แผนบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศ
ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
พ.ศ. ๒๕๖๒

สารบัญ

๑. บทนำ

ด้วยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้นำระบบคอมพิวเตอร์และระบบสารสนเทศที่ทันสมัยเข้ามาให้บริการเพื่อสนับสนุนการปฏิบัติงานแก่บุคลากร สคร. ทั้งในภารกิจหลักประกอบด้วย ภารกิจด้านรัฐวิสาหกิจ ด้านหลักทรัพย์ของรัฐ และด้านการให้เอกชนร่วมลงทุนในกิจการของรัฐ และภารกิจสนับสนุนสำหรับการบริหารจัดการภายใน สคร. รวมทั้งการประชาสัมพันธ์ข้อมูลข่าวสารให้กับบุคคลภายนอกที่สนใจ อย่างไรก็ตาม ในการให้บริการดังกล่าวอาจมีความเสี่ยงที่เกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศอันเนื่องมาจากเหตุการณ์ที่ไม่พึงประสงค์ต่างๆ เช่น ไฟฟ้าดับ อัคคีภัย และเหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เป็นต้น ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง 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) และภัยพิบัติหรือสถานการณ์อื่นๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต และการสำรองและกู้คืนข้อมูลสารสนเทศ เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. พ.ศ. ๒๕๖๒ สำหรับใช้เป็นแนวทางในการปฏิบัติงานต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้ สคร. มีแนวทางในการระบุและประเมินความเสี่ยงด้านสารสนเทศ รวมถึงการกำหนดแนวทางบริหารความเสี่ยงด้านสารสนเทศ โดยการป้องกัน จัดการ และลดความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และทำให้ สคร. สามารถดำเนินงานได้อย่างต่อเนื่อง

๒.๒ เพื่อให้ สคร. มีแนวทางในการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศและสามารถเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤตที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงมีแนวปฏิบัติในการบริหารจัดการ กำกับ ตรวจสอบ และดูแลรักษาระบบคอมพิวเตอร์และระบบสารสนเทศ ให้มีความมั่นคง ปลอดภัย มีเสถียรภาพ และพร้อมใช้งานตลอดเวลา

๒.๓ เพื่อให้ สคร. มีแนวทางในการสำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

/๓. ขอบเขต...

๓. ขอบเขต

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของ สคร. พ.ศ. ๒๕๖๒ ฉบับนี้ เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤตในพื้นที่ สคร. ดังนี้

๓.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.

๓.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี

๓.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)

๓.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค

๓.๕ เหตุการณ์ไฟฟ้าดับ

๓.๖ เหตุการณ์อัคคีภัย

๓.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง

๔. การวิเคราะห์ความเสี่ยงด้านสารสนเทศ

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

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีดังนี้

๔.๑ ความเสี่ยงที่เกิดจากบุคคล ดังนี้

๔.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. หมายถึง บุคลากรของ สคร. ขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ด้านซอร์ฟแวร์ และด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ไม่เหมาะสม

๔.๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี หมายถึง ผู้ที่หวังก่อกวน เจาะทำลายระบบเพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ หากไม่ได้รับการป้องกันด้วยเครื่องมือหรืออุปกรณ์ที่มีมาตรฐานและอัพเดทให้ทันสมัย เช่น Firewall ระบบ IPS และระบบป้องกันไวรัส

/๓) เหตุการณ์...

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

๔.๒ ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ในห้องศูนย์ข้อมูล (Data Center) ทำงานไม่เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูล (Process Device) ชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบปรับอากาศชำรุดส่งผลให้อุณภูมิห้องศูนย์ข้อมูล (Data Center) สูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ที่ให้บริการหยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้ หรืออาจได้รับความเสียหาย

๔.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

๔.๓.๑ เหตุการณ์ไฟฟ้าดับ หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟฟ้าดับ ซึ่งส่งผลให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ไม่มีแหล่งพลังงานที่ใช้ในการเปิดระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับให้บริการ เช่น สายไฟฟ้าขาด ไฟฟ้าช็อต หม้อแปลงไฟฟ้าที่ติดตั้งบริเวณกระทรวงการคลังระเบิดเสียหาย เนื่องจาก สคร. ใช้ไฟฟ้าจากแหล่งจ่ายไฟฟ้าดังกล่าว

