



แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)
ของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)
กรกฎาคม 2566

คำนำ

ข้อมูลสารสนเทศถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อการดำเนินงานของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานของบุคลากรในองค์กร ฝ่ายเทคโนโลยีสารสนเทศ ได้ตระหนักถึงความสำคัญของข้อมูลและระบบสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยจากภายในมากระทบทำให้ข้อมูลและระบบสารสนเทศรวมทั้งระบบอุปกรณ์ต่าง ๆ เสียหายได้

เพื่อให้สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) มีการจัดการข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยมีความพร้อมใช้ข้อมูลได้อย่างเต็มประสิทธิภาพตลอดเวลาและนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร ตลอดจนเลือกใช้วิธีการที่เหมาะสมในการบริหารจัดการความเสี่ยงที่ได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและให้การดำเนินงานของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) อยู่ในระดับที่สามารถยอมรับได้ จึงจำเป็นต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan) เป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่อาจนำไปสู่ผลเสียหรือความเสียหายได้ทั้งทางตรงและทางอ้อม

สารบัญ

เรื่อง	หน้า
คำนำ	2
สารบัญ	3
แผนรองรับสถานการณ์ฉุกเฉิน	
1. วัตถุประสงค์	4
2. การวิเคราะห์ผลกระทบทางธุรกิจ	4
3. การจัดลำดับความสำคัญของระบบสารสนเทศ	5
4. การสมมติฐานของแผนรองรับสถานการณ์ฉุกเฉิน	6
5. ขอบเขตของแผนรองรับสถานการณ์ฉุกเฉิน	6
6. การจัดองค์กรปฏิบัติการงานฉุกเฉิน	10
7. การวิเคราะห์ทรัพยากรที่สำคัญ	11
8. แผนการสำรองและกู้คืนข้อมูล	12
9. แผนการทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม	14
10. การกำหนดผู้รับผิดชอบ	14
11. การติดตามและรายงานผล	14

แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan)

แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan) จัดทำขึ้นสำหรับเป็นแนวทางเพื่อให้สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) สามารถนำแผนดังกล่าวไปประยุกต์ใช้เพื่อตอบสนอง และสามารถปฏิบัติงานในสภาวะวิกฤติ หรือในสถานะการณ์ฉุกเฉินต่าง ๆ ซึ่งเกิดขึ้นจากหลายปัจจัย อาทิ ภัยธรรมชาติ อุบัติเหตุ และการประสงคร้ายต่อองค์กรฯ เป็นต้น โดยบริหารจัดการมิให้เกิดสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินอันจะส่งผลกระทบต่อระบบสารสนเทศขององค์กรต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง และมีประสิทธิภาพ

แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan) จึงเป็นสิ่งสำคัญที่จะช่วยขับเคลื่อนระบบสารสนเทศขององค์กรให้สามารถตั้งรับกับสถานะการณ์ฉุกเฉินที่คาดไม่ถึง อีกทั้งยังทำให้กระบวนการที่สำคัญ (Critical Business Process) สามารถกลับมาดำเนินการได้อย่างปกติ หรือตามระดับการให้บริการที่กำหนดไว้ ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่จะเกิดขึ้นต่อระบบสารสนเทศขององค์กรในอนาคต

1. วัตถุประสงค์

1.1. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ตลอดจนการสร้างกรอบและแนวทางในการดำเนินงานให้แก่บุคลากรในองค์กร ในการดูแลรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

1.2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

1.3. เพื่อใช้เป็นแนวทางในการดำเนินการ การกำกับดูแล การตรวจสอบการบริหารจัดการ และดูแลรักษาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ มีความพร้อมสำหรับการใช้งาน และเฝ้าระวังความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

1.4. เพื่อบริหารจัดการความไม่แน่นอนที่จะเกิดขึ้น และสามารถแก้ไขสถานการณ์ได้อย่างทัน่วงทีกรณีที่เกิดสถานการณ์ความไม่แน่นอนหรือภัยพิบัติที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ให้อยู่ระดับที่ยอมรับได้

