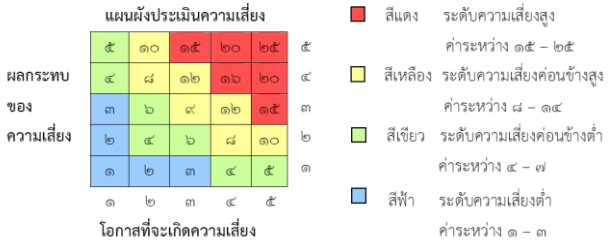
ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด

ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย

ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง

ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก

ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด



**๙. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต**

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศข้างต้น ศทส. จึงได้ดำเนินการจัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

๙.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๑.๑ กำหนดให้ปฏิบัติตามประกาศ สคร. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๙.๑.๒ การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้น โดยการจัดอบรมให้กับบุคลากร สคร. หรือส่งไปอบรมร่วมกับหน่วยงานภายนอกที่จัดขึ้น เพื่อลดความเสี่ยงด้านสารสนเทศ รวมถึงการจัดทำคู่มือการใช้งานและเผยแพร่ประชาสัมพันธ์ให้บุคลากรได้รับทราบ

๙.๑.๓ มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่างๆ ตามความเหมาะสม เช่น ผ่านระบบ Web Portal, Line, Facebook ของ สคร. เป็นต้น

๙.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๒.๑ ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

๙.๒.๒ ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๙.๒.๓ ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ

ทั้งนี้ สคร. ได้ติดตั้งระบบสำรองข้อมูลเพื่อการสำรองข้อมูลสารสนเทศไว้ที่ห้องศูนย์ข้อมูล (Data Center) ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. จ. ปทุมธานี ซึ่งมีระบบรักษาความปลอดภัยที่มีมาตรฐาน มีการควบคุมการเข้าถึงอย่างเข้มงวด และมีการสำรองข้อมูลแบบอัตโนมัติเฉพาะส่วนที่มีการเพิ่มขึ้น (Incremental Backup) และส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน และสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ซึ่งหากระบบเกิดเหตุฉุกเฉิน ขัดข้อง หรือข้อมูลเกิดการสูญหาย ยังสามารถกู้คืนให้นำกลับมาใช้งานได้โดยเร็ว

๙.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๓.๑ มีมาตรการควบคุมการเข้า - ออกห้องศูนย์ข้อมูล (Data Center) ซึ่งติดตั้งอยู่ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. จ. ปทุมธานี ดังนี้

(๑) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) ตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. กำหนด

(๒) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ เข้า – ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ก่อนเริ่มดำเนินการทุกครั้ง

(๓) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่มีการประสานเพื่อขออนุญาตกับ ศทส. สคร. และ สคร. แจ้งไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. เพื่อขออนุมัติรายชื่อบุคคล หมายเลขทะเบียนรถ แจ้งกำหนดการก่อนเข้าพื้นที่ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี

(๔) ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา และต้องไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ในห้องศูนย์ข้อมูล (Data Center)

(๕) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง

(๖) มีการติดตั้งระบบควบคุมการเข้าถึง (Access Control) ห้องศูนย์ข้อมูล (Data Center) ด้วยระบบอิเล็กทรอนิกส์

(๗) มีการติดตั้งกล้องวงจรปิดบันทึกเหตุการณ์บริเวณทางเข้าและภายในห้องศูนย์ข้อมูล (Data Center) เพื่อเฝ้าระวังเหตุการณ์หรือภัยที่จะเกิดขึ้น

๙.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๔.๑ มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) รวมถึงสาย fiber optic หรือ switch ในการรับสัญญาณ ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ ๑ ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device) หรืออุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งานให้รายงานให้ผู้อำนวยการ ศทส. ทราบเพื่อรายงานตามลำดับชั้นและสั่งการแก้ไขด้วยการซ่อมแซมหรือจัดซื้อทดแทนต่อไป

๙.๔.๒ มีการตรวจสอบปริมาณการเข้าถึงเครือข่ายภายนอก (Internet) เพื่อสังเกตปริมาณการใช้งาน อัตราความเร็วของข้อมูล เพื่อเฉลี่ยแบนด์วิดท์ (Bandwidth) ให้ทั่วถึงทั้งองค์กร และป้องกันไม่ให้ผู้ใช้งาน (User) มีการใช้แบนด์วิดท์ (Bandwidth) มากเกินไป

๙.๔.๓ กรณีสาย fiber optic ขาด หรือ switch ในการรับสัญญาณเสียหาย ศทส. ประสานงานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. และบริษัทที่ดำเนินการจ้างเหมาบริการเพื่อหาทางแก้ไขปัญหาและประสานให้บุคลากร สคร. ทราบ

๙.๕ เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดเหตุไฟฟ้าดับ

๙.๖ เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๖.๑ มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องศูนย์ข้อมูล (Data Center) อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงที เพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

๙.๖.๒ มีการติดตั้งระบบดับเพลิงที่มีมาตรฐานเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟเริ่มลุกลามถึงขั้นรุนแรง

หมายเหตุ : ห้องศูนย์ข้อมูล (Data Center) ณ จังหวัดปทุมธานี อยู่ในความดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. ซึ่งมีระบบรักษาความปลอดภัยที่มีมาตรฐาน มีการควบคุมการเข้าถึงอย่างเข้มงวด

๙.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย แผ่นดินไหว หรือเกิดเหตุและการชุมนุมประท้วงความไม่สงบทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๙.๗.๑ ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk เพื่อกรณีที่ไม่สามารถเข้าพื้นที่ปฏิบัติงาน ณ สคร. ได้ยังสามารถปฏิบัติงานจากที่พักหรือสถานที่ปฏิบัติงานสำรองที่ สคร. จัดเตรียมได้

๙.๗.๒ มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าไปภายในห้องศูนย์ข้อมูล (Data Center) โดยไม่ได้รับอนุญาต

๙.๗.๓ มีการตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศอย่างสม่ำเสมอเพื่อให้มีความพร้อมใช้สำหรับผู้ใช้งาน (User) ในการปฏิบัติงานจากภายนอก สคร.

๙.๗.๔ เมื่อได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง รวมถึงสถานการณ์ความไม่ปลอดภัยต่างๆ บริเวณสถานที่ปฏิบัติงาน ณ อาคาร ๑๕๐ ปี กระทรวงการคลัง ซึ่งอาจถูกปิดกั้นการเข้าออก สคร. ได้มีการกำหนดให้ปฏิบัติงานนอกสถานที่ (Work from Anywhere) ได้โดยใช้เครื่องคอมพิวเตอร์ส่วนตัว อุปกรณ์ที่สำนักงานจัดหาให้ และอินเทอร์เน็ตจากที่พักอาศัยของตนเพื่อเข้าถึงระบบงานต่างๆ ภายในสำนักงาน ซึ่ง ศทส. ได้เตรียมระบบและจัดหาอุปกรณ์เพื่อรองรับกรณีการปฏิบัติงานจากที่พักดังกล่าวไว้แล้ว

๙.๘ เหตุการณ์ที่เกิดจากโรคระบาดต่อเนื่อง ซึ่งอาจส่งผลกระทบในลักษณะที่ไม่สามารถเข้าปฏิบัติงานพื้นที่ สคร. ได้ ซึ่งกรณีที่เกิดโรคระบาดในช่วงที่ผ่านมา สคร. มีความพร้อมในการดำเนินการตามมาตรการด้านสาธารณสุขที่กำหนดขึ้นในการรักษาระยะห่างและนโยบายการให้บุคลากรสามารถปฏิบัติงานจากที่พักได้ เนื่องจาก ศทส. มีความพร้อมด้านระบบและมีการจัดหาอุปกรณ์ Notebook / tablet การประชุมแบบ Conference การใช้งานลายเซ็นอิเล็กทรอนิกส์ และระบบสารบรรณอิเล็กทรอนิกส์เพื่อรองรับสถานการณ์ดังกล่าว

