แผนบริหารความต่อเนื่อง

(Business Continuity Plan: BCP)

ด้านเทคโนโลยีสารสนเทศ

สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

คำนำ

ตามที่หน่วยเทคโนโลยีสารสนเทศ ได้จัดทำแผนบริหารความต่อเนื่องหรือต่อไปนี้จะเรียกว่า “Business Continuity Plan : BCP” เพื่อทำให้มั่นใจว่าระบบงาน และสถานที่ทำงาน มีการเตรียมความพร้อมต่อภัยพิบัติหรือภาวะฉุกเฉิน โดยได้คำนึงถึงการป้องกัน การจัดการความต่อเนื่อง ของการดำเนินการและการฟื้นฟูสู่สภาพเดิม โดยได้วิเคราะห์สถานการณ์หรือภาวะฉุกเฉินที่อาจเกิดขึ้น และมีผลกระทบต่อกระบวนการทำงานที่สำคัญของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย เพื่อเป็นแนวทางในการเตรียมความพร้อม และสามารถบริหารจัดการด้านเทคโนโลยีสารสนเทศ ให้สามารถปฏิบัติงานในภารกิจหลักที่มีความสำคัญได้อย่างมีประสิทธิภาพ และสามารถให้บริการนักศึกษา อาจารย์ และบุคลากร ได้อย่างต่อเนื่อง ซึ่งหน่วยเทคโนโลยีสารสนเทศจะได้ทดสอบ ซักซ้อม และปรับปรุงแผนเพื่อจัดทำแผนบริหารความต่อเนื่องต่อไป หน่วยเทคโนโลยีสารสนเทศ คาดหวังว่าแผนบริหารความต่อเนื่องเล่มนี้ จะเป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงานในสภาวะวิกฤต และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

หน่วยเทคโนโลยีสารสนเทศ

สารบัญ

แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)
ด้านเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

1. บทนำ

แผนบริหารความต่อเนื่องหรือต่อไปนี้จะเรียกว่า “Business Continuity Plan : BCP” จัดทำขึ้น เพื่อให้ “หน่วยเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย” สามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติหรือ เหตุการณ์ฉุกเฉินต่าง ๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร โดยไม่ให้สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินดังกล่าวส่งผลให้หน่วยงานต้องหยุดการดำเนินงานหรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

การที่หน่วยงานไม่มีกระบวนการรองรับให้การดำเนินงานเป็นไปอย่างต่อเนื่อง อาจส่งผลกระทบต่อหน่วยงานในด้านต่าง ๆ เช่น ด้านการให้บริการทางระบบงานคอมพิวเตอร์และระบบเครือข่าย ด้านการพัฒนาระบบสารสนเทศ ด้านการเข้าช่วยเหลือเพื่อซ่อมบำรุงอุปกรณ์ระบบคอมพิวเตอร์ ด้านการให้บริการระบบอินเทอร์เน็ตกับสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย ที่มีผลต่อพันธกิจของสถาบัน ดังนั้นการจัดทำแผนบริหารความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้หน่วยงานสามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิดและทำให้กระบวนการสำคัญ (Critical Business Process) สามารถกลับมาดำเนินการได้อย่างปกติหรือตามระดับการให้บริการ (Service Level Agreement : SLA) ที่กำหนดไว้ ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อสถาบันได้

กรอบแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต 4 ขั้นตอน คือ

1. การสร้างความรู้ความเข้าใจให้กับบุคลากรภายในหน่วยเทคโนโลยีสารสนเทศ
2. การเตรียมความพร้อมของหน่วยเทคโนโลยีสารสนเทศ ในการจัดทำแผนรองรับการดำเนินภารกิจการให้บริการด้านเทคโนโลยีสารสนเทศ ตามบทบาทหน้าที่ ได้อย่างต่อเนื่อง (Business Continuity Plan: BCP)
3. การซักซ้อมแผนและนำไปปฏิบัติได้จริง
4. การจัดการหลังเกิดภัย

โดยแนวคิดการบริหารความต่อเนื่องของหน่วยเทคโนโลยีสารสนเทศ คือ การควบคุมดูแลและป้องกันทรัพยากรที่สำคัญต่อการดำเนินงานหรือการให้บริการ เพื่อสร้างประโยชน์สูงสุดสำหรับผู้รับบริการและผู้มีส่วนได้เสีย ซึ่งภายในช่วงระยะเวลาแรกจะเป็นช่วงของการตอบสนองต่ออุบัติการณ์ (Incident/Emergency Management) และในกรณีที่เหตุการณ์และความเสียหายขยายตัวไปในวงกว้าง การตอบสนองอาจจำเป็นต้องยกระดับเป็นการบริหารจัดการวิกฤต (Crisis Management) ภายหลังจากนั้นจะเป็นช่วงของการทำให้เกิดความต่อเนื่องของกระบวนการทางธุรกิจ (Continuity Management) เพื่อให้สถาบันสามารถกลับมาดำเนินงานได้ จึงมีความจำเป็นที่สถาบันต้องจัดทำแผนความต่อเนื่อง (Business Continuity Plan : BCP) ฉบับนี้

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง

2.2 เพื่อให้หน่วยเทคโนโลยีสารสนเทศมีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤตตามแผนที่ได้กำหนดไว้

2.3 เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ

2.4 เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

2.5 เพื่อให้หน่วยงานภายในสถาบัน ประชาชน บุคลากรสถาบัน ผู้ที่หน่วยเทคโนโลยีสารสนเทศให้และรับบริการ ตลอดจนผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพขององค์กร แม้ต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

2.6 เพื่อปกป้องและรักษาความปลอดภัยของชีวิตเจ้าหน้าที่

แผนบริหารความต่อเนื่อง หรือ (Business Continuity Plan: BCP) เป็นชุดเอกสารคำแนะนำและวิธีการที่ช่วยให้ธุรกิจ/บริการขององค์กรสามารถตอบสนองต่อการเกิดอุบัติเหตุ ภัยพิบัติ ภาวะฉุกเฉินและหรือภัยคุกคามได้โดยไม่ต้องหยุดชะงัก/หรือมีอุปสรรคที่สำคัญต่อการดำเนินงาน เรียกอีกอย่างว่า “การเริ่มต้นใหม่ของธุรกิจ” ซึ่งจำเป็นต้องมีแผนการกู้คืนระบบหรือแผนการกู้คืนทรัพยากรบุคคลและกระบวนการทำงาน เพื่อให้สามารถปฏิบัติงานหรือสามารถให้บริการแก่ประชาชนต่อไปได้ แผนดังกล่าวจัดทำขึ้นโดยประยุกต์ตามแนวทางของการบริหารความต่อเนื่อง (Business Continuity Management: BCM) ที่สอดคล้องตามมาตรฐานสากล BS25999 (Business Continuity Management : BCM)

Standard หมายถึง รหัสมาตราฐานของ British Standards Institution (BSI) ที่องค์กรทั่วโลกยอมรับ ซึ่งกำหนดให้มี 6 องค์ประกอบหลักเป็นวงจรการบริหารความต่อเนื่อง (BCM Life Cycle) ดังหัวข้อต่อไปนี้

1. การบริหารโครงการจัดการความต่อเนื่อง (BCM Program Management)
2. การศึกษาและทำความเข้าใจองค์กร (Understanding of Organization)
3. การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง BCM (Determining BCM Strategy) (เช่น Recovery Strategy)
4. การพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน (Developing and Implementing BCM Response) (เช่น Incident Management Plan (IMP), Emergency/Crisis Management Plan (CMP), Business Continuity Plan (BCP), Recovery Plan (RP)
5. การทดสอบ ปรับปรุงและทบทวนแผน (Exercising Monitoring and Reviewing) (เช่น Call Tree, Table Top Testing, Simulation, Full BCP Exercise)
6. การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (Embedding BCM in the Organization’s Culture)

3. สมมติฐานของแผนบริหารความต่อเนื่อง (BCP Assumptions)

โดยเอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

3.1 เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่าง ๆ แต่มิได้ส่งผลกระทบต่อสถานที่ที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้

3.2 ทีมงานหลักกลุ่มงาน/ฝ่าย ที่รับผิดชอบในการดำเนินงานตามบทบาทหน้าที่ ตลอดจนการสำรองระบบสารสนเทศต่าง ๆ มิได้รับผลกระทบจากเหตุการณ์ฉุกเฉิน

3.3 หน่วยงาน ทีมงาน สถานที่ในการสำรองข้อมูล ระบบสารสนเทศต่าง ๆ โดยระบบคอมพิวเตอร์ ระบบเครือข่าย มิได้รับผลกระทบจากเหตุการณ์ฉุกเฉิน

3.4 ระบบสารสนเทศหลักของแต่ละหน่วยงานภายในสถาบันมีเจ้าหน้าที่ระบบงานคอมพิวเตอร์ หรือผู้ประสานงานด้านระบบคอมพิวเตอร์ ทำหน้าที่ดูแลระบบในส่วนของแต่ละหน่วยงาน รวมทั้งมีการสำรองข้อมูลในส่วนระบบงานของแต่ละหน่วยงานอย่างสม่ำเสมอ

3.5 บุคลากรที่มีการระบุในเอกสารนี้ หมายถึง บุคลากรสถาบัน และลูกจ้างประจำทั้งหมดของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

3.6 หน่วยเทคโนโลยีสารสนเทศดูแลเฉพาะระบบ VM (Virtual Machine) ส่วนระบบภายใน VM หน่วยงานจะเป็นผู้ดูแล

4. ขอบเขตของแผนบริหารความเสี่ยง (Scope of BCP)

แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Management :BCP) ฉบับนี้ใช้รองรับสถานที่การณ์ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินในพื้นที่ของสถาบันหรือหน่วยงานภายในสถาบันด้วยเหตุการณ์ต่อไปนี้

4.1 ภัยธรรมชาติ เช่น อุทกภัย อัคคีภัย วาตภัย

4.2 ชุมนุมประท้วง/จลาจล

4.3 โรคระบาด

4.4 ก่อการร้าย

4.5 อุบัติเหตุ เช่น อาคารถล่ม หรือ ไฟฟ้าดับเป็นเวลานาน หรือ ระบบคอมพิวเตอร์ หรือ ระบบสื่อสารหลักเกิดความเสียหาย ระบบข้อมูลเสียหายรุนแรง เป็นต้น

4.6 ภัยคุกคามทางไซเบอร์ (Cyber Security) เช่น การโจมตีทางไซเบอร์ หรือช่องโหว่เว็บไซต์

5. การวิเคราะห์ทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน มีหลากหลายรูปแบบ ดังนั้น เพื่อให้หน่วยเทคโนโลยีสารสนเทศสามารถบริหารจัดการการดำเนินงานของหน่วยงานให้มีความต่อเนื่อง การดูแลและจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็นและต้องระบุไว้ในแผนบริหารความต่อเนื่อง ซึ่งเตรียมการทรัพยากรที่สำคัญจากผลกระทบใน 5 ด้าน ดังนี้

