



## แผนที่ 4

แผนรับมือสถานการณ์ฉุกเฉิน

ด้านระบบเทคโนโลยีสารสนเทศ

รับผิดชอบโดย : ศูนย์คอมพิวเตอร์

### 1. หลักการและเหตุผล

ศูนย์คอมพิวเตอร์ ได้กำหนดให้การบริหารความเสี่ยงเป็นกลไกหนึ่งในการบริหารงานเพื่อช่วยสนับสนุนให้การบริหารงานบรรลุตามวิสัยทัศน์ พันธกิจ เป้าหมายของมหาวิทยาลัยที่กำหนดไว้ อันนำไปสู่การบริหารงานที่มีประสิทธิภาพ การพัฒนาการแข่งขัน โดยลดความเสียหายและอยู่ในระดับที่ยอมรับได้ สามารถควบคุม ตรวจสอบ และประเมินได้อย่างเป็นระบบ เนื่องด้วย ระบบเทคโนโลยีสารสนเทศ เป็นระบบที่มีความสำคัญต่อการดำเนินงานของมหาวิทยาลัยทั้งระบบเครือข่ายคอมพิวเตอร์ ระบบสื่อสารโทรคมนาคม ระบบสารสนเทศ และระบบคอมพิวเตอร์ ฉะนั้น หากระบบสารสนเทศมีการหยุดชะงักหรือเกิดข้อผิดพลาด ย่อมก่อให้เกิดผลกระทบต่อการทำงานของปฏิบัติงานต่างๆในวงกว้าง

ศูนย์คอมพิวเตอร์ ซึ่งเป็นหน่วยงานสนับสนุนให้บริการระบบเทคโนโลยีสารสนเทศและฐานข้อมูลสำคัญของมหาวิทยาลัยจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉิน (Contingency Plan) ขึ้นเพื่อเตรียมความพร้อมต่อสถานการณ์ฉุกเฉินที่เกิดขึ้นและรุนแรงส่งผลกระทบต่อความเสียหายที่จะต้องมีการแก้ไขอย่างฉับพลัน ทันเวลา มีแนวปฏิบัติที่ชัดเจนในการบริหารความต่อเนื่องเพื่อไม่ให้เกิดการชะงักงันของการดำเนินการ

### 2. วัตถุประสงค์

- 2.1 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงานในการดูแลระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 2.2 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยวลัยลักษณ์ให้มีเสถียรภาพและมีความพร้อมใช้งาน
- 2.3 เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
- 2.4 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยวลัยลักษณ์
- 2.5 เพื่อเป็นแนวทางในการบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยวลัยลักษณ์

### 3. เหตุภัยพิบัติ สภาวะวิกฤติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมหาวิทยาลัยวลัยลักษณ์ ซึ่งสามารถจำแนกประเภทของภัยได้ดังนี้

- 3.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องคอมพิวเตอร์หลัก (Main Computer Room) ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

- 3.2 การโจรกรรมอุปกรณ์ระบบคอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- 3.3 ระบบสื่อสารของห้องศูนย์กลางข้อมูลที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง
- 3.4 กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ
- 3.5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล
- 3.6 ไวรัสคอมพิวเตอร์
- 3.7 ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

#### 4. แนวทางป้องกันและแก้ไขปัญหาความเสียหายจากภัยพิบัติ

ภัยธรรมชาติ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องคอมพิวเตอร์หลัก ได้แก่ อัคคีภัย อุทกภัย และการป้องกัน ความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

##### 4.1 การป้องกันอัคคีภัย

- 1) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน
- 2) จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากร ทุกคนอย่างน้อยปีละ 1 ครั้ง
- 3) บำรุงรักษาระบบดับเพลิงอัตโนมัติสำหรับห้องศูนย์คอมพิวเตอร์หลักเป็นประจำทุกปี