ทั้งนี้ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้และ สคร. ได้มีประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ ประกาศ ณ วันที่ ๕ มีนาคม ๒๕๖๒ หมวด ๗ การจัดทำระบบสำรองของระบบสารสนเทศ นโยบาย ข้อ ๔ กำหนดให้ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. อย่างน้อยปีละ ๑ ครั้ง ซึ่งในปีงบประมาณ พ.ศ. ๒๕๖๗ ศทส. ได้คัดเลือกระบบสารสนเทศเพื่อทำการทดสอบ จำนวน ๒ ระบบ ดังนี้

- ระบบ Director’s Pool
- ระบบ GFMIS - SOE

โดย ศทส. ได้ดำเนินการตามข้อกำหนดการทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ โดยการจำลองสถานการณ์กรณีที่เกิดจากผู้ไม่ประสงค์ดีเข้ามาบุกรุกระบบเครือข่ายคอมพิวเตอร์ของ สคร. ส่งผลให้บุคลากร สคร. ไม่สามารถเข้าใช้งานระบบได้ ศทส. จึงได้ดำเนินการแก้ไขสถานการณ์ดังกล่าว เมื่อวันที่ ๒๓ กันยายน ๒๕๖๗ โดยการกู้คืนระบบ Director’s Pool และระบบ GFMIS -SOE ที่สำรองไว้ในระบบสำรองข้อมูล Veritas NetBackup Appliance แล้วนำกลับมาติดตั้งใช้งานใหม่ โดยที่ระบบจะทำการสำรองข้อมูลทั้งหมดทุกวันเวลา ๒๐.๐๐ น. การกู้คืนระบบสามารถทำได้โดยเลือกระบบที่จะกู้คืนและวันเวลาที่ต้องการกู้คืนข้อมูล ซึ่งทุกระบบจะดำเนินการเหมือนกัน และเป็นแบบ Restore virtual machine คือกู้คืนแบบทั้งเครื่องไปยังตำแหน่งเดิม และจากการดำเนินการดังกล่าว ศทส. สามารถกู้คืนระบบได้เป็นผลสำเร็จ

**๑๐. กลยุทธ์ความต่อเนื่องในสภาวะวิกฤต**

หากเหตุการณ์หรือภัยได้เกิดขึ้นแล้ว ต้องมีการดำเนินกลยุทธ์ความต่อเนื่องในสภาวะวิกฤตเพื่อให้การปฏิบัติงานของบุคลากร สคร. ดำเนินการไปได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุด ดังนี้

| ทรัพยากร | กลยุทธ์ความต่อเนื่อง |
|---|---|
| ๑. สถานที่ปฏิบัติงาน อาคาร ๑๕๐ ปี กระทรวงการคลัง | ๑. กำหนดพื้นที่ปฏิบัติงานสำรอง ได้แก่ ห้องคอมพิวเตอร์หรือพื้นที่อื่นๆ ของกรมบัญชีกลาง โดยประสานงานและสำรวจความเหมาะสมของสถานที่ร่วมกับกรมบัญชีกลาง<br>๒. ประสานขอใช้พื้นที่กับส่วนราชการหรือรัฐวิสาหกิจเป็นสถานที่ปฏิบัติงานสำรองเพิ่มเติม<br>๓. หากพื้นที่ปฏิบัติงานสำรองมีพื้นที่จำกัด หรืออาจเกิดอันตรายระหว่างเดินทางไปปฏิบัติงาน ให้บุคลากร สคร. ปฏิบัติงานนอกสถานที่ (Work from Anywhere) |
| ๒. วัสดุอุปกรณ์ | ๑. จัดหาเครื่องคอมพิวเตอร์สำรองพร้อมอุปกรณ์ในการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศได้ทั้งในและนอกสถานที่<br>๒. จัดเตรียมอุปกรณ์สารสนเทศสำหรับนำมาใช้ในการปฏิบัติงาน เช่น เครื่องพิมพ์ (Printer) เครื่องสแกนเนอร์ (Scaner) และสายเชื่อมต่อระบบเครือข่ายเฉพาะที่ (Lan)<br>๓. ผู้ใช้งาน (User) สามารถใช้คอมพิวเตอร์แบบพกพาส่วนตัวในการปฏิบัติงานได้ |

| ทรัพยากร | กลยุทธ์ความต่อเนื่อง |
|---|---|
| ๓. ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ | ๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศของ สคร. ได้มีการติดตั้งและจัดเก็บไว้ใน ณ ห้องศูนย์ข้อมูล (Data Center) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. จ. ปทุมธานี ซึ่งมีมาตรฐานและรองรับการเข้าถึงจากภายนอกโดยการรับส่งข้อมูลผ่านคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI) และมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)<br>๒. ประสานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. เพื่อจัดเตรียมไซต์สำรอง (Disaster Recovery Site : DR Site) เมื่อเกิดเหตุฉุกเฉินหรือสภาวะวิกฤต<br>๓. สคร. ได้ติดตั้งระบบสำรองข้อมูลเพื่อการสำรองข้อมูลสารสนเทศไว้ที่ห้องศูนย์ข้อมูล (Data Center) ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. จ. ปทุมธานี ซึ่งมีการสำรองข้อมูลแบบอัตโนมัติเฉพาะส่วนที่มีการเพิ่มขึ้น (Incremental Backup) และส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน และสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ซึ่งหากระบบเกิดเหตุฉุกเฉินขัดข้องหรือข้อมูลเกิดการสูญหาย ยังสามารถกู้คืนได้โดยผู้ดูแลระบบ (Administrator) ของ ศทส. จะทำการกู้คืนระบบและข้อมูลต่างๆ<br>๔. ระบบสารสนเทศตามภารกิจของ สคร. เพื่อการให้บริการแก่บุคลากร สคร. หน่วยงานรัฐวิสาหกิจ และส่วนราชการที่เกี่ยวข้อง ก็ติดตั้งอยู่ ณ ห้องศูนย์ข้อมูล (Data Center) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. จ. ปทุมธานี เช่นเดียวกัน ในกรณีที่เกิดเหตุฉุกเฉิน ณ ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี ผู้ดูแลระบบ (Administrator) ของ ศทส. จะประสานงานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. เพื่อจัดหา DR site สำรองต่อไป<br>๕. ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศที่จำเป็นและสำคัญไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk<br>๖. กำหนดให้มีการสำรองข้อมูล และทดสอบการนำกลับมาใช้อย่างสม่ำเสมอ |

| ทรัพยากร | กลยุทธ์ความต่อเนื่อง |
|---|---|
| ๔. บุคลากร สคร. | ๑. หากผู้ดูแลระบบ (Administrator) มีจำนวนไม่เพียงพอต่อการปฏิบัติหน้าที่ให้ผู้รับจ้างที่ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศให้การสนับสนุนด้านเทคนิค<br>๒. อนุญาตให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก สคร. โดยเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)<br>๓. กำหนดบุคลากรสำรอง เพื่อปฏิบัติหน้าที่แทนกันในกลุ่มงาน |
| ๕. ผู้รับบริการ และผู้ที่เกี่ยวข้อง | ๑. แจ้งสถานที่การติดต่อราชการสำรองผ่านทางหน้าเว็บไซต์ของ สคร.<br>๒. บุคลากร สคร. ที่มีหน้าที่ปฏิบัติงานร่วมกับรัฐวิสาหกิจ ให้ประสานงานทางโทรศัพท์เคลื่อนที่หรือจดหมายอิเล็กทรอนิกส์ (E - Mail) หรือหากระบบคอมพิวเตอร์และระบบสารสนเทศอยู่ระหว่างดำเนินการกู้คืน ให้พิจารณาใช้จดหมายอิเล็กทรอนิกส์ (E - Mail) จากภายนอกที่มีความน่าเชื่อถือ |

