แผนรองรับสถานการณ์ฉุกเฉิน

(IT Contingency Plan)

สำนักงานกองทุนน้ำมันเชื้อเพลิง (สกนช.)

Oil Fuel Fund Office (OFFO)

โดย กลุ่มงานบริหารสารสนเทศ สำนักนโยบายและยุทธศาสตร์

เดือนมีนาคม ๒๕๖๕

แผนรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

บทนำ

ปัจจุบัน สำนักงานกองทุนน้ำมันเชื้อเพลิง (สกนช.) มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีการจัดการข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

สกนช. จึงได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของ สกนช. ดังนั้น เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

(๑) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

(๒) เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

(๓) เพื่อให้ระบบเทคโนโลยีสารสนเทศ สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

(๔) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ สกนช.

(๕) เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของ สกนช.

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑ การวิเคราะห์เหตุการณ์ภัยพิบัติ

แผนรองรับสถานการณ์ฉุกเฉินที่จะเกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของ สกนช. จะครอบคลุมเหตุการณ์ ต่อไปนี้

(๑) เหตุการณ์อุทกภัย

(๒) เหตุการณ์อัคคีภัย/ไฟดับ

(๓) เหตุการณ์ถูกโจมตีทางไซเบอร์

(๔) เหตุการณ์ชุมนุม ประท้วง จลาจล

(๕) เหตุการณ์โรคระบาด

ทั้งนี้ สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้น เพื่อให้หน่วยงานสามารถบริหารจัดการการดำเนินงานขององค์กรให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็น และต้องระบุไว้ในแผนดำเนินธุรกิจอย่างต่อเนื่อง ซึ่งการเตรียมการทรัพยากรที่สำคัญ จะพิจารณาจากผลกระทบใน ๕ ด้าน ดังนี้

๑. **ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้ และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว ซึ่งรวมทั้งการที่ผู้รับบริการไม่สามารถเข้าถึงสถานที่ให้บริการของหน่วยงานด้วย

๒. **ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้

๓. **ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

๔. **ผลกระทบด้านบุคลากรหลัก** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

๕. **ผลกระทบด้านคู่ค้า/ผู้ให้บริการที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อ สกนช. มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) โดยกลุ่มงานบริหารสารสนเทศ เพื่อนำมาสรุปเป็นข้อมูลต่อไปนี้

สถานการณ์ หรือ ภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน ๕ คะแนน)			คะแนนรวม	จัดเรียงลำดับ
	ต่อระบบงาน	ต่อพันธกิจ	ต่อผู้ใช้บริการ		
กรณีอัคคีภัย/ไฟดับ	๕	๕	๕	๑๕	๑
กรณีถูกโจมตีทางไซเบอร์	๕	๕	๕	๑๕	๑
กรณีอุทกภัย	๕	๓	๓	๑๑	๒
กรณีชุมนุม/ประท้วง/จลาจล	๓	๒	๔	๙	๓
กรณีโรคระบาด	๒	๒	๓	๗	๔

การกำหนดระดับความรุนแรงของผลกระทบ

ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
๔	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

๒. แนวทางการป้องกันและการเตรียมการเบื้องต้น

๒.๑ การประกาศแผน (Activation)

สกนช. ต้องการประกาศใช้แผนรองรับสถานการฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการสำนักนโยบายและยุทธศาสตร์จะทำการแจ้งให้ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิงทราบ เพื่อพิจารณาและประการใช้แผนต่อไป

๒.๒ กระบวนการดำเนินงาน (Procedure)

กลุ่มงานบริหารสารสนเทศ จัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติใน สกนช. โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่าง ๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๒.๓ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกลุ่มงานบริหารสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- ✓ แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- ✓ เทปสำรองข้อมูลและระบบงานที่สำคัญ
- ✓ แผ่นโปรแกรม antivirus/spyware
- ✓ แผ่น driver อุปกรณ์ต่าง ๆ
- ✓ ระบบสำรองไฟฉุกเฉิน
- ✓ อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๒.๔ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดย สกนช. มีการสำรองข้อมูลของทุกกลุ่มงานโดย External Harddisk เป็นประจำทุกเดือน และมีระบบ Network Attach Storage (NAS) สำรองข้อมูลในระบบเครือข่ายโดยอัตโนมัติเป็นประจำทุกวัน

๓. การเตรียมความพร้อมและการดำเนินการรองรับสถานการณ์ฉุกเฉิน

๓.๑ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

๔) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือน เป็นอย่างน้อย

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้ เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อการควบคุมเพลิงเบื้องต้น

๒) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือน เป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ที่ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้