๔.๓.๒ เหตุการณ์อัคคีภัย หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้างความเสียหายร้ายแรงที่สุด ทำให้ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ถูกไฟไหม้จนทำให้ไม่สามารถปฏิบัติงานได้ ซึ่งเกิดได้หลายสาเหตุ เช่น ไฟฟ้าลัดวงจร หรือไฟไหม้บริเวณอื่นแล้วไหม้ลุกลามมาที่ห้องศูนย์ข้อมูล (Data Center)

๔.๓.๓ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง หมายถึง อันเกิดจากภัยตามธรรมชาติหรือสถานการณ์ที่เกิดจากกลุ่มบุคคล ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่จะเกิดผลกระทบต่อการเข้าไปปฏิบัติงานภายในพื้นที่ สคร.

/๕. การประเมิน...

๕. การประเมินความเสี่ยงด้านสารสนเทศ

ศทส. ได้ประเมินความเสี่ยงด้านสารสนเทศจากความเสี่ยงที่เกิดจากบุคคล จากด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ในข้อ ๓ และ ๔ มาเป็นแนวทางในการดำเนินงาน โดย ศทส. ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของ สคร. แล้วปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๑. เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.	- ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเทอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผลข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้	๕	๑	๕	ค่อนข้างต่ำ	- ผู้ดูแลระบบ (Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่ายภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว - หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
๒. เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี	- ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบ หน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศล่มได้	๓	๔	๑๒	ค่อนข้างสูง	- ตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ได้ใช้งานโดยทันที

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๓. เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)	- อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ สคร. โดยเฉพาะข้อมูลที่เป็นความลับ - ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถให้บริการได้เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้	๑	๕	๕	ค่อนข้างต่ำ	- ผู้พบเหตุรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (Administrator) ตรวจสอบความครบถ้วนและความเสียหายของอุปกรณ์ประมวลผลข้อมูล (Process Device) และผลกระทบต่อระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ
๔. เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค	- อุปกรณ์ประมวลผลข้อมูล (Process Device) บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศได้ไม่เต็มประสิทธิภาพ - ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูล (Data Center) สูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย - การปฏิบัติงานเกิดความล่าช้า เนื่องจากต้องรอการซ่อมแซมแก้ไข	๓	๒	๖	ค่อนข้างต่ำ	- ผู้พบเหตุรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) หรือระบบปรับอากาศที่ได้รับความเสียหาย หากเสียหายเล็กน้อยให้ดำเนินการแก้ไข และเปิดใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศต่อไป

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕. เหตุการณ์ไฟฟ้าดับ	- อุปกรณ์ประมวลผลข้อมูล (Process Device) หยุดทำงาน - การปฏิบัติงานด้านระบบคอมพิวเตอร์และระบบสารสนเทศเกิดความล่าช้าเนื่องจากต้องรอการซ่อมแซมแก้ไข	๕	๒	๑๐	ค่อนข้างสูง	- ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) และระบบปรับอากาศ พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบเพื่อสั่งการต่อไป - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากไฟฟ้าดับ - ศทส. ประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงการคลัง เพื่อสอบถามปัญหา และระยะเวลาการแก้ไขที่จะสามารถกลับมาให้บริการได้ - ผู้ดูแลระบบ (Administrator) เปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้แล้ว
๖. เหตุการณ์อัคคีภัย	- สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ไม่สามารถให้บริการได้	๑	๕	๕	ค่อนข้างต่ำ	<u>กรณีที่ ๑ ไฟเริ่มไหม้หรือสามารถดับไฟได้</u> - ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับและให้แจ้ง ศทส. ทราบโดยเร็ว - ผู้ดูแลระบบ (Administrator) ประเมินสถานการณ์ในเบื้องต้นว่าควรหยุดให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการ ศทส. ประชาสัมพันธ์ ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากเหตุไฟไหม้

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์ข้อมูล (Data Center) พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (Administrator) ดำเนินการแก้ไขและเปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้แล้ว

/ตาราง (ต่อ)..