**๑๑. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต**

จากการวิเคราะห์ผลกระทบจากความเสี่ยงในข้อ ๘ เพื่อให้บุคลากรสามารถปฏิบัติงานด้วยความต่อเนื่อง จึงกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต ดังนี้

| กระบวนงาน | ระดับผลกระทบ | ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต | | | |
|---|---|---|---|---|---|
| | | ภายใน ๑ วัน | ภายใน ๓ วัน | ภายใน ๗ วัน | มากกว่า ๗ วัน |
| ๑. เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. | ค่อนข้างต่ำ | ✓ | | | |
| ๒. เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี | ค่อนข้างสูง | | ✓ | | |
| ๓. เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) | ค่อนข้างต่ำ | | | ✓ | |
| ๔. เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค | ค่อนข้างต่ำ | ✓ | | | |
| ๕. เหตุการณ์ไฟฟ้าดับ | ค่อนข้างต่ำ | ✓ | | | |
| ๖. เหตุการณ์อัคคีภัย | ค่อนข้างต่ำ | | | | ✓ |
| ๗. เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ | ค่อนข้างต่ำ | | | ✓ | |
| ๘. เหตุการณ์ที่เกิดจากโรคระบาดต่อเนื่อง | ต่ำ | ไม่ส่งผลกระทบต่อระบบสารสนเทศ | | | |

**๑๒. โครงสร้างและทีมบริหารความต่อเนื่อง (BCP Team)**

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง (BCP Team) ซึ่งประกอบด้วยผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Office : DCIO) ผู้อำนวยการ ศทส. และบุคลากรของ ศทส. เนื่องจากมีความรู้ความสามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่เป็นผู้ดูแลระบบ (Administrator) ของ สคร.

๑๒.๑ หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง (BCP Team) ดังนี้

๑๒.๑.๑ หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้ที่รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหารระดับสูง สคร. ได้รับทราบ

๑๒.๑.๒ ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอก สคร. และจัดเตรียมเอกสารข้อมูลที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

๑๒.๑.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลติดต่อประสานงานกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.กค. เพื่อดูแลห้องศูนย์ข้อมูล (Data Center) ณ จังหวัดปทุมธานี

๑๒.๒ รายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ

| ชื่อ | บทบาท | โทรศัพท์ |
|---|---|---|
| นางนัทีวรรณ สีมาเงิน | หัวหน้าทีมบริหารความต่อเนื่อง (BCP Team) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๐๐๒๑<br>- ๐๘๑ ๘๘๙ ๖๕๒๐ |
| นายชวเจต สุนทรวิทย์ | รองหัวหน้าทีมบริหารความต่อเนื่อง (BCP Team) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๑<br>- ๐๘๕ ๑๓๓ ๑๒๖๖ |
| นายกรินทร์ ศิริพัฒน์พิบูลย์ | ผู้ดูแลระบบ (Administrator) (บุคลากรหลัก) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๒<br>- ๐๘๑ ๙๓๐ ๕๓๖๐ |
| นายประวิทย์ บัวคอม | | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๕<br>- ๐๘๘ ๖๒๐ ๐๔๔๐ |
| นายณัฐพล จรัสดำรงนิตย์ | ผู้ดูแลระบบ (Administrator) (บุคลากรสำรอง) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๖<br>- ๐๘๓ ๘๕๑ ๓๓๖๐ |
| นายอภิรัตน์ เพ็งจางค์จิตต์ | | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๘<br>- ๐๘๔ ๐๘๓ ๕๙๙๕ |
| นายสิรภพ บุญฤทธิ์ | | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๑๐<br>- ๐๙๔ ๔๘๓ ๙๕๙๐ |

| ชื่อ | บทบาท | โทรศัพท์ |
|---|---|---|
| นายณัฐพล จรัสดำรงนิตย์ | ผู้ประสานงาน (บุคลากรหลัก) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๖<br>- ๐๘๓ ๘๕๑ ๓๓๖๐ |
| นางสาวอรรวรรณ เหลืองวิพัฒน์ | ผู้ประสานงาน (บุคลากรสำรอง) | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๐๗<br>- ๐๘๐ ๔๖๕ ๕๔๖๒ |
| นายสิรภพ บุญฤทธิ์ | | - ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๖๑๔๑๐<br>- ๐๙๔ ๔๘๓ ๙๕๙๐ |

**ผู้ประสานงานภายนอก**

| ลำดับ | หน่วยงาน | หมายเลขโทรศัพท์ |
|---|---|---|
| ๑. | ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง | ๐๒ ๑๒๖ ๕๙๐๐ |
| ๒. | บริษัท โทรคมนาคมแห่งชาติ จำกัด | ๐๒ ๑๐๔ ๑๑๑๑ |

โดยทุกตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในหน่วยงานให้สามารถบริหารความต่อเนื่องและกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่อง (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลัก

**๑๓. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)**

กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในทีมบริหารความต่อเนื่องตามรายชื่อที่ปรากฏในตารางรายชื่อบุคลากร โดยมีวัตถุประสงค์เพื่อให้สามารถบริหารจัดการในการติดต่อบุคลากรของหน่วยงาน ภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือสภาวะวิกฤต

กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) ตามแนวทางของแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. หมายถึง ขั้นตอนการแจ้งเหตุฉุกเฉินหรือการแจ้งปัญหาระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นและสั่งการให้ผู้ที่มีหน้าที่รับผิดชอบดำเนินการแก้ไขตามระดับความรุนแรงของเหตุนั้น เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถให้บริการสนับสนุนการปฏิบัติงานแก่บุคลากร สคร. ได้อย่างต่อเนื่อง ที่กำหนดรายละเอียดไว้ตามรายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ ทั้งนี้ ในกรณีที่บุคลากรหลักในแต่ละบทบาทไม่สามารถปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบปฏิบัติหน้าที่แทน

**๑๔. แผนการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ (Diaster Recovery Plan : DR Plan)**

๑๔.๑ ความเป็นมาและวัตถุประสงค์

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องศูนย์ข้อมูล (Data Center) จ. ปทุมธานี ซึ่งเข้าถึงด้วยเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing) ซึ่งเป็นการอำนวยความสะดวกแก่ผู้ใช้งาน (User) เป็นอย่างมาก และเนื่องจากเป็นลักษณะแบบรวมศูนย์กลาง ศทส. ซึ่งเป็นผู้ดูแลรับผิดชอบหลัก จึงจัดทำแผนการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ (Diaster Recovery Plan : DR Plan) เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วในกรณีที่เกิดปัญหา

๑๔.๒ ผู้รับผิดชอบ

รายละเอียดบุคลากรและหน้าที่ความรับผิดชอบ ตามข้อ ๑๒.๒

๑๔.๓ แผนปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศตลอดจนอุปกรณ์ประมวลผลข้อมูล (Process Device)

ศทส. มอบหมายให้ผู้ดูแลระบบ (Administrator) ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๑๔.๔ แผนปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

