Emergency Response Protocol

**กองทรัพยากรทุนมนุษย์ สำนักงานมหาวิทยาลัย มหาวิทยาลัยเชียงใหม่ ประจำปี 2569**

**หัวข้อ:** การรับมือกรณีฉุกเฉิน เช่น ระบบล่ม ข้อมูลหาย การโจมตีทางไซเบอร์หรือภัยพิบัติอื่น ๆ

**1. วัตถุประสงค์ (Objectives)**

1. เพื่อกำหนดแนวทางปฏิบัติที่ชัดเจนเมื่อเกิดเหตุการณ์ ระบบล่ม, ข้อมูลหาย, การโจมตีทางไซเบอร์, หรือ ภัยพิบัติอื่น ๆ
2. ลดผลกระทบต่อการดำเนินงานและป้องกันความเสียหายของข้อมูล
3. สร้างความมั่นใจในการกู้คืนระบบอย่างมีประสิทธิภาพ

**2. ขอบเขต (Scope)**

ครอบคลุมถึงระบบทั้งหมด เช่น

- Application / Web System
- Database / Data Warehouse
- Server / Cloud Infrastructure
- Network และ Storage
- ผู้ใช้งานระบบ (End Users)

**3. คำจำกัดความ (Definitions)**

| คำศัพท์ | ความหมาย |
|---|---|
| System Down | ระบบไม่สามารถใช้งานได้ เช่น เว็บไซต์ล่ม ฐานข้อมูลไม่ตอบสนอง |
| Data Loss | ข้อมูลสูญหาย เช่น การลบโดยไม่ตั้งใจ หรือการถูกโจมตีจาก Malware/Ransomware |
| RTO (Recovery Time Objective) | เวลาสูงสุดที่ระบบต้องกลับมาใช้งานได้ เช่น 4 ชั่วโมง |
| RPO (Recovery Point Objective) | จุดเวลาล่าสุดที่ข้อมูลสามารถกู้คืนได้ เช่น Backup ล่าสุดไม่เกิน 24 ชั่วโมง |

**4. ระดับความรุนแรง (Incident Severity Level)**

| ระดับ | คำอธิบาย | ตัวอย่าง |
|---|---|---|
| Critical (P1) | ระบบหลักล่มทั้งหมด ผู้ใช้ไม่สามารถทำงานได้ | เว็บไซต์หลักไม่เปิด, Database ล่ม |
| High (P2) | ระบบบางส่วนใช้งานไม่ได้ ส่งผลกระทบสูง | API Error, ข้อมูลบางส่วนไม่เข้าระบบ |
| Medium (P3) | มีปัญหาแต่ยังมีทางแก้ไขชั่วคราว | ระบบช้ากว่าปกติ |
| Low (P4) | ปัญหาน้อย ไม่กระทบผู้ใช้ส่วนใหญ่ | Bug บางส่วน, UI ผิดพลาด |

**5. ขั้นตอนการดำเนินการ (Emergency Procedure)**

5.1 ขั้นตอนเมื่อระบบล่ม (System Down)

| ลำดับ | ขั้นตอน | ผู้รับผิดชอบ |
|---|---|---|
| 1 | ตรวจสอบและยืนยันปัญหา | ศูนย์ส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลและการธรรมาภิบาลข้อมูล มหาวิทยาลัยเชียงใหม่ (PDPG CMU) |
| 2 | แจ้งเตือนทีมที่เกี่ยวข้องผ่าน Line/Email/Microsoft Team | นักวิชาการคอมพิวเตอร์ |
| 3 | ระบุ Severity Level | นักวิชาการคอมพิวเตอร์ |
| 4 | ตรวจสอบสาเหตุ เช่น Network, Database, API | นักวิชาการคอมพิวเตอร์ |
| 5 | แก้ไขปัญหาและรายงานสถานะทุก 30 นาที | นักวิชาการคอมพิวเตอร์ |
| 6 | เมื่อแก้ไขแล้ว ทดสอบระบบก่อนเปิดให้ใช้งาน | นักวิชาการคอมพิวเตอร์ |
| 7 | สรุปรายงานเหตุการณ์ (Post-Mortem Report) ภายใน 24 ชม. | นักวิชาการคอมพิวเตอร์ |

**5.2 ขั้นตอนเมื่อข้อมูลหาย (Data Loss)**

| ลำดับ | ขั้นตอน | ผู้รับผิดชอบ |
|---|---|---|
| 1 | หยุดระบบชั่วคราวเพื่อป้องกันการเขียนข้อมูลทับ | นักวิชาการคอมพิวเตอร์ |
| 2 | ตรวจสอบสาเหตุ เช่น ลบโดยผู้ใช้, DB Crash, Malware | นักวิชาการคอมพิวเตอร์ |
| 3 | ประเมินขอบเขตข้อมูลที่หาย | นักวิชาการคอมพิวเตอร์ |
| 4 | กู้ข้อมูลจาก Backup ล่าสุด ตาม RPO | นักวิชาการคอมพิวเตอร์, ITSC |
| 5 | ทดสอบความสมบูรณ์ของข้อมูล | นักวิชาการคอมพิวเตอร์ |
| 6 | แจ้งผู้ใช้งานเกี่ยวกับข้อมูลที่กู้คืนได้/ไม่ได้ | นักวิชาการคอมพิวเตอร์ |
| 7 | จัดทำ Incident Report และปรับปรุงมาตรการป้องกัน | นักวิชาการคอมพิวเตอร์ |