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- หากเสียหายมาก ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป <u>กรณีที่ ๒ ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง</u> - ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิงเป็นลำดับแรก และแจ้งให้ ศทส. ทราบโดยเร็ว - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ให้ออกจากพื้นที่โดยเร็ว - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการเนื่องจากเหตุไฟไหม้

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์ข้อมูล (Data Center) พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๗. เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง	- เช่น กรณีการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณกระทรวงการคลัง ซึ่งส่งผลกระทบต่อห้องศูนย์ข้อมูล (Data Center) หรือสถานที่ปฏิบัติงานบริเวณอาคารธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	๓	๔	๑๒	ค่อนข้างสูง	- ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไขข้อ ๕ - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ สคร. กำหนด

หมายเหตุ เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

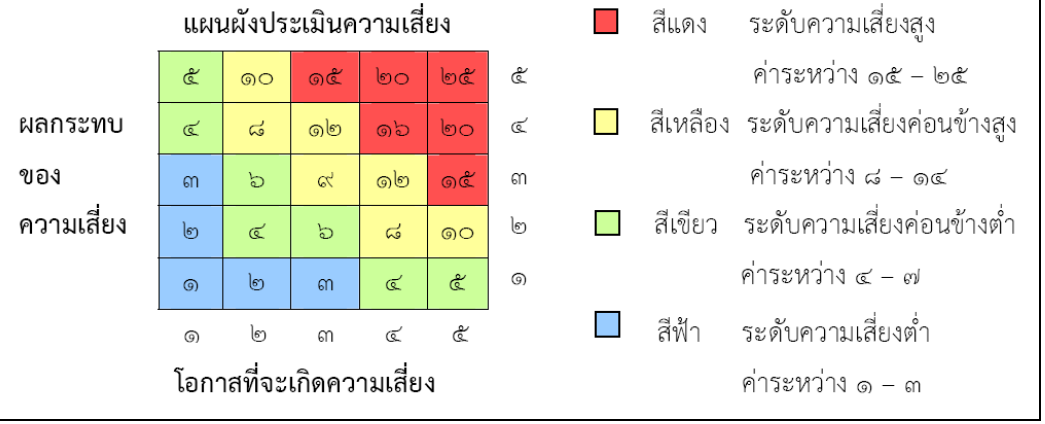
ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด

ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย

ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง

ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก

ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด



/๖. การเตรียม...

๖. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศข้างต้น ศทส. จึงได้ดำเนินการจัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

๖.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๑.๑ กำหนดให้ปฏิบัติตามประกาศ สคร. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๑.๒ การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้น โดยการจัดอบรมให้กับบุคลากร สคร. หรือส่งไปอบรมร่วมกับหน่วยงานภายนอกที่จัดขึ้น เพื่อลดความเสี่ยงด้านสารสนเทศ

๖.๑.๓ มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่างๆ ตามความเหมาะสม เช่น ผ่านระบบ Web Portal ติดบอร์ดประชาสัมพันธ์ Line, G - Chat, Facebook ของ สคร. เป็นต้น

๖.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๒.๑ ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

๖.๒.๒ ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๖.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๓.๑ มีมาตรการควบคุมการเข้า - ออกห้องศูนย์ข้อมูล (Data Center) ดังนี้

(๑) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) ตามที่ ศทส. กำหนด

(๒) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจาก ศทส. ก่อนเริ่มดำเนินการทุกครั้ง

(๓) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจาก ศทส.

(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

/๖.๔ เหตุการณ์...

๖.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๔.๑ มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ ๑ ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device) หรืออุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งาน ให้รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการแก้ไขด้วยการซ่อมแซมหรือจัดซื้อทดแทนต่อไป

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

๖.๕ เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) จำนวน ๒ เครื่อง ขนาด ๓๐ KVA และ ๒๐ KVA เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) โดยทั้ง ๒ เครื่อง สามารถสำรองไฟฟ้าได้เป็นเวลาประมาณ ๓๐ นาที ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดไฟฟ้าดับ

๖.๖ เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๖.๑ มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องศูนย์ข้อมูล (Data Center) อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือน เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงที เพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

๖.๖.๒ มีการติดตั้งถังดับเพลิงชนิดที่ใช้สารเคมีไม่ทำอันตรายต่ออุปกรณ์ประมวลผลข้อมูล (Process Device) ไว้ในห้องศูนย์ข้อมูล (Data Center) จำนวน ๑ ถัง และหน้าห้องศูนย์ข้อมูล (Data Center) จำนวน ๒ ถัง เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟเริ่มลุกลามถึงขั้นรุนแรง

๖.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๗.๑ ให้ผู้ใช้งาน (User) สำรองข้อมูลสารเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk

๖.๗.๒ มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าไปภายในห้องศูนย์ข้อมูล (Data Center) โดยไม่ได้รับอนุญาต

๖.๗.๓ ตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก สคร. (Teleworking) โดยผ่านเครือข่ายภายนอก (Internet) ได้

/๔) ตรวจสอบ...