๑๔.๔.๑ ผู้ดูแลระบบ (Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศตามขั้นตอนของโปรแกรม Symantec NetBackup

๑๔.๔.๒ ผู้ดูแลระบบ (Administrator) ต้องจัดเก็บรายงานการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

๑๔.๔.๓ รายละเอียดการสำรองข้อมูล กำหนดดังนี้

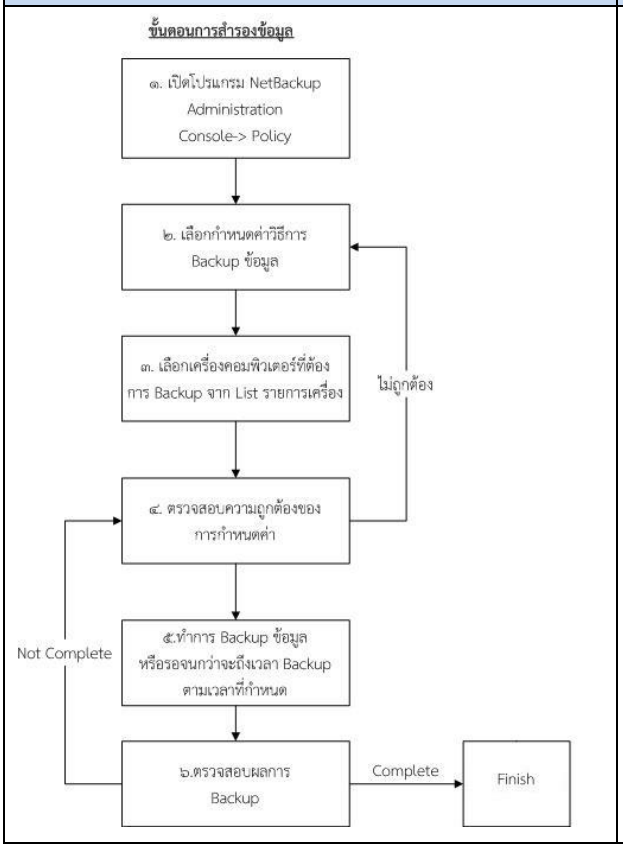
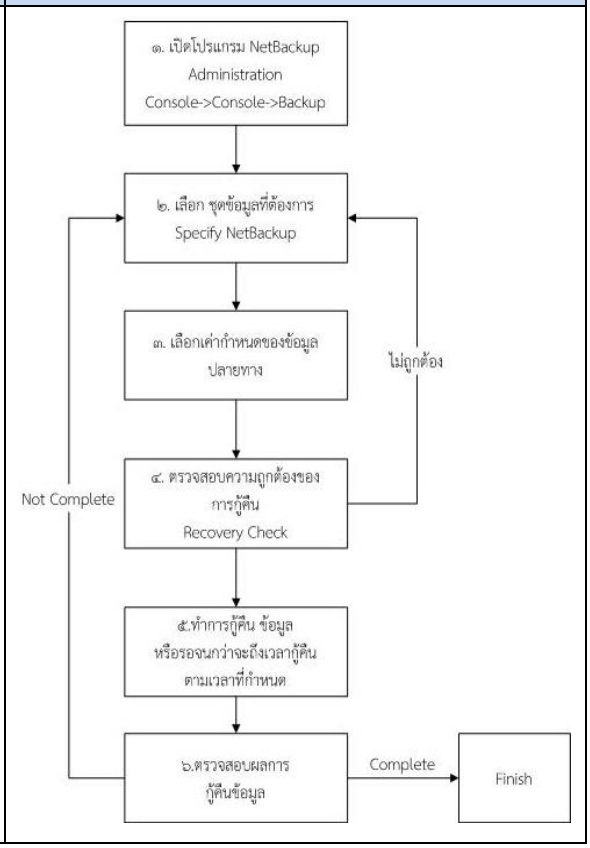
| ลำดับ | รายการ | จำนวน (หน่วย) | ข้อมูลที่สำรอง |
|---|---|---|---|
| ๑ | เครื่องคอมพิวเตอร์แม่ข่าย (Server Farm) | ๓ เครื่อง | ค่า Configuration |
| ๒ | เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน สำหรับประมวลผลระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI) | ๕ เครื่อง | ค่า Configuration |
| ๓ | เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (Data Analytics) | ๔ เครื่อง | ค่า Configuration |

| ลำดับ | รายการ | จำนวน (หน่วย) | ข้อมูลที่สำรอง |
|---|---|---|---|
| ๔ | เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (Data Analytics) (เครื่อง VM) | ๒๐ เครื่อง | ค่า Configuration และ Data |
| ๕ | เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (เครื่อง VM) | ๑๒๐ เครื่อง | ค่า Configuration และ Data |
| ๖ | ระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI) | ๒๕๐ เครื่อง | ค่า Configuration และ Data |

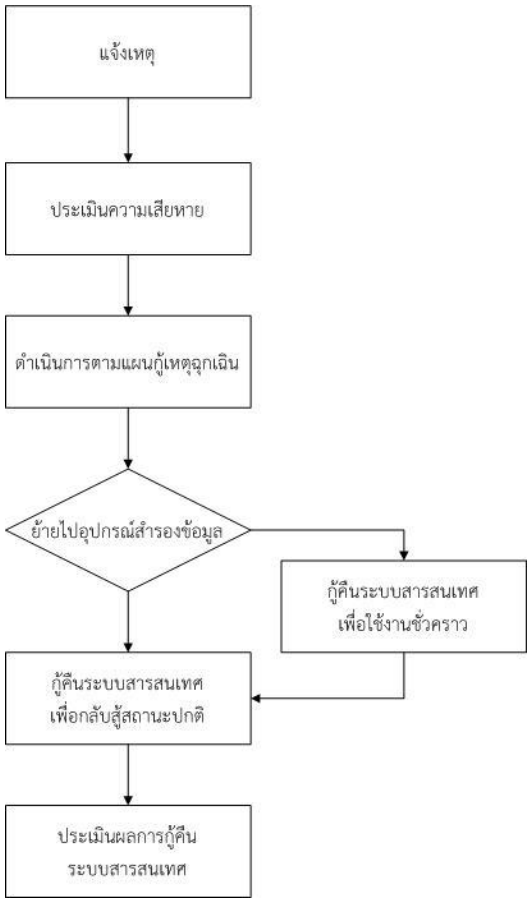
๑๔.๔ แผนปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศเกิดปัญหาไม่สามารถใช้งานได้ หรือข้อมูลสารสนเทศสูญหาย ให้ผู้ดูแลระบบ (Administrator) ดำเนินการกู้คืนข้อมูลสารสนเทศเพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน

๑๔.๕ แผนผังการสำรองและกู้คืนระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศ ด้วยโปรแกรม Symantec NetBackup

| การสำรองข้อมูล | การกู้คืนข้อมูล |
|---|---|
|  |  |

๑๔.๖ ขั้นตอนการปฏิบัติงานแผนการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ




๑๔.๗ การทดสอบแผน

ศทส. ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๑๔.๗.๑ พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการทดสอบ พร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