##### 4.2 การป้องกันอุทกภัย ความชื้น และอุณหภูมิที่ไม่เหมาะสม

- 1) เปิดเครื่องปรับอากาศแบบควบคุมความชื้น (Precision Air Conditioning Unit) ให้ทำงานสลับกันอย่างอัตโนมัติตลอด 24 ชั่วโมง ตรวจสอบการทำงานทุกสัปดาห์
- 2) ติดตั้งอุปกรณ์วัดอุณหภูมิและระบบแจ้งเตือนแบบอัตโนมัติเมื่อมีเหตุผิดปกติ
- 3) ตรวจสอบการรั่วซึมของฝ้าและหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำทิ้งจากระบบอากาศและน้ำฝน
- 4) บำรุงรักษาระบบปรับอากาศแบบควบคุมความชื้นเป็นประจำทุกปี

##### 4.3 การโจรกรรมอุปกรณ์ระบบคอมพิวเตอร์ในส่วนของการจัดเก็บและให้บริการข้อมูล

- 1) ควบคุมการเข้าออกห้องคอมพิวเตอร์หลัก โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป
- 2) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์เครือข่ายคอมพิวเตอร์และคอมพิวเตอร์แม่ข่าย ได้แก่ ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan)
- 3) ติดตั้งกล้องวงจรปิด
- 4) มีเวรรักษาความปลอดภัยตรวจตราเฝ้าระวังในช่วงนอกเวลาทำการ

##### 4.4 ระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

- 1) ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา
- 2) จัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้กรณีทีระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

##### 4.5 กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ



- 1) มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์และระบบคอมพิวเตอร์ที่ติดตั้งภายในห้องคอมพิวเตอร์หลัก
- 2) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลา ตรวจสอบการทำงานของระบบทุกสัปดาห์ บำรุงรักษาให้อยู่ในสภาพพร้อมใช้งาน

#### 4.6 ไวรัสคอมพิวเตอร์

- 1) ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ ใช้โปรแกรมในการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง
- 2) ระมัดระวังจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
- 3) ใช้ความระมัดระวังในการเปิดอีเมล เช่น ไม่เปิดอีเมลที่ไม่ทราบแหล่งที่มา หรือลบอีเมลทั้งหมดที่ถ้าไม่ทราบแหล่งที่มา
- 4) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆจากอินเทอร์เน็ต

#### 4.7 ระบบบริการหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

- 1) สำรองข้อมูลตามมาตรการการสำรองข้อมูล ได้แก่ การสำรองข้อมูลอัตโนมัติโดยเครื่องคอมพิวเตอร์แม่ข่ายทุกวัน การสำรองข้อมูลไปยังฮาร์ดดิสก์ภายนอกโดยเจ้าหน้าที่ผู้ดูแลระบบ และการสำรองข้อมูลไปยังเครื่องแม่ข่ายที่ไซต์สำรองที่ห้องคอมพิวเตอร์ อาคารศูนย์เครื่องมือวิทยาศาสตร์และเทคโนโลยี 8
- 2) ทดสอบการกู้คืนข้อมูลและฐานข้อมูล ที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบ อย่างน้อยปีละ 1 ครั้ง
- 3) บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสียหายของข้อมูล

#### 4.8 การบูรณาการเชื่อมโยงระบบเครือข่าย และภัยคุกคามทางคอมพิวเตอร์

- 1) มีระบบยืนยันตัวตน เพื่อตรวจสอบสิทธิ์ก่อนการเข้าใช้งานระบบเครือข่าย
- 2) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เปิดใช้งานตลอดเวลา
- 3) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายขององค์กรเพื่อสังเกตประมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป
- 4)

### 5. การเตรียมความพร้อมในการรับมือสถานการณ์ฉุกเฉิน

- 5.1. จัดให้มีการประเมินสถานะวิกฤติ และทบทวนมาตรการ อย่างน้อยปีละ 2 ครั้ง
- 5.2. สื่อสารทำความเข้าใจ ชักซ้อมแผนเพื่อให้พร้อมจัดการสถานะวิกฤติ อย่างน้อยปีละ 1 ครั้ง