๖.๗.๔ ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ได้บันทึกลงในตลับเทปแม่เหล็ก (Magnetic Tape Drive) สำหรับเตรียมนำไปกู้คืน ณ ไซต์สำรอง (Disaster Recovery Site : DR Site) ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง หรือตามที่ผู้บริหารเห็นชอบ หากเกิดเหตุการณ์ฉุกเฉินในสภาวะวิกฤตจนส่งผลให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องปิดระบบการให้บริการถูกปิดลง

๖.๗.๕ เมื่อ ศทส. ได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมืองบริเวณกระทรวงการคลัง ซึ่งอาจถูกปิดกั้นการเข้าออก และอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำ ให้ผู้ดูแลระบบ (Administator) นำตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองข้อมูลไว้ไปเก็บในสถานที่ปลอดภัย

๗. กลยุทธ์ความต่อเนื่องในสภาวะวิกฤต

หากเหตุการณ์หรือภัยได้เกิดขึ้นแล้ว ต้องมีการดำเนินกลยุทธ์ความต่อเนื่องในสภาวะวิกฤต เพื่อให้การปฏิบัติงานของบุคลากร สคร. ดำเนินการไปได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุด ดังนี้

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
๑. สถานที่ปฏิบัติงาน อาคารธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	๑. กำหนดพื้นที่ปฏิบัติงานสำรอง ได้แก่ ห้องคอมพิวเตอร์หรือพื้นที่อื่นๆ ของกรมบัญชีกลาง โดยประสานงานและสำรวจความเหมาะสมของสถานที่ร่วมกับกรมบัญชีกลาง ๒. ประสานขอใช้พื้นที่กับส่วนราชการหรือรัฐวิสาหกิจเป็นสถานที่ปฏิบัติงานสำรองเพิ่มเติม ๓. หากพื้นที่ปฏิบัติงานสำรองมีพื้นที่จำกัด หรืออาจเกิดอันตรายระหว่างเดินทางไปปฏิบัติงาน ให้บุคลากร สคร. ปฏิบัติงานจากที่พักอาศัย
๒. วัสดุอุปกรณ์	๑. จัดหาเครื่องคอมพิวเตอร์สำรองพร้อมอุปกรณ์ในการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศได้ ๒. จัดเตรียมอุปกรณ์สารสนเทศสำหรับนำมาใช้ในการปฏิบัติงาน เช่น เครื่องพิมพ์ (Printer) เครื่องสแกนเนอร์ (Scaner) และสายเชื่อมต่อระบบเครือข่ายเฉพาะที่ (Lan) ๓. ผู้ใช้งาน (User) สามารถใช้คอมพิวเตอร์แบบพกพาส่วนตัวในการปฏิบัติงานได้

/ตาราง (ต่อ)...

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
๓. ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ	๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศได้ติดตั้งและจัดเก็บไว้ใน ณ ห้องศูนย์ข้อมูล (Data Center) อาคารกรมบัญชีกลาง ๓ ชั้น ๖ ซึ่งรองรับการเข้าถึงจากภายนอก โดยการรับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) และมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL) ๒. ประสานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เพื่อจัดเตรียมไซต์สำรอง (Disaster Recovery Site : DR Site) เมื่อเกิดเหตุฉุกเฉินหรือสภาวะวิกฤต ๓. ศทส. พิจารณาและนำตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ ณ ห้องศูนย์ข้อมูล (Data Center) ไปไว้ในสถานที่ปลอดภัย ๔. สำหรับระบบ GFMIS - SOE ซึ่งเป็นระบบสารสนเทศตามภารกิจหลักเพื่อบริการแก่บุคลากร สคร. หน่วยงานรัฐวิสาหกิจ และส่วนราชการที่เกี่ยวข้อง ได้ติดตั้ง ณ ศูนย์คอมพิวเตอร์พิบูลสงคราม และศูนย์คอมพิวเตอร์สำรองบางบัวทอง ๕. ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศที่จำเป็นและสำคัญไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk
๔. บุคลากร สคร.	๑. หากผู้ดูแลระบบ (Administrator) มีจำนวนไม่เพียงพอต่อการปฏิบัติหน้าที่ให้ผู้รับจ้างที่ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศให้การสนับสนุนด้านเทคนิค ๒. อนุญาตให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก สคร. (Teleworking) โดยเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System)
๕. ผู้รับบริการและผู้ที่เกี่ยวข้อง	๑. แจ้งสถานที่การติดต่อราชการสำรองผ่านทางหน้าเว็บไซต์ของ สคร. ๒. บุคลากร สคร. ที่มีหน้าที่ปฏิบัติงานร่วมกับรัฐวิสาหกิจ ให้ประสานงานทางโทรศัพท์เคลื่อนที่หรือจดหมายอิเล็กทรอนิกส์ (E - Mail) หรือหากระบบคอมพิวเตอร์และระบบสารสนเทศอยู่ระหว่างดำเนินการกู้คืน ให้พิจารณาใช้จดหมายอิเล็กทรอนิกส์ (E - Mail) จากภายนอกที่มีความน่าเชื่อถือ