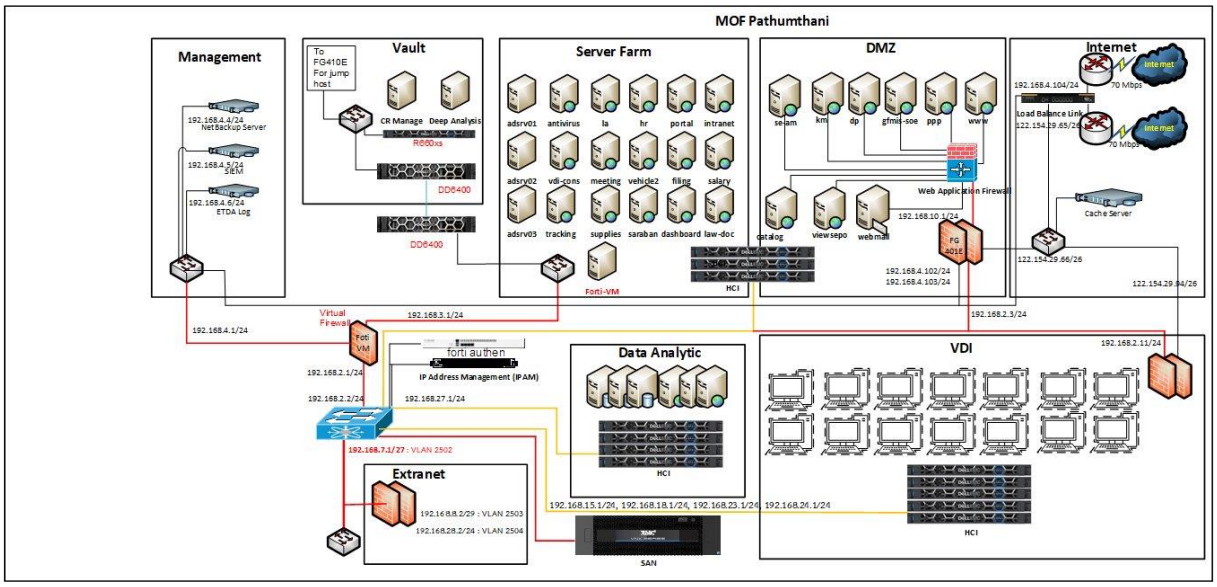
๑๔.๗.๒ ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

๑๔.๗.๓ จัดทำรายงานเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Office : DCIO)

๑๔.๘ การปรับปรุงแผน

ศทส. ต้องทำการปรับปรุงแผนการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศให้เป็นปัจจุบันอยู่เสมอ เพื่อให้แน่ใจว่าแผนนั้นยังสามารถไปใช้งานได้อย่างมีประสิทธิผล และประสิทธิภาพตามที่คาดหมายไว้โดยจะมีการปรับปรุงอย่างน้อยปีละ ๑ ครั้ง

ผังแสดงสถาปัตยกรรมโครงข่ายคอมพิวเตอร์ (Network Infrastructure Diagram) และ
ผังแสดงสถาปัตยกรรมระบบเครื่องคอมพิวเตอร์ลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)



## ข้อมูลด้านระบบสารสนเทศและการรักษาความมั่นคงปลอดภัย

ระบบสารสนเทศของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ในปัจจุบันแบ่งออกเป็น ๓ ประเภท ดังนี้

| ระบบที่ดำเนินการใช้งานในปัจจุบัน |
| --- |
| **๑. ระบบคอมพิวเตอร์และระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน** |
| ๑.๑ ระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (VDI) |
| ๑.๒ ระบบ Web Portal |
| ๑.๓ ระบบสารบรรณอิเล็กทรอนิกส์ |
| ๑.๔ ระบบจัดเก็บและบริหารจัดการไฟล์เอกสาร E - Filing |
| ๑.๕ ระบบลาราชการ |
| ๑.๖ ระบบจองห้องประชุม |
| ๑.๗ ระบบจองยานพาหนะ |
| ๑.๘ ระบบฐานข้อมูลบุคลากร |
| ๑.๙ ระบบพัสดุ |
| ๑.๑๐ ระบบสลิปเงินเดือน |
| ๑.๑๑ ระบบการจัดการองค์ความรู้ (Insight Out) |
| ๑.๑๒ ระบบ E – Mail |
| ๑.๑๓ ระบบลงเวลา Work from Anywhere |

| **๒. ระบบสารสนเทศเพื่อการให้บริการข้อมูลข่าวสารแก่ประชาชนโดยผ่านทางอินเทอร์เน็ต** |
|---|
| ๒.๑ เว็บไซต์ สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (www.sepo.go.th) |
| ๒.๒ เว็บไซต์ GFMIS-SOE (gfmis-soe.sepo.go.th) |
| ๒.๓ ระบบ GFMIS-SOE |
| ๒.๓.๑ ระบบฐานข้อมูลการเงินรัฐวิสาหกิจ |
| ๒.๓.๒ ระบบการติดตามงบลงทุนรัฐวิสาหกิจ |
| ๒.๓.๓ ระบบฐานข้อมูลทั่วไปกิจการรัฐวิสาหกิจ |
| ๒.๓.๔ ระบบฐานข้อมูลผู้บริหาร พนักงาน |
| ๒.๓.๕ ระบบฐานข้อมูลกรรมการรัฐวิสาหกิจ |
| ๒.๔ เว็บไซต์ ระบบฐานข้อมูลหลักทรัพย์ของรัฐ |
| ๒.๕ เว็บไซต์ ระบบฐานข้อมูลการร่วมลงทุนระหว่างรัฐและเอกชน |
| ๒.๖ เว็บไซต์ กรรมการรัฐวิสาหกิจ |
| ๒.๗ เว็บไซต์ การร่วมลงทุนระหว่างรัฐและเอกชน |
| ๒.๘ เว็บไซต์ ธรรมาภิบาลข้อมูลภาครัฐ |
| ๒.๙ ระบบสารสนเทศทรัพยากรบุคคลระดับกรม DPIS |
| ๒.๑๐ ระบบประเมินผล SE-AM Center |

| **๓. ระบบสารสนเทศเพื่อการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย** |
|---|
| ๓.๑ ระบบ Antivirus สำหรับเครื่องคอมพิวเตอร์แม่ข่าย |
| ๓.๒ ระบบ Antivirus สำหรับผู้ใช้งาน |
| ๓.๓ ระบบบริหารจัดการสิทธิผู้ใช้งาน Active Directory |
| ๓.๔ ระบบ Domain name server |
| ๓.๕ ระบบ Dynamic Host Configuration Protocol |
| ๓.๖ ระบบกู้คืนข้อมูล |
| ๓.๗ ระบบอุปกรณ์จัดเก็บสำรองข้อมูลแบบเบ็ดเสร็จ (Backup Appliance) |
| ๓.๘ ระบบอุปกรณ์ป้องกันเครือข่ายชั้นภายนอก (External Firewall) |
| ๓.๙ ระบบอุปกรณ์ป้องกันเครือข่ายสำหรับผู้ใช้งาน (Internal Firewall) |
| ๓.๑๐ ระบบ Multi-Factor Authentication (MFA) |

## ข้อมูลด้านอุปกรณ์เครือข่ายคอมพิวเตอร์และผู้ให้บริการเครือข่าย

| รายการ |
| --- |
| **๑. อุปกรณ์เครือข่ายคอมพิวเตอร์** |
| ๑.๑ Core Switching ๒ ชุด |
| ๑.๒ Access Switching ๒ ชุด |
| ๑.๓ Switching ๓ ชุด |
| ๑.๔ Top of Rack Switching ๒ ชุด |

| **๒. ผู้ให้บริการเครือข่าย** |
| --- |
| บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) |