### 6. ขั้นตอนการตอบสนองต่อสถานการณ์ฉุกเฉิน

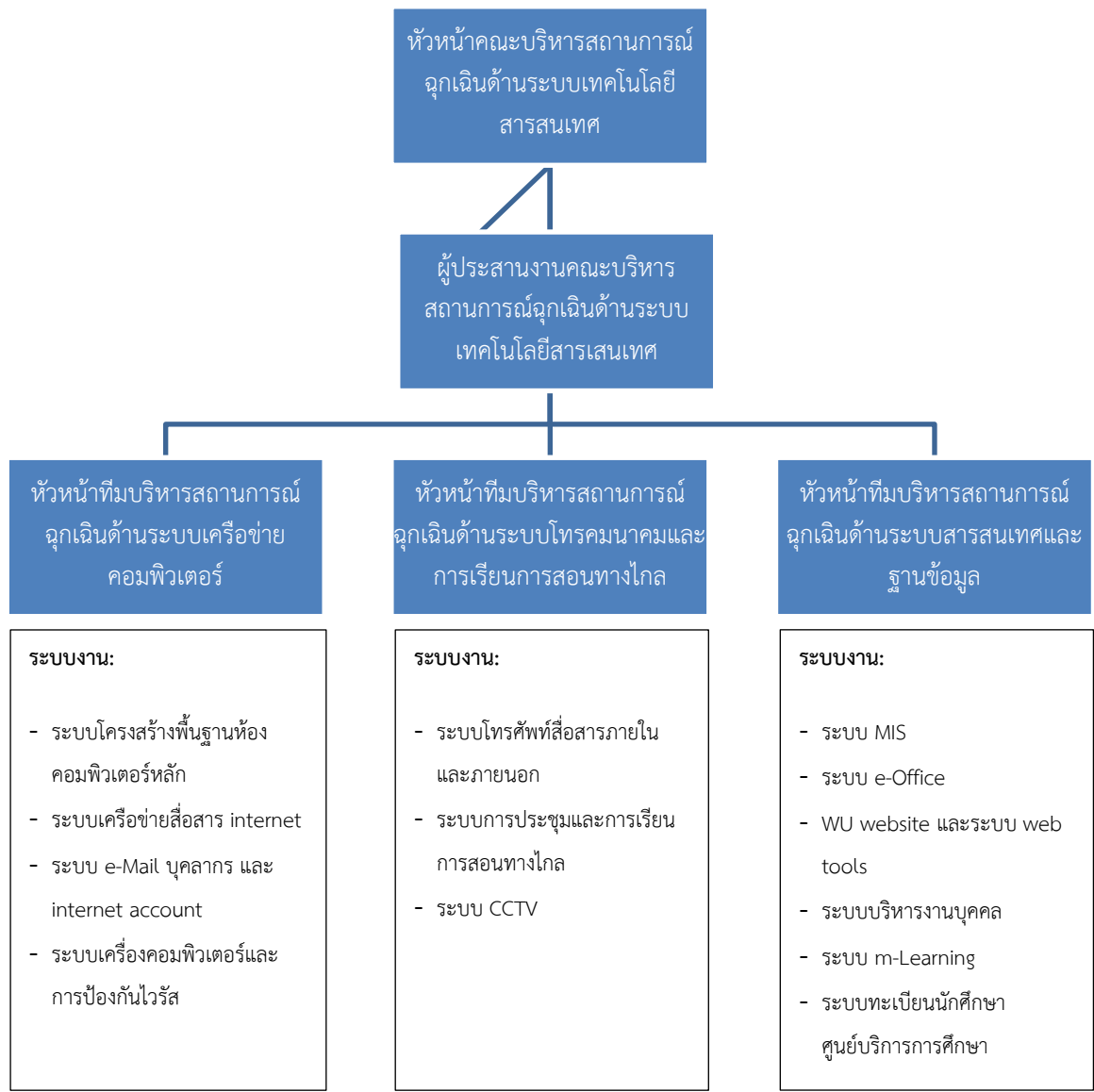
#### 6.1. โครงสร้างทีมงานแผนรับมือสถานการณ์ฉุกเฉิน

เพื่อให้แผนรับมือสถานการณ์ฉุกเฉินสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล ส่งผลให้เกิดความต่อเนื่องในการดำเนินงานของมหาวิทยาลัย จะต้องตั้งทีมงานบริหารสถานการณ์ฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศขึ้น ประกอบด้วยโครงสร้างดังต่อไปนี้

- 1) หัวหน้าคณะบริหารสถานการณ์ฉุกเฉิน (รองอธิการบดีฝ่ายบริหาร)