5.1 ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ที่ปฏิบัติงานหลักได้รับความเสียหาย หรือไม่สามารถใช้สถานที่ที่ปฏิบัติงานหลักได้ และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว

5.2 ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญหรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้

5.3 ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย หรือข้อมูลที่สำคัญ ไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

5.4 ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นซึ่งทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

5.5 ผลกระทบด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย หมายถึง เหตุการณ์ที่เกิดขึ้นซึ่งทำให้/ผู้ที่หน่วยเทคโนโลยีสารสนเทศให้บริการหรือรับบริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

6. การประเมินผลกระทบต่อกระบวนการดำเนินงาน

ระดับผลกระทบ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ
สูงมาก	- เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูงมาก (มากกว่า 10 ล้านบาท)
	- โอกาสที่จะเกิดความเสี่ยง 1 ครั้งต่อเดือน หรือมากกว่า
	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่า ร้อยละ 50
	- เกิดการสูญเสียชีวิตและ/หรือภัยคุกคามต่อสาธารณชน
	- มีการพาดหัวข่าวในทางเสื่อมเสียจนไม่สามารถแก้ข่าวได้
	- ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศและนานาชาติ
สูง	- เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูง (มากกว่า 5 - 9 ล้านบาท)
	- โอกาสที่จะเกิดความเสี่ยง 1 ครั้ง ภายใน 6 เดือน
	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ 25-50
	- เกิดการบาดเจ็บต่อผู้รับบริการ/บุคคล/กลุ่มคน
	- มีการเผยแพร่ข่าวในวงกว้างซึ่งต้องใช้เวลามากในการเผยแพร่ชี้แจง
	- ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศ
ปานกลาง	- เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับปานกลาง (มากกว่า 1 - 4 ล้านบาท)
	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ 10-25
	- โอกาสที่จะเกิดความเสี่ยง 1 ครั้ง ต่อปี
	- ต้องมีการรักษาพยาบาลและหยุดงานมากกว่า 5 วัน
	- มีการเผยแพร่ข่าวแต่สามารถแก้ข่าวได้ภายใน 1 – 3 วัน
	- ระบบสารสนเทศ มีปัญหาและมีความสูญเสียไม่มาก
ต่ำ	- เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำ (มากกว่า 1 - 9 แสนบาท)
	- โอกาสที่จะเกิดความเสี่ยง 1 ครั้ง ภายใน 4 ปี
	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ 5-10
	- ต้องมีการปฐมพยาบาล
	- ระบบสารสนเทศ เกิดเหตุที่แก้ไขได้และไม่มีความสูญเสีย
ต่ำมาก	- เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำมาก (ไม่เกิน 1 แสนบาท)
	- โอกาสที่จะเกิดความเสี่ยง 1 ครั้งภายใน 5 ปี
	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงน้อยกว่าร้อยละ 5
	- อันตรายต่อร่างกายขั้นปฐมพยาบาลเบื้องต้น
	- เกิดเหตุที่ไม่มีความสำคัญกับระบบสารสนเทศ

7. สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

เหตุการณ์สภาวะวิกฤต	ผลกระทบ				
	ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	ด้านคู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย
1. เหตุการณ์ภัยธรรมชาติ เช่น อุทกภัย อัคคีภัย วาตภัย	✓	✓	✓	✓	✓
2. เหตุการณ์ชุมนุมประท้วง/จลาจล	✓	✓	✓	✓	✓
3. เหตุการณ์โรคระบาด	✓			✓	✓
4. เหตุการณ์ก่อการร้าย	✓	✓	✓	✓	✓
5. อุบัติเหตุ อาคารถล่มหรือไฟฟ้าดับเป็นเวลา นานหรือระบบคอมพิวเตอร์ หรือระบบสื่อสาร หลักเกิดความเสีย หาย ระบบข้อมูลเสียหายรุนแรง เป็นต้น	✓	✓	✓	✓	✓
6. ภัยคุกคามทางไซเบอร์		✓	✓	✓	✓

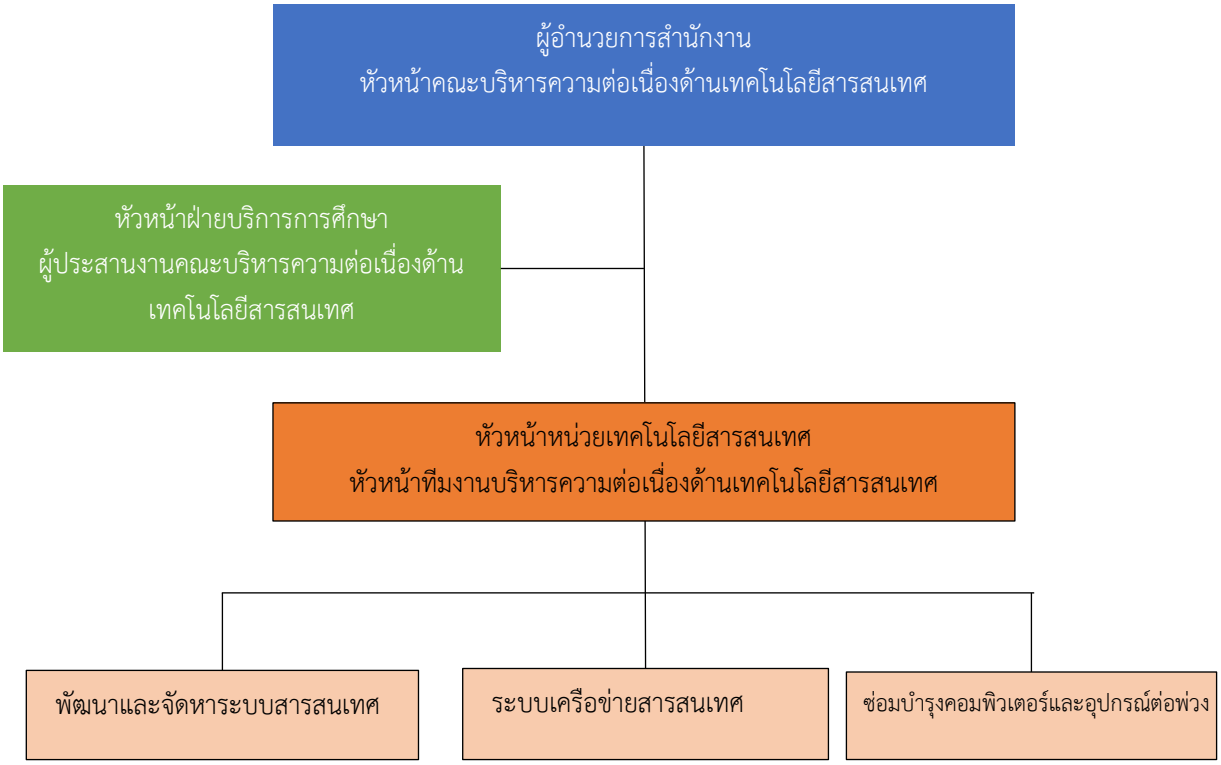
แผนบริหารความต่อเนื่อง (Business Continuity Management :BCP) ฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องจากการดำเนินงานปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของหน่วยงาน

เนื่องจากหน่วยเทคโนโลยีสารสนเทศยังสามารถบริหารจัดการ หรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้บริหารหน่วยงาน หรือหัวหน้าและทีมงานกลุ่มงาน/ฝ่าย สามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

8. การบริหารความต่อเนื่องของหน่วยเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

8.1 ทีมงานแผนบริหารความต่อเนื่อง (Business Continuity Plan Team)

เพื่อให้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Management : BCP) ของหน่วยเทคโนโลยีสารสนเทศสถาบันสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล ดังนั้นหน่วยเทคโนโลยีสารสนเทศ จึงจัดตั้งทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Team) ของหน่วยเทคโนโลยีสารสนเทศ มีโครงสร้างและบทบาทหน้าที่สอดคล้องกับแผนผังโครงสร้างของหน่วยเทคโนโลยีสารสนเทศด้านล่างต่อไปนี้



รูปภาพแผนผังโครงสร้างของหน่วยเทคโนโลยีสารสนเทศ

ทีมงานแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	
บทบาท	**ผู้รับผิดชอบ**
หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	ผู้อำนวยการสำนักงาน
ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	หัวหน้าฝ่ายบริการการศึกษา
หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	หัวหน้าหน่วยเทคโนโลยีสารสนเทศ
ทีมพัฒนาและจัดหาระบบสารสนเทศ	นายอำนาจ บุญอริยะ, นายปวริศ กิตตินันทพันธุ์
ทีมระบบเครือข่ายสารสนเทศ	นายเจษฎา เลอวิทย์วรพงศ์
ทีมซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	นางสาวพิชญ์สินี เชียงเครือ

โดยแต่ละตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงานและกู้คืนเหตุการณ์ฉุกเฉินในส่วนงานของตนเองให้สามารถบริหารจัดการความต่อเนื่องและกลับสู่สภาวะปกติได้โดยรวดเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองเป็นผู้รับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลักไปก่อน ดังตารางต่อไปนี้

ตำแหน่ง / งาน	บุคลากรหลัก	บุคลากรสำรอง
หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	นายณัฐวุฒิ เลี่ยมสุวรรณ	นางศรัณยา จันทรตรี
ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	นางศรัณยา จันทรตรี	นายวิโชค มณีสงค์
หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	นายวิโชค มณีสงค์	นายอำนาจ บุญอริยะ,
งานพัฒนาและจัดหาระบบสารสนเทศ	นายอำนาจ บุญอริยะ	นายปวริศ กิตตินันทพันธุ์
งานระบบเครือข่ายสารสนเทศ	นายเจษฎา เลอวิทย์วรพงศ์	นางสาวพิชญ์สินี เชียงเครือ
งานซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	นางสาวพิชญ์สินี เชียงเครือ	นายเจษฎา เลอวิทย์วรพงศ์

รายชื่อหน่วยงานที่เกี่ยวข้องและผู้เกี่ยวข้อง/ผู้มีส่วนได้ส่วนเสีย (ภายนอกสถาบัน)