**5.3 ขั้นตอนเมื่อถูกวาง Script หรือไฟล์ที่น่าสงสัย (Suspicious Script/File Detected)**

| ลำดับ | ขั้นตอน | ผู้รับผิดชอบ |
|---|---|---|
| 1 | หยุดการรัน script/ไฟล์ทันที ถ้าอยู่บน server | นักวิชาการคอมพิวเตอร์ |
| 2 | ตรวจสอบไฟล์ว่าเป็น malware, ransomware หรือ script อันตราย | นักวิชาการคอมพิวเตอร์ |
| 3 | แยก/ลบไฟล์ออกจากระบบ | นักวิชาการคอมพิวเตอร์ |
| 4 | ตรวจสอบ log การเข้าถึงและ source ของไฟล์ | นักวิชาการคอมพิวเตอร์ |
| 5 | ประเมินผลกระทบ เช่น ข้อมูลที่ถูกแก้ไข/ลบ, ระบบถูกเข้าถึง | นักวิชาการคอมพิวเตอร์ |
| 6 | ทำการล้างไฟล์อันตรายและ restore ข้อมูลจาก backup หากจำเป็น | นักวิชาการคอมพิวเตอร์ |
| 7 | แจ้งผู้ใช้งานและทีมที่เกี่ยวข้อง พร้อมแนะนำวิธีป้องกัน | Communication Team |
| 8 | จัดทำรายงานเหตุการณ์และปรับปรุงระบบป้องกัน | นักวิชาการคอมพิวเตอร์ |

**6. แนวทางป้องกัน (Preventive Measures)**

6.1 Backup

- Daily Backup: ฐานข้อมูลสำคัญต้อง Backup
- เก็บ Backup 7 วันย้อนหลัง บน Cloud Storage
- ทำ Offsite Backup สัปดาห์ละ 1 ครั้ง
- ทั้งนี้ตาม Policy ของสำนักบริการสารสนเทศ

6.2 Monitoring & Alert

- ใช้ระบบ Monitoring
- ตั้ง Alert ผ่าน Line เมื่อ:
    - เชื่อมต่อฐานข้อมูลไม่ได้
    - ไม่ตอบสนอง > 5 วินาที
    - สำรองข้อมูลไม่ได้

**7. การสื่อสาร (Communication Plan)**

| ช่องทาง | การแจ้งเตือน | กลุ่มเป้าหมาย |
|---|---|---|
| Line Group/ Email/Microsoft Team | แจ้งปัญหาทันที + Update ทุก 30 นาที | นักวิชาการคอมพิวเตอร์ |
| Line Group/ Email/Microsoft Team | รายงานสรุปหลังแก้ไข | นักวิชาการคอมพิวเตอร์ |
| Status Page | แจ้งผู้ใช้ระบบทั่วไป | End Users |

**8. แบบฟอร์ม Incident Report (ตัวอย่าง)**

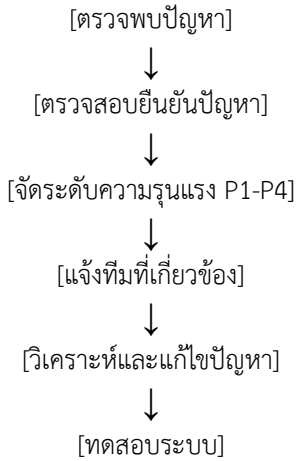
Incident Report

- วันที่เกิดเหตุ: ____/____/_____
- เวลาเริ่ม: ____:____
- เวลาแก้ไขเสร็จ: ____:____
- รายละเอียดเหตุการณ์: _____
- สาเหตุหลัก (Root Cause): _____
- มาตรการป้องกันในอนาคต: _____
- ผู้รับผิดชอบ: _____

**9. RTO / RPO มาตรฐาน**

| ระบบ | RTO | RPO |
|---|---|---|
| Core Database | 4 ชั่วโมง | 1 ชั่วโมง |
| Web Application | 6 ชั่วโมง | 2 ชั่วโมง |
| Backup System | 8 ชั่วโมง | 24 ชั่วโมง |

**10. Flowchart การรับมือกรณีฉุกเฉิน**



↓

[ระบบกลับมาใช้งานได้]

↓

[รายงานสรุปเหตุการณ์]

**11. ผู้รับผิดชอบ (Key Roles)**

| ตำแหน่ง | หน้าที่ |
|---|---|
| ITSC | สำนักบริการเทคโนโลยีสารสนเทศ ดูแลระบบ Cloud Server |
| PDPG | ศูนย์ส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลและการธรรมาภิบาลข้อมูล มหาวิทยาลัยเชียงใหม่ (PDPG CMU) |
| นักวิชาการคอมพิวเตอร์ | ควบคุมเหตุการณ์, สื่อสารกับ Stakeholders |
| Communication Team | แจ้งผู้ใช้งาน |

ประกาศ ณ วันที่

นายธรรมนูญ น่วมอนงค์
ผู้อำนวยการกองทรัพยากรทุนมนุษย์