/๘. ระยะ...

๘. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต

จากการวิเคราะห์ผลกระทบจากความเสี่ยงในข้อ ๕ เพื่อให้บุคลากรสามารถปฏิบัติงานด้วยความต่อเนื่อง จึงกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต ดังนี้

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

๙. โครงสร้างและทีมบริหารความต่อเนื่อง (BCP Team)

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง (BCP Team) ซึ่งประกอบด้วยผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) ผู้อำนวยการ ศทส. และบุคลากรของ ศทส. เนื่องจากมีความรู้ความสามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่เป็นผู้ดูแลระบบ (Administrator) ของ สคร.

/๙.๑ หน้าที่...

๙.๑ หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง (BCP Team) ดังนี้

๙.๑.๑ หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้ที่รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหารระดับสูง สคร. ได้รับทราบ

๙.๑.๒ ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอก สคร. และจัดเตรียมเอกสารข้อมูลที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

๙.๑.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลห้องศูนย์ข้อมูล (Data Center)

๙.๒ รายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ

ชื่อ	บทบาท	โทรศัพท์
นางสาวรสา กาญจนสาย	หัวหน้าทีมบริหารความต่อเนื่อง (BCP Team)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๓๓๐๐ - ๐๘๑ ๘๕๔ ๙๓๓๑
นางสาวภัทรา นิยะถิระกุล	รองหัวหน้าทีมบริหารความต่อเนื่อง (BCP Team)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๗๕ - ๐๘๑ ๘๑๕ ๔๕๓๓
นายกรินทร์ ศิริพัฒน์พิบูลย์	ผู้ดูแลระบบ (Administrator) (บุคลากรหลัก)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๗๓ - ๐๘๑ ๙๓๐ ๕๓๖๐
นายโชคชัย อภัยโส		- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๔ - ๐๘๑ ๒๗๙ ๙๗๐๘
นายณัฐพล จรัสดำรงนิตย์	ผู้ดูแลระบบ (Administrator) (บุคลากรสำรอง)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๒ - ๐๘๓ ๘๕๑ ๓๓๖๐
นายวันชัย เพ็งจางค์		- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๐ - ๐๘๔ ๐๘๓ ๕๙๙๕
นายณัฐวุฒิ สมภารเพียง	ผู้ประสานงาน (บุคลากรหลัก)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๓ - ๐๙๑ ๑๗๑ ๙๕๙๕
นางสาวจตุพร นันทพรหม	ผู้ประสานงาน (บุคลากรสำรอง)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๓ - ๐๘๖ ๓๘๖ ๓๒๒๑

/๑๐. กระบวนการ...

๑๐. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

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

๑๑. การสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องศูนย์ข้อมูล (Data Center) ซึ่งเข้าถึงด้วยเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing) ซึ่งเป็นการอำนวยความสะดวกแก่ผู้ใช้งาน (User) เป็นอย่างมาก แต่ก็มีความเสี่ยงสูงมากเช่นกันเพราะเป็นลักษณะแบบรวมศูนย์กลาง ศทส. ซึ่งเป็นผู้ดูแลรับผิดชอบหลักจึงจัดทำแนวปฏิบัติการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วหากเกิดปัญหา

๑๑.๑ ผู้รับผิดชอบ

รายละเอียดบุคลากรและหน้าที่ความรับผิดชอบ ตามข้อ ๙

๑๑.๒ แนวปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนอุปกรณ์ประมวลผลข้อมูล (Process Device)

ศทส. มอบหมายให้ผู้ดูแลระบบ (Administrator) ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) ณ ห้องศูนย์ข้อมูล (Data Center) อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง หากพบข้อผิดพลาดให้รายงาน ศทส. โดยทันที

๑๑.๓ แนวปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

๑๑.๓.๑ ผู้ดูแลระบบ (Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) ตามขั้นตอนของโปรแกรม Symantec NetBackup

๑๑.๓.๒ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

/๑๑.๓.๓ รายละเอียด...