- 2) ผู้ประสานงานคณะกรรมการณุกเงิน (ผู้อำนวยการศูนย์คอมพิวเตอร์ เป็นหัวหน้าคณะผู้ประสานงาน รองผู้อำนวยการศูนย์คอมพิวเตอร์ เป็นรองหัวหน้าคณะผู้ประสานงาน ฝ่ายบริการ โครงสร้างพื้นฐานและคอมพิวเตอร์ ฝ่ายบริการและพัฒนาระบบสารสนเทศ ฝ่ายธุรการ ศูนย์คอมพิวเตอร์ เป็นคณะทำงาน)
- 3) หัวหน้าทีมบริหารสถานการณุกเงิน (หัวหน้างานเครือข่ายคอมพิวเตอร์ หัวหน้างานระบบสื่อสาร โทรคมนาคม หัวหน้างานระบบMIS เป็นหัวหน้าทีมบริหารสถานการณุกเงิน แบ่งออกเป็น 3 ทีม) โดยทุกตำแหน่งต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน คุ้มกันสถานการณุกเงิน สามารถบริหารความต่อเนื่องให้สถานการณุกเงินกลับคืนสู่สภาวะปรกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารสถานการณุกเงิน และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในบทบาทของบุคคลหลัก ปรากฏดังตารางที่ 1

**โครงสร้างทีมบริหารสถานการณุกเงินด้านระบบเทคโนโลยีสารสนเทศ**



**ตารางที่ 1** รายชื่อบุคลากรและบทบาทหน้าที่ของทีมงานบริหารสถานการณ์ฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์ติดต่อภายใน/มือถือ		ชื่อ	เบอร์ติดต่อภายใน/มือถือ
ผศ.ดร.สุวิทย์ วุฒิสุทธิเมธาวี (รองอธิการบดีฝ่ายบริหาร)	3802 086-966-xxxx	หัวหน้าคณะบริหาร สถานการณ์ฉุกเฉิน	อาจารย์ ดร.อรรถโส ขำวิจิตร (ผู้อำนวยการศูนย์คอมพิวเตอร์)	3433 081-676-7244
อาจารย์ ดร.อรรถโส ขำวิจิตร (ผู้อำนวยการศูนย์คอมพิวเตอร์)	3433 081-676-7244	หัวหน้าคณะผู้ ประสานงานคณะบริหาร สถานการณ์ฉุกเฉิน	อาจารย์ ดร.ชัยโรจน์ ใหญ่ ประเสริฐ	3431 094-292-4669
นายชัยรัตน์ กาณจนอารี (หัวหน้าฝ่ายบริการโครงสร้าง พื้นฐานและคอมพิวเตอร์)	3411 081-963-7740	ผู้ประสานงานคณะ บริหารสถานการณ์ ฉุกเฉิน	นายจักรินทร์ ล้วนศิริ (หัวหน้างานเครือข่าย คอมพิวเตอร์)	3448 091-775-8066
นางเปรมฤดี นุ่นสังข์ (หัวหน้าฝ่ายบริการและพัฒนา ระบบสารสนเทศ)	3450 085-692-9244	ผู้ประสานงานคณะ บริหารสถานการณ์ ฉุกเฉิน	นายพงศ์ธน ฤดีอักษรเสรี (หัวหน้างานระบบ MIS )	3453 081-638-3600
นางรัฐธาดา เลขาพันธ์ (หัวหน้าฝ่ายธุรการ)	3424 0816773219	ผู้ประสานงานคณะ บริหารสถานการณ์ ฉุกเฉิน	นางสุวภา วรรณเพชร (เจ้าหน้าที่บริหารงานทั่วไป)	3423 0815973819
นายจักรินทร์ ล้วนศิริ (หัวหน้างานเครือข่าย คอมพิวเตอร์)	3448 091-775-8066	หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉินด้าน ระบบเครือข่าย คอมพิวเตอร์	นายสาธิต ขวัญชุม (วิศวกร)	3442 081-958-7721
นายไพศาล พุ่มดวง (หัวหน้างานระบบสื่อสาร โทรคมนาคม)	3413 089-469-8444	หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉินด้าน ระบบโทรคมนาคมและ การเรียนการสอน ทางไกล	นายจักรินทร์ ล้วนศิริ (หัวหน้างานเครือข่าย คอมพิวเตอร์)	3448 091-775-8066
นายพงศ์ธน ฤดีอักษรเสรี (หัวหน้างานระบบ MIS )	3453 081-638-3600	หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉินด้าน ระบบสารสนเทศและ ฐานข้อมูล	นางนภาพร ไชยเสน (เจ้าหน้าที่วิเคราะห์ระบบ)	3441 081-543-3142