**๑๕. กระบวนการบริหารจัดการเหตุการณ์ (Incident Management Process)**

Incident Management Process คือ กระบวนการที่ใช้ในการบริหารจัดการกับเหตุการณ์ (Incident) ที่ไม่คาดคิดซึ่งส่งผลกระทบต่อการให้บริการของระบบ IT หรือกระบวนการทำงาน โดยมีเป้าหมายหลักเพื่อฟื้นฟูการให้บริการให้กลับมาใช้งานได้ตามปกติโดยเร็วที่สุด ลดผลกระทบต่อการดำเนินภารกิจขององค์กร เช่น ระบบอีเมลล่ม เว็บไซต์หลักเข้าไม่ได้ เครื่องพิมพ์ไม่สามารถเชื่อมต่อกับเครือข่าย ผู้ใช้งานล็อกอินระบบไม่ได้ มักเป็นเหตุการณ์ส่วนหนึ่งของ IT service กรณีเหตุการณ์ที่มีความรุนแรงมากขึ้น จนถึงระดับวิกฤต และส่งผลกระทบในวงกว้างและมีผลต่อการปฏิบัติงาน เช่น ระบบงานหลักล่มทั้งระบบ เกิดการโจมตีด้านไซเบอร์ ไฟไหม้ศูนย์ Data Center หรือโครงข่ายอินเทอร์เน็ตล่มทั้งเครือข่าย ซึ่งเหตุการณ์เหล่านี้จะต้องใช้ Business Continuity Plan (BCP) ซึ่งจะมุ่งเน้นการวางแผนเพื่อให้องค์กรสามารถดำเนินงานต่อไปได้ แม้จะเกิดเหตุการณ์วิกฤต เช่น ภัยธรรมชาติ ไฟไหม้ หรือระบบ IT ล่มทั้งระบบ โดยมีแผนสำรอง กระบวนการทำงานชั่วคราว หรือการย้ายสถานที่ปฏิบัติงาน

๑๕.๑ ขั้นตอนหลักของ Incident Management Process

๑๕.๑.๑ การแจ้งเหตุการณ์ (Incident Identification) ผู้ใช้แจ้งปัญหา หรือระบบตรวจพบความผิดปกติ

๑๕.๑.๒ การบันทึกเหตุการณ์ (Incident Logging) บันทึกรายละเอียด เช่น วันเวลา ผู้แจ้ง รายละเอียดปัญหา

๑๕.๑.๓ การจัดประเภทเหตุการณ์ (Categorization) จำแนกว่าปัญหาเกี่ยวข้องกับอะไร เช่น ระบบเครือข่าย ซอฟต์แวร์ ฮาร์ดแวร์

๑๕.๑.๔ การจัดลำดับความสำคัญ (Prioritization) ระบุระดับความเร่งด่วน/ผลกระทบเพื่อจัดลำดับการดำเนินการ

๑๕.๑.๕ การวินิจฉัยเบื้องต้น (Initial Diagnosis) วิเคราะห์ปัญหาเบื้องต้นเพื่อหาสาเหตุ

๑๕.๑.๖ การส่งต่อ (Escalation) หากแก้ไม่ได้ จะส่งต่อให้ทีมผู้เชี่ยวชาญ

๑๕.๑.๗ การแก้ไขและกู้คืน (Resolution and Recovery) ดำเนินการแก้ไข

๑๕.๑.๘ การปิดเหตุการณ์ (Incident Closure) ตรวจสอบว่าผู้ใช้ยืนยันว่าปัญหาได้รับการแก้ไขแล้ว และปิดเคส

๑๕.๒ ตัวอย่างการจัดลำดับ Incident ตามระดับความรุนแรง (Severity Level) เพื่อใช้ในกระบวนการ Incident Management

๑๕.๒.๑ Low (Minor Incident)

| | |
|---|---|
| ลักษณะ | ไม่กระทบต่อผู้ใช้จำนวนมาก ยังทำงานได้ตามปกติ |
| ตัวอย่าง | เครื่องพิมพ์ไม่ทำงาน ผู้ใช้คนหนึ่งรีเซ็ตรหัสผ่านไม่ได้ |
| การตอบสนอง | แก้ไขตามลำดับงานปกติ |

๑๕.๒.๒ Medium (Moderate Incident)

| | |
|---|---|
| ลักษณะ | กระทบผู้ใช้หลายคน บางฟังก์ชันทำงานไม่ได้ แต่ยังมีทางเลือกใช้งานได้ |
| ตัวอย่าง | ระบบอีเมลภายในส่งไม่ได้แต่รับได้ Application บางส่วนไม่โหลด |
| การตอบสนอง | แก้ไขภายในระยะเวลาที่กำหนดตามความสำคัญ |

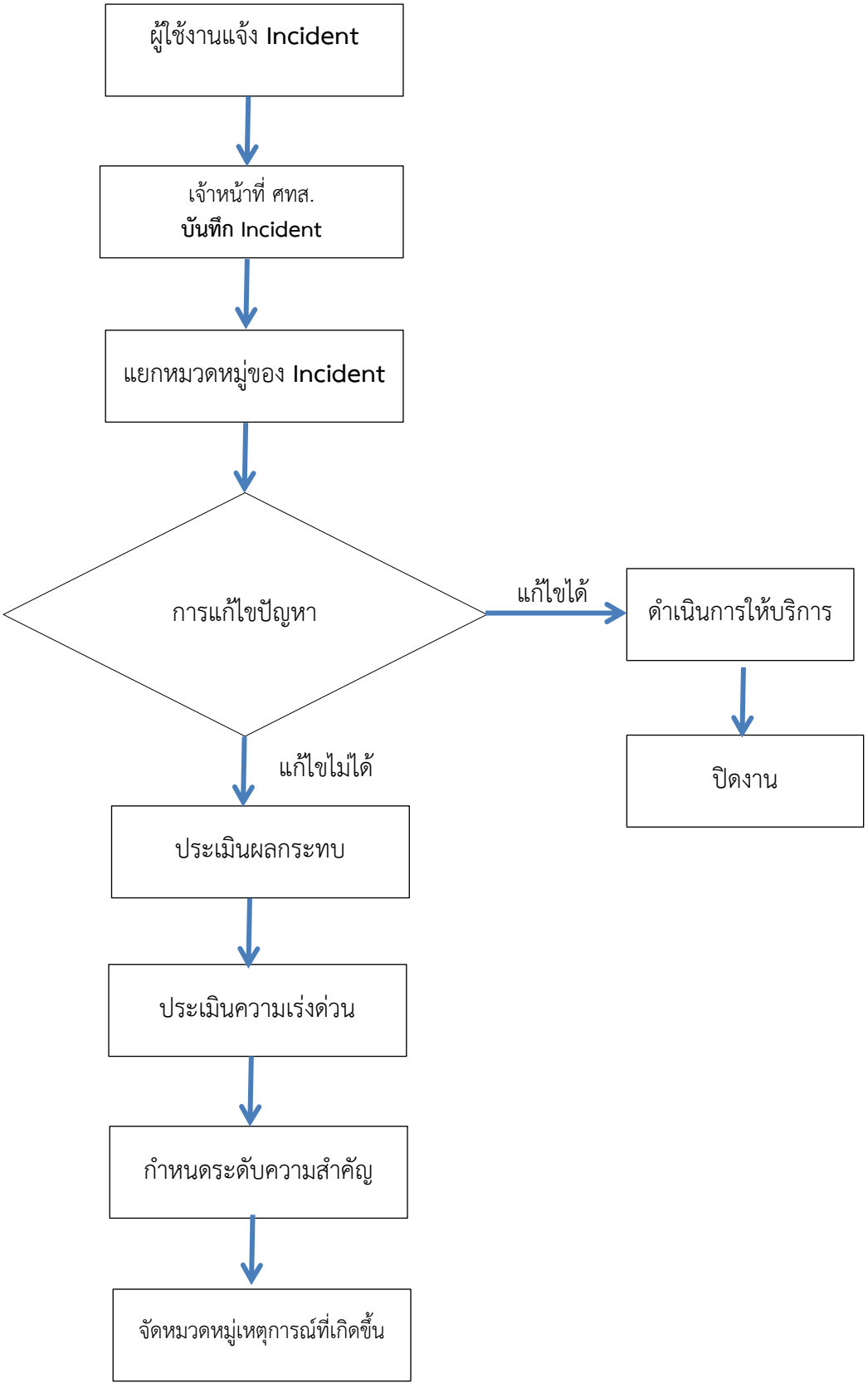
๑๕.๒.๓ High (Major Incident)

| | |
|---|---|
| ลักษณะ | กระทบงานหลักของแผนกหรือหลายแผนกไม่มีทางเลือกในการทำงาน |
| ตัวอย่าง | อินทราเน็ตองค์กรเข้าไม่ได้ทั้งบริษัท |
| การตอบสนอง | แจ้งเตือนเร่งด่วน ทีม IT และผู้จัดการร่วมติดตาม |