๑๑.๓.๓ รายละเอียดการสำรองข้อมูล กำหนดดังนี้

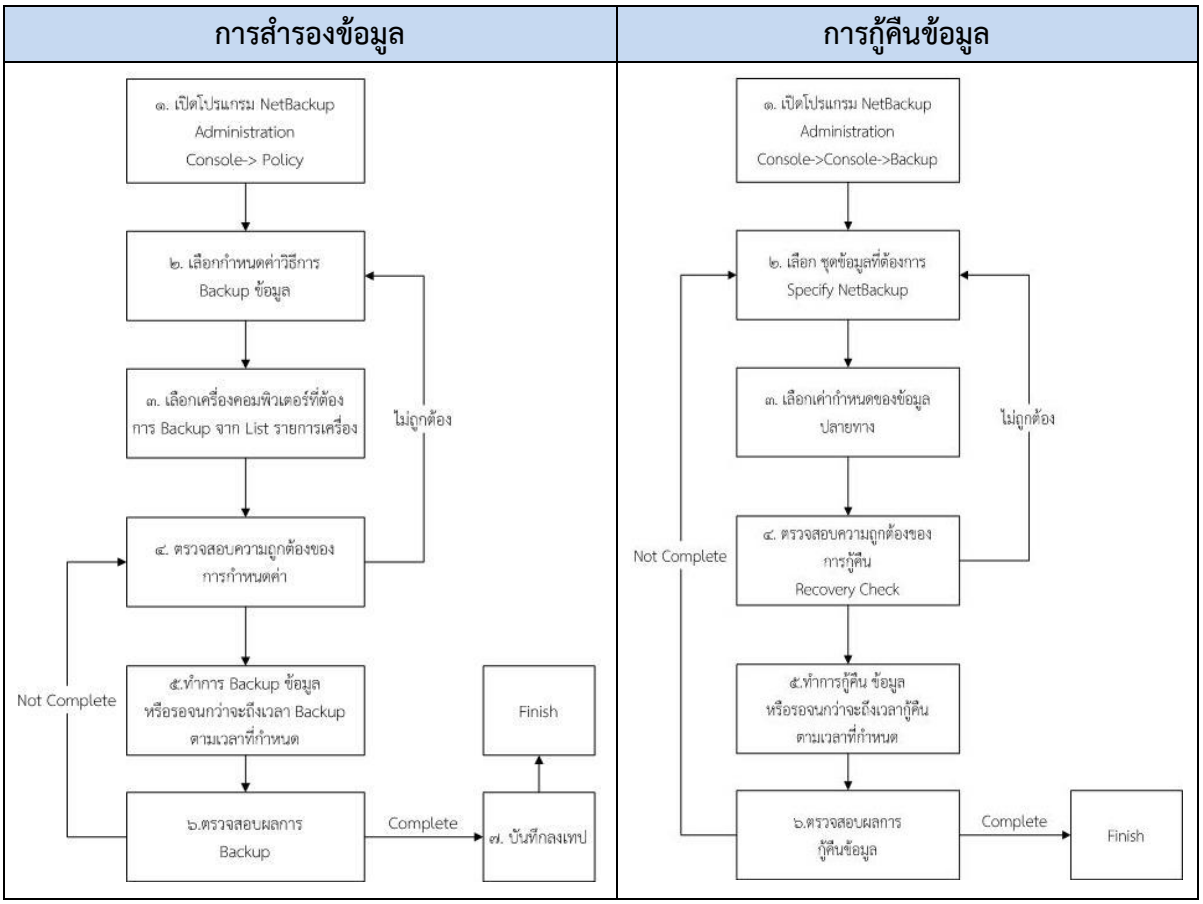
ลำดับ	รายการ	จำนวน (หน่วย)	ข้อมูลที่สำรอง
๑	เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับประมวลผลระบบเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (VDI)	๔ เครื่อง	ค่า Configuration
๒	เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (VDI) สำหรับประมวลผลระบบสารสนเทศ	๓๖ เครื่อง	Full
๓	เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับประมวลผลระบบเครื่องคอมพิวเตอร์ลูกข่ายแบบเสมือน (VDI)	๑๒ เครื่อง	ค่า Configuration
๔	เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน สำหรับประมวลผลระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI)	๖ เครื่อง	Full
๕	ระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI)	๒๐๐ เครื่อง	Drive Z