1.5. เพื่อให้เจ้าหน้าที่องค์กร หน่วยงานภาครัฐและเอกชน ประชาชนทั่วไป รวมทั้งผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพขององค์กร แม้ว่าองค์กรต้องเผชิญกับเหตุการณ์ร้ายแรง และส่งผลกระทบต่อการทำงานต้องหยุดชะงักลง

2. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA)

การวิเคราะห์ผลกระทบทางธุรกิจ หรือ Business Impact Analysis (BIA) หมายถึง กระบวนการในการ วิเคราะห์ถึงกิจกรรมทางธุรกิจ และผลกระทบที่จะเกิดขึ้นจากการหยุดชะงักของกิจกรรมนั้น ๆ มีขั้นตอนการดำเนินการ ดังนี้

ขั้นตอนที่ 1 การระบุกิจกรรม กระบวนการ บริการหลัก จากการพิจารณาการปฏิบัติราชการ กระบวนการตามโครงสร้างและอำนาจหน้าที่ของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) โดยระบุกิจกรรม กระบวนการ กรอบเวลา หรือกรอบเวลาในการทำงานผู้ส่งมอบงานหน่วยงานที่เกี่ยวข้องและผู้รับบริการเพื่อให้เห็นถึงผลกระทบที่จะเกิดขึ้นในแต่ละกระบวนการ กิจกรรมการทำงาน

ขั้นตอนที่ 2 ระบุถึงผลกระทบที่จะเกิดขึ้นจากการหยุดชะงักและพิจารณาถึงการเปลี่ยนแปลงของผลกระทบเมื่อเวลาผ่านไป

การระบุผลกระทบในขั้นตอนนี้จะเริ่มต้นที่การประเมินความเสี่ยง และภัยคุกคามซึ่งแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan) ฉบับนี้ใช้รองรับสถานการณ์กรณีเกิดสภาวะวิกฤตหรือ เหตุการณ์ฉุกเฉินในพื้นที่ภายในสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)

กระบวนการงาน	ความเสี่ยงและภัยคุกคาม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
			0 - 2 ชั่วโมง	2 - 4 ชั่วโมง	4 - 24 ชั่วโมง	2 - 7 วัน	1 - 2 สัปดาห์	2 สัปดาห์ขึ้นไป
การดำเนินการบริหารจัดการระบบสารสนเทศ	อุทกภัย	สูง	✓	✓	✓	✓	✓	✓
	อัคคีภัย	สูงมาก	✓	✓	✓	✓	✓	✓
	ไฟดับในวงกว้าง	สูง	✓	✓	✓	✓	✓	✓
	จากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)	ปานกลาง		✓	✓	✓	✓	✓
	จากภัยคุกคามและจากการจารกรรมข้อมูล	สูง		✓	✓	✓	✓	✓
	จากอินเทอร์เน็ตล่ม	ปานกลาง		✓	✓	✓	✓	✓
	อุปกรณ์ในห้อง Data Center ทำงานไม่ปกติ	ปานกลาง		✓	✓	✓	✓	✓
	การประท้วง/การจลาจล	ปานกลาง		✓	✓	✓	✓	✓

3. การจัดลำดับความสำคัญของระบบสารสนเทศ ดังต่อไปนี้

- 3.1 ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ (Firewall)
- 3.2 โปรแกรมป้องกันไวรัส (Anti-Virus)
- 3.3 ระบบ Active Directory
- 3.4 เว็บไซต์องค์กร
- 3.5 ระบบ ERP
- 3.6 ระบบ e-Commerce
- 3.7 ระบบฐานข้อมูลสมาชิก
- 3.8 ระบบ sacit Archives
- 3.9 ระบบสารบรรณอิเล็กทรอนิกส์

4. สมมติฐานของแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

4.1 เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่าง ๆ แต่มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้

4.2 ฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบในการสำรองระบบสารสนเทศต่าง ๆ โดยระบบสารสนเทศสำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก

4.3 “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และผู้ปฏิบัติงานทั้งหมดขององค์กร

5. ขอบเขตของแผนรองรับสถานการณ์ฉุกเฉิน

แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan) ฉบับนี้ ใช้รับรองสถานการณ์กรณีเกิดสภาวะวิกฤต หรือเหตุการณ์ฉุกเฉินภายในพื้นที่สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) อาทิ เหตุการณ์ต่างๆ ดังต่อไปนี้

5.1 เหตุการณ์อัคคีภัย

จัดเป็นภัยร้ายแรงที่ทำให้ความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้ให้ความสำคัญ และระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยในลักษณะดังกล่าวขึ้น แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากอัคคีภัย สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้นจึงได้ดำเนินการ ดังนี้

5.1.1 ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้อง หรือมีควันไฟเกิดขึ้นภายในห้อง Data Center อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่โทรศัพท์มือถือของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศทุกคน เพื่อรับทราบ และเร่งดำเนินการระงับเหตุฉุกเฉินอย่างทันที่ ซึ่งปัจจุบันมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

5.1.2 ติดตั้งระบบสารพัดดับเพลิง ภายในห้อง Data Center เพื่อใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

5.2 เหตุการณ์จากอุทกภัยหรือผลกระทบจากอุทกภัย

เป็นภัยที่เกิดขึ้นหลายครั้งในเขตจังหวัดพระนครศรีอยุธยา และสถานที่ตั้งของหน่วยงานอยู่ใกล้กับแม่น้ำเจ้าพระยา จึงมีความเสี่ยงต่อการประสบภัยจากอุทกภัยได้ง่าย ถึงแม้ห้อง Data Center ที่ทำหน้าที่ควบคุมระบบเครือข่ายอยู่บริเวณชั้น 3 ของอาคาร ซึ่งมีความเสี่ยงต่อความเสียหายจากน้ำท่วมน้อยมาก แต่ผลกระทบจากอุทกภัยจะมีผลกับการเข้าปฏิบัติงานภายในตัวอาคาร ถือเป็นภัยร้ายแรงที่ทำให้ความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้ให้ความสำคัญ และระมัดระวังเป็นอย่างยิ่ง จึงได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์จากภัยน้ำท่วม (อุทกภัย) ที่อาจจะเกิดขึ้นได้ ดังนี้

5.2.1 เผื่อระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาและกรมชลประทานตลอดเวลา

5.2.2 เมื่อระดับน้ำสูงกว่าปกติและมีแนวโน้มว่าน้ำท่วมเพิ่มขึ้นเรื่อย ๆ และท่วมมาถึงบริเวณด้านหน้าสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ให้เผื่อระวังควบคุมการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดอย่างใกล้ชิด

- 5.2.3 เปิดระบบสารสนเทศ ณ สถานที่สำรองระบบสารสนเทศ (DR Site) เพื่อการใช้งานได้อย่างต่อเนื่อง
- 5.2.4 ดำเนินการปิดเครื่องคอมพิวเตอร์แม่ข่ายพร้อมอุปกรณ์เครือข่ายทั้งหมด และตัดระบบไฟฟ้าภายในห้อง Data Center โดยปิดเบรกเกอร์เครื่องปรับอากาศ เครื่องสำรองไฟฟ้า เพื่อป้องกันอุปกรณ์ภายในห้องได้รับเสียหาย
- 5.2.5 กรณีน้ำลดลงเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้อง Data Center ว่าสามารถใช้งานได้ปกติหรือไม่
- 5.2.6 เมื่อระบบไฟฟ้าใช้งานได้ปกติ ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้อง ทำการเปิดระบบสารสนเทศพร้อมทดสอบระบบ ก่อนการเปิดให้บริการ