๑๕.๑.๔ Critical (Severe Incident / Crisis)

| | |
|---|---|
| ลักษณะ | กระทบทั้งองค์กรหรือธุรกิจหยุดชะงัก, อาจมีผลทางกฎหมายหรือชื่อเสียง |
| ตัวอย่าง | Ransomware โจมตีระบบหลัก ไฟไหม้ Data Center หรือศูนย์คอมพิวเตอร์ |
| การตอบสนอง | Activate BCP จัดตั้ง War Room แจ้งผู้บริหารระดับสูง |

**แผนผังรับมือ Incident Management Process**



**บทบาท (Roles) ตามกระบวนการ Incident Management**
**สามารถแบ่งออกเป็นหลายตำแหน่งที่มีหน้าที่ชัดเจน ดังนี้:**

| | |
|---|---|
| **๑. ผู้แจ้งเหตุ** (Incident Reporter / End User) สังเกตพบปัญหาและแจ้งเหตุผ่านระบบหรือช่องทางที่กำหนด โทรศัพท์ Line แจ้งข้อมูลครบถ้วน เช่น เวลาเกิดเหตุ, ระบบที่เกี่ยวข้อง, อาการผิดปกติ | **บุคลากร สคร.** |
| **๒. เจ้าหน้าที่รับแจ้งเหตุ (Service Desk / Helpdesk)**<br>รับแจ้งเหตุ ตรวจสอบความถูกต้องเบื้องต้น<br>จัดลำดับความสำคัญ ให้คำแนะนำพื้นฐานหรือแก้ไขปัญหาที่ไม่ซับซ้อนได้ทันที หรือประเมินเพื่อส่งต่อให้ทีมที่เกี่ยวข้องหากเกินขอบเขต | **บุคลากร ศทส.**<br>เจ้าพนักงานธุรการ<br>นายณัฐพล จรัสดำรงนิตย์<br>นายอภิรัตน์ เพ็งจางค์จิตร<br>นายสิรภพ บุญฤทธิ์<br>นางสาวอรรวรรณ เหลืองวิพัฒน์ |
| **๓. ผู้ดูแลระบบ (System/Network/Application Support)**<br>วิเคราะห์ปัญหาเชิงลึก และลงมือแก้ไข<br>สื่อสารกับ Helpdesk และผู้ใช้งาน | นายกรินทร์ ศิริพัฒน์พิบูลย์<br>นายประวิทย์ บัวคอม |
| **๔. ผู้จัดการเหตุการณ์ (Incident Manager)**<br>ควบคุม ติดตาม และประสานงานระหว่างทีม ประเมินความรุนแรง สื่อสารกับผู้บริหารในกรณีที่เหตุการณ์ร้ายแรง สรุปเหตุการณ์และจัดทำรายงานหลังเหตุการณ์ (Post Incident Review) | นายชวเจต สุนทรวิทย์<br>ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ |
| **๕. ผู้บริหาร/เจ้าของระบบ (Service Owner / IT Manager)**<br>ตัดสินใจในเหตุการณ์ระดับวิกฤต อนุมัติการ Activate BCP หรือเปลี่ยนแปลงระบบกรณีพิเศษ ตรวจสอบและรับรองรายงานการจัดการเหตุการณ์ | นางนัทีวรรณ สีมาเงิน ในฐานะ DCIO<br>และรายงานคณะผู้บริหารระดับสูง สคร. |
| **๖. ทีมรักษาความมั่นคงปลอดภัย (Cybersecurity / IT Security)**<br>ตรวจสอบหากเหตุการณ์เกี่ยวข้องกับภัยคุกคามหรือการโจมตีทางไซเบอร์ | นายกรินทร์ ศิริพัฒน์พิบูลย์<br>นายประวิทย์ บัวคอม<br>ร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานปลัดกระทรวงการคลัง |

## การปฏิบัติงานนอกสถานที่กรณีเกิดสภาวะวิกฤต (Work From Anywhere)

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจมีประกาศ เรื่อง แนวทางการปฏิบัติงานนอกสถานที่ตั้ง พ.ศ. ๒๕๖๗ ประกาศ ณ วันที่ ๒๕ กรกฎาคม ๒๕๖๗ และประกาศ เรื่อง หลักเกณฑ์การปฏิบัติงานนอกสถานที่ตั้งของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ฉบับที่ ๑/๒๕๖๗ ประกาศ ณ วันที่ ๒๖ ธันวาคม ๒๕๖๗ เพื่อให้การปฏิบัติราชการของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจเกิดประโยชน์สูงสุด โดยเจ้าหน้าที่สามารถปฏิบัติงานได้โดยไม่มีข้อจำกัดด้านสถานที่ โดยมีการรายงานการเข้าปฏิบัติงานผ่านระบบ https://wfa.sepo.go.th โดยดำเนินการตามระเบียบสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจว่าด้วยการลงเวลาปฏิบัติราชการของข้าราชการ พนักงานราชการและลูกจ้างชั่วคราวของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจด้วยวิธีการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๗ ประกาศ ณ วันที่ ๒๖ ธันวาคม ๒๕๖๗ และศูนย์เทคโนโลยีสารสนเทศได้สร้างช่องทางการเข้าใช้งานระบบสำคัญผ่านทาง www.sepo.go.th ในส่วนของ smart back office ประกอบด้วย ระบบลงเวลา Work from Anywhere ระบบสารบรรณอิเล็กทรอนิกส์ เช็คเมล (Web Mail) และ ระบบ VDI

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

ศปษ.ด้านการประเมินผลฯ
เลขที่รับ 1246
วันที่ 21 พ.ค. 2568

# บันทึกข้อความ

**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศ ส่วนบริหารเทคโนโลยีและข้อมูลสารสนเทศ โทร. ๖๑๔๐๔

**ที่** กค ๐๘๐๒.๒/๗๔๓ **วันที่** ๒๑ พฤษภาคม ๒๕๖๘

**เรื่อง** ขอความเห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

เรียน ที่ปรึกษาด้านการประเมินผลรัฐวิสาหกิจ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer)

ด้วยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้มีประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ ประกาศ ณ วันที่ ๕ มีนาคม ๒๕๖๒ (ประกาศฯ) โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ พ.ศ. ๒๕๖๒ แนบท้ายประกาศฯ หมวด ๗ การจัดทำระบบสำรองของระบบสารสนเทศ ได้กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) ดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. (แผนความต่อเนื่องด้านสารสนเทศฯ) เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง รวมทั้งให้ปรับปรุงแผนดังกล่าวทุก ๒ ปี รายละเอียดปรากฏตามเอกสารแนบ ๑ โดย สคร. ได้เห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ (แผนฯ ปี ๖๗) รายละเอียดปรากฏตามเอกสารแนบ ๒