ชื่อหน่วยงาน	รายชื่อผู้ติดต่อ	โทรศัพท์ที่ทำงาน	โทรศัพท์มือถือ	E-Mail
บริษัท ซีดีจี ซิสเต็มส์ จำกัด	พลฤกษ์ โพธิ์ถาวี	02-678-0978	081-647-1005	phonlaruk.p@cdg.co.th
บริษัท เอ็นซีซีเน็ทเวิร์ค จำกัด	วัชรพงศ์ สุขวณิช		090-1619166	watcharapong@networks.co.th
บริษัท อินโฟลิสท์ จำกัด	ธีรวุฒิ กาญจนเวชกุล สาธิต สุวรรณธาราเรือง	02-089-0090	061-561-4287	support@infolyst.net
บริษัท เทคโนโลยี อินฟราสตรัคเจอร์ จำกัด	พิชญา พาริวงค์	02-434-9799	081-497-1329	monnapa@ti.co.th
บริษัท บริษัท เมาท์ทูเมาท์ คอมมูนิเคชัน จำกัด	ฐิตาภรณ์ เทศพงศ์	02-434-9010	088-530-2355	parachute@mouthtomouth.co.th
บริษัท ดั๊บเบิ้ล เอ ดิจิตอล ซินเนอร์จี จำกัด	วรินทร สายศิริ		085-8352346	
บริษัทฟูจิตสึ (ประเทศไทย) จำกัด	ชญานิศ ติณเวส	02-302-1500	093-6294994	chayanit@fujitsu.com
บริษัท เอซอฟท์วัน จำกัด	ศิวะวงศ์ วิเชียรชัยยะ	02-286-7794	086-334-7213	sivawong@asoft1.com
บริษัท ซีนิธคอมพ์ จำกัด	พัสวียา บุญภูงา	02-273-0727	089-811-5589	Patsaveeya@zenithcomp.co.th
บริษัท อิเล็กทรอนิก คอมเมิร์ซ จำกัด			097-297-0150	

รายชื่อหน่วยงานที่เกี่ยวข้องและผู้เกี่ยวข้อง/ผู้มีส่วนได้ส่วนเสีย (ผู้ประสานงานภายในสภากาชาดไทย)

ชื่อหน่วยงาน	รายชื่อผู้ติดต่อ	โทรศัพท์ที่ทำงาน	โทรศัพท์มือถือ	E-Mail
สำนักงานเทคโนโลยีสารสนเทศและดิจิทัล สภากาชาดไทย	นายจักรพันธุ์ สุขเจริญ	4015	061-401-2683	chakaphan.s@redcross.or.th

9. กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน 5 ด้าน ดังนี้

9.1 ด้านอาคาร/สถานที่ปฏิบัติงานหลักและสำรอง กำหนดให้อาคารสิรินธรานุสรณ์ ๖๐ พรรษา เป็นอาคารหลักและอาคารเฉลิมพระเกียรติ ๖ รอบ เป็นอาคารสำรอง

1. ห้องคอมพิวเตอร์ หน่วยเทคโนโลยีสารสนเทศ อาคารสิรินทรานุสรณ์ ๖๐ พรรษา ชั้น 2
2. ห้องศูนย์เทคโนโลยีสารสนเทศเพื่อการศึกษา อาคารเฉลิมพระเกียรติฯ ชั้น 10
3. ปฏิบัติงานจากที่บ้านเป็นการชั่วคราว (Work At Home)

9.2 ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ คือ

1. จัดเตรียมจัดหาคอมพิวเตอร์สำรองใช้งาน (Desktop/ Laptop) (กรณีที่ไม่สามารถหาได้ให้เช่าจากเอกชน)
2. อินเทอร์เน็ต (Internet) การให้บริการระบบคลาวด์ (Cloud Computing)
3. จัดเตรียมจัดหาวัสดุอุปกรณ์ต่าง ๆ ที่จำเป็นต้องใช้งาน ทั้งวัสดุสิ้นเปลืองและอื่น ๆ ให้เพียงพอตามความเหมาะสม

9.3 ด้านเทคโนโลยีสารสนเทศและข้อมูลสำคัญ คือ

1. จัดทำระบบงานสำรองข้อมูลสารสนเทศเพื่อรองรับกรณีที่หน่วยเทคโนโลยีสารสนเทศ และศูนย์ข้อมูลหลักไม่สามารถใช้งานได้ ให้จัดเก็บสำรองไว้ที่ DR-Site (Disaster Recovery Site) โดยวิธีการเช่าใช้บริการ Cloud Computing บริการผ่านอินเตอร์เนต ช่วยให้สามารถจัดเก็บข้อมูล ดำเนินการและจัดการข้อมูลต่างๆ
2. เครื่อง Server เคลื่อนย้ายไปยังที่ปลอดภัย หรือ พื้นที่ปฏิบัติงานสำรอง ในกรณีที่จำเป็นต้องดำเนินการและสามารถทำได้
3. อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่ายของทั้งสถาบัน
4. ระบบสารสนเทศของหน่วยงานภายในสถาบัน
5. ข้อมูลแผนงาน งบประมาณ และข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสถาบัน

9.4 ด้านบุคลากรหลัก

1. ทีมปฏิบัติโดยมีบุคลากรหลักและสำรองในแต่ละภารกิจ / ทดแทนภายในกลุ่มงานเดียวกัน
2. กำหนดให้ใช้บุคลากรนอก หรือกลุ่มงาน โดยการจ้างในกรณีที่บุคลากรไม่เพียงพอหรือขาดแคลน

9.5 ด้านคู่ค้า / ผู้ให้บริการที่สำคัญ / ผู้มีส่วนได้เสีย

1. ระบบ Internet หาก Link หลักล่มสามารถใช้ Link คู่ขนานหรือ Link สำรองแทนได้ ปัจจุบัน มี Link เครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (Inter University Network) หรือที่เรียกว่า เครือข่าย “UniNet” 2. Link 3BB เป็น Link สำรอง
2. ประสานงานผู้ให้บริการทั้งรายปัจจุบันและ/หรือรายใหม่เพื่อรองรับการให้บริการแทนภายใน SLA ที่กำหนดไว้ เช่น ภายใน 4 ชั่วโมง (Response time)
3. ใช้ระบบ Internet แบบพกพา เพื่อใช้งานชั่วคราวกรณีที่จำเป็น
4. ประสานงานติดต่อสื่อสารผู้เกี่ยวข้องผ่านทางระบบ Internet

หมายเหตุ : พื้นที่สำหรับปฏิบัติงานที่บ้าน หมายถึง พื้นที่ปฏิบัติงานในที่พักอาศัย 1 แห่ง โดยในช่วงแรกหลังเกิดเหตุการณ์วิกฤต ให้เจ้าหน้าที่ที่พักอาศัยอยู่ในพื้นที่ใกล้เคียงกันไปร่วมปฏิบัติงานร่วมกัน ณ ที่พักอาศัยของเจ้าหน้าที่ที่พร้อมสำหรับใช้เป็นพื้นที่ในการปฏิบัติงาน

10. การทดสอบแผนความต่อเนื่อง (Testing the Plan)

10.1 มีการทดสอบแผนบริหารความต่อเนื่องฯ บางส่วนหรือทั้งหมดเป็นประจำทุกปี เพื่อให้มั่นใจว่าหน่วยงานมีการเตรียมตัวและมีความสามารถในการกู้คืนธุรกิจสำคัญภายในระยะเวลาที่กำหนดไว้

10.2 ควรทดสอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยการสร้างสถานการณ์จำลอง (Simulation Exercises) เป็นประจำทุกปี โดยต้องมีการปรับเปลี่ยนหมุนเวียนสถานการณ์จำลอง เพื่อให้แน่ใจว่าได้มีการทดสอบความสูญเสีย/เสียหายของปัจจัยหลักที่เกี่ยวข้องทุกๆ 1 ปี

10.3 ข้อบกพร่องใด ๆ (GAP) ที่เกิดจากการทดสอบบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ จะต้องมีการติดตามให้เสร็จสิ้นภายใน 3 เดือน นับตั้งแต่วันที่ทดสอบ ถ้าไม่สามารถดำเนินการติดตามได้ตามเวลาที่กำหนดให้หัวหน้าทีมบริหารและผู้ประสานงานความต่อเนื่องด้านเทคโนโลยีสารสนเทศได้แจ้งผู้บริหารระดับสูงเพื่อพิจารณาแนวทางแก้ไขข้อบกพร่องนั้น ๆ ให้หมดไปโดยเร็ว

11. การดูแลปรับปรุงแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Maintenance of the plan)

กำหนดให้ต้องมีการปรับปรุงแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ให้เป็นปัจจุบันทุกปีหรือทุกครั้งหลังการทดสอบหรือภายใน 3 เดือน ในกรณีที่มีการเปลี่ยนแปลงสำคัญ เช่น รายชื่อผู้ที่จะต้องได้รับการแจ้งเหตุ (Staff Recall List) ควรมีการปรับปรุงให้เป็นปัจจุบันทุก ๆ ไตรมาส การลดความซับซ้อนของขั้นตอนต่าง ๆ และส่งสำเนาให้กับเลขานุการคณะกรรมการจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เพื่อให้ทราบการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของทีม การปฏิบัติหน้าที่และขั้นตอนปฏิบัติต่าง ๆ ที่สอดคล้องกับบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ฐานข้อมูลบัญชีรายการ/รายชื่อ และคู่มือปฏิบัติงานทั้งหมด ซึ่งเป็นส่วนหนึ่งของบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ หรือต้องมีการอ้างอิงไว้ในบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ต้องปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

12. การดำเนินการเมื่อเกิดเหตุการณ์ฉุกเฉิน (Emergency Response)

12.1 ปฏิบัติการโดยทันที เคลื่อนย้ายบุคลากรที่ได้รับผลกระทบและประเมินความเสียหายหรือผลกระทบวัตถุประสงค์สำคัญของการดำเนินการเมื่อเกิดเหตุการฉุกเฉิน การลดความสูญเสีย/เสียหายที่เกิดขึ้นกับชีวิต ทรัพย์สินและการดำเนินงานให้น้อยที่สุด

12.2 จัดทำแผนปฏิบัติการดำเนินการเมื่อเกิดเหตุฉุกเฉิน (Emergency Response Action Plan : ERAP) ระดับหน่วยงาน เพื่อให้หน่วยงานที่เกี่ยวข้องรับมือกับสถานที่การณ์ฉุกเฉิน ซึ่งแผนนี้จะกำหนดกรอบการทำงานเพื่อให้มีการดำเนินการเมื่อเกิดเหตุการณ์ฉุกเฉินอย่างเป็นลำดับขั้นตอนในระดับผู้บริหาร (Management Level) เพื่อใช้ในกรณีที่เกิดวิกฤตสำคัญที่ทำให้การปฏิบัติราชการหยุดชะงัก

12.3 เจ้าหน้าที่ปฏิบัติการในการดำเนินการเมื่อเกิดเหตุการณ์ฉุกเฉินที่สำคัญของหน่วยงานนอกเหนือจากหัวหน้าทีมบริหารความต่อเนื่อง มีดังนี้

1. ผู้รับผิดชอบด้านอัคคีภัย (Fire warden)

ผู้รับผิดชอบหลักด้านอัคคีภัย มีบทบาทหน้าที่เพื่อให้มั่นใจว่าได้เคลื่อนย้ายบุคลากรออกจากสถานที่ที่เกิดเหตุตามขั้นตอนปฏิบัติการ และต้องรายงานผลการเคลื่อนย้ายบุคลากรให้ผู้ดูแลความปลอดภัยอาคารสถานที่ที่ (Building Safety Manager) และให้ความช่วยเหลือในการติดตามบุคลากรที่หายไปหรือไม่ได้รายงานตัว