5.3 เหตุการณ์ไฟฟ้าดับในวงกว้าง

เป็นภัยหรือผลกระทบจากระบบไฟฟ้าดับในวงกว้าง จัดเป็นภัยหรือผลกระทบที่ทำให้ระบบเทคโนโลยีสารสนเทศหยุดชะงักได้ ซึ่งสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้ให้ความสำคัญ และระมัดระวังเป็นอย่างยิ่งในการลดความเสี่ยง และผลกระทบดังกล่าว แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยหรือผลกระทบจากระบบไฟฟ้าดับในวงกว้างที่อาจจะเกิดขึ้น ดังนี้

ฝ่ายเทคโนโลยีสารสนเทศ ได้ทำการติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) ยี่ห้อ Schneider ขนาด 20 KVA และ 40 KVA เพื่อใช้ควบคุมการจ่ายกระแสไฟฟ้าให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบสำรองไฟฟ้าสามารถสำรองไฟฟ้าสำหรับการใช้งานได้อย่างน้อย 1.30 ชั่วโมง ในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง เพื่อให้ผู้ดูแลระบบสามารถดำเนินการปิดระบบสารสนเทศได้อย่างทันท่วงที และสำรองข้อมูลไว้อย่างปลอดภัย

5.4 เหตุการณ์หรือภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ดังนี้

- 5.4.1 จัดหลักสูตรอบรมให้กับเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เป็นการลดความเสี่ยงด้าน Human error ให้น้อยที่สุด เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้ และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ส่งผลให้ความเสี่ยงที่อาจจะเกิดจาก Human error ลดน้อยลง
- 5.4.2 กำหนดนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศ โดยแจ้งเวียนแนวทางปฏิบัติดังกล่าวให้เจ้าหน้าที่ทุกคน ทราบ และถือปฏิบัติ

5.5 เหตุการณ์ที่เกิดจากภัยคุกคาม และการจารกรรมข้อมูล

เหตุการณ์หรือภัยที่เกิดจากภัยคุกคาม และการจารกรรมข้อมูล ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse)

ข่าวไวรัสหลอกลวง (Hoax) และไวรัสเรียกค่าไถ่ (Ransomware) เป็นต้น ภัยคุกคามเหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ใช้งานไม่ได้ แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์จากภัยคุกคาม สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ได้ตระหนักถึงปัญหาเหล่านี้จึงได้ทำการ

- 5.5.1 ติดตั้ง Firewall ที่ห้อง Data Center ชั้น 3 ยี่ห้อ Palo alto ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ Trend Micro Server Protect ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่ในการดักจับภัยคุกคามที่พยายามเข้ามาในระบบเครือข่าย และดำเนินการจำกัดการเข้าถึง (Block) ระบบสามารถตรวจสอบได้ว่ามีภัยคุกคามชนิดใดที่พยายามเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)
 - 5.5.2 แจ้งข้อมูลเตือนภัยเกี่ยวกับไวรัสคอมพิวเตอร์ชนิดใหม่ผ่านทางสื่อสารขององค์กรต่อเจ้าหน้าที่ เช่น ทางระบบ Line อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกัน และการกำจัดภัยที่จะเกิดจากภัยคุกคามดังกล่าว ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกัน และแก้ไขปัญหาในเบื้องต้นได้
 - 5.5.3 ระบบสำรองข้อมูล โดยฝ่ายเทคโนโลยีสารสนเทศ ได้ทำการติดตั้งระบบสำรองข้อมูล (Backup) เพื่อป้องกันการสูญหายของข้อมูลโดยจัดเก็บไว้ทั้งหมด 2 แห่ง ถ้าระบบสารสนเทศเกิดความเสียหายจากภัยคุกคาม สามารถดำเนินการกู้คืนระบบสารสนเทศได้ โดยการนำข้อมูลที่สำรองไว้กลับมาติดตั้งระบบใหม่ (Restore)
 - 5.5.4 มีมาตรการในการควบคุมการเข้าออกห้อง Data Center โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องดังกล่าวเว้นแต่จะได้รับอนุญาตจากเจ้าหน้าที่ผู้ดูแลห้องดังกล่าว
- 5.6 เหตุการณ์ หรือภัย หรือผลกระทบจากระบบเครือข่ายอินเทอร์เน็ตล่ม
- 5.6.1 ดำเนินการสลับเส้นทางเครือข่ายอินเทอร์เน็ตจากเส้นทางหลักไปยังเส้นทางสำรอง (Backup Link) เพื่อการใช้งานในกรณีฉุกเฉิน ซึ่งฝ่ายเทคโนโลยีสารสนเทศ ได้ทำการตั้งค่าให้ระบบสามารถใช้งาน Link สำรองได้ทันทีหากมีเหตุเกิดขึ้น
 - 5.6.2 หากระบบเครือข่ายอินเทอร์เน็ตที่ให้บริการแก่สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) หยุดชะงัก หรือไม่สามารถให้บริการได้นานกว่า 5 นาที ให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ประสานแจ้งปัญหาไปยังผู้ให้บริการ (Internet Service Provider) เพื่อตรวจสอบ และแก้ไขปัญหา
- 5.7 เหตุการณ์หรือภัยหรือผลกระทบจากอุปกรณ์ในห้องควบคุม (Data Center) ทำงานไม่ปกติ
- ในกรณีที่อุปกรณ์ภายในห้องควบคุม (Data Center) เช่น เครื่องปรับอากาศ เครื่องสำรองไฟฟ้า ระบบแจ้งเตือน ไม่สามารถทำงานได้ตามปกติอาจส่งผลกระทบต่อระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) รวมถึงระบบสารสนเทศที่สำคัญต่าง ๆ ดังนั้น หากพบว่าอุปกรณ์ภายในห้องควบคุม (Data Center) ไม่สามารถทำงานได้ตามปกติให้ผู้ดูแลระบบปฏิบัติดังนี้