๓) อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย

๔) ให้เจ้าหน้าที่กลุ่มงานบริหารสารสนเทศ แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๕) กรณีถูกไวรัส เพื่อจำกัดความเสียหายที่อาจแพร่กระจากไปยังเครื่องอื่น ๆ ในระบบเครือข่าย ให้ทำการจำกัดการเชื่อมต่อระบบเครือข่าย

๖) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

๗) ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

๘) ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๙) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ ให้แจ้งเหตุให้กลุ่มงานบริหารสารสนเทศทราบ หรือ กรณีมีเหตุอันทำให้กลุ่มงานบริหารสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานภายในทราบ

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากการถูกโจมตีทางไซเบอร์ เช่น แทรกแซง บุกรุก การโจมตีระบบเครือข่าย และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) กำหนดมาตรการควบคุมการเข้าออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ หากจำเป็นต้องเข้าไป ให้มีเจ้าหน้าที่ของกลุ่มงานบริหารสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตของ สกนช. และการกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตของ สกนช. เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศที่มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) มีการป้องกันชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๖) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ฉบับที่ ๒ พ.ศ. ๒๕๖๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ได้เป็นอย่างดี

๗) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของ Firewall ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้ และแจ้งให้ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง ทราบโดยด่วน

๘) กรณีการเชื่อมโยงเครือข่ายล้มเหลว ผู้ดูแลระบบต้องรีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

๓.๕ การเตรียมความพร้อมรับสถานการณ์จากกรณีอุทกภัย เป็นเหตุการณ์ที่อาจส่งผลให้เกิดเหตุฉุกเฉินในช่วงฤดูฝน และประเมินสถานการณ์น้ำในพื้นที่ ดังนี้

๑) หัวหน้าทีมงานประเมินสถานการณ์ความเสี่ยง ว่ามีผลกระทบพนักงาน และผู้ใช้บริการหรือไม่ อย่างไร

๒) กำหนดจุด/พื้นที่ปลอดภัย เส้นทางอพยพหน่วยงาน ทีมงานทำการอพยพพนักงานและผู้ใช้บริการ

๓) จัดเตรียมเครื่องอำนวยความสะดวกให้เพียงพอเหมาะสมระหว่างอพยพ กรณีไม่สามารถกลับเข้าสำนักงานได้ หรือไม่สามารถเดินทางกลับเข้าที่พักอาศัยได้

๓.๖ การเตรียมความพร้อมรับสถานการณ์จากกรณีความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุม ประท้วง จลาจล

๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งให้ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง ทราบโดยด่วน

๒) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบตรวจสอบรายการทรัพย์สิน ตรวจสอบความชำรุดเสียหาย ซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการแก้ไข

๓.๗ การเตรียมความพร้อมรับสถานการณ์จากกรณีโรคระบาด ให้ความสำคัญกับการดำเนินการให้สอดคล้องกับมาตรการป้องกันโรคของกระทรวงสาธารณสุข และให้ดำเนินการ ดังนี้

๑) แต่ละสำนัก/กลุ่มงาน เตรียมความพร้อมด้านเอกสาร ข้อมูลที่สำคัญและอุปกรณ์สำนักงานที่จำเป็น ในกรณีมีการย้ายสถานที่ปฏิบัติงาน และเตรียมความพร้อมในการทำงานที่บ้าน (Work From Home) ผ่านระบบอิเล็กทรอนิกส์ หรือผ่านระบบออนไลน์

๒) ผู้บริหารร่วมกับผู้อำนวยการสำนัก/กลุ่มงาน ประเมินสถานการณ์ โดยการจัดประชุมเตรียมความพร้อม

๓) กรณีเกิดโรคระบาดร้ายแรง จำเป็นต้องปิดสำนักงาน ให้เจ้าหน้าที่รับเรื่องจากผู้มารับบริการ และแจ้งว่าจะดำเนินการทันทีที่สามารถดำเนินการได้

๔) กรณีพบว่าเจ้าหน้าที่ผู้ปฏิบัติงานมีอาการป่วยเข้าข่ายอาการของโรคระบาด ให้ดำเนินการแจ้งสถานพยาบาลที่อยู่ในพื้นที่ใกล้เคียง หรือตามที่กระทรวงสาธารณสุขกำหนดโดยเร็ว

๓.๘ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่กลุ่มงานต่าง ๆ ภายใน สกนช. ขาดทักษะความรู้ความเข้าใจในเครื่องมือและอุปกรณ์คอมพิวเตอร์ โดยผู้ดูแลระบบชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจด้านฮาร์ดแวร์ และซอฟต์แวร์เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๓.๙ การเตรียมความพร้อมรับสถานการณ์จากอุปกรณ์จัดเก็บข้อมูลเสียหาย ผู้ดูแลระบบแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ และรีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลทดแทน และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว จากนั้น ทดสอบความสมบูรณ์ของข้อมูลและแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

