แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
กองทรัพยากรทุนมนุษย์ สำนักงานมหาวิทยาลัย มหาวิทยาลัยเชียงใหม่ ประจำปี 2569

1. วัตถุประสงค์ (Objectives)

1. เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
2. เพื่อมีแนวทางที่ชัดเจนในการตอบสนองและกู้คืนระบบเมื่อเกิดเหตุการณ์
3. เพื่อปกป้อง ข้อมูลสำคัญ (Critical Data) และ ทรัพย์สินทางดิจิทัล (Digital Assets) ขององค์กร
4. เพื่อให้การปฏิบัติสอดคล้องกับ กฎหมาย PDPA

2. ขอบเขต (Scope)

แผนนี้ครอบคลุม:

1. ระบบสารสนเทศทั้งหมดขององค์กร (Internal + Cloud)
2. ผู้ใช้งานระบบทุกระดับ (พนักงาน, ผู้รับจ้าง, Vendor)
3. เหตุการณ์ด้าน Cybersecurity เช่น
    - Malware / Ransomware
    - Phishing / Social Engineering
    - Data Breach / Data Leak
    - DDoS Attack
    - Privilege Escalation / Unauthorized Access
    - Zero-day Exploit

3. ทีมรับมือเหตุการณ์ (Incident Response Team - IRT)

บทบาท	หน้าที่ความรับผิดชอบ
Incident Response Manager	บริหารจัดการและตัดสินใจขั้นสุดท้าย, รายงานผู้บริหาร
Security Analyst	วิเคราะห์ภัยคุกคาม, ตรวจสอบ Log, ระบุ Root Cause
IT Support / System Admin	ดำเนินการทางเทคนิค เช่น ปิดระบบ, Restore Backup
Legal & Compliance	ตรวจสอบด้านกฎหมาย เช่น PDPA, แจ้งหน่วยงานกำกับ
PR / Communication	จัดการสื่อสารภายในและภายนอกองค์กร
Data Owner	ให้ข้อมูลเกี่ยวกับระบบและความสำคัญของข้อมูล

ช่องทางติดต่อฉุกเฉิน:

- โทรศัพท์ : 053-941112
- Email : cmuhr@cmu.ac.th
- Line Official : @cmuhr

4. ขั้นตอนการรับมือ (Incident Response Lifecycle)

1. การเตรียมการ (Preparation)

วัตถุประสงค์: ลดโอกาสและผลกระทบจากภัยคุกคาม

แนวทางปฏิบัติ:

- มี Policy ด้านความปลอดภัยสารสนเทศ
- จัดทำ Asset Inventory ระบุข้อมูลสำคัญ, Critical Systems
- ติดตั้งและอัปเดต Firewall, IDS/IPS, Endpoint Security
- กำหนด User Access Control
- ทำ Training บุคลากร เรื่อง Cybersecurity Awareness
- จัดเตรียม Backup และ Disaster Recovery Plan

2. การตรวจจับและวิเคราะห์ (Detection & Analysis)

วัตถุประสงค์: ระบุเหตุการณ์ที่อาจเป็นภัยคุกคามอย่างรวดเร็ว

แนวทางปฏิบัติ:

- การตรวจสอบ Log และระบบแจ้งเตือน (Alert)
- ประเมินความเสียหายและจัดลำดับความสำคัญของเหตุการณ์ เพื่อกำหนดขอบเขตและผลกระทบของภัยคุกคาม

3. การควบคุมความเสียหาย (Containment)

วัตถุประสงค์: จำกัดขอบเขตของภัยคุกคามไม่ให้แพร่กระจาย

แนวทางปฏิบัติ:

- ตัดการเชื่อมต่อของระบบที่ติดมัลแวร์หรือถูกโจมตีออกจากเครือข่าย
- ปิดบริการที่ไม่จำเป็น, ใช้ Firewall เพื่อบล็อก IP Address ที่น่าสงสัย
- เปลี่ยนรหัสผ่านของระบบที่ได้รับผลกระทบทันที
- ปรับปรุง Firewall Rules