- 5.7.1 ประสานแจ้งปัญหาไปยังผู้ให้บริการ (Vender) เพื่อตรวจสอบและแก้ไขปัญหาที่เกี่ยวข้องกับอุปกรณ์ภายในห้องควบคุม (Data Center) โดยทันที
- 5.7.2 ดำเนินการปิดอุปกรณ์ที่ทำงานไม่ปกติ เพื่อป้องกันอุปกรณ์ภายในห้องได้รับเสียหาย
- 5.7.3 เมื่ออุปกรณ์สามารถทำงานได้เป็นปกติ ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้อง ทำการเปิดและทดสอบอุปกรณ์

5.8 เหตุการณ์หรือภัยหรือผลกระทบจากการประท้วง/การจลาจล

- 5.8.1 ฝ่ายเทคโนโลยีสารสนเทศ ได้ทำการติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) ยี่ห้อ Schneider ขนาด 20 KVA และ 40 KVA เพื่อใช้ควบคุมการจ่ายกระแสไฟฟ้าให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าสามารถสำรองไฟฟ้าสำหรับการใช้งานได้อย่างน้อย 1.30 ชั่วโมง ในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง เพื่อให้ผู้ดูแลระบบสามารถดำเนินการปิดระบบสารสนเทศได้อย่างทันท่วงที และสำรองข้อมูลไว้อย่างปลอดภัย
- 5.8.2 ดำเนินการสำรองข้อมูลระบบสารสนเทศที่มีความสำคัญและเคลื่อนย้ายข้อมูลไปเก็บไว้ในสถานที่ที่มีความปลอดภัยแห่งอื่น
- 5.8.3 หากระบบสารสนเทศและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยังสามารถใช้งานได้ตามปกติให้ผู้ดูแลระบบ บริหารจัดการระบบเครือข่ายจากระยะไกล (Remote Management) การจัดเตรียมอุปกรณ์ที่จำเป็นในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ จะต้องดำเนินการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น ในกรณีเครื่องคอมพิวเตอร์แม่ข่าย (server) เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้
 - (1) แผ่น Boot Disk / USB Boot
 - (2) แผ่นติดตั้งระบบปฏิบัติการ และระบบเครือข่าย
 - (3) โปรแกรม Anti virus
 - (4) แผ่น Driver อุปกรณ์ต่างๆ
 - (5) ระบบสำรองไฟฉุกเฉิน
 - (6) Hard Disk สำรอง
 - (7) สำเนารายละเอียดการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