## 6.2 กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารสถานการณ์ฉุกเฉิน และทีมงานบริหารสถานการณ์ฉุกเฉินตามรายชื่อที่ปรากฏในตารางข้อมูลรายชื่อ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อบุคลากรภายหลังจากมีการประกาศเหตุการณฉุกเฉิน

จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะบริหารสถานการณ์ฉุกเฉินแจ้งให้ผู้ประสานงานคณะบริหารสถานการณ์ฉุกเฉิน โดยผู้ประสานงานฯ จะแจ้งให้หัวหน้าทีมบริหารสถานการณ์ฉุกเฉิน รับทราบเหตุการณฉุกเฉินและการประกาศใช้แผนรับมือสถานการณ์ฉุกเฉินตามสายงานการบังคับบัญชา จากนั้นหัวหน้ากลุ่มงานมีหน้าที่แจ้งไปยังบุคลากรภายใต้การบังคับบัญชาของตนรับทราบเหตุการณฉุกเฉินและปฏิบัติตามขั้นตอนการรับมือสถานการณ์ฉุกเฉิน

ในกรณีที่ไมติดต่อหัวหน้าทีมสามารถได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา

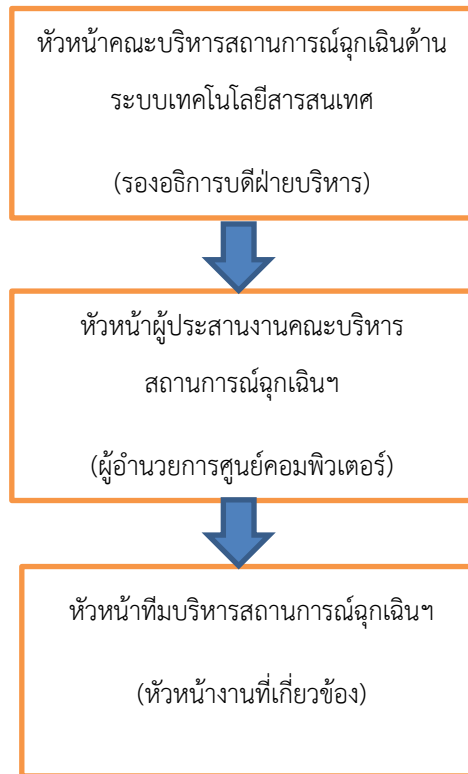
- ถ้าเหตุการณเกิดขึ้นในเวลาทำงาน ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ ภายในเป็นช่องทางแรก
- ถ้าเหตุการณเกิดขึ้นนอกเวลาทำงานหรือสถานที่ปฏิบัติการหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก

ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลัก ดังต่อไปนี้

- 1) สรุปสถานการณ์ของเหตุการณฉุกเฉินและประกาศการใช้แผนรองรับสถานการณ์ฉุกเฉิน
- 2) เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วน สำหรับทีมงานบริหารความเสี่ยง และหน่วยงานที่เกี่ยวข้อง
- 3) ขั้นตอนการปฏิบัติงาน เพื่อแก้ไขสถานการณ์ฉุกเฉินและบริหารความต่อเนื่องต่อไป

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าทีมบริหารสถานการณ์ฉุกเฉินมีหน้าที่โทรกลับไปแจ้งยังหัวหน้าผู้ประสานงานคณะบริหารสถานการณ์ฉุกเฉิน เพื่อรวบรวมสรุปความพร้อมของหน่วยงานในการแก้ไขสถานการณ์และบริหารความต่อเนื่อง รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยงานและเจ้าหน้าที่ทั้งหมดในหน่วยงาน ทีมบริหารสถานการณ์ฉุกเฉินมีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อเจ้าหน้าที่ภายในหน่วยงานสามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่ เกิดเหตุการณฉุกเฉินและมีการประกาศใช้แผนรองรับสถานการณ์ฉุกเฉิน

