แผนเตรียมความพร้อมกรณีฉุกเฉิน
ด้านระบบข้อมูลสารสนเทศ ขององค์การคลังสินค้า

สำนักเทคโนโลยีสารสนเทศ
ปรับปรุง ๑๐ กันยายน ๒๕๕๘

สารบัญ

หน้า

๖ แผนรองรับสถานการณ์ฉุกเฉิน

๗ แผนการทดสอบและซ้อมการกู้คืนระบบ

ส่วนที่ ๑ แนวนโยบายการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

แนวนโยบายการเตรียมความพร้อมกรณีฉุกเฉิน

ด้านระบบสารสนเทศ ขององค์การคลังสินค้า

๑. บทนำ

๑.๑หลักการและเหตุผล

ปัจจุบันองค์การคลังสินค้ามีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น อีกทั้งข้อมูลและสารสนเทศต่างๆ เป็นทรัพย์สินที่มีความสำคัญต่อองค์กรที่จะต้องได้รับการดูแลรักษาให้เกิดความมั่นคงและปลอดภัยเพื่อให้สามารถนำไปใช้ประโยชน์ในการดำเนินงานขององค์การคลังสินค้าได้อย่างมีประสิทธิภาพ

องค์การคลังสินค้ามีความตระหนักในความสำคัญของระบบเทคโนโลยีสารสนเทศ ข้อมูล และสารสนเทศต่างๆ ซึ่งอาจได้รับผลกระทบทั้งจากปัจจัยภายนอกและปัจจัยภายในที่จะส่งผลให้ระบบเทคโนโลยีสารสนเทศ ข้อมูล และสารสนเทศ รวมทั้งอุปกรณ์ต่างๆ เสียหายได้ โดยเฉพาะอย่างยิ่งระบบสารสนเทศที่สำคัญซึ่งใช้ในการดำเนินงานตามพันธกิจและการบริหารจัดการขององค์การคลังสินค้า ดังนั้นองค์การคลังสินค้าจึงได้จัดแผนเตรียมความพร้อมกรณีฉุกเฉินด้านระบบสารสนเทศขององค์การคลังสินค้าขึ้นเพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาระบบสารสนเทศให้ทำงานได้อย่างปกติ ตลอดจนการดูแลรักษาระบบให้มีเสถียรภาพและพร้อมใช้งาน

๑.๒วัตถุประสงค์

๑.๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศขององค์การคลังสินค้า

๑.๒.๒ เพื่อลดความเสียหายและเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ

๑.๒.๓ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน โดยจัดทำแผนการเตรียมความพร้อมกรณีฉุกเฉินด้านระบบสารสนเทศ

๑.๒.๔ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒. ขอบเขตของการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้านระบบสารสนเทศ

๒.๑ ต้องครอบคลุมเหตุการณ์ภัยคุกคามที่กำหนดไว้ในแผนการบริหารความพร้อมต่อภาวะวิกฤตขององค์การคลังสินค้า

๒.๒ หน่วยงานอาจทำการวิเคราะห์ปัจจัยเสี่ยงเพิ่มเติมเพื่อให้ครอบคลุมเหตุการณ์ภัยคุกคามที่มีผลต่อหน่วยงานของตนเอง

๒.๓ ต้องมีการกำหนดผู้รับผิดชอบในการดำเนินงานแต่ละระดับ เพื่อให้การทำงานที่สำคัญของระบบสารสนเทศสามารถดำเนินการอย่างต่อเนื่อง และ/หรือ สามารถกู้คืนได้

๓. บทบาทและความรับผิดชอบ

สำนักเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินสำหรับระบบสารสนเทศแต่ละระบบที่จำเป็นต่อการดำเนินงานที่สำคัญขององค์การคลังสินค้า

๔. ทรัพยากรที่จำเป็นในการดำเนินงาน

องค์การคลังสินค้าต้องจัดหาและบำรุงรักษาทรัพยากรต่างๆ ที่จำเป็นในการดำเนินงานเพื่อให้เป็นไปตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

๕. การอบรม

องค์การคลังสินค้าต้องให้การสนับสนุนในการฝึกอบรมบุคลากรซึ่งมีหน้าที่ปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ ให้มีทักษะที่จำเป็นในการดำเนินงานตามแผนได้

๖. แผนการทดสอบและซ้อมการกู้คืนระบบ

องค์การคลังสินค้าต้องสนับสนุนการดำเนินงานของสำนักเทคโนโลยีสารสนเทศในการทดสอบและซ้อมการปฏิบัติงานของบุคลากรตามแผนการกู้คืนระบบเป็นประจำทุกปี เพื่อหาจุดอ่อนหรือจุดบกพร่องในการดำเนินงาน

๗. การทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

สำนักเทคโนโลยีสารสนเทศต้องมีการทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศเป็นประจำทุกปีและพิจารณาปรับปรุงแผนตามความจำเป็น เช่น การเปลี่ยนแปลงในฟังก์ชั่นทางธุรกิจและระบบสนับสนุนต่าง ๆ การเปลี่ยนแปลงด้านสภาพแวดล้อม การควบคุมทางด้านเทคนิคและสภาพแวดล้อม และด้านบุคลากรและตำแหน่งความรับผิดชอบ เพื่อให้แผนการบริหารความต่อเนื่องให้กับธุรกิจ เป็นแผนที่สามารถนำมาใช้งานได้ในทุกสภาวะ

๘. การสำรองข้อมูลและการจัดเก็บสื่อสำรองข้อมูล

ให้ดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้า

ส่วนที่ ๒ แผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

แผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

ขององค์การคลังสินค้า

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติงานเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

๑.๒ เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑.๓ เพื่อให้ระบบสารสนเทศที่สำคัญต่อการดำเนินงานขององค์การคลังสินค้าสามารถทำงานได้อย่างต่อเนื่องและช่วยลดความเสียหายที่จะเกิดขึ้นต่อองค์กร

๒. ขอบเขตของแผน

แผนเตรียมความพร้อมกรณีฉุกเฉินด้านระบบข้อมูลสารสนเทศ โดยครอบคลุมระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบที่เกี่ยวข้องกับการให้บริการด้านระบบสารสนเทศ ที่ตั้งอยู่ที่องค์การคลังสินค้า ๕๖๓ ถนนนนทบุรี ตำบลบางกระสอ อำเภอเมือง จังหวัดนนทบุรี ๑๑๐๐๐

การดำเนินการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้านระบบข้อมูลสารสนเทศ ต้องดำเนินการวิเคราะห์และปัจจัยเสี่ยงของระบบสารสนเทศหลักที่มีความสำคัญต่อภารกิจและการบริการของหน่วยงาน เพื่อให้ครอบคลุมเหตุการณ์ภัยคุกคามที่มีผลต่อหน่วยงาน รวมถึงกำหนดผู้รับผิดชอบในการดำเนินงานแต่ละระดับ เพื่อให้การทำงานที่สำคัญของระบบสารสนเทศสามารถดำเนินการอย่างต่อเนื่อง และ/หรือ สามารถกู้คืนได้

๓. การวิเคราะห์ปัจจัยความเสี่ยง

๓.๑ การประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินงาน

สำนักเทคโนโลยีสารสนเทศได้ทำการวิเคราะห์ปัจจัยเสี่ยงที่มีผลกระทบต่อการทำงานหรือกระบวนการปฏิบัติงานที่สำคัญของสำนักเทคโนโลยีสารสนเทศ เพื่อใช้ในการกำหนดขอบเขตของแผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ โดยแบ่งออกเป็น ปัจจัยภายนอกและปัจจัยภายใน ดังนี้

๑) ปัจจัยภายนอก

ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
๑	ฝุ่น (Dust)	ต่ำ	- ควบคุมสภาวะแวดล้อมของห้องคอมพิวเตอร์แม่ข่าย ให้เป็นพื้นที่ปิด	ต่ำ	ไม่มี
๒	ควัน (Smoke)	ต่ำ	- ควบคุมสภาวะแวดล้อมของห้อง Data Center ให้เป็นพื้นที่ปิด - มีการจัดการระบบระบายอากาศของห้อง Data Center ให้เหมาะสม	ต่ำ	ไม่มี
๓	เพลิงไหม้ (Fire)	ต่ำ	- ห้องคอมพิวเตอร์แม่ข่าย ได้ทำการติดตั้งระบบ Fire Suppression System ได้แก่ ๑) อุปกรณ์ตรวจจับควัน ๒) ระบบสัญญาณเตือนอัคคีภัย อัตโนมัติ ๓) ระบบดับเพลิงอัตโนมัติ และถังดับเพลิง - มีแผนการจัดทำศูนย์สำรองข้อมูล DR Site - มีการตรวจสอบอุปกรณ์เกี่ยวกับระบบไฟฟ้าต่าง ๆ เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ปลอดภัยอย่างสม่ำเสมอ - มีการตรวจสอบการทำงาน Fire Suppression System เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ	สูง	มี
๔.	น้ำดับเพลิง, น้ำท่วมขังหรือรอยรั่วที่เกิดจากการสร้างไม่ได้มาตรฐาน (Water or Supply Failure)	ต่ำ	- ดำเนินการตัดระบบกระจายน้ำดับเพลิงอัตโนมัติที่ติดตั้งอยู่ภายในห้อง Data Center	กลาง	ไม่มี
๕	แรงสั่นสะเทือน (Vibration)	ต่ำ	- ห้อง Data Center ตั้งอยู่ในพื้นที่ห่างจากแรงสั่นสะเทือนจากรถไฟ และแผ่นดินไหว	ต่ำ	ไม่มี

๖	ถูกโจรกรรมและวินาศกรรม (Theft)	กลาง	- มีศูนย์สำรองข้อมูล DR Site - มีระบบการควบคุมการเข้าออกพื้นที่ (Access Control System)	กลาง	มี
ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
๗	การประท้วง/ปิดล้อมสถานที่	กลาง	- มีศูนย์สำรองข้อมูล DR Site - มีระบบการควบคุมการเข้าออกพื้นที่ (Access Control System) - มีเครื่องคอมพิวเตอร์สำรองสำหรับ Remote	กลาง	มี
๘	น้ำท่วม	กลาง	- มีศูนย์สำรองข้อมูล DR Site	สูง	มี

๒) ปัจจัยภายใน

ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
๑	ไฟฟ้าดับในวงกว้าง	กลาง	- ติดตั้งอุปกรณ์ UPS และเครื่องกำเนิดไฟฟ้าเพื่อรองรับความไม่เสถียรของระบบไฟฟ้า ที่จ่ายไฟให้กับระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์คอมพิวเตอร์ที่สำคัญทั้งหมด - มีการตรวจสอบอุปกรณ์ UPS เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ	สูง	มี
๒	ความล้มเหลวของอุปกรณ์ (Technical Failure)	กลาง	- มีศูนย์สำรองข้อมูล DR Site - ทำสัญญาข้อตกลงกับบริษัทที่ดูแลระบบเพื่อรองรับความไม่เสถียรของระบบ หากระบบมีปัญหาจนไม่สามารถทำงานได้ - มีการฝึกอบรมผู้ดูแลระบบให้มีความรู้ความเข้าใจในการใช้งานและบำรุงรักษาอุปกรณ์ที่มีการติดตั้งใช้งาน - มีการตรวจสอบอุปกรณ์ต่าง ๆ เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ - มีระบบเครือข่าย ๒ ชุดและ มีวงจรอินเทอร์เน็ต ๒ ชุด	กลาง	มี

๓	ความล้มเหลวของการปฏิบัติงาน (Operation Failure)	ต่ำ	- มีการฝึกอบรมผู้ใช้งานระบบให้มีความรู้ความเข้าใจในการใช้งาน - มีการกระบวนการรับเรื่องเมื่อเกิดเหตุขัดข้อง	สูง	มี
ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
๔	การเชื่อมโยงเครือข่ายล้มเหลว	กลาง	- มีศูนย์สำรองข้อมูล DR Site - มีการตรวจสอบอุปกรณ์ต่าง ๆ เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ - ทำสัญญาข้อตกลงกับบริษัทที่ดูแลระบบเพื่อรองรับความไม่เสถียรของระบบ หากระบบมีปัญหาจนไม่สามารถทำงานได้ - มีการฝึกอบรมผู้ดูแลระบบให้มีความรู้ความเข้าใจในการใช้งานและบำรุงรักษาอุปกรณ์ที่มีการติดตั้งใช้งาน	สูง	มี
๕	เครื่องแม่ข่ายฐานข้อมูลเสีย/ข้อมูลสูญหาย	กลาง	- มีศูนย์สำรองข้อมูล DR Site - มีการตรวจสอบอุปกรณ์ต่าง ๆ เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ - ทำสัญญาข้อตกลงกับบริษัทที่ดูแลระบบเพื่อรองรับความไม่เสถียรของระบบ หากระบบมีปัญหาจนไม่สามารถทำงานได้ - มีการฝึกอบรมผู้ดูแลระบบให้มีความรู้ความเข้าใจในการใช้งานและบำรุงรักษาอุปกรณ์ที่มีการติดตั้งใช้งาน	สูง	มี

๓.๒ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

จากการประเมินผลกระทบต่อการดำเนินงานและความเสี่ยงของระบบสารสนเทศ สามารถสรุปถึงโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี ได้ดังนี้

ตารางสรุปผลการวิเคราะห์และประเมินผลกระทบต่อการดำเนินงาน

บริการหลัก	**กิจกรรม**	**ลำดับความสำคัญ (Critical) (ใช่/ไม่ใช่)**	**เป้าหมายการบริหารความต่อเนื่อง (Business Continuity Objective)**		
			MTP (ชม.)	**RPO**	**RTO (ชม.)**

ระบบสารสนเทศ	ระบบไฟฟ้า	Yes	๒๔	ระบบไฟฟ้าสามารถจ่ายไฟฟ้าได้	๒
	ระบบเครือข่ายภายใน	Yes	๒๔	ระบบเครือข่ายภายในสามารถใช้งานได้	๒
	ระบบเครือข่ายอินเทอร์เน็ต (Internet)	Yes	๒๔	ระบบเครือข่ายอินเทอร์เน็ต (Internet) สามารถใช้งานได้	๔
	เครื่องคอมพิวเตอร์แม่ข่าย	Yes	๒๔	เครื่องคอมพิวเตอร์แม่ข่ายสามารถใช้งานได้	๒๒

หมายเหตุ:

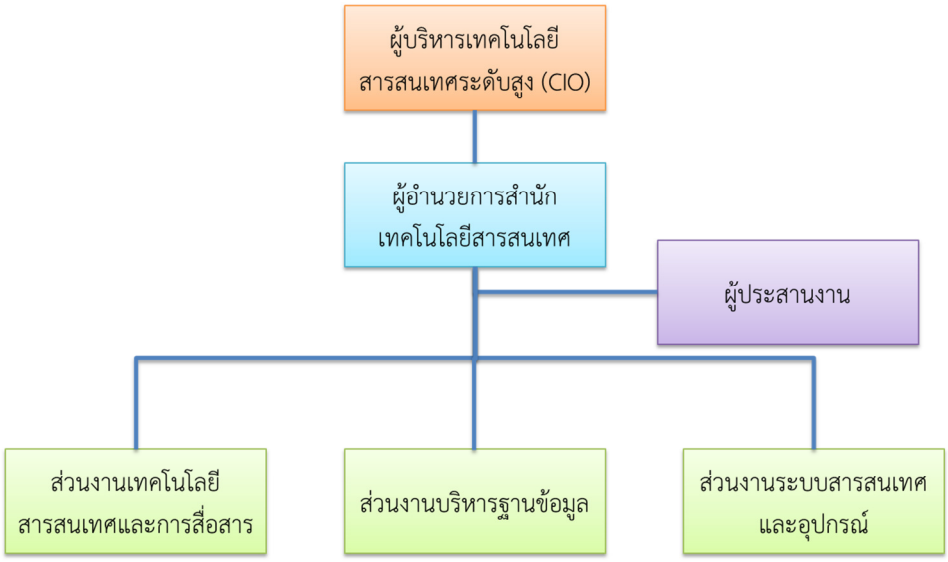
(๑) MTP หมายถึง ระยะเวลาที่องค์กรสามารถคงอยู่ได้ ภายหลังจากที่ไม่สามารถกู้คืนการดำเนินงานได้ตามปกติ

(๒) RTO หมายถึง เป้าหมายของระยะเวลา สำหรับการกู้คืนสภาพการดำเนินงานปกติ หลังจากเกิด Incident หรือ การกลับสู่ศักยภาพ/ประสิทธิภาพของการดำเนินกิจกรรมปกติ หลังจากเกิด Incident หรือ การกู้คืนระบบเทคโนโลยีสารสนเทศ หรือระบบสารสนเทศสู่สภาพปกติ หลังจากเกิด Incident

(๓) RPO หมายถึง ระดับความต้องการขั้นต่ำ/ทรัพยากรขั้นต่ำเพื่อให้สามารถดำเนินกิจกรรมทางธุรกิจให้ต่อเนื่องไปได้ระหว่างที่เกิด Incident

๔. การเตรียมการก่อนการเกิดวิกฤติ

๔.๑ โครงสร้างการตอบสนองต่อวิกฤติการณ์



โครงสร้างการตอบสนองต่อวิกฤติการณ์

หน้าที่ ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศเป็นดังนี้

๔.๑.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๑) รองผู้อำนวยการองค์การคลังสินค้าที่กำกับดูแลสำนักเทคโนโลยีสารสนเทศ

๒) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๔.๑.๒ ระดับปฏิบัติ

มีหน้าที่ปฏิบัติตามแผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศฉบับนี้ โดยแบ่งความรับผิดชอบตามส่วนงานดังนี้

๑) ส่วนงานเทคโนโลยีและการสื่อสาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการส่วนงานและบุคลากรในส่วนงาน

นายพิชญ์พิพัฒน์	สารัตถานนท์	นักคอมพิวเตอร์ ๖
น.ส.มะลิวัลย์	แสงแก้ว	ลูกจ้าง ๔
น.ส.วันเพ็ญ	สภาพพร	ลูกจ้าง ๔
น.ส.จุฑารัตน์	ชูชอบ	ลูกจ้าง ๔

รับผิดชอบดังต่อไปนี้

- ออกแบบระบบงานประยุกต์ ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบบริการ และระบบเครือข่ายสื่อสารให้เหมาะสมกับระบบงานขององค์กรให้ทันสมัย
- เขียนโปรแกรมคำสั่ง ทดสอบโปรแกรมคำสั่งเพื่อสร้างระบบงานประยุกต์
- ให้คำปรึกษา และแนะนำการใช้งานโปรแกรมประยุกต์ โปรแกรมสำเร็จรูป
- ศึกษาค้นคว้าเทคโนโลยีใหม่ทางด้านคอมพิวเตอร์และนำมาพัฒนาใช้กับระบบงานขององค์การคลังสินค้าให้มีประสิทธิภาพเพิ่มขึ้น
- พัฒนาระบบงานประยุกต์ และวิธีเขียนโปรแกรมคำสั่ง

๒) ส่วนงานบริหารฐานข้อมูล ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการส่วนงานและบุคลากรในส่วนงาน

นายธเนศ	แย้มนิยม	นักคอมพิวเตอร์ ๗
น.ส.กุสุมาลย์	ภูบุญเพชร	นักคอมพิวเตอร์ ๕
น.ส.กุหลาบ	มะเครือสี	ลูกจ้าง ๔

รับผิดชอบดังต่อไปนี้

- ติดตั้งและบริหารจัดการระบบเทคโนโลยีสารสนเทศด้านการบริหารฐานข้อมูล ได้แก่ ระบบคอมพิวเตอร์ ระบบปฏิบัติการเครื่องคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล ระบบฐานข้อมูล และระบบบริการ
- บริหารจัดการการเชื่อมโยงข้อมูล การจัดการเครือข่ายสื่อสารข้อมูล ฐานข้อมูล และระบบบริการ
- จัดทำระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศและระบบป้องกันภัยการบุกรุก
- จัดทำระบบร่องรอยการตรวจสอบของระบบ เพื่อตรวจสอบการใช้งานและผู้บุกรุก
- ดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศ

๓) ส่วนงานระบบสารสนเทศและอุปกรณ์ ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการส่วนงานและบุคลากรในส่วนงาน

นางจันทนา	อักษรเจริญสุข	นักคอมพิวเตอร์ ๗
นางทัศณี	สวนปาน	นักคอมพิวเตอร์ ๕
นางธัญวรัตม์	แย้มนิยม	พนักงานธุรการ ๕
นายนพฤทธิ์	ปานกัน	พนักงานธุรการ ๓
น.ส.พัชรกมล	คงศรีทอง	ลูกจ้าง ๔
ว่าที่ ร.ต.ชาตรี	คุ้มสมบัติ	ลูกจ้าง ๔
นายชยพล	สว่างศรี	ลูกจ้าง ๔

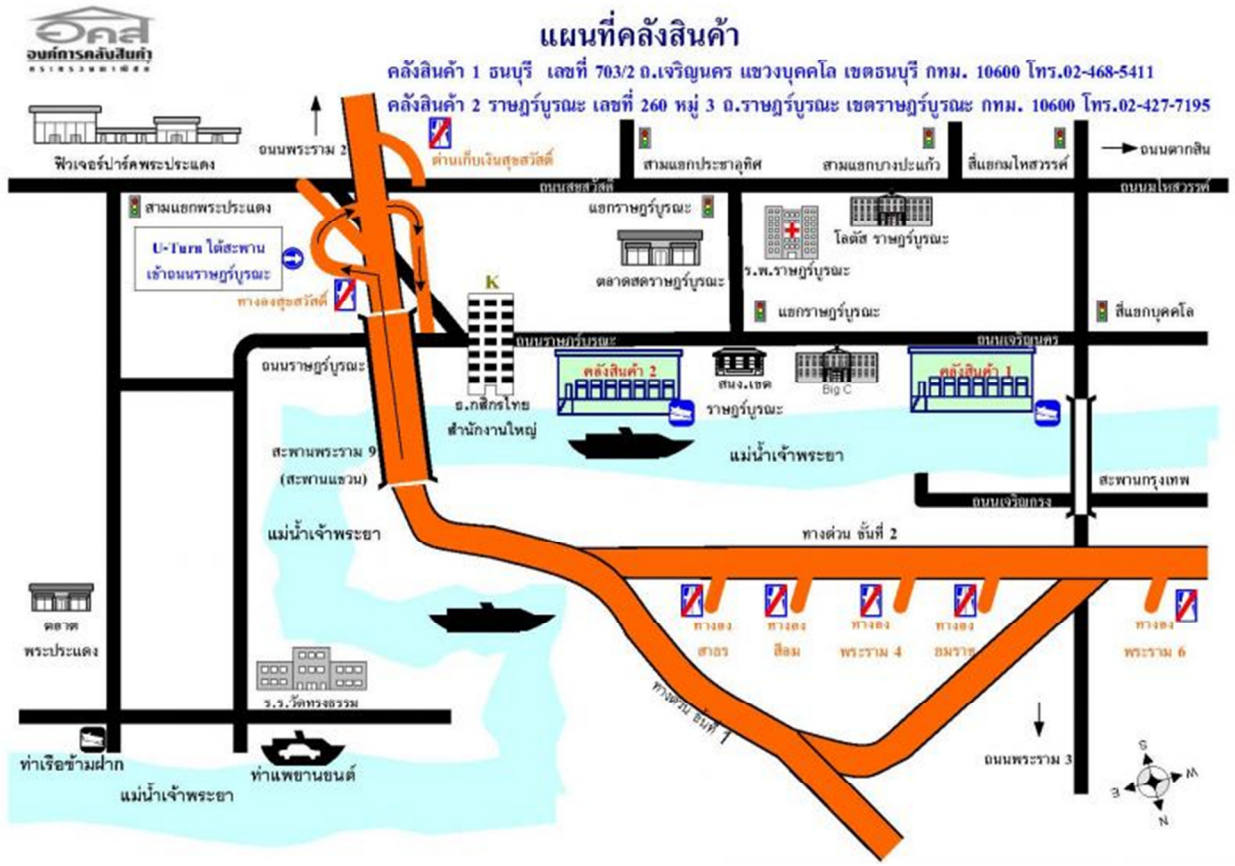
รับผิดชอบดังต่อไปนี้

- แก้ไขโปรแกรมระบบงานประยุกต์ตามที่ผู้ใช้งานร้องขอ
- จัดทำสำเนาโปรแกรมคำสั่งและระบบที่เกี่ยวข้อง
- เก็บเอกสารประกอบระบบงานประยุกต์ โปรแกรมคำสั่ง และคู่มือการใช้งาน
- ดูแลบำรุงรักษาและซ่อมแซมแก้ไขคอมพิวเตอร์และอุปกรณ์
- ควบคุมดูแลสื่อข้อมูลและวัสดุอุปกรณ์คอมพิวเตอร์ให้ใช้งานได้ตลอดเวลา

๔.๒ สถานที่ปฏิบัติงานทดแทน

สถานที่สำหรับใช้ในการปฏิบัติงานแทนในกรณีเกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้สถานที่ทำงานเดิมในการปฏิบัติงานได้คือ

คลังสินค้า ๑ ธนบุรี ๗๐๓/๒ ถ.เจริญนคร แขวงบุคคโล เขตธนบุรี กทม. ๑๐๖๐๐ โทรศัพท์ : ๐๒-๔๖๘-๕๔๑๑



๔.๓ การจัดเตรียมเครื่องมือสนับสนุนการทำงานของสถานที่ปฏิบัติงานทดแทน

เพื่อให้สถานที่ปฏิบัติงานทดแทนมีความพร้อมสำหรับใช้งานและการเข้าปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องของสำนักเทคโนโลยีสารสนเทศ ซึ่งต้องมีการดำเนินการจัดเตรียมความพร้อมในด้านต่างๆ ดังนี้

๔.๓.๑ จัดเตรียมสิ่งอำนวยความสะดวก ซึ่งจำเป็นต้องใช้ในการปฏิบัติงานในสถานที่ปฏิบัติงานทดแทนในระหว่างการเกิดวิกฤติ จะต้องมีการทบทวนและตรวจสอบรายการเครื่องมือสนับสนุนการทำงานของสถานที่ปฏิบัติงานทดแทนรวมถึงรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงานทดแทนให้อยู่ในสภาพพร้อมใช้งาน อย่างน้อยปีละ ๑ ครั้ง (รายละเอียดตามตารางรายการสิ่งอำนวยความสะดวกของสถานที่ปฏิบัติงานทดแทน)

ตารางรายการสิ่งอำนวยความสะดวกของสถานที่ปฏิบัติงานทดแทน

รายการ	**จำนวน**	**จัดหาและเตรียมความพร้อมโดย**
๑. โทรศัพทเคลื่อนที่ (พร้อมใช้งาน)	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร
๒. คอมพิวเตอร์แบบพกพา (พร้อมใช้งาน)/	๑ ชุด	ส่วนงานระบบสารสนเทศและอุปกรณ์

รายการ	จำนวน	จัดหาและเตรียมความพร้อมโดย
ส่วนบุคคล		
๓. เครื่องพิมพ์	๑ ชุด	ส่วนงานระบบสารสนเทศและอุปกรณ์
๔. โต๊ะ-เก้าอี้	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร
๕. กระดานไวท์บอร์ด/ปากกาเขียนไวท์บอร์ด	๑ ชุด/๒ ด้าม	ส่วนงานเทคโนโลยีและการสื่อสาร
๖. เครื่องเขียน - ปากกา ดินสอ	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร
๗. ตู้จัดเก็บเอกสาร	๑ ตู้	ส่วนงานเทคโนโลยีและการสื่อสาร

๔.๓.๒ ทำการสำรองสื่อและบันทึกที่สำคัญ ๆ และจัดเก็บ ณ สถานที่ปฏิบัติงานทดแทนทุกครั้งที่มีการเปลี่ยนแปลง (รายละเอียดตามตารางรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงานทดแทน)

ตารางรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงานทดแทน

รายการ	จำนวน	จัดหาและเตรียมความพร้อมโดย
๑. แผนการบริหารความต่อเนื่องในการดำเนินงาน	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร
๒. รายชื่อพนักงาน/เจ้าหน้าที่ของ สำนักเทคโนโลยีสารสนเทศทุกท่าน	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร
๓. รายชื่อบริษัทฯ ที่เกี่ยวข้องกับระบบ	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร

๔.๓.๓ จัดเตรียมสิ่งอำนวยความสะดวก ซึ่งจำเป็นต้องใช้ในการปฏิบัติงานในสถานที่ปฏิบัติงานทดแทนในระหว่างการเกิดวิกฤติ จะต้องมีการทบทวนและตรวจสอบรายการเครื่องมือสนับสนุนการทำงานของสถานที่ปฏิบัติงานทดแทน รวมถึงรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงานทดแทนให้อยู่ในสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง (รายละเอียดตามตารางรายการสิ่งอำนวยความสะดวกของสถานที่ปฏิบัติงานทดแทน)

ตารางรายการสิ่งอำนวยความสะดวกของสถานที่ปฏิบัติงานทดแทน

รายการ	จำนวน	จัดหาและเตรียมความพร้อมโดย
๑. เครื่องคอมพิวเตอร์	๑ เครื่อง	ส่วนงานระบบสารสนเทศและอุปกรณ์
๒. Internet สำหรับใช้งาน	-	ส่วนงานบริหารฐานข้อมูล

๔.๓.๔ ทำการสำรองสื่อและบันทึกที่สำคัญ ๆ และจัดเก็บ ณ สถานที่ปฏิบัติงานทดแทนทุกครั้งที่มีการเปลี่ยนแปลง (รายละเอียดตามตารางรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงาน

ทดแทน)

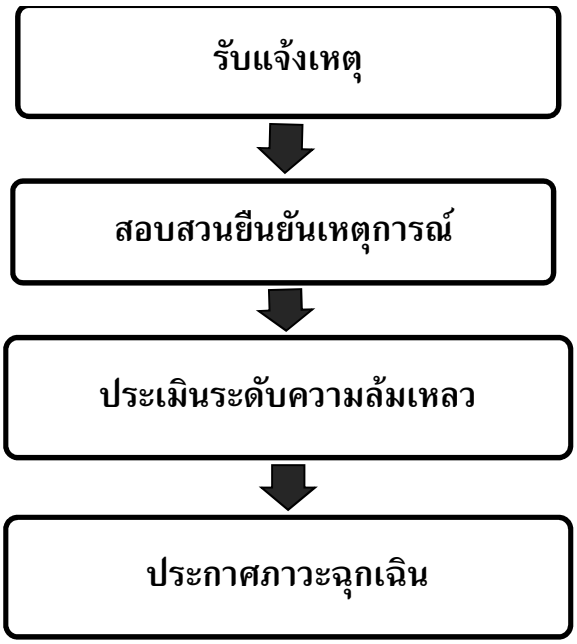
ตารางรายการสื่อและบันทึกที่สำคัญของสถานที่ปฏิบัติงานทดแทน

รายการ	**จำนวน**	**จัดหา และเตรียม ความพร้อมโดย**
๑. เอกสารทางด้านเทคนิคของระบบ สารสนเทศ ๑.๑คู่มือการเรียกคืนข้อมูลของระบบ	๑ ชุด	ส่วนงานเทคโนโลยีและการสื่อสาร ส่วนงานบริหารฐานข้อมูล ส่วนงานระบบสารสนเทศและอุปกรณ์

๕. การตอบสนองต่อวิกฤติการณ์

๕.๑ การส่งต่อและการเริ่มใช้แผนการเตรียมความพร้อมกรณีฉุกเฉิน

ในกรณีที่เกิดวิกฤติการณ์หรือสถานการณ์ฉุกเฉิน มีขั้นตอนการปฏิบัติเพื่อตอบสนองต่อวิกฤติการณ์นั้นๆ ดังนี้



ภาพขั้นตอนการปฏิบัติเพื่อตอบสนองต่อวิกฤติการณ์

๕.๒ การติดต่อผู้ที่เกี่ยวข้อง (Call Tree)

เมื่อมีการประกาศภาวะภัยพิบัติจะต้องเริ่มแจ้งหน่วยงานที่เกี่ยวข้องตามรายชื่อผู้ที่เกี่ยวข้อง (Call Tree) โดยผู้ประสานงานจะโทรแจ้งผู้ที่เกี่ยวข้องตามรายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กรตามความรับผิดชอบเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องเริ่มเข้าปฏิบัติงานตามแผนการบริหารความต่อเนื่องให้กับธุรกิจ

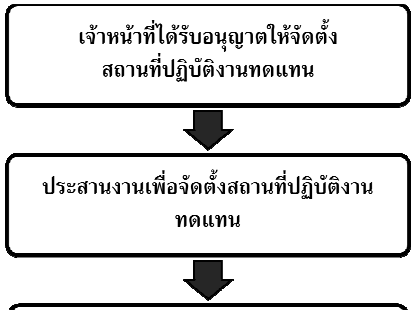
๕.๒.๑ รายชื่อผู้ที่เกี่ยวข้อง (Call Tree)

ตารางรายชื่อบุคลากรหลักที่ต้องติดต่อเมื่อเกิดวิกฤตการณ์หรือสถานการณ์ฉุกเฉิน

ชื่อ	ตำแหน่ง	โทรศัพท์พื้นฐาน	โทรศัพท์มือถือ
ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูงขององค์การคลังสินค้า			
พ.ต.ท.ปิยวิชญ์ วงศ์สวัสดิ์	รองผู้อำนวยการองค์การคลังสินค้า	๐-๒๕๐๗-๕๓๖๔	๐๘๑-๘๑๒-๒๐๒๐
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ			
นางมณี สิงหรา ณ อยุธยา	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ	๐-๒๕๐๗-๕๑๒๕	๐๘๑-๖๙๖-๖๘๖๑
ส่วนงานเทคโนโลยีและการสื่อสาร			
นางทิพวัลย์ จันทร์รัตน์	ผู้อำนวยการส่วนงาน	๐-๒๕๐๗-๕๑๓๙	๐๘๓-๒๔๙-๑๐๖๕
นายพิชญ์พิพัฒน์ สารัตถานนท์	นักคอมพิวเตอร์ ๕	๐-๒๕๐๗-๕๑๓๓	๐๘๑-๘๒๙-๙๓๒๙
ส่วนงานบริหารฐานข้อมูล			
นางสาวสุมาลิ จิตอนุรักษ์	ผู้อำนวยการส่วนงาน	๐-๒๕๐๗-๕๑๓๒	๐๙๕-๗๗๓-๐๘๖๐
นายธเนศ แย้มนิยม	นักคอมพิวเตอร์ ๗	๐-๒๕๐๗-๕๑๓๗	๐๘๕-๘๓๙-๖๒๗๕
ส่วนงานบริหารระบบสารสนเทศ			
นางจันทนา อักษรเจริญสุข	นักคอมพิวเตอร์ ๗	๐-๒๕๐๗-๕๑๒๙	๐๘๖-๓๙๓-๕๕๒๗
นางธัญวรัตม์ แย้มนิยม	พนักงานธุรการ ๕	๐-๒๕๐๗-๕๑๓๑	๐๘๕-๘๓๙-๖๒๗๖

๕.๒.๒ จัดตั้งสถานที่

เมื่อมีการประกาศภาวะภัยพิบัติ และมีความจำเป็นต้องจัดตั้งสถานที่ปฏิบัติงานทดแทนมีขั้นตอนการปฏิบัติ เพื่อให้การดำเนินงานจัดตั้งสถานที่ปฏิบัติงานทดแทนเป็นไปอย่างมีประสิทธิภาพ และพร้อมรองรับการปฏิบัติงานเมื่อมีการประกาศภาวะภัยพิบัติ ดังนี้



ภาพขั้นตอนปฏิบัติในการดำเนินงานจัดตั้งสถานที่ปฏิบัติงานทดแทน

๕.๓ การรายงานสถานการณ์/วิกฤติการณ์

ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูงขององค์การคลังสินค้าหรือ CIO จะเป็นผู้ประสานงานหลักในการสื่อสารกับบุคคลภายนอกในระหว่างภัยพิบัติ และ พนักงานที่ไม่ได้รับการมอบหมายให้เป็นโฆษกผู้รายงานหรือผู้รับผิดชอบในการประสานงานจะต้องไม่สื่อสารกับบุคคลภายนอกรวมทั้งสื่อหรือนักข่าว เกี่ยวกับเหตุการณ์ที่เกิดขึ้นไม่ว่าจะในเรื่องใดทั้งสิ้น

๖. แผนรองรับสถานการณ์ฉุกเฉิน

๖.๑ แผนการปฏิบัติงานกรณีเหตุการณ์อุทกภัย

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีเหตุการณ์อุทกภัยจะกระทำเมื่อเกิดเหตุการณ์อุทกภัยไม่สามารถเข้าพื้นที่ได้เกิน ๒๔ ชั่วโมง

๑.๒) การแจ้งเตือนก่อนการปฏิบัติตามแผน

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแล

ระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหายแก่ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาสั่งการ

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ตรวจสอบและจัดตั้งสถานที่ปฏิบัติงานทดแทน

๒.๒) นำข้อมูลที่สำรองไว้กู้คืนเพื่อติดตั้งระบบที่จำเป็นต่อการปฏิบัติงานติดตั้งที่สถานที่ปฏิบัติงานทดแทน และทดสอบระบบ

๒.๓) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่องค์การคลังสินค้า

๒.๔) แจ้งให้เจ้าหน้าที่เข้าปฏิบัติงานที่สถานที่ปฏิบัติงานทดแทน

๒.๕) เมื่อสามารถเข้าพื้นที่ เจ้าหน้าที่ที่รับผิดชอบต้องตรวจสอบความเสียหายของระบบที่องค์การคลังสินค้า และสำรองข้อมูลที่สถานที่ปฏิบัติงานทดแทน เพื่อกู้คืนที่องค์การคลังสินค้า

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงาน

ดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๒ แผนการปฏิบัติงานกรณีเหตุการณ์อัคคีภัย

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีเหตุการณ์อัคคีภัยจะกระทำเมื่อเกิดเหตุการณ์อัคคีภัยไม่สามารถเข้าพื้นที่ได้เกิน ๒๔ ชั่วโมง

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหาย

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ตรวจสอบและจัดตั้งสถานที่ปฏิบัติงานทดแทน

๒.๒) นำข้อมูลที่สำรองไว้กู้คืนเพื่อติดตั้งระบบที่จำเป็นต่อการปฏิบัติงานติดตั้งที่สถานที่ปฏิบัติงานทดแทน และทดสอบระบบ

๒.๓) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่องค์การคลังสินค้า

๒.๔) แจ้งให้เจ้าหน้าที่เข้าปฏิบัติงานที่สถานที่ปฏิบัติงานทดแทน

๒.๕) เมื่อสามารถเข้าพื้นที่ เจ้าหน้าที่ที่รับผิดชอบต้องตรวจสอบความเสียหายของระบบที่องค์การคลังสินค้า และสำรองข้อมูลที่สถานที่ปฏิบัติงานทดแทน เพื่อกู้คืนที่องค์การคลังสินค้า

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๓ แผนการปฏิบัติงานกรณีไฟฟ้าดับในวงกว้าง

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีไฟฟ้าดับในวงกว้างจะกระทำเมื่อไฟฟ้าดับเป็นระยะเวลาเกิน ๓๐ นาที

๑.๒) การแจ้งเตือนก่อนการปฏิบัติตามแผน

ก) เจ้าหน้าที่ผู้ดูแลห้อง Data Center ได้แก่

-นายธเนศ แย้มนิยม

-น.ส.กุสุมาลย์ ภูบุญเพชร

-น.ส.กุหลาย มะเครือสี

แจ้งไปยังฝ่ายอาคาร องค์การคลังสินค้า เพื่อให้แจ้งปัญหาต่อไปยังฝ่ายอาคารสำนักงานปลัดกระทรวงพาณิชย์

ข) เจ้าหน้าที่ผู้ดูแลห้อง Data Center แจ้งผู้อำนวยการส่วนงานเพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงาน มอบหมายเจ้าหน้าที่ผู้ดูแลห้อง Data Center ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการกู้คืนระบบให้ทำงานเป็นปกติ เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่าย ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วน แจ้งผลการประเมินความเสียหายแก่ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาสั่งการ

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) สำรองข้อมูลของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๒.๒) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย

๒.๓) ปิดการทำงานของอุปกรณ์เครือข่าย

๒.๔) เมื่อไฟฟ้าเป็นปกติแล้ว ให้เปิดการทำงานของอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และระบบสารสนเทศที่เปิดใช้งานเมื่อไฟฟ้าเป็นปกติแล้ว ว่ามีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน โดยดำเนินการดังนี้

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๔ แผนการปฏิบัติงานกรณีการโจรกรรมทางข้อมูล

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีการโจรกรรมทางข้อมูลจะกระทำเมื่อ

ก) มีการตรวจพบการเจาะระบบ หรือโจรกรรมข้อมูล

ข) ตรวจพบไวรัสที่ทำงานในลักษณะการโจรกรรมข้อมูล

๑.๒) การแจ้งเตือนก่อนการปฏิบัติตามแผน

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ที่ดูแลระบบสารสนเทศและเครือข่าย ได้แก่

-นางจันทนา อักษรเจริญสุข

-นายธเนศ แย้มนิยม

-นางธัญวรัตม์ แย้มนิยม

-นายพิชญ์พิพัฒน์ สารัตถานนท์

หรือเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการกู้คืนระบบให้ทำงานเป็นปกติ เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่าย ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหายแก่ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาสั่งการ

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ตัดการเชื่อมต่ออินเตอร์เน็ตของเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์

๒.๒) ตรวจสอบและวิเคราะห์ Log files ต่างๆ ที่เกี่ยวข้อง เช่น Log ของ OS, Log ของ Web Server เพื่อหาข้อมูลที่เกี่ยวข้อง

๒.๓) ปิด Service ของโปรแกรม Remote ทุกประเภท

๒.๔) Update Patch ต่างๆ ให้เป็นปัจจุบัน หรือหากมีความจำเป็นให้ติดตั้งระบบปฏิบัติการใหม่ทั้งหมด

๒.๕) ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบัน

๒.๖) กรณีข้อมูลสำคัญสูญหายให้ทำการกู้คืน

๒.๗) เปลี่ยนรหัสผ่านสำหรับ Service/บัญชีผู้ใช้ ที่ได้รับผลกระทบ

๒.๘) เปิดใช้งาน Service เท่าที่จำเป็นเท่านั้น

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน โดยดำเนินการดังนี้

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบทำการสำรองแบบ Full backup ให้กับระบบทันทีที่สามารถดำเนินการได้

ค) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๕ แผนการปฏิบัติงานกรณีแผ่นดินไหวรุนแรง

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีแผ่นดินไหวรุนแรงจะกระทำเมื่อแผ่นดินไหวรุนแรงไม่สามารถเข้าพื้นที่ได้เกิน ๒๔ ชั่วโมง

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหาย

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ตรวจสอบและจัดตั้งสถานที่ปฏิบัติงานทดแทน

๒.๒) นำข้อมูลที่สำรองไว้กู้คืนเพื่อติดตั้งระบบที่จำเป็นต่อการปฏิบัติงานติดตั้งที่สถานที่ปฏิบัติงานทดแทน และทดสอบระบบ

๒.๓) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่องค์การคลังสินค้า

๒.๔) แจ้งให้เจ้าหน้าที่เข้าปฏิบัติงานที่สถานที่ปฏิบัติงานทดแทน

๒.๕) เมื่อสามารถเข้าพื้นที่ เจ้าหน้าที่ที่รับผิดชอบต้องตรวจสอบความเสียหายของระบบที่องค์การคลังสินค้า และสำรองข้อมูลที่สถานที่ปฏิบัติงานทดแทน เพื่อกู้คืนที่องค์การคลังสินค้า

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิด

เหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๖ แผนการปฏิบัติงานกรณีเหตุการณ์ชุมนุมประท้วง

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีเหตุการณ์ชุมนุมประท้วงจะกระทำเมื่อเหตุการณ์ชุมนุมประท้วงไม่สามารถเข้าพื้นที่ได้เกิน ๒๔ ชั่วโมง

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหาย

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ตรวจสอบและจัดตั้งสถานที่ปฏิบัติงานทดแทน

๒.๒) นำข้อมูลที่สำรองไว้กู้คืนเพื่อติดตั้งระบบที่จำเป็นต่อการปฏิบัติงานติดตั้งที่สถานที่

ปฏิบัติงานทดแทน และทดสอบระบบ

๒.๓) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายที่องค์การคลังสินค้า

๒.๔) แจ้งให้เจ้าหน้าที่เข้าปฏิบัติงานที่สถานที่ปฏิบัติงานทดแทน

๒.๕) เมื่อสามารถเข้าพื้นที่ เจ้าหน้าที่ที่รับผิดชอบต้องตรวจสอบความเสียหายของระบบที่องค์การคลังสินค้า และสำรองข้อมูลที่สถานที่ปฏิบัติงานทดแทน เพื่อกู้คืนที่องค์การคลังสินค้า

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๗ แผนการปฏิบัติงานกรณีเกิดความล้มเหลวของอุปกรณ์ (Technical Failure)

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีเครื่องแม่ข่ายฐานข้อมูลเสียหาย/ข้อมูลสูญหายจะกระทำเมื่อเกิดความล้มเหลวของอุปกรณ์เกิน ๔ ชั่วโมง

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๒) การแจ้งเตือนก่อนการปฏิบัติตามแผน

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหาย

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ปิดการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายที่เสียหาย

๒.๒) จัดหาและตั้งค่าเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายสำรอง

๒.๓) ทดสอบการใช้งานเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายสำรอง

๒.๔) นำเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายไปซ่อมแซม

๒.๕) เมื่อซ่อมแซมเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายแล้ว ให้ตั้งค่าเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย นำทดสอบและมาใช้งานทดแทนเครื่องสำรอง

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่

ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๖.๘ แผนการปฏิบัติงานกรณีความล้มเหลวของการปฏิบัติงาน (Operation Failure)

๑) การเริ่มปฏิบัติตามแผนและการแจ้งเตือน

๑.๑) แผนการปฏิบัติงานกรณีระบบสารสนเทศล้มเหลวจะกระทำเมื่อเกิดความล้มเหลวของของการปฏิบัติงานเกิน ๘ ชั่วโมง

๑.๒) การแจ้งเตือนก่อนการปฏิบัติตามแผน

ก) ให้ผู้พบเหตุการณ์แจ้งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ฝ่ายระบบสารสนเทศและเครือข่าย แจ้งผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย

๑.๓) การประเมินความเสียหาย

ก) ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย มอบหมายเจ้าหน้าที่ ที่ดูแลระบบสารสนเทศและเครือข่าย ประเมินความเสียหายที่เกิดขึ้น เช่น สาเหตุของความเสียหาย ผลกระทบเพิ่มเติมจากเหตุการณ์ดังกล่าว ผลกระทบต่อฮาร์ดแวร์และซอฟต์แวร์ของระบบสารสนเทศ ฮาร์ดแวร์ที่จำเป็นต้องเปลี่ยน และระยะเวลาโดยประมาณในการจัดตั้งจัดตั้งสถานที่ปฏิบัติงานทดแทน เป็นต้น

กรณีมีผู้รับจ้างดูแลระบบเครือข่ายหรือระบบสารสนเทศ ให้เจ้าหน้าที่ประสานงานกับบริษัทผู้รับจ้างเพื่อร่วมประเมินความเสียหาย

ข) ให้ผู้อำนวยการส่วนงานระบบสารสนเทศและเครือข่าย แจ้งผลการประเมินความเสียหาย

๒) การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ

๒.๑) ปิดการทำงานของระบบที่เสียหาย

๒.๒) จัดหาและตั้งค่าเครื่องแม่ข่ายสำหรับติดตั้งระบบสำรอง รวมถึงกู้คืนข้อมูลล่าสุดที่สำรองไว้

๒.๓) ทดสอบการใช้งานระบบ

๒.๔) ให้ผู้พัฒนาตรวจสอบและปรับปรุงระบบ

๒.๕) เมื่อปรับปรุงระบบแล้ว ทดสอบและนำมาใช้งานทดแทนระบบสำรอง สำรองข้อมูลล่าสุดและกู้คืนข้อมูลล่าสุดบนระบบเดิม

๓) การกลับคืนสู่การทำงานปกติ

๓.๑) การตรวจสอบความถูกต้องของการกู้คืนระบบ

ให้เจ้าหน้าที่ที่รับผิดชอบทำการตรวจสอบความถูกต้อง ครบถ้วนของการกู้คืนระบบดังนี้

ก) การตรวจสอบความครบถ้วนของข้อมูลที่กู้คืน เพื่อตรวจสอบว่าข้อมูลได้รับการกู้คืนครบถ้วนและเป็นข้อมูลล่าสุดที่ได้มีการสำรองไว้

ข) การตรวจสอบการทำงานของระบบ เพื่อตรวจสอบว่าเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์เมื่อได้ทำการกู้คืนระบบแล้ว มีการทำงานเป็นปกติหรือไม่

๓.๒) การยกเลิกการปฏิบัติตามแผน

ก) การแจ้งการยกเลิก เมื่อระบบสามารถทำงานได้เป็นปกติแล้ว ให้เจ้าหน้าที่ผู้รับผิดชอบแจ้งให้ผู้อำนวยการส่วนงานรับทราบ เพื่อแจ้งการยกเลิกการปฏิบัติตามแผนต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ข) เจ้าหน้าที่ผู้รับผิดชอบบันทึกรายละเอียดการดำเนินงานในการกู้คืนและการกลับสู่การทำงานปกติของระบบ รวมทั้งปัญหาต่างๆ ที่เกิดขึ้นระหว่างการดำเนินงานดังกล่าวส่งให้ผู้อำนวยการส่วนงานเพื่อรายงานต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๗. การอบรม

สำนักเทคโนโลยีสารสนเทศจะต้องจัดให้มีการฝึกอบรมทักษะที่เกี่ยวข้องในการดำเนินงานต่างๆ ตามแผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศให้แก่บุคลากรที่เกี่ยวข้องตามหน้าที่และความรับผิดชอบที่ระบุไว้ในแผนดังกล่าวเป็นประจำทุกปี

ทั้งนี้ควรมีการจัดทำแผนการฝึกอบรมทักษะที่เกี่ยวข้องกับการดำเนินงานตามแผนการเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ โดยการสำรวจจากบุคลากรที่เกี่ยวข้อง

๘. แผนการทดสอบและซ้อมการกู้คืนระบบ

๘.๑ สำนักเทคโนโลยีสารสนเทศจะต้องทำการทดสอบและซ้อมการปฏิบัติงานของบุคลากรตามแผนการกู้คืนระบบเป็นประจำทุกปี

๘.๒ ให้ทำการซ้อมด้วยวิธีการใดวิธีการหนึ่งดังต่อไปนี้

๑) การซ้อมโดยการพูดคุย เป็นการซ้อมโดยการพูดคุยถึงบทบาทและหน้าที่ในขณะเกิดแต่ละเหตุการณ์ฉุกเฉิน โดยให้ผู้ดำเนินการประชุม จำลองเหตุการณ์ต่างๆ และสอบถาม ถึงบทบาทหน้าที่ วิธีการตอบสนองต่อเหตุการณ์ การประสานงานกับผู้ร่วมงาน รวมถึงการตัดสินใจต่างๆ กับผู้ร่วมประชุมที่เกี่ยวข้องกับเหตุการณ์ดังกล่าว

๒) การจำซ้อมโดยการจำลองสถานการณ์ เป็นการซ้อมโดยจำลองเหตุการณ์ฉุกเฉินในกรณีต่างๆ ที่สามารถจำลองเหตุการณ์ได้ และให้มีการซักซ้อมการปฏิบัติเพื่อแก้ไขปัญหา โดยปฏิบัติตามขั้นตอนที่กำหนด เช่นเดียวกับกรณีที่เกิดเหตุการณ์จริง

๙. การทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศ

สำนักเทคโนโลยีสารสนเทศต้องมีการทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน ด้านระบบสารสนเทศเป็นประจำทุกปีและพิจารณาปรับปรุงแผนตามความจำเป็น เช่น การเปลี่ยนแปลงในฟังก์ชั่นทางธุรกิจและระบบสนับสนุนต่าง ๆ การเปลี่ยนแปลงด้านสภาพแวดล้อม การควบคุมทางด้านเทคนิคและสภาพแวดล้อม และด้านบุคลากรและตำแหน่งความรับผิดชอบ เพื่อให้แผนการบริหารความต่อเนื่องให้กับธุรกิจ เป็นแผนที่สามารถนำมาใช้งานได้ในทุกสภาวะ

ทั้งนี้ให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นผู้สอบทานการปรับปรุงแผนดังกล่าวก่อนนำเสนอต่อผู้บังคับบัญชาในลำดับถัดไป