4. การกำจัดภัยคุกคาม (Eradication)

วัตถุประสงค์: กำจัดภัยคุกคามให้หมดไป

แนวทางปฏิบัติ:

- อัปเดต Software
- เปลี่ยนรหัสผ่านที่อาจรั่วไหลทั้งหมด
- ลบ Backdoor หรือ Script แปลกปลอมที่ผู้โจมตีอาจสร้างไว้
- ปรับปรุงสิทธิ์การเข้าถึงระบบ (Access Control)

5. การกู้คืนระบบ (Recovery)

วัตถุประสงค์: คืนระบบสู่สภาวะปกติและป้องกันการเกิดซ้ำ

แนวทางปฏิบัติ:

- Restore ข้อมูลจาก Backup ที่ผ่านการตรวจสอบแล้วว่าสะอาดและไม่มีมัลแวร์
- ทดสอบและตรวจสอบระบบที่กู้คืนมาแล้ว เพื่อให้แน่ใจว่าไม่มีการติดเชื้อซ้ำ
- นำระบบกลับสู่การใช้งานตามปกติ และเฝ้าระวังอย่างใกล้ชิด

6. กิจกรรมหลังเกิดเหตุการณ์ (Post-Incident Activity)

วัตถุประสงค์: ป้องกันเหตุซ้ำและพัฒนาแผนให้ดียิ่งขึ้น

แนวทางปฏิบัติ:

- รวบรวมข้อมูลทั้งหมดที่เกี่ยวข้องกับเหตุการณ์และจัดทำรายงานสรุป (Post-Incident Report)
- ทบทวนกระบวนการที่ผ่านมา วิเคราะห์จุดแข็ง จุดอ่อน และสิ่งที่ควรปรับปรุง
- นำข้อสรุปที่ได้ไปปรับปรุงแผนการรับมือ, เพิ่มมาตรการป้องกัน, และฝึกอบรมบุคลากร
- วางแผนการออกแบบระบบด้วยแนวคิดหลักด้าน Cybersecurity / Information Security

  1. C – Confidentiality (การรักษาความลับของข้อมูล)

ความหมาย: ปกป้องข้อมูลไม่ให้ **ผู้**ที่ไม่มีสิทธิ์ เข้าถึง, ดู, หรือดัดแปลง
เป้าหมาย: ให้เฉพาะ Authorized Users เท่านั้นที่เข้าถึงข้อมูลได้
ตัวอย่างมาตรการ

- การเข้ารหัสข้อมูล (Encryption)
- การกำหนดสิทธิ์ผู้ใช้งาน (Access Control, Role-Based Access)
- การยืนยันตัวตน (Authentication, MFA)
- การป้องกันการดักฟัง (VPN, SSL/TLS)

ตัวอย่างเหตุการณ์ที่กระทบ Confidentiality

- ข้อมูลลูกค้าถูกแฮก ⟶ ข้อมูลส่วนตัวรั่วไหล
- รหัสผ่านรั่วออกสู่สาธารณะ

2. I – Integrity (ความถูกต้องและครบถ้วนของข้อมูล)

ความหมาย: รักษาให้ข้อมูล ถูกต้อง ครบถ้วน ไม่ถูกดัดแปลงโดยไม่ได้รับอนุญาต
เป้าหมาย: ป้องกัน Unauthorized Modification หรือความเสียหายของข้อมูล
ตัวอย่างมาตรการ

- Digital Signature เพื่อยืนยันความน่าเชื่อถือของข้อมูล
- Backup และระบบป้องกันข้อมูลเสียหาย

ตัวอย่างเหตุการณ์ที่กระทบ Integrity

- ข้อมูลในฐานข้อมูลเสียหายจาก Malware
- ไฟล์ Log ถูกแก้ไขเพื่อลบหลักฐานการโจมตี

3. A – Availability (ความพร้อมใช้งานของระบบ/ข้อมูล)

ความหมาย: ทำให้ระบบและข้อมูล พร้อมใช้งานตลอดเวลา เมื่อผู