## แผนผังกระบวนการแจ้งเหตุฉุกเฉิน Call Tree



ขั้นตอนการรับมือสถานการณ์ฉุกเฉินและบริหารความต่อเนื่อง

วันที่ 1 ( ภายใน 24 ชั่วโมง) การตอบสนองต่อเหตุการณ์ทันที

ในการปฏิบัติการใดๆ ให้บุคลากร คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยศูนย์คอมพิวเตอร์อย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
1. แจ้งเหตุฉุกเฉิน วิกฤติ ตามกระบวนการ Call Tree ให้กับหัวหน้าคณะบริหารสถานการณ์ฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ	หัวหน้าผู้ประสานงานคณะบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
2. จัดประชุมทีมบริหารสถานการณ์ฉุกเฉิน เพื่อประเมินความเสียหาย ผลกระทบต่อการดำเนินงาน การให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการแก้ไขสถานการณ์และบริหารความต่อเนื่อง	ทีมผู้ประสานงาน / ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
3. ทบทวนกระบวนการที่มีความเร่งด่วน หรือส่งผลกระทบอย่างสูง (หากไม่ดำเนินการ) ดังนั้น จำเป็นต้องดำเนินงานหรือปฏิบัติด้วยมือ (Manual Processing)	ทีมผู้ประสานงาน / ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
4. ระบุและสรุปรายชื่อบุคลากรในสำนัก ที่ได้รับบาดเจ็บหรือเสียชีวิต	หัวหน้าทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
5. รายงานหัวหน้าคณะบริหารสถานการณ์ฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ โดยครอบคลุมประเด็น ดังนี้ <ul style="list-style-type: none"> <li>• จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ / เสียชีวิต</li> <li>• ความเสียหายและผลกระทบต่อการดำเนินงานและการให้บริการ</li> <li>• ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง</li> <li>• กระบวนการที่มีความเร่งด่วนและส่งผลกระทบอย่างสูง หากไม่ดำเนินการ และจำเป็นต้องดำเนินงานหรือปฏิบัติงานด้วยมือ</li> </ul> - รายงาน อธิการบดี เพื่อรับทราบและพิจารณาอนุมัติดำเนินการปฏิบัติงานและกิจกรรมต่างๆ	ทีมผู้ประสานงาน / ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
6. สื่อสารและรายงานสถานการณ์แก่บุคลากรของมหาวิทยาลัยให้ทราบตามเนื้อหาและข้อความที่ได้รับการพิจารณาและเห็นชอบจากคณะบริหารสถานการณ์ฉุกเฉินแล้ว	หัวหน้าทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
7. ประเมินและระบุกระบวนการหลัก และงานเร่งด่วนที่จำเป็นต้องดำเนินการให้แล้วเสร็จ ภายใน 1 - 5 วันข้างหน้า	หัวหน้าและทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
8. ประเมินศักยภาพและความสามารถของศูนย์ ในการดำเนินงานเร่งด่วน ชำงตัน ภายใต้ข้อจำกัดและสภาวะวิกฤตพร้อมระบุทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่องตามแผนการจัดหาทรัพยากร	หัวหน้าและทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>





ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
9. รายงานความคืบหน้าให้อธิการบดีทราบ	หัวหน้าคณะบริหาร สถานการณ์ฉุกเฉิน	<input type="checkbox"/>
10. ติดต่อและประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการแก้ไขสถานการณ์และบริหารความต่อเนื่อง ได้แก่ <ul style="list-style-type: none"> <li>• สถานที่ปฏิบัติงานสำรอง</li> <li>• วัสดุอุปกรณ์ที่สำคัญ</li> <li>• เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ</li> <li>• บุคลากรหลัก</li> <li>• คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย</li> </ul>	หัวหน้าผู้ประสานงานคณะ บริหารสถานการณ์ฉุกเฉิน/ หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉิน	<input type="checkbox"/>
11. บันทึก (Log Book) และทบทวนกิจกรรมและงานต่างๆที่ทีมบริหารสถานการณ์ฉุกเฉิน ต้องดำเนินการ (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลา) อย่างสม่ำเสมอ	ทีมบริหารสถานการณ์ ฉุกเฉิน	<input type="checkbox"/>
12. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการ สำหรับในวันถัดไปให้กับบุคลากรหลัก เพื่อรับทราบและดำเนินการ อาทิ แจ้งวัน เวลา และสถานที่ปฏิบัติงานสำรอง	หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉิน	<input type="checkbox"/>
13. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารสถานการณ์ฉุกเฉินอย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	หัวหน้าผู้ประสานงานคณะ บริหารสถานการณ์ฉุกเฉิน/ ทีมบริหารสถานการณ์ ฉุกเฉิน	<input type="checkbox"/>