2. หัวหน้าผู้ดูแลอาคาร (Building Manager) / ผู้ดูแลประจำชั้นอาคาร (Floor Manager) หัวหน้าผู้ดูแลอาคารและผู้ดูแลประจำชั้นอาคาร มีบทบาทหน้าที่ในการจัดการและประสานงาน ณ สถานที่ที่เกิดเหตุทันทีที่เกิดเหตุการณ์ฉุกเฉินที่คุกคามชีวิตและความปลอดภัยของบุคลากร รวมถึงทรัพย์สินของสถาบัน

13. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) สามารถจำแนกกระบวนการทำงานที่กลุ่มงาน/ฝ่ายส่วนงานต้องให้ความสำคัญและกลับมาดำเนินงานหรือฟื้นคืนให้ได้ภายในระยะเวลาตามที่กำหนดดังตารางต่อไปนี้

กระบวนการหลัก	ระดับความเร่งด่วน	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (ไม่เกิน)						
		1 ชั่วโมง	4 ชั่วโมง	8 ชั่วโมง	1 -3 วัน	4 -6 วัน	1 สัปดาห์	2 สัปดาห์
ระบบเครือข่ายอาคารสิรินธรานุสรณ์	สูง			✓				
ระบบเครือข่ายอาคารเฉลิมพระเกียรติ	สูง			✓				
ระบบเครือข่ายอาคารบรมคุณ	สูง			✓				
ระบบโทรศัพท์ (IP Phone)	สูง			✓				
ระบบทะเบียนนักศึกษา	สูง			✓				
ระบบบริหารงานบุคคล	สูง			✓				
ระบบการเรียนการสอนออนไลน์ E-Learning	สูง			✓				
การจัดหาเครื่องคอมพิวเตอร์	สูง		✓					
ระบบแม่ข่าย	สูง			✓				
ระบบเว็บไซต์สถาบัน	ปานกลาง			✓				
การจัดหาเครื่องพิมพ์	ปานกลาง			✓				
ระบบบันทึกเวลาเข้า - ออกของบุคลากรสถาบัน	ปานกลาง				✓			

สำหรับกระบวนงานอื่นๆ ที่ประเมินแล้วอาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมาก หรือมีความยืดหยุ่นสามารถชะลอการดำเนินงานและการให้บริการได้ โดยให้หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศประเมินความจำเป็นและเหมาะสม ทั้งนี้หากมีความจำเป็น ให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกับกระบวนงานหลัก

14. การวิเคราะห์เพื่อกำหนดความต้องการทรัพยากรที่สำคัญในการบริหารความต่อเนื่อง

14.1 พื้นที่หลักและพื้นที่สำรอง

1. **พื้นที่ทำงานของหน่วยเทคโนโลยีสารสนเทศ**

- อาคารสิรินทรานุสรณ์ ๖๐ พรรษา ชั้น 2 มีพื้นที่ 720 ตารางเมตร และมีห้อง Data Center

2. **พื้นที่ทำงานสำรอง**

- อาคารเฉลิมพระเกียรติฯ ชั้น 10 พื้นที่ประมาณ 108 ตารางเมตร ศูนย์เทคโนโลยีสารสนเทศเพื่อการศึกษา
- อาคารเฉลิมพระเกียรติฯ ชั้น 7 พื้นที่ประมาณ 12 ตารางเมตร ห้อง Data Center
- พื้นที่ที่สถาบันประกาศใช้งานในกรณีฉุกเฉิน

14.2 ความต้องการด้านเครื่องคอมพิวเตอร์และวัสดุอุปกรณ์ต่าง ๆ ที่จำเป็น

เช่น เครื่องคอมพิวเตอร์ Desktop Laptop เครื่องพิมพ์ Printer โทรศัพท์มือถือ อุปกรณ์เครือข่ายที่สำคัญ เครื่องถ่ายเอกสาร อุปกรณ์ด้านพัสดุ พร้อมระบุที่มาของการจัดหาและจำนวนเครื่องและวัสดุต่าง ๆ

15. ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูลที่หน่วยเทคโนโลยีสารสนเทศ ต้องใช้ดำเนินการ

เนื่องจากระบบบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยเทคโนโลยีสารสนเทศ รองรับระบบและข้อมูลของหน่วยงานภายในสถาบันในลักษณะแบบรวมศูนย์ ดังนั้น หน่วยงานจึงใช้ข้อมูลสารสนเทศโดยการเชื่อมโยงระบบของหน่วยงานเข้ากับหน่วยหน่วยเทคโนโลยีสารสนเทศ ผ่านเครือข่ายอินเทอร์เน็ตและเครือข่ายภายในสถาบัน ดังนั้นหากระบบมีปัญหา ต้องรอให้หน่วยเทคโนโลยีสารสนเทศกู้คืนระบบก่อน หน่วยงานภายในต่างๆ จึงจะสามารถใช้งานระบบได้ต่อไป

หน่วยเทคโนโลยีสารสนเทศจึงมีความจำเป็นสำคัญที่จะต้องดูแลระบบสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายให้พร้อมรองรับความต่อเนื่องในการใช้งานของหน่วยงานต่างๆ ตามตารางดังต่อไปนี้

ประเภททรัพยากร	แหล่งข้อมูล	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ						
		1 ชั่วโมง	4 ชั่วโมง	8 ชั่วโมง	1 วัน	3 วัน	7 วัน	15 วัน
Internet Link 2 Link และ Backup Link	Data Center/ UniNet / 3BB			✓				
DNS /DHCP Server	Data Center			✓				
Firewall	Data Center			✓				
Core Switch	Data Center/ DR Site			✓				
ระบบ AD (Active Directory)	Data Center			✓				
E-Mail/ Intranet	Microsoft Cloud			✓				
Physical Server	Data Center			✓				
ระบบ VPN Virtual Private Network	Data Center/ DR			✓				

ประเภททรัพยากร	แหล่งข้อมูล	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ						
		1 ชั่วโมง	4 ชั่วโมง	8 ชั่วโมง	1 วัน	3 วัน	7 วัน	15 วัน
ระบบห้อง Data Center, AirInRow ระบบไฟฟ้า การสำรองไฟฟ้า Generator ที่เกี่ยวข้องระบบ	Data Center		✓					
ระบบรักษาความปลอดภัยห้อง Data Center	Data Center		✓					
Wi-Fi สถาบัน	Data Center			✓				
CCTV	Data Center			✓				

16. จำนวนบุคลากรหลักที่จำเป็น

ประเภททรัพยากร	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ						
	1 ชั่วโมง	4 ชั่วโมง	8 ชั่วโมง	1 วัน	3 วัน	7 วัน	15 วัน
หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	1	1	1	1	1	1	1
ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	1	1	1	1	1	1	1
หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	1	1	1	1	1	1	1
กลุ่มงานพัฒนาและจัดหาระบบสารสนเทศ	1	1	2	2	2	2	2
กลุ่มงานระบบเครือข่ายสารสนเทศ	1	1	1	1	1	1	1
กลุ่มงานซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	1	1	1	1	1	1	1
รวม	6	6	7	7	7	7	7

หมายเหตุ : ในกรณีที่ระบบเครือข่ายหลักและสำรองไม่สามารถให้บริการได้ภายในระยะเวลาที่กำหนด ให้จัดหาอุปกรณ์เชื่อมโยงระบบเครือข่ายต่อผ่านอินเทอร์เน็ตของผู้ให้บริการโทรศัพท์มือถือ โดยวิธีแชร์สัญาณ Wifi จากมือถือ หรือทำมือถือเป็น Wifi Hotspot เชื่อมโยงการบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยเทคโนโลยีสารสนเทศ

17. กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

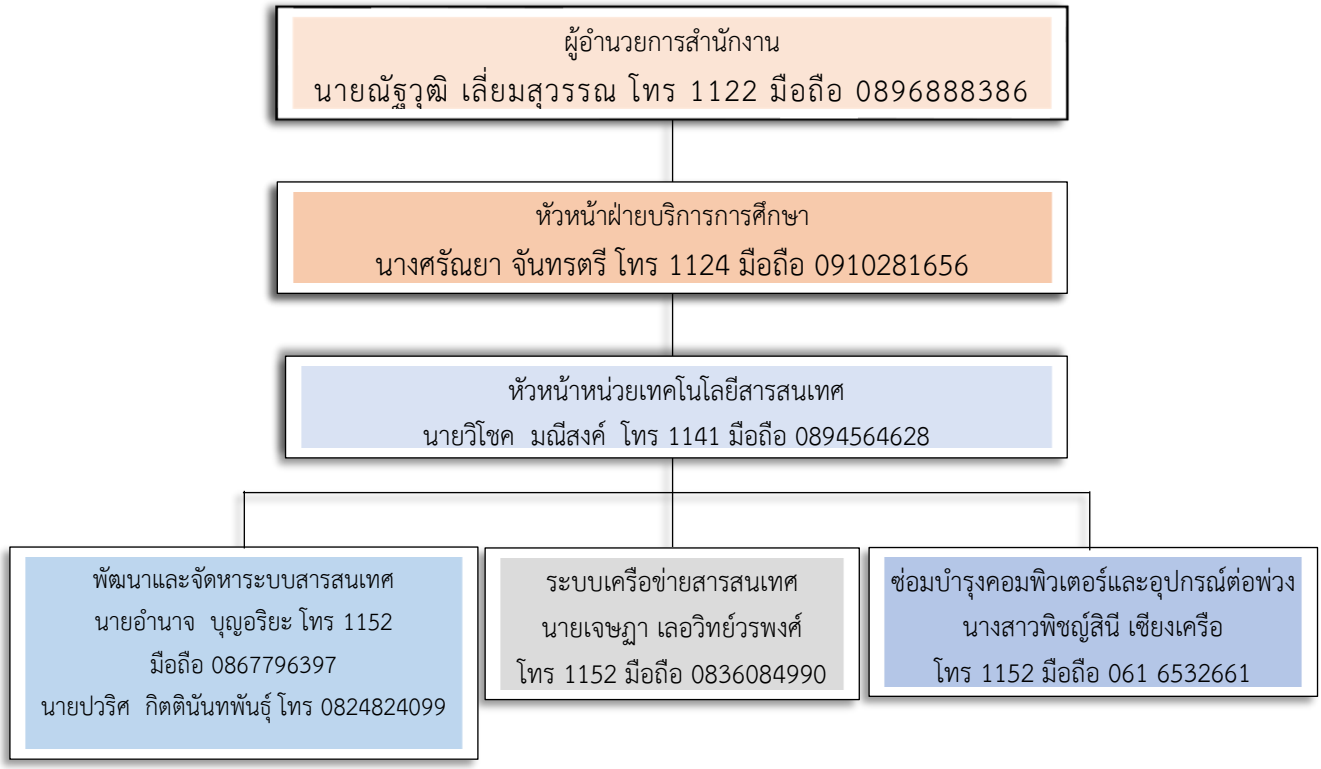
กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับผังรายชื่อทางโทรศัพท์ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อบุคลากร ภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของหน่วยเทคโนโลยีสารสนเทศ

จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ แจ้งผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยผู้ประสานงานฯ จะแจ้งให้หัวหน้าทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

จากนั้นหัวหน้าทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ จะดำเนินการติดต่อและแจ้งไปยังทีมงานของตน ตลอดจนบุคลากรภายใต้การบังคับบัญชาตามสายงานบังคับบัญชา เพื่อรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ของหน่วยเทคโนโลยีสารสนเทศ ที่ได้รับผลกระทบตามรายชื่อและช่องทางติดต่อสื่อสาร ที่ได้ระบุไว้ในหัวข้อที่ 8 ประกอบด้วย หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

กรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณาดังนี้

1. ถ้าเหตุการณ์เกิดขึ้นในเวลาทำการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก
2. ถ้าเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
3. ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบ ดังต่อไปนี้
   - 3.1 สรุปสถานที่การณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนบริหารความต่อเนื่อง
   - 3.2 เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับผู้บริหารของหน่วยงานและทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
   - 3.3 ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศต่อไป เช่น สถานที่ที่รวมพลในกรณีที่มีการย้ายสถานที่ที่ทำการไปยังสถานที่สำรอง อาคารเฉลิมพระเกียรติฯ ชั้น 10



รูปภาพแผนผังโครงสร้าง Call Tree ของหน่วยเทคโนโลยีสารสนเทศ

18. กระบวนการแจ้งเหตุ Call Tree

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เพื่อรวบรวมสรุปความพร้อมของหน่วยเทคโนโลยีสารสนเทศ ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยเทคโนโลยีสารสนเทศและเจ้าหน้าที่ทั้งหมด

ทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อพนักงานภายในหน่วยสามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงในระยะเวลาที่คาดหวังในกรณีที่เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ


ขั้นตอนการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
เมื่อเกิดเหตุฉุกเฉิน
1
2
ทีมอาคาร/สถานที่ปฏิบัติงานหลัก เข้าระงับเหตุ ประสานกับ ผู้ที่เกี่ยวข้อง
3
หัวหน้าคณะบริหารฯ เรียกประชุม คณะบริหารความต่อเนื่องด้าน เทคโนโลยีสารสนเทศ ผ่าน Call Tree
4
คณะบริหารความต่อเนื่อง ด้านเทคโนโลยีสารสนเทศ ประเมินสถานการณ์
5
ทีมต่างๆ ที่เกี่ยวข้องดำเนินการเพื่อ จัดการเหตุโดยครอบคลุม
ทีมพัฒนาและจัดหาระบบ
ทีมระบบเครือข่ายสารสนเทศ
ตรวจสอบจำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บและเสียชีวิต
ทีมซ่อมบำรุงเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง
สนับสนุนด้านอุปกรณ์จัดการอุปกรณ์
6
คณะบริหารความต่อเนื่องด้าน เทคโนโลยีสารสนเทศ พิจารณา ประกาศภาวะวิกฤตและสั่งการย้าย
7
ทีมต่างๆ ที่เกี่ยวข้องดำเนินการเพื่อ เตรียมการย้ายไปปฏิบัติงานที่ศูนย์
8
บุคลากรหลัก/บุคลากรสำรอง ดำเนินการ ตามแผนบริหารความ ต่อเนื่อง โดยปฏิบัติกระบวนงาน สำคัญ และรายงานต่อ หัวหน้าทีม
9
แจ้งสรุปเหตุการณ์และขั้นตอนการดำเนินการให้กับ บุคลากรในหน่วยงาน เพื่อรับทราบและดำเนินการ อาทิ แจ้งวัน เวลาในการปฏิบัติงานที่ศูนย์ปฏิบัติการ
แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)
ด้านเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

19. Checklist ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ ระยะสั้น ระยะกลาง ระยะยาว

ในการปฏิบัติการใด ๆ ให้บุคลากรของหน่วยเทคโนโลยีสารสนเทศ คำนึงถึงความปลอดภัยในชีวิตของตนเอง รวมทั้งบุคลากรอื่น ๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติที่หน่วยกำหนดขึ้นอย่างเคร่งครัด

19.1 วันที่ 1 (ภายใน 24 ชั่วโมง: รวมทั้งรายงานสรุปที่ได้ดำเนินการไปตาม SLA ภายใน 4 ชั่วโมง)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
1. แจ้งเหตุฉุกเฉิน วิกฤติ ตามกระบวนการ Call Tree ภายหลังได้รับแจ้งจากหัวหน้าทีมคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศของหน่วยเทคโนโลยีสารสนเทศ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
2. จัดประชุม หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เพื่อประเมินความเสียหาย ผลกระทบต่อการดำเนิน งานการให้บริการและทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ 2.1 ทบทวนกระบวนงานที่มีความเร่งด่วน หรือส่งผลกระทบอย่างสูงหากไม่ได้ดำเนินการเพื่อพิจารณาสิ่งที่ต้องดำเนินงานหรือปฏิบัติงานแบบ Manual (Manual Processing)	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
3. ระบุและสรุปรายชื่อบุคลากรในหน่วยเทคโนโลยีสารสนเทศ ที่ได้รับบาดเจ็บหรือเสียชีวิต	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
4. รายงานผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศทราบ โดยครอบคลุมประเด็นดังนี้ 4.1 จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ / เสียชีวิต 4.2 ความเสียหายและผลกระทบต่อการดำเนินงานและการให้บริการ 4.3 ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ 4.4 กระบวนงานที่มีความเร่งด่วนและส่งผลกระทบอย่างสูงหากไม่ดำเนิน การและจำเป็นต้องดำเนินงานหรือปฏิบัติแบบ Manual	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
5. สื่อสาร รายงานสถานการณ์แก่บุคลากรในหน่วยเทคโนโลยีสารสนเทศ ตามเนื้อหาและข้อความที่ได้รับการพิจารณาและเห็นชอบจาก หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
6. ประเมินและระบุกระบวนการหลักและงานเร่งด่วนที่จำเป็นต้องดำเนินการให้แล้วเสร็จภายใน 1-5 วัน	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
7. ประเมินศักยภาพและความสามารถของหน่วยเทคโนโลยีสารสนเทศ ในการดำเนินงานเร่งด่วน ข้างต้นภายใต้ข้อจำกัดและสภาวะวิกฤต พร้อมระบุทรัพยากรจำเป็นต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ตามแผนการจัดหาทรัพยากร	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
8. รายงานความคืบหน้าให้แก่ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศเพื่อทราบ	หัวหน้าทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
9. ติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ได้แก่ 9.1 สถานที่ที่ปฏิบัติงานสำรอง 9.2 วัสดุอุปกรณ์ที่สำคัญ 9.3 เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ 9.4 บุคลากรหลัก 9.5 คู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
10. ประเมินและวิเคราะห์สถานการณ์และดำเนินการให้เกิดการใช้งานระบบอย่างต่อเนื่องในสิ่งที่สำคัญจำเป็นเร่งด่วน ในส่วนของงานด้านระบบคอมพิวเตอร์และเครือข่าย (Internet / Network and Computer System) ที่หน่วยเทคโนโลยีสารสนเทศดูแลในปัจจุบัน 10.1 รวมทั้งวิเคราะห์ ประเมินและดำเนินการในส่วนที่ต้องกู้คืนระบบตามแผนการกู้คืนระบบ (DRP: Disaster Recovery Plan)	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
11. พิจารณาดำเนินการหรือปฏิบัติงานแบบ Manual เฉพาะงานเร่งด่วน หากไม่ดำเนิน การจะส่งผลกระทบอย่างสูงและไม่สามารถรอได้ ทั้งนี้ต้องได้รับการอนุมัติ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
12. ระบุหน่วยงานที่เป็นคู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการเร่งด่วน เพื่อแจ้งสถานการณ์และแนว ทางในการบริหารงานให้มีความต่อเนื่องตามความเห็นของคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
13. บันทึก (Log Book) และทบทวนกิจกรรมและงานต่างๆที่ทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการ (พร้อมระบุรายละเอียดผู้ดำเนินการและเวลา) อย่างสม่ำเสมอ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและผู้รับผิดชอบส่วนงาน	☐	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
14. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการสำหรับวันถัดไป ให้กับบุคลากรหลัก เพื่อรับทราบและดำเนินการ อาทิ แจ้งวัน เวลาและสถานที่ที่ปฏิบัติงานสำรอง	หัวหน้าทีมงานบริหารความต่อเนื่อง	☐	
15. รายงานความคืบหน้าให้แก่ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอหรือตามที่กำหนดไว้	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

19.2 วันที่ 2 ถึงวันที่ 7 (รวมรายงานสรุปที่ได้ดำเนินการไปตาม SLA ภายใน 4 ชั่วโมงของวันที่ 2 - 7)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
1. ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
2. ตรวจสอบประเมิน ความพร้อมและข้อจำกัดในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ได้แก่ 2.1 สถานที่ที่ปฏิบัติงานสำรอง 2.2 วัสดุอุปกรณ์ที่สำคัญ 2.3 เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ 2.4 บุคลากรหลัก 2.5 คู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
3. รายงานผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ถึงความพร้อม ข้อจำกัดและข้อเสนอแนะในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
4. ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ได้แก่ 4.1 สถานที่ที่ปฏิบัติงานสำรอง 4.2 วัสดุอุปกรณ์ที่สำคัญ 4.3 เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ 4.4 บุคลากรหลัก 4.5 คู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
5. ติดตามสถานะ / ประเมินและวิเคราะห์สถานที่การณ์และดำเนินการให้เกิดการใช้งานระบบอย่างต่อเนื่องในสิ่งที่สำคัญจำเป็นเร่งด่วน ในส่วนของงานด้านระบบคอมพิวเตอร์และเครือข่าย (Internet / Network and Computer System) ที่หน่วยเทคโนโลยีสารสนเทศ ดูแลในปัจจุบัน 5.1 รวมทั้งวิเคราะห์ ประเมินและดำเนินการในส่วนที่ต้องตามแผนกู้คืนระบบเทคโนโลยีสารสนเทศ IT (DRP: Disaster Recovery Plan) (ถ้ามี)	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและผู้รับผิดชอบส่วนงาน	☐	
6. ดำเนินการกอบกู้และจัดหาข้อมูลและรายงานต่าง ๆ ที่จำเป็นต้องใช้ในการดำเนินงานและให้บริการ ตามตารางในหัวข้อที่15 ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูลที่หน่วยเทคโนโลยีสารสนเทศต้องใช้ดำเนินการ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
7. ดำเนินการและให้บริการภายใต้ทรัพยากรที่จัดหาเพื่อบริหารความต่อเนื่อง 7.1 สถานที่ที่ปฏิบัติงานสำรอง 7.2 วัสดุอุปกรณ์ที่สำคัญ 7.3 เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ 7.4 บุคลากรหลัก คู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
8. แจ้งสถานการณ์และแนวทางในการบริหารความต่อเนื่องกับคู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและผู้รับผิดชอบส่วนงาน		
9. บันทึก (Log Book) และทบทวนกิจกรรมและงานต่าง ๆ ที่ทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ของส่วนงาน (พร้อมระบุรายละเอียด ผู้ดำเนินการและเวลาอย่างสม่ำเสมอ)	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
10. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการต่อไปสำหรับในวันถัดไปให้กับบุคลากรในส่วนงาน	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
11. รายงานความคืบหน้าให้แก่ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศตามเวลาที่ได้กำหนดไว้	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