๑๑.๔ แนวปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศเกิดปัญหาไม่สามารถใช้งานได้ หรือข้อมูลสารสนเทศสูญหาย ให้ผู้ดูแลระบบ (Administrator) ดำเนินการกู้คืนข้อมูลสารสนเทศที่สำรองไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) เพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน

/๑๑.๕ แผนผัง...

๑๑.๕ แผนผังการสำรองและกู้คืนระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศด้วยโปรแกรม Symantec NetBackup



๑๑.๖ ศทส. ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๑๑.๖.๑ พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการทดสอบพร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

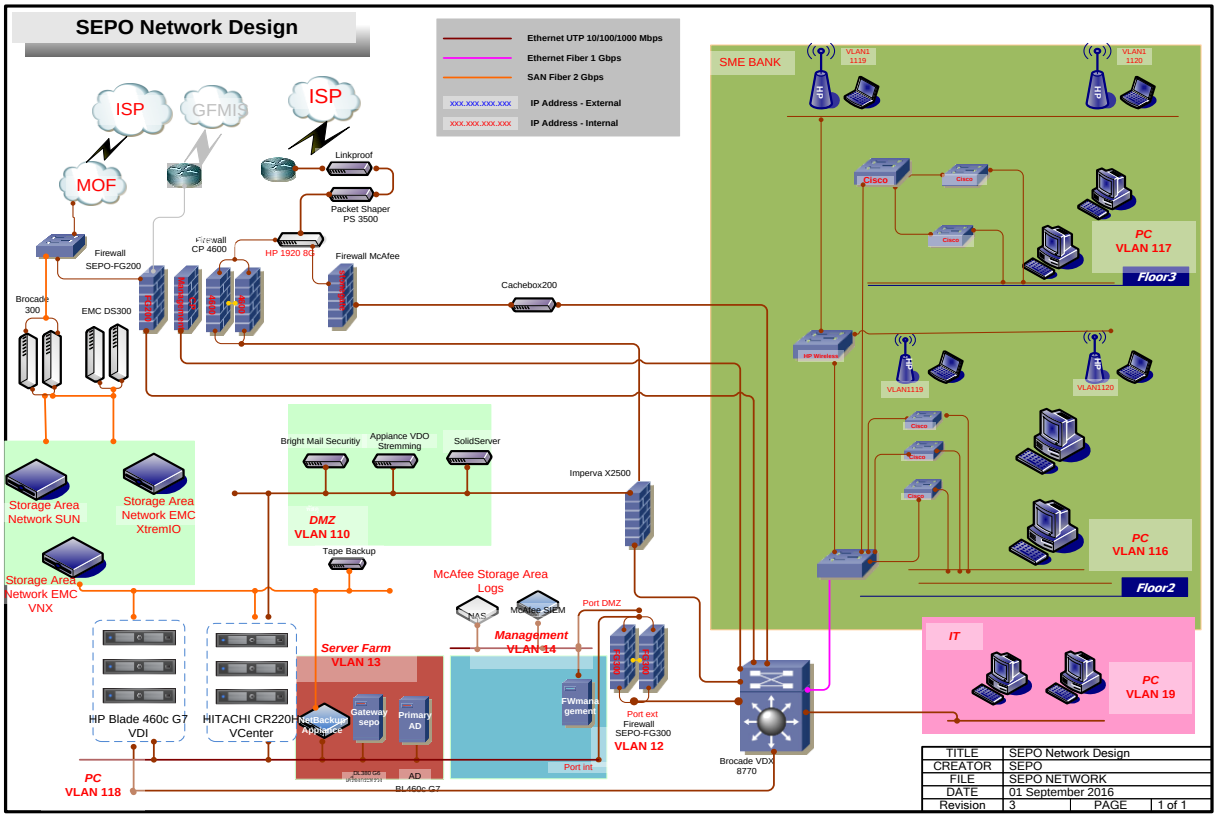
๑๑.๖.๒ จัดทำรายงานเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ก่อนดำเนินการทดสอบ

๑๑.๖.๓ ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

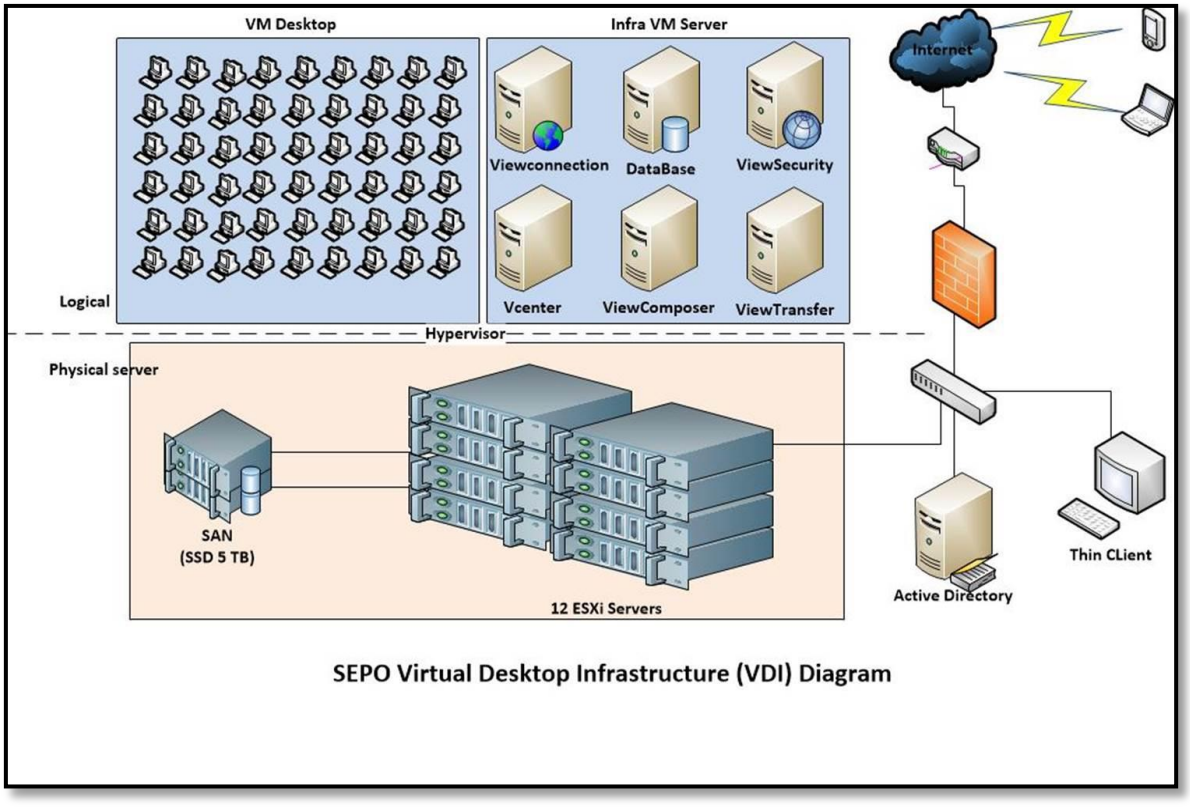
๑๑.๖.๔ รายงานผลการทดสอบเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

/ภาคผนวก...

๑. ผังแสดงสถาปัตยกรรมโครงข่ายคอมพิวเตอร์ (Network Infrastructure Diagram) ของ สคร.



๒. ผังแสดงสถาปัตยกรรมระบบเครื่องคอมพิวเตอร์ลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)



/๓. ผู้ประสานงาน...

๓. ผู้ประสานงานภายนอก

ลำดับ	หน่วยงาน	หมายเลขโทรศัพท์
๑.	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง	๐๒ ๒๗๓ ๙๕๒๕-๖
๒.	บริษัท ทีโอที จำกัด	๐๒ ๕๗๔ ๘๘๔๘-๙ หรือสายด่วน ๑๑๐๐
๓.	บริษัท กสท โทรคมนาคม จำกัด (มหาชน)	๐๒ ๑๐๔ ๔๗๗๖ หรือสายด่วน ๑๓๒๒
๔.	สถานีดับเพลิง สำนักงานเขตพญาไท	๐๒ ๓๕๔ ๖๘๕๘ หรือสายด่วน ๑๙๙
๕.	สถานีตำรวจนครบาลเขตพญาไท	๐๒ ๓๕๔ ๖๙๕๘ หรือสายด่วน ๑๙๑