### วันที่ 2 - 7 การตอบสนองในระยะสั้น

ในการปฏิบัติภารกิจใดๆ ให้บุคลากร คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยศูนย์คอมพิวเตอร์อย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
14. ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมผู้ประสานงาน/ทีมบริหาร สถานการณ์ฉุกเฉิน	<input type="checkbox"/>
15. ตรวจสอบกับหน่วยงาน ความพร้อมและข้อจำกัดในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการแก้ไขสถานการณ์ฉุกเฉินและบริหารความต่อเนื่อง ได้แก่ <ul style="list-style-type: none"> <li>• สถานที่ปฏิบัติงานสำรอง</li> <li>• วัสดุอุปกรณ์ที่สำคัญ</li> <li>• เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ</li> <li>• บุคลากรหลัก</li> <li>• คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย</li> </ul>	หัวหน้าผู้ประสานงาน/ หัวหน้าทีมบริหาร สถานการณ์ฉุกเฉิน	<input type="checkbox"/>

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
16. รายงานหัวหน้าคณะบริหารสถานการณ์ฉุกเฉิน เรื่องความพร้อม ข้อจำกัด และข้อเสนอแนะ ในการจัดทำทรัพยากรที่จำเป็นต้องใช้ในการแก้ไขสถานการณ์ฉุกเฉินและบริหารความต่อเนื่อง	หัวหน้าผู้ประสานงาน / ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
17. ประสานงานและดำเนินการจัดทำทรัพยากรที่จำเป็นต้องใช้ในการแก้ไขสถานการณ์ฉุกเฉินและบริหารความต่อเนื่อง: • สถานที่ปฏิบัติงานสำรอง • วัสดุอุปกรณ์ที่สำคัญ • เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ • บุคลากรหลัก • คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าผู้ประสานงาน/ทีมประสานงาน	<input type="checkbox"/>
18. ดำเนินงานและให้บริการ ภายใต้ทรัพยากรที่จัดหา เพื่อแก้ไขสถานการณ์ฉุกเฉินและบริหารความต่อเนื่อง: • สถานที่ปฏิบัติงานสำรอง • วัสดุอุปกรณ์ที่สำคัญ • เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ • บุคลากรหลัก • คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย	ทีมประสานงาน / ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
19. ดำเนินการกอบกู้และจัดหาข้อมูลและรายงานต่างๆที่จำเป็นที่ต้องใช้ในการดำเนินงานและให้บริการ	หัวหน้าทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
20. แจ้งสถานการณ์และแนวทางในการบริหารความต่อเนื่องแก่หน่วยงานพลະผู้ให้บริการที่ได้รับผลกระทบ	หัวหน้าผู้ประสานงาน/ทีมประชาสัมพันธ์ศูนย์คอมพิวเตอร์	<input type="checkbox"/>
21. บันทึก (Log Book) และทบทวนกิจกรรมและงานต่างๆที่ทีมงานบริหารสถานการณ์ฉุกเฉินต้องดำเนินการ (พร้อมระบุรายละเอียด ผู้ดำเนินการ และเวลา) อย่างสม่ำเสมอ	ทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
22. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการต่อไปสำหรับวันถัดไปให้กับบุคลากรของศูนย์คอมพิวเตอร์	หัวหน้าคณะบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>
23. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารสถานการณ์ฉุกเฉินอย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	หัวหน้าผู้ประสานงานคณะบริหารสถานการณ์ฉุกเฉิน/หัวหน้าทีมบริหารสถานการณ์ฉุกเฉิน	<input type="checkbox"/>