19.3 วันที่ 8 ถึงวันที่ 15 ในช่วงการตอบสนอง (รวมรายงานสรุปที่ได้ดำเนินการไปตาม SLA ภายใน 4 ชั่วโมงของวันที่ 8 ถึง วันที่ 15 ในช่วงการตอบสนอง)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
1. ติดตามสถานที่ะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและผู้รับผิดชอบส่วนงาน	☐	
2. ระบุทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนิน งานและให้บริการตามปกติ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและผู้รับผิดชอบส่วนงาน	☐	
3. รายงานผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบและทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
4. ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ 4.1 สถานที่ที่ปฏิบัติงานสำรอง 4.2 วัสดุอุปกรณ์ที่สำคัญ 4.3 เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ 4.4 บุคลากรหลัก 4.5 คู่ค้า/ผู้ที่หน่วยเทคโนโลยีสารสนเทศ ให้และรับบริการ/ผู้มีส่วนได้ส่วนเสีย 4. 6 ด้านการทำสัญญางบประมาณ การเงินบัญชี บุคลากร พัสดุ จัดซื้อจัดจ้าง	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
5. ติดตามสถานนะ / ประเมินและวิเคราะห์สถานที่การณ์และดำเนินการให้เกิดการใช้งานระบบอย่างต่อเนื่องในสิ่งที่สำคัญจำเป็นเร่งด่วน ในส่วนของงานด้านระบบคอมพิวเตอร์และเครือข่าย (Internet /Network and Computer System) ที่หน่วยเทคโนโลยีสารสนเทศ ดูแลในปัจจุบัน 5.1 รวมทั้งวิเคราะห์ ประเมินและดำเนินการในส่วนที่ต้องกู้คืนระบบตามแผนการกู้คืนระบบ (DRP : Disaster Recovery Plan) (ถ้ามี) 5.2 วิเคราะห์ประเมิน ด้านการ MA : Maintenance ระบบคอมพิวเตอร์และเครือข่าย Internet / Computer and Network System รวมทั้งสัญญาต่างๆ ที่เกี่ยวข้อง	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
6. แจ้งสรุปสถานที่การณ์และการเตรียมความพร้อมด้านทรัพยากรต่างๆ เพื่อดำเนินงานและให้บริการตามปกติ ให้กับบุคลากรในหน่วยเทคโนโลยีสารสนเทศ	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	
7. บันทึก (Log Book) และทบทวนกิจกรรมและงานต่างๆ ที่ทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ส่วนงาน (พร้อมระบุรายละเอียดผู้ดำเนินการและเวลาอย่างสม่ำเสมอ)	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบส่วนงาน	☐	
8. รายงานความคืบหน้าให้แก่ผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศตามเวลาที่ได้กำหนดไว้	หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	☐	

19.4 ตารางกำหนดการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

ลำดับ	การทดสอบ (Exercises)	ประเภทการทดสอบ	กำหนดวันเวลาในการทดสอบ	ผลการทดสอบ
1.	ความเสียหายที่เกิดกับสถานที่ที่ทำงาน (รวมถึงเอกสารข้อ มูลสำคัญ)	1. แบบบันทึกการขอเข้าใช้สถานที่ที่ปฏิบัติงานสำรองชั่วคราว 2. การทดสอบความพร้อมของสถานที่ที่ปฏิบัติงานสำรองชั่วคราว	กรกฎาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน
2.	คอมพิวเตอร์และอุปกรณ์ต่างๆ ที่จำเป็นต้องใช้	มีเอกสารจำนวนทรัพยากรที่ต้องใช้และวิธีการจัดหาให้ได้มาซึ่งวัสดุอุปกรณ์ที่จำเป็น	สิงหาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน
3.	ความสูญเสียบุคลากรสำคัญ	มีเอกสารรายชื่อการติดต่อบุคลากรหลักและบุคลากรสำรองของกระบวนงานหลักที่สำคัญ	กรกฎาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน
4.	ความขัดข้องของระบบเทคโนโลยีสารสนเทศ IT / Network /ข้อมูลสำคัญ	การทดสอบแผนรองรับการดำเนินการปฏิบัติงานต่อเนื่อง	สิงหาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน
5.	ผู้ให้บริการไม่สามารถให้บริการกับหน่วยเทคโนโลยีสารสนเทศ ได้	คู่มือการทดสอบใช้งานระบบสำรองและการ Link ระบบและข้อมูลต่างๆ	กรกฎาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน
6.	กรณีที่หน่วยเทคโนโลยีสารสนเทศไม่สามารถให้บริการกู้คืนระบบได้	คู่มือการกู้คืนระบบเทคโนโลยีสารสนเทศ IT ระบบแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (DRP)	พฤษภาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน

ลำดับ	การทดสอบ (Exercises)	ประเภทการทดสอบ	กำหนดวันเวลาในการทดสอบ	ผลการทดสอบ
7.	สิ่งที่ต้องใช้เมื่อเกิดเหตุการณ์วิกฤต	1. แผน BCP 2. Call Tree 3. รายชื่อผู้ให้/รับบริการของหน่วยเทคโนโลยีสารสนเทศพร้อมช่องทางติดต่อสื่อสารของแต่ละหน่วยงาน 4. เอกสารยืนยันการอนุมัติให้ใช้อาคารสถานที่ที่ปฏิบัติงานชั่วคราว	พฤษภาคม 2565	☐ ผ่าน ☐ ไม่ผ่าน

20. แผนการสื่อสารของหน่วยงาน

ในช่วงเวลาที่เกิดเหตุการณ์ความเสียหายเกิดขึ้น สิ่งสำคัญสำหรับหน่วยเทคโนโลยีสารสนเทศ คือการสื่อสารข้อความสำคัญ (Key Messages) ให้ผู้บริการ/ผู้ใช้บริการของตนทราบอย่างรวดเร็วและมีประสิทธิผล เพื่อให้ผู้ให้บริการและผู้รับบริการเหล่านั้นได้รับทราบถึงสถานที่การณ์และข้อชี้แนะพิเศษในการดำเนินการ จึงจำเป็นต้องมีแผนการสื่อสารของหน่วยงานเตรียมการไว้ล่วงหน้า

แผนการสื่อสารของหน่วยเทคโนโลยีสารสนเทศ ควรประกอบด้วย แผนการสื่อสารที่จะดำเนินการและข้อความที่มีการร่างไว้ล่วงหน้า รวมถึงคำถามที่พบบ่อย ภายใต้สถานที่การณ์เหตุการณ์ความเสียหายที่แตกต่างกัน ดังนั้น เมื่อมีการประกาศใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Management :BCP) ให้ปฏิบัติดังนี้

1. เจ้าหน้าที่ที่ประจำอยู่ที่สถานที่ที่ทำงานหลัก (Primary Site) จะต้องนำป้ายประกาศติดไว้ใกล้สถานที่ที่ทำการเดิมเพื่อให้ผู้มาติดต่อรับทราบถึงที่ทำการชั่วคราว

ตัวอย่างเนื้อความของป้ายประกาศ

จากวันที่ ..... หน่วยเทคโนโลยีสารสนเทศ สถาบัน ได้ย้ายที่ทำการเป็นการชั่วคราวไปที่
เลขที่ ..... อาคาร ..... ถนน ..... หมายเลขโทรศัพท์ .....
หมายเลขโทรสาร .....

2. ผู้ประสานงาน BCP นำแบบฟอร์มหนังสือขออนุญาตเข้าปฏิบัติงาน ณ อาคารสถานที่ที่ปฏิบัติงานสำรองชั่วคราว (ที่ได้จัดทำและเก็บไว้) มากรอกด้วยลายมือ และลงลายมือชื่อเจ้าหน้าที่บริหารฝ่ายเพื่อดำเนินการนำไปยังอาคารสถานที่ที่ปฏิบัติงานสำรองชั่วคราว (เนื่องด้วยเวลาเกิดเหตุอาจไม่มีระบบจัดพิมพ์หนังสือ หนังสือขออนุญาตเข้าปฏิบัติงานจึงควรจัดทำไว้ล่วงหน้า และจัดเก็บ 1 ชุดที่บ้านของผู้ประสานงาน BCP กรณีเหตุการณ์เกิดหลังเวลาทำการ)

3. เมื่อไปถึงอาคารสถานที่ที่ปฏิบัติงานสำรองชั่วคราว นำแบบฟอร์มจดหมายและแจ้งหน่วยงานส่วนกลางการสั่งย้ายสถานที่ที่ปฏิบัติงาน จัดส่งโทรสารให้กับหน่วยงานส่วนกลางเพื่อแจ้งแก่หน่วยงานภายในสถาบัน

4. ผู้ประสานงาน BCP จัดทำหนังสือติดต่อคู่ค้า หน่วยงานที่หน่วยเทคโนโลยีสารสนเทศ ให้/รับบริการให้ทราบการเปลี่ยนแปลงสถานที่ที่ปฏิบัติงาน หากเครื่องคอมพิวเตอร์และเครื่องโทรสารยังไม่สามารถใช้งานได้ ระหว่างนั้นอาจจะแจ้งทางโทรศัพท์ก่อน

5. ณ อาคารสถานที่ที่ปฏิบัติงานสำรองชั่วคราว ผู้ประสานงาน BCP จัดทำประกาศแจ้งให้ทราบว่า มีบริการใดบ้างที่ยังให้บริการอยู่และระบบใดใช้การได้ ระบบใดยังใช้การไม่ได้ อาจมีความล่าช้าหรือต้องรอคอยเป็นเวลาเท่าไร

6. จัดให้มีการตอบรับโทรศัพท์แจ้งการย้ายสถานที่และบริการ ที่ยังให้บริการอยู่หรือบริการใดสามารถใช้ได้ ณ สถานที่ใดทดแทนได้แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ

ภาคผนวก

คำสั่งแต่งตั้งคณะกรรมการจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

คำสั่งสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

ที่ 22 /2565

เรื่อง แต่งตั้งคณะกรรมการจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

เพื่อให้สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย มีแผนบริหารความต่อเนื่อง Business Continuity Plan : BCP ด้านเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้น และให้สถาบันสามารถปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร ได้อย่างมีประสิทธิภาพ ไม่ส่งผลกระทบต่อการดำเนินงานของสถาบัน จึงขอแต่งตั้งผู้มีรายนามและตำแหน่งต่อไปนี้ เป็นคณะกรรมการจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย ดังนี้

1. **ที่ปรึกษา**
   1.1 นายสุรเชษฐ์ เชื้อทอง
   รองผู้อำนวยการสำนักงานตรวจสอบ
   1.2 รองอธิการบดีฝ่ายยุทธศาสตร์และประกันคุณภาพ

2. **รายนามคณะกรรมการ**

2.1 ผู้อำนวยการสำนักงานสถาบัน	ประธานกรรมการ
2.2 นายชนะชัย ลัดกรูด เจ้าหน้าที่ระบบงานคอมพิวเตอร์ 7	กรรมการ
2.3 หัวหน้าฝ่ายบริการการศึกษา	กรรมการ
2.4 หัวหน้าฝ่ายยุทธศาสตร์และประกันคุณภาพการศึกษา	กรรมการ
2.5 หัวหน้าฝ่ายวิจัยและบริการวิชาการ	กรรมการ
2.6 หัวหน้าฝ่ายบริหารวิชาการ	กรรมการ
2.7 นายอำนาจ บุญอริยะ	กรรมการ
2.8 นายเจษฎา เลอวิหย์วรพงศ์	กรรมการ
2.9 นายปวริศ กิตตินันทพันธุ์	กรรมการ
2.11 หัวหน้าหน่วยเทคโนโลยีสารสนเทศ	กรรมการและเลขานุการ
2.12 นางสาวพิชญ์สินี เชียงเครือ	กรรมการและผู้ช่วยเลขานุการ

3. **ภารกิจ**
   3.1 จัดทำแผนการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศของสถาบัน
   3.2 ให้ข้อเสนอแนะแก่สถาบัน และปฏิบัติหน้าที่อื่นตามที่ได้รับมอบหมาย

สั่ง ณ วันที่ 25 เดือน มกราคม พ.ศ. 2565

(ผู้ช่วยศาสตราจารย์ ดร.วรุณยุพา รอยกุลเจริญ)
อธิการบดีสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ

IT Disaster Recovery Plan -(IT-DRP)

บทนำ

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ IT Disaster Recovery Plan -(IT-DRP) ฉบับนี้จัดทำขึ้นเพื่อให้หน่วยเทคโนโลยีสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย สามารถนำไปใช้ในการปฏิบัติงานในสภาวะวิกฤติ เช่น การเกิดอัคคีภัย การเกิดอุทกภัย การก่อการร้าย ประท้วง จลาจล ที่จะส่งผลให้ระบบสารสนเทศที่ใช้ปฏิบัติงานหลัก ไม่สามารถให้บริการได้ โดยแผนกู้คืนระบบสาระสนเทศ ได้แนวทางการวิเคราะห์ความสำคัญของกระบวนการในภารกิจที่มีระบบสารสนเทศที่ใช้งานเป็นหลัก ซึ่งเมื่อมีการหยุดชะงักจะก่อให้เกิดผลกระทบต่อภาระหน้าที่ และฐานข้อมูลหลักของสถาบัน เช่น ระบบฐานข้อมูลเพื่อรองรับอนาคต ระบบสารสนเทศเพื่อการตัดสินใจ BI และระบบต่าง ๆ ของสถาบันมาจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสามารถกลับมาดำเนินการได้ตามปกติหรือให้บริการได้ในสภาวะฉุกเฉินในระยะเวลาที่เหมาะสม ลดความความรุนแรงของ เหตุการที่เกิดขึ้นได้

วัตถุประสงค์

1. จัดทำแผนกู้คืนระบบสาระสนเทศเพื่อนำไปปฏิบัติใช้เมื่อเกิดเหตุการณ์ภัยภิบัติที่อาจส่งผลกระทบต่อการปฏิบัติงานภายในสถาบัน

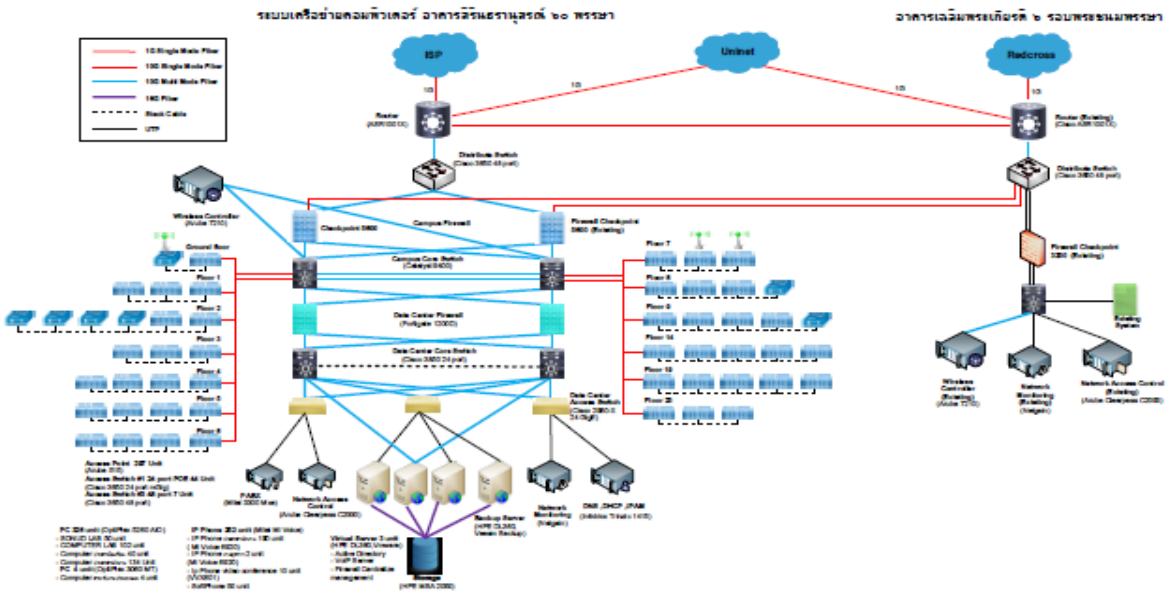
2. เพื่อให้เจ้าหน้าที่หน่วยเทคโนโลยีสารสนเทศหรือผู้ที่เกี่ยวข้องทราบขั้นตอนการรับมือ

3. เพื่อลดผลกระทบจากการหยุดชะงักในการให้บริการ

4. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของสถาบันให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

ขอบเขต

แผนกู้คืนระบบสาระสนเทศ จะถูกนำมาใช้เมื่อมีการประสบเหตุการภัยพิบัติที่เกิดขึ้น เช่น อาคารสำนักงาน/หน่วยเทคโนโลยีสารสนเทศ ได้รับความเสียหาย ไฟไหม้ น้ำท่วม การก่อการประท้วง/จลาจล จนระบบหยุดชะงักไม่สามารถใช้งานได้



ผังโครงสร้างระบบเครือข่ายสถาบันการพยาบาลศรีสวินทิรา สภากาชาดไทย

1. Application Server และฐานข้อมูลภายในสถาบันประกอบไปด้วยระบบต่าง ๆ ที่ใช้งาน ระบบสำคัญหลัก คือ ระบบทะเบียนนักศึกษา ระบบทรัพยากรบุคคล ระบบสารสนเทศเพื่อการตัดสินใจ BI ระบบ E-Learning ระบบ MIS ระบบจองห้องประชุม และระบบบันทึกเวลาทำงาน

2. ระบบเครือข่ายและอินเตอร์เน็ต สำหรับเชื่อมต่อกับภายนอกและอาคารต่าง ๆ โดยผ่านไฟร์วอลล์เพื่อป้องกันการบุกรุก

3. หน่วยงานที่เกี่ยวข้องหรือใช้งานระบบสารสนเทศหลัก จะประกอบไปด้วย สาขาวิชา ฝ่ายบริหารงานทั่วไป ฝ่ายพัฒนานักศึกษา ฝ่ายบริการการศึกษา ฝ่ายวิจัยและบริการวิชาการ ฝ่ายบริหารวิชาการ ฝ่ายการคลังและทรัพย์สิน และฝ่ายยุทธศาสตร์และประกันคุณภาพการศึกษา

ลำดับความสำคัญของกระบวนการหลักและเป้าหมายการทำงาน

กระบวนการหลักที่ต้องให้ความสำคัญและจำเป็นต้องดำเนินให้บริการได้ และเป้าหมายระยะเวลาสูงสุดที่ยอมรับ ได้ในการยอมให้คอมพิวเตอร์ ระบบเครือข่าย หรือ แอปพลิเคชันหยุดทำงานได้ หลังเกิดเหตุขัดข้อง คือ 2 วัน และปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้คือ 1 วัน

กระบวนการหลัก	รายละเอียด	ระดับความสำคัญ	Recovery Time Objective(RTO) (Day)	Recovery Point Objective(RPO) (Day)
ระบบเครือข่ายคอมพิวเตอร์	ระบบเครือข่ายคอมพิวเตอร์ภายในสถาบัน	1	90	1
ระบบทะเบียนนักศึกษา	ข้อมูลนักศึกษาทั้งหมด การลงทะเบียน ผลการศึกษา	2	1	2
ระบบบริหารงานบุคคล	ข้อมูลบุคลากร ประวัติบุคลากร รายได้ ภาษี	3	1	2
ระบบสารสนเทศเพื่อการตัดสินใจ BI	ข้อมูลเพื่อการตัดสินใจของผู้บริหารสถาบัน	4	1	2
ระบบ E-Learning	ข้อมูลการเรียนการสอนแต่ละรายวิชา	5	1	2
ระบบเว็บไซต์สถาบัน	ข้อมูลเว็บไซต์สถาบัน	6	1	2
ระบบ EMIS	ระบบสารสนเทศเพื่อการจัดการ	7	1	2

กระบวนการดำเนินการแผนกู้คืนระบบเทคโนโลยีสารสนเทศ

1. เจ้าหน้าที่ที่เกี่ยวข้องกับการกู้คืนระบบเทคโนโลยีสารสนเทศที่ทำหน้าที่ประสานงาน หรือปฏิบัติงานในส่วนงานที่เกี่ยวข้องโดยมีหน้าที่ดังต่อไปนี้

- กำหนดแนวทางแผนการกู้คืนระบบ
- บริหารจัดการเกี่ยวกับการแจ้งเตือน และสั่งการไปยังบุคคลากรที่เกี่ยวข้อง รวมทั้ง Third Party เกี่ยวกับภัยพิบัติที่เกิดขึ้น
- กำหนดอุปกรณ์ทั้งฮาร์ดแวร์และซอฟต์แวร์ เน็ตเวิร์คต่างๆ ที่มีความจำเป็นในการกู้คืน
- กำหนดขั้นตอนการตั้งค่าคอนฟิคต่างๆ
- ทดสอบระบบการใช้งาน