6. การจัดการปฏิบัติการงานฉุกเฉินในระบบสารสนเทศสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) เมื่อเกิดเหตุฉุกเฉิน

การจัดการจัดการปฏิบัติการงานฉุกเฉินหรือผู้รับผิดชอบตามสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

6.1 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO)

- 6.1.1 กำหนดนโยบายให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบ
- 6.1.2 ให้คำปรึกษาแก่ผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย
- 6.1.3 กำหนดอัตรากำลังพลวัสดุอุปกรณ์และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

6.2 หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

- 6.2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ
- 6.2.2 มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ
- 6.2.3 มีอำนาจสั่งเพื่อการระงับเหตุฉุกเฉิน
- 6.2.4 ประชุมหารือกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เพื่อจัดการระบบเครือข่ายคอมพิวเตอร์
- 6.2.5 ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผน ฯ ตามความเหมาะสม
- 6.2.6 รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บัญชาการสถาบันส่งเสริมศิลปหัตถกรรมไทยรับทราบ

6.3 เจ้าหน้าที่อาวุโสฝ่ายเทคโนโลยีสารสนเทศ ทำหน้าที่ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย

- 6.3.1 วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- 6.3.2 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ จะสั่งระงับเหตุฉุกเฉิน
- 6.3.3 สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ
- 6.3.4 ทำหน้าที่แทนหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ ระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่หัวหน้าฝ่ายเทคโนโลยีสารสนเทศระงับเหตุฉุกเฉินไม่อยู่
- 6.3.5 ประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะ และหน่วยดับเพลิง เป็นต้น
- 6.3.6 รายงานให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ ระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว
- 6.3.7 ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

6.4 เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ทำหน้าที่เป็นประสานผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย

- 6.4.1 กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง
- 6.4.2 พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย
- 6.4.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน
- 6.4.4 ป้องกันชีวิตทรัพย์สินและสิ่งแวดลอมให้ได้รับความเสียหายน้อยที่สุด
- 6.4.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศรับทราบอุปกรณ์ที่ต้องตรวจสอบ ได้แก่
 - (1) ทำการตรวจสอบระบบ Firewall
 - (2) ทำการตรวจสอบ Virus, Worm, Spy ware
 - (3) ทำการตรวจสอบ UPS
 - (4) ทำการตรวจสอบ Transaction log files
 - (5) ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
 - (6) ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ

- (7) ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- (8) ทำการตรวจสอบค่า Configuration ของระบบ
- 6.4.6 เตรียมเครื่องมืออุปกรณ์ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว
- 6.4.7 ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่รับผิดชอบในส่วนต่าง ๆ เพื่อทำการกู้คืนระบบ
- 6.4.8 ทำการสำรองข้อมูลทุกวัน
- 6.4.9 ต้องเก็บสิ่งสำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บ
- 6.4.10 นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

7. การวิเคราะห์ทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้นเพื่อให้หน่วยงานสามารถบริหารจัดการ การดำเนินงานขององค์กรให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็นและต้องระบุไว้ในแผนรองรับสถานการณ์ฉุกเฉิน ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบใน 5 ด้าน ดังนี้

- 7.1 ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้งานที่ปฏิบัติงานหลักได้และส่งผลกระทบต่อบุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว
- 7.2 ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ การจัดหา จัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญหรือไม่สามารถจัดหา จัดส่งวัสดุอุปกรณ์ที่สำคัญได้
- 7.3 ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ เช่น การปรับตั้งค่าระบบ (Config) ผู้ดูแลระบบสามารถนำข้อมูลที่มีการสำรองล่าสุด ที่จัดเก็บไว้ในอุปกรณ์จัดเก็บ (Flash Drive) มาทำการตั้งค่าระบบใหม่
- 7.4 ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ
- 7.5 ผลกระทบด้านลูกค้า ผู้ให้บริการที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ลูกค้า ผู้ให้บริการ ผู้มีส่วนได้ส่วนเสียไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