ศทส. ขอเรียนดังนี้

๑. เมื่อวันที่ ๔ กุมภาพันธ์ ๒๕๖๘ สคร. ได้เห็นชอบแผนบริหารความต่อเนื่องของ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ รายละเอียดปรากฏตามเอกสารแนบ ๓ โดยเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘ ศทส. ได้ดำเนินการหารือแนวทางการดำเนินการตามแผนบริหารความต่อเนื่องของ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ร่วมกับกลุ่มพัฒนาระบบบริหาร โดยสรุปว่า ศทส. จะได้ดำเนินการร่วมกับ กพร. ดำเนินการซักซ้อมและดำเนินการให้ความรู้แก่บุคลากร สคร. ในส่วนที่เกี่ยวข้องต่อไป

๒. เมื่อวันที่ ๑๑ เมษายน ๒๕๖๘ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้เผยแพร่แบบสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทย หน่วยงานระดับกรมหรือเทียบเท่า (แบบสำรวจฯ) ประจำปี ๒๕๖๘ พร้อมกับเอกสารที่เกี่ยวข้อง ซึ่งแบบสำรวจฯ ประจำปี ๒๕๖๘ มีเนื้อหาครอบคลุมถึงแผนความต่อเนื่องด้านสารสนเทศฯ โดยได้เสนอแนะให้มีการเพิ่มเติมเนื้อหาในส่วนของการเตรียมแผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan : DR Plan) และกระบวนการจัดการเหตุการณ์ผิดปกติ (Incident Management Process) ด้วย รายละเอียดปรากฏตามเอกสารแนบ ๔

/๓. ศทส. ...

๓. ศทส. ได้ดำเนินการจัดทำร่างแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ เพื่อเป็นการปรับปรุงแผนฯ ปี ๖๗ ให้มีความสอดคล้องกับประเด็นตามข้อ ๑ และ ๒ ข้างต้นแล้ว รายละเอียดปรากฏตามเอกสารแนบ ๕

ในการนี้ จึงเห็นควรนำเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer) พิจารณาให้ความเห็นชอบก่อนนำเสนอผู้อำนวยการ สคร. เพื่อขอความเห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ต่อไป ทั้งนี้ ตามคำสั่ง สคร. ที่ ๔๔๗/๒๕๖๓ สั่ง ณ วันที่ ๙ ธันวาคม พ.ศ. ๒๕๖๓ เรื่อง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer) และผู้ช่วยผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ (Department Chief Information Officer Assistant) ข้อ ๑ แต่งตั้งที่ปรึกษาฯ (ประเภทวิชาการ ระดับทรงคุณวุฒิ) หรือรองผู้อำนวยการ สคร. ที่กำกับดูแลงานของ ศทส. เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer) รายละเอียดปรากฏตามเอกสารแนบ ๖

จึงเรียนมาเพื่อโปรดพิจารณา

(นายชวเจต สุนทรวิทย์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

เห็นชอบ

22/5/68

(นางนันทีวรรณ สีมาเงิน)
ที่ปรึกษาด้านการประเมินผลรัฐวิสาหกิจ

21 พ.ค. 68

สปษ.ด้านการประเมินผลฯ
เลขที่รับ 1287
วันที่ 28 พ.ค. 2568
ผอ.สคร.
เลขที่รับ 2941
วันที่ 28 พ.ค. 2568

# บันทึกข้อความ

**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศ ส่วนบริหารเทคโนโลยีและข้อมูลสารสนเทศ โทร. ๖๑๔๐๔

**ที่** กค ๐๘๐๒.๒/ ๑๔๘ **วันที่** ๒๘ พฤษภาคม ๒๕๖๘

**เรื่อง** ขอความเห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

เรียน ผอ. สคร. (ผ่านที่ปรึกษาด้านการประเมินผลรัฐวิสาหกิจ) 28/5/68

ด้วยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้มีประกาศ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ ประกาศ ณ วันที่ ๕ มีนาคม ๒๕๖๒ (ประกาศฯ) โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ พ.ศ. ๒๕๖๒ แนบท้ายประกาศฯ หมวด ๗ การจัดทำระบบสำรองของระบบสารสนเทศ ได้กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) ดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. (แผนความต่อเนื่องด้านสารสนเทศฯ) เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง รวมทั้งให้ปรับปรุงแผนดังกล่าวทุก ๒ ปี รายละเอียดปรากฏตามเอกสารแนบ ๑ โดย สคร. ได้เห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ (แผนฯ ปี ๖๗) รายละเอียดปรากฏตามเอกสารแนบ ๒

ศทส. ขอเรียน ดังนี้

๑. หนังสือกลุ่มพัฒนาระบบบริหาร (กพร.) ที่ กค ๐๘๐๙/๑๓ ลงวันที่ ๔ กุมภาพันธ์ ๒๕๖๘ เรื่อง แผนบริหารความต่อเนื่องของ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ผอ. สคร. ได้เห็นชอบแผนบริหารความต่อเนื่องของ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ รายละเอียดปรากฏตามเอกสารแนบ ๓ โดยเมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๘ ศทส. ได้ดำเนินการหารือแนวทางการดำเนินการตามแผนบริหารความต่อเนื่องของ สคร. ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ ร่วมกับ กพร. โดยสรุปว่า ศทส. จะได้ดำเนินการร่วมกับ กพร. ดำเนินการซักซ้อมและดำเนินการให้ความรู้แก่บุคลากร สคร. ในส่วนที่เกี่ยวข้องต่อไป

๒. หนังสือสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ที่ สพร ๒๕๖๘/ว๑๒๑๑ ลงวันที่ ๑๘ เมษายน ๒๕๖๘ เรื่อง ขอความอนุเคราะห์ตอบแบบสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐประจำปี พ.ศ. ๒๕๖๘ (แบบสำรวจฯ) โดยส่วนราชการสามารถเริ่มทำแบบสำรวจฯ ประจำปี ๒๕๖๘ ในระบบได้ตั้งแต่วันอังคารที่ ๖ พฤษภาคม ๒๕๖๘ ถึง วันศุกร์ที่ ๓๐ พฤษภาคม ๒๕๖๘ เวลา ๒๓.๕๙ น. รายละเอียดปรากฏตามเอกสารแนบ ๔ ซึ่งแบบสำรวจฯ ประจำปี ๒๕๖๘ มีเนื้อหาครอบคลุมถึงแผนความต่อเนื่องด้านสารสนเทศฯ โดยได้เสนอแนะให้มีการเพิ่มเติมเนื้อหาในส่วนของการเตรียมแผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan : DR Plan) และกระบวนการจัดการเหตุการณ์ผิดปกติ (Incident Management Process) ด้วย

/๓. ศทส. ...

๓. ศทส. ได้ดำเนินการจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ เพื่อเป็นการปรับปรุงแผนฯ ปี ๖๗ ให้มีความสอดคล้องกับประเด็นตามข้อ ๑ และ ๒ โดยได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer) เรียบร้อยแล้ว รายละเอียดปรากฏตามเอกสารแนบ ๕

ในการนี้ จึงเห็นควรนำเสนอผู้อำนวยการ สคร. พิจารณาให้ความเห็นชอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ เพื่อ ศทส. ดำเนินการในส่วนที่เกี่ยวข้องต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

(นายชวเจต สุนทรวิทย์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

เห็นชอบ

(นายธิบดี วัฒนกุล)
ผู้อำนวยการสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
๒๘ พ.ค. ๒๕๖๘