รายชื่อผู้รับผิดชอบการกู้คืนระบบ Call Tree การแจ้งเหตุฉุกเฉินให้กับสมาชิกในทีมงานให้รับทราบ หลังจากมีการเฝ้าระวังเหตุฉุกเฉินหรือเกิดเหตุฉุกฉิน ทั้งนี้ให้หัวหน้าหน่วยเทคโนโลยีสารสนเทศ แจ้งให้ผู้ประสานงานระบบต่างๆ ทราบและดำเนินการตามแผนกู้คืนระบบ

ชื่อ/บริษัท	รายละเอียด/หน้าที่รับผิดชอบ	หมายเลขติดต่อ
นาย วิโชค มณีสงค์ หัวหน้าหน่วยเทคโนโลยีสารสนเทศ	- ประสานงานระบบบริหารงานบุคคล	089-456-4628
นายอำนาจ บุญอริยะ	- ประสานงานระบบทะเบียนนักศึกษา - ระบบระบบสารสนเทศเพื่อการตัดสินใจ BI - ระบบ EMIS	086-779-6397
นายเจษฎา เลอวิทย์วรพงศ์	- ประสานงานระบบเครือข่ายคอมพิวเตอร์ - ประสานงานระบบการเงินและบัญชีพัสดุ - ประสานระบบ E-Learning	083-608-4990
นายปวริศ กิตตินันทพันธุ์	- ประสานงานระบบเว็บไซต์สถาบัน - ประสานงานการใช้งาน Soft ware ลิขสิทธ์	082-482-4099
นางสาวพิชญ์สินี เชียงเครือ	- ซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ต่อพ่วง - ประสานงานการเช่าใช้เครื่องพิมพ์สี-ขาวดำ	090-963-7680
หน่วยงานภายนอก		
สำนักเทคโนโลยีสารสนเทศและดิจิทัล สภากาชาดไทย	ผู้ให้บริการเชื่อมต่อระบบเครือข่าย	061-401-2683
บริษัท ซีดีจี ซิสเต็มส์ จำกัด	ผู้ให้บริการระบบ EMIS	081-647-1005
บริษัท NCC Networks (Thailand) Co.,Ltd	ผู้ให้บริการระบบทะเบียนนักศึกษา ระบบบริหารงานบุคล	090-1619166
บริษัทอินโพลิส	ผู้ให้บริการระบบสารสนเทศเพื่อการตัดสินใจ BI	061-561-4287
บริษัท Technology Infrastructure	ผู้ให้บริการเครือข่ายคอมพิวเตอร์ อาคารสิรินธรานุสรณ์ ๖๐ พรรษา	081-497-1329
บริษัท M 2 M	ผู้ให้บริการเครือข่ายคอมพิวเตอร์ อาคารเฉลิมพระเกียรติฯ	083-299-2058
บริษัท ด๊ับเบิ้ล เอ ดิจิตอล ซินเนอร์จี กำกัด	ให้บริการเครื่องพิมพ์ สี ขาวดำ	085-8352346
บริษัทฟูจิตสึ (ประเทศไทย)จำกัด	ผู้ให้บริการระบบป้องไวรัสคอมพิวเตอร์	086-334-7213

ชื่อ/บริษัท	รายละเอียด/หน้าที่รับผิดชอบ	หมายเลขติดต่อ
บริษัท เอซอฟท์วัน จำกัด	ผู้ให้บริการ Soft ware ลิขสิทธ์	086-334-7213
บริษัท ซีนิธคอมพ์ จำกัด	ผู้ให้บริการเครือข่ายไร้สาย	089-811-5589
บริษัท อิเล็กทรอนิก คอมเมิร์ซ จำกัด	ผู้ให้บริการ Server และจดทะเบียนโดเมนเน็ม Stin.ac.th	097-297-0150

2. สถานที่ใช้ในการกู้คืนระบบเทคโนโลยีสารสนเทศ (DR-Site) กำหนดให้ใช้พื้นที่ความเหมาะสมการเตรียมความพร้อมล่วงหน้า ผ่านระบบ Cloud ของสถาบันที่เช่าใช้

3. การสรรหาอุปกรณ์ที่สำคัญ คือ คอมพิวเตอร์แบบพกพา (Notebook) ให้โดยหาอุปกรณ์สำรองที่มีอยู่ในสถาบัน โดยมีคุณสมบัติที่สามารถใช้เชื่อมโยงต่อผ่านเข้าสู่ระบบอินเตอร์เน็ตได้

4. การเชื่อมต่อระบบอินเตอร์เน็ตสำรอง เช่น อินเตอร์เน็ตผ่านระบบมือถือ (Hotspot) โดยการใช้ Notebook เชื่อมต่อเพื่อการตั้งค่า Config ระบบ DR-site หรือ Upload ฐานข้อมูลเพื่อใช้ในการ Start DR site

เกณฑ์การประเมินระดับเหตุการณ์

ระดับเหตุการณ์	คำอธิบาย
0	เหตุการณ์ปกติและระบบสำคัญยังสามารถใช้งานได้ปกติ เช่น คอมพิวเตอร์ไม่สามารถใช้งานได้ ความผิดพลาดจากเจ้าหน้าที่ปฏิบัติงาน ผู้ใช้งานแจ้งปัญหาการใช้งาน ทำให้เกิดการหยุดชะงักเพียงเล็กน้อย
1	เกิดเหตุการณ์ไม่ปกติ เช่น ภัยจากการชุมนุมประท้วง น้ำท่วม ไฟไหม้บริเวณข้างเคียง แต่ระบบสำคัญยังใช้งานได้
2	เกิดเหตุการณ์ที่ส่งผลให้ระบบสำคัญไม่สามารถใช้งานได้เป็นระยะเวลานาน เช่น กระแสไฟฟ้าแรงสูงขัดข้อง มีเกิดการโจมตีโดยไวรัสคอมพิวเตอร์ ซึ่งต้องใช้เวลานานในการแก้ไข แต่ยังสามารถเข้าออกศูนย์คอมพิวเตอร์หลักได้
3	เกิดเหตุการที่มีความรุนแรงมากที่สุดเช่น อัคคีภัย อุทกภัย เสียหายต่อตัวอาคารหรือศูนย์คอมพิวเตอร์หลักและระบบสำคัญ เป็นเหตุให้ไม่สามารถให้บริการระบบเทคโนโลยีสารสนเทศได้เป็นเวลานาน

แนวทางการปฏิบัติการตามระดับเหตุการณ์

ระดับเหตุการณ์	0
ผลกระทบ	เหตุการณ์ปกติและระบบสำคัญยังสามารถใช้งานได้ปกติ
แนวทางปฏิบัติ	• การแจ้งซ่อมจากผู้ใช้บริการ • ดำเนินการแก้ไข • ปฏิบัติตามคู่มือปฏิบัติงานตามปกติ
ระดับเหตุการณ์	1
ผลกระทบ	เกิดเหตุการณ์ไม่ปกติ เช่น ภัยจากการชุมนุมประท้วง น้ำท่วม ไฟไหม้บริเวณข้างเคียง แต่ระบบสำคัญยังใช้งานได้
แนวทางปฏิบัติ	• แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree • ประเมินสถานการณ์เฝ้าระวัง • สำรองข้อมูลระบบสำคัญ
ระดับเหตุการณ์	2
ผลกระทบ	เกิดเหตุการณ์ที่ส่งผลให้ระบบสำคัญไม่สามารถใช้งานได้เป็นระยะเวลานาน เช่น กระแสไฟฟ้าแรงสูงขัดข้อง มีเกิดการโจมตีโดยไวรัสคอมพิวเตอร์ ซึ่งต้องใช้เวลานานในการแก้ไขแต่ยังสามารถเข้าออกศูนย์คอมพิวเตอร์หลักได้
แนวทางปฏิบัติ	• แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree • เข้าตรวจปัญหา/ประเมินผลความเสียหายและสถานการณ์ • เตรียมการตั้งค่าที่ DR Site • จัดเตรียมคอมพิวเตอร์ชั่วคราวที่สามารถเชื่อมต่ออินเตอร์เน็ตผ่านระบบมือถือได้ • ดำเนินการแก้ไข • ทำสอบการใช้งานระบบ
ระดับเหตุการณ์	3
ผลกระทบ	เกิดเหตุการที่มีความรุนแรงมากที่สุดเช่น อัคคีภัย อุทกภัย เสียหายต่อตัวอาคารหรือศูนย์คอมพิวเตอร์หลักและระบบสำคัญ เป็นเหตุให้ไม่สามารถให้บริการระบบเทคโนโลยีสารสนเทศได้เป็น เวลานาน

แนวทางปฏิบัติ	• แจ้งเหตุการณ์ต่อผู้เกี่ยวข้อง Call Tree • เข้าตรวจปัญหา/ประเมินผลความเสียหายและสถานการณ์ • จัดเตรียมคอมพิวเตอร์ชั่วคราวที่สามารถเชื่อมต่ออินเตอร์เน็ตผ่านระบบมือถือได้ • ประกาศใช้แผน IT-DPR • เปิดใช้ระบบงานสำรอง • ทดสอบการใช้งานระบบ • ประสานงานหน่วยงานต่างๆ เพื่อใช้ระบบงานสำรอง

มาตรการลดความเสี่ยงที่อาจทำให้ระบบหยุดชะงัก

ระบบสารสนเทศ	ปัจจัยเสี่ยง	มาตรการ
ระบบทะเบียนนักศึกษา ระบบบริหารงานบุคคล	• ไวรัสคอมพิวเตอร์ • การ update ระบบปฏิบัติการ/ patch • การปฏิบัติการผิดพลาดจากผู้ใช้งาน/ ผู้ดูแลระบบ	• ติดตั้งระบบป้องกันไวรัส • ตรวจสอบการตั้งค่า Firewall • สำรองฐานข้อมูล • สำรองระบบเวอร์ชั่นเก่า
อุปกรณ์แม่ข่าย (Server)	• ความเสียหายทาง Physical	• ตรวจสอบบำรุงรักษาโดยการทำ (Maintenance Service Agreement) อยู่เป็นประจำต่อเนื่อง • จัดทำ/ดูแล/ตรวจสอบความพร้อมใช้งานระบบป้องกันห้อง Data Center ให้พร้อมใช้งานและได้มาตรฐาน
ระบบเครือข่าย	• ระบบอินเตอร์เน็ตเสียหาย/ชำรุด • สายสัญญาณภายในสถาบันเสียหาย/ ชำรุด	• ติดตั้ง Link หลักเป็น และจัดหา Link สำรองผ่าน Fiber • จัดหาอุปกรณ์กระจายสัญญาณอินเตอร์เน็ตผ่านมือถือ (Hotspot) • ตั้งจุดสำรองการกระจายสัญญาณไว้ใช้ในกรณีฉุกเฉิน