เหตุการณ์สภาวะวิกฤต		ผลกระทบ				
		ด้านอาคาร/ สถานที่ ปฏิบัติงาน หลัก	ด้านวัสดุอุปกรณ์ที่ สำคัญ/การจัดหา จัดส่งวัสดุอุปกรณ์ ที่สำคัญ	ด้านเทคโนโลยี สารสนเทศและ ข้อมูลที่สำคัญ	ด้าน บุคลากร หลัก	ลูกค้า/ ผู้ให้บริการ/ผู้มี ส่วนได้ส่วนเสีย
1	เหตุการณ์อัคคีภัย	✓	✓	✓	✓	✓
2	เหตุการณ์อุทกภัย หรือผลกระทบจาก อุทกภัย	✓	✓	✓	✓	✓

เหตุการณ์สภาวะวิกฤต		ผลกระทบ				
		ด้านอาคาร/ สถานที่ ปฏิบัติงาน หลัก	ด้านวัสดุอุปกรณ์ที่ สำคัญ/การจัดการ จัดส่งวัสดุอุปกรณ์ ที่สำคัญ	ด้านเทคโนโลยี สารสนเทศและ ข้อมูลที่สำคัญ	ด้าน บุคลากร หลัก	ลูกค้า/ ผู้ให้บริการ/ผู้มี ส่วนได้ส่วนเสีย
3	เหตุการณ์ไฟฟ้าดับ ในวงกว้าง	✓	✓	✓	✓	✓
4	เหตุการณ์หรือภัยที่ เกิดจากเจ้าหน้าที่		✓	✓	✓	✓
5	เหตุการณ์ที่เกิดจาก ภัยคุกคาม และจาก การจารกรรมข้อมูล	✓	✓	✓	✓	✓
6	เหตุการณ์ หรือภัย หรือผลกระทบจาก อินเทอร์เน็ตล่ม			✓	✓	✓
7	เหตุการณ์หรือภัย หรือผลกระทบจาก อุปกรณ์ในห้อง Data Center	✓	✓	✓	✓	✓
8	เหตุการณ์หรือภัย หรือผลกระทบจาก การประท้วง/การ จลาจล	✓	✓	✓	✓	✓

8. แผนการสำรองและกู้คืนข้อมูล (Backup and Recovery Plan)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) อยู่ในสภาพพร้อมรองรับการให้บริการได้ ตลอด 24 ชั่วโมง ให้ผู้ดูแลระบบปฏิบัติตามแผนการ Backup and Recovery Plan ดังนี้

8.1 Backup Plan

- 8.1.1 จัดหา จัดเตรียมพื้นที่จัดเก็บข้อมูล (Storage) สำหรับใช้ในการเก็บข้อมูลที่
ต้องการสำรอง รวมถึง Software ที่ใช้ในการสำรองและกู้คืน
- 8.1.2 ทำการสำรองระบบงาน
- 8.1.3 ตรวจสอบความถูกต้องของระบบงาน หลังจากที่ทำสำรอง
- 8.1.4 หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการสำรองข้อมูล จนเป็นเหตุให้ไม่
สามารถสำรองข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง
เพื่อปรึกษาและหาแนวทางในการสำรองข้อมูลอีกครั้ง