๓.๑๐ การเตรียมความพร้อมรับสถานการณ์จากกรณีโจรกรรม

๑) ผู้ปฏิบัติงานแจ้งให้ผู้บังคับบัญชาทราบโดยด่วน

๒) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

๓) ผู้ดูแลระบบ รีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบต่าง ๆ ได้โดยเร็ว

๓.๑๑ การเตรียมความพร้อมรับสถานการณ์จากกรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

๑) แจ้งให้ผู้บังคับบัญชาทราบ

๒) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

๔. คณะทำงานบริหารความต่อเนื่อง (Business Continuity Plan Team)

สำนักงานกองทุนน้ำมันเชื้อเพลิง ได้มีการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง สำหรับการบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Plan : BCP) และมีการจัดตั้งคณะทำงานบริหารความต่อเนื่อง (BCP Team) ประกอบด้วย หัวหน้าทีมงานบริหารความต่อเนื่อง และทีมงานบริหารความต่อเนื่อง

โดยทุกตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในฝ่ายงานของตนเอง ให้สามารถบริหารความต่อเนื่องและกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่อง (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลัก ดังนี้

รายชื่อบุคลากรและบทบาทของทีมงานบริหารความต่อเนื่อง (BCP Team)

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์โทรศัพท์		ชื่อ	เบอร์โทรศัพท์
นายพรชัย จิรกุลไพศาล (ผู้อำนวยการสำนักนโยบายและยุทธศาสตร์)	๐๒ ๗๙๔ ๖๐๖๓	หัวหน้าทีมงานบริหารความต่อเนื่อง	นางสาววนิดา สมันแก้ว (ผู้อำนวยการกลุ่มงานบัญชี)	๐๒ ๗๙๔ ๖๐๖๐
นางสาวกิ่งกาญจน์ บรรจงอักษร (ผู้อำนวยการกลุ่มงานยุทธศาสตร์และแผน)	๐๒ ๗๙๔ ๖๐๗๓	ทีมงานบริหารความต่อเนื่อง	นายทศพล จันทจิตร (ผู้อำนวยการกลุ่มงานการเงิน)	๐๒ ๗๙๔ ๖๐๕๘
นายสิริศักดิ์ พันธ์สังข์ (ผู้อำนวยการกลุ่มงานบริหารสารสนเทศ)	๐๒ ๗๙๔ ๖๐๖๔	ทีมงานบริหารความต่อเนื่อง	นางสาวกุลธิดา สมิตไมตรี (ผู้อำนวยการกลุ่มงานบริหารกลาง)	๐๒ ๗๙๔ ๖๐๕๓

ทั้งนี้ บทบาทหน้าที่ของคณะทำงานบริหารความต่อเนื่อง มีดังต่อไปนี้

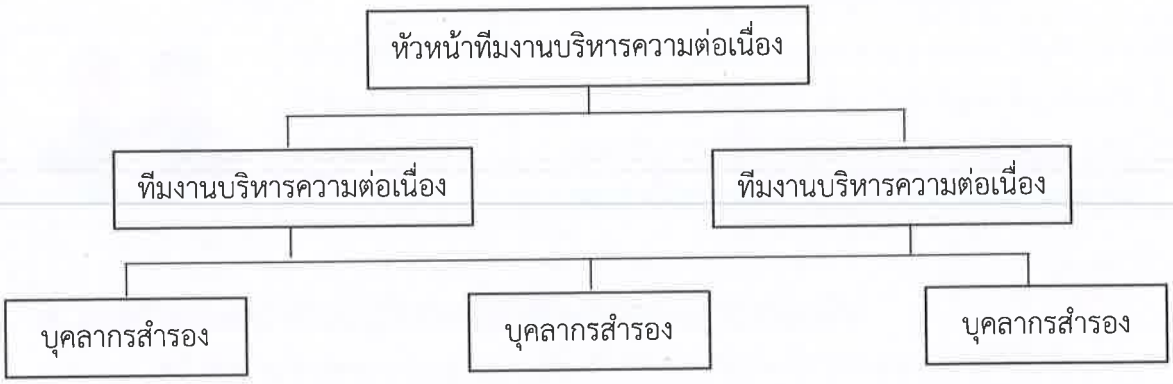
๑. หัวหน้าทีมงานบริหารความต่อเนื่อง มีหน้าที่ในการประเมินลักษณะขอบเขตและแนวโน้มของเหตุการณ์ที่เกิดขึ้น เพื่อตัดสินใจประกาศใช้แผนบริหารความต่อเนื่อง และดำเนินการตามขั้นตอนและแนวทางการบริหารความต่อเนื่อง ตลอดจนสรรหาทรัพยากรตามที่ได้กำหนดไว้

๒. ทีมงานบริหารความต่อเนื่อง มีหน้าที่ในการสนับสนุนการปฏิบัติงานของหัวหน้าทีมงานบริหารความต่อเนื่อง และบริหารจัดการให้มีการดำเนินตามขั้นตอนและแนวทางการบริหารความต่อเนื่อง

๓. บุคลากรสำรอง มีหน้าที่ในการติดต่อประสานงานภายในหน่วยงาน และให้การสนับสนุนในการติดต่อสื่อสารกับบุคลากรภายในสำนักงาน และดำเนินการตามขั้นตอนและแนวทางการบริหารความต่อเนื่อง

๕. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการ Call Tree คือกระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในทีมบริหารความต่อเนื่องและผู้ที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อบุคลากร ภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของหน่วยงาน



จุดเริ่มต้นของกระบวนการแจ้งเหตุฉุกเฉินจะเริ่มจากหัวหน้าทีมงานบริหารความต่อเนื่องแจ้งให้ทีมงานบริหารความต่อเนื่อง รับทราบเหตุการณ์ฉุกเฉินและประกาศใช้แผนบริหารความต่อเนื่อง ตามสายงานบังคับบัญชาของแต่ละสายงาน ผู้อำนวยการสำนักแต่ละท่านจะติดต่อและแจ้งไปยังบุคลากรภายใต้การบังคับบัญชาเพื่อรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนบริหารความต่อเนื่อง ในกรณีที่ไม่สามารถติดต่อได้ ให้ติดต่อไปยังบุคลากรสำรอง เพื่อแจ้งข้อมูล นัดหมายการประชุมเพื่อหารือ สรุปสถานการณ์ และขั้นตอนการปฏิบัติงานตามแผนบริหารความต่อเนื่องในภาวะฉุกเฉินฯ ต่อไป

๖. กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy)

สกนช. ได้มีการกำหนดกลยุทธ์ความต่อเนื่อง (Business Continuity Strategy) เพื่อเป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ดังนี้

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**อาคาร/สถานที่ปฏิบัติงานสำรอง**	■ กำหนดให้ใช้พื้นที่ปฏิบัติการสำรองในสำนักงานที่ไม่ได้รับผลกระทบ โดยมีการสำรวจความหมาะสมของสถานที่
	**วัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ**	■ กำหนดให้มีการจัดหาคอมพิวเตอร์สำรอง ที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมโยงต่อผ่านอินเตอร์เน็ต ■ กำหนดให้ใช้คอมพิวเตอร์แบบพกพา (Laptop หรือ Notebook Computer) ที่อาจจะเป็นเครื่องส่วนบุคคลจนกว่าจะดำเนินการหาเครื่องสำรองได้
	**เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ**	■ กำหนดให้แต่ละหน่วยงานมีการพัฒนาระบบสำรองข้อมูล และให้มีกำหนดการสำรองข้อมูล (Back-up) ให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้สามารถนำข้อมูลมาใช้งานได้อย่างต่อเนื่อง
	**บุคลากรหลัก**	■ กำหนดให้ใช้บุคลากรสำรอง ทดแทนภายในกลุ่มงานเดียวกัน ■ กำหนดให้ใช้บุคลากรนอกฝ่าย หรือกลุ่มงานในกรณีที่บุคลากรไม่เพียงพอหรือขาดแคลน

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย**	▪ ระบบเทคโนโลยีสารสนเทศของ สกนช. ใช้บริการจากผู้ให้บริการอินเตอร์เน็ต คือ บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) รวมทั้งการใช้งานระบบ e Saraban และ G-Cloud ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๗. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เป็นดังนี้

๗.๑ ระดับนโยบาย

ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ ได้แก่

๑) ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง
๒) ผู้อำนวยการสำนักนโยบายและยุทธศาสตร์

๗.๒ ระดับปฏิบัติ

ผู้รับผิดชอบการปฏิบัติงาน ดูแลระบบของหน่วยงาน ดูแลห้องเครื่องแม่ข่าย รักษาความปลอดภัยระบบฐานข้อมูลและระบบสารสนเทศ และประสานหน่วยงานที่เกี่ยวข้อง ได้แก่

๑) กลุ่มงานบริหารสารสนเทศ
๒) ผู้ดูแลระบบสารสนเทศและเครือข่ายของหน่วยงาน (Outsourcing)