8.2 Recovery Plan

- 8.2.1 รายงานปัญหาสาเหตุ ที่ต้องทำการกู้คืนข้อมูล ต่อผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย ทราบ
- 8.2.2 หากความเสียหายที่เกิดขึ้นกับระบบสารสนเทศ หรือระบบเครือข่าย ที่ส่งผลกระทบต่อการใช้งานหรือการให้บริการ หรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที
- 8.2.3 ใช้ข้อมูลล่าสุด ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ โดยต้องดำเนินการดังนี้
 - (1) กรณีเกิดความเสียหายขึ้นกับระบบงาน (Source Code) จะทำการติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด
 - (2) กรณีเกิดความเสียหายขึ้นกับฐานข้อมูล (Database) จะนำฐานข้อมูลที่เก็บไว้ล่าสุด มาทำการกู้คืน เพื่อให้สามารถใช้งานได้ต่อเนื่อง โดยที่ข้อมูลสูญหายน้อยที่สุด
 - (3) กรณีเกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ Hardware ยังคงทำงานปกติ จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด รวมถึงทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
 - (4) กรณีเกิดความเสียหายขึ้นกับ Hardware ผู้ดูแลระบบ ทำการแก้ไขเบื้องต้นให้ Hardware สามารถกลับมาทำงานได้ตามปกติ
- 8.2.4 ดำเนินการกู้คืนข้อมูลระบบงานที่มีปัญหา
- 8.2.5 ตรวจสอบความถูกต้องของระบบงานหลังจากทำการกู้คืนระบบเสร็จเรียบร้อยแล้ว
- 8.2.6 หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการกู้คืนข้อมูล จนเป็นเหตุให้ไม่สามารถ กู้คืนข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้องเพื่อปรึกษาและหาแนวทางในการกู้คืนข้อมูลอีกครั้ง
- 8.2.7 แจ้งผลการกู้คืนข้อมูลให้ผู้ใช้งานทราบ และรายงานผลต่อผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย

9. แผนการทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม

การกู้คืนข้อมูลเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

- 9.1 จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
- 9.2 ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียให้แล้วเสร็จภายใน 48 ชั่วโมง
- 9.3 นำอุปกรณ์ Backup ที่จัดเก็บข้อมูลที่สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ และผู้รับจ้าง (Vender) การบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้คืนระบบกลับมาโดยเร็ว ภายใน 48 ชั่วโมง

9.4 ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

10. การกำหนดผู้รับผิดชอบ

สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) มอบหมายหน้าที่ความรับผิดชอบเพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

- 10.1 ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแลควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติงาน ผู้รับผิดชอบ ได้แก่
- (1) ผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย
 - (2) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
- 10.2 ผู้รับผิดชอบการปฏิบัติงาน (สศท.) ดูแลระบบ ดูแลห้อง Data Center ดูแลแอปพลิเคชัน ทำการสำรองข้อมูล การกู้คืนข้อมูล กำกับ ดูแลควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติงาน (Vender) ผู้รับผิดชอบ ได้แก่
- (1) นางสาวรัตนา ปันงาม เบอร์โทรศัพท์ติดต่อ 084-242-8397
 - (2) นายสุวเรศ ไพธนาธิปไตย เบอร์โทรศัพท์ติดต่อ 095-697-1974
- 10.3 ผู้รับผิดชอบการปฏิบัติงาน (ภายนอกองค์กร) ดูแลระบบ ดูแลห้อง Data Center ดูแลแอปพลิเคชัน ทำการสำรองข้อมูล การกู้คืนข้อมูล
- (1) นางสาวณัฐชฎา พิชะ เบอร์โทรศัพท์ติดต่อ 02-5077297
(ผู้ประสานงาน ณ กระทรวงพาณิชย์)
 - (2) นางสาวพิมลฤดี ทรัพย์สาร เบอร์โทรศัพท์ติดต่อ 099-3299691
(ระบบเครือข่าย Internet NT และ Private Link)
 - (3) นาย สหพร หงษาครประเสริฐ เบอร์โทรศัพท์ติดต่อ 085-2465386
(ดูแลระบบและอุปกรณ์ภายในห้อง Data Center)

11. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินงานหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้ผู้อำนวยการสถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน) ทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ฉบับนี้ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศต่อไป

(ลงชื่อ).....

(นางญาณิดา ปานเกษม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม
สถาบันส่งเสริมศิลปหัตถกรรมไทย (องค์การมหาชน)
วันที่.....๖.....เดือน...กรกฎาคม...พ.ศ...2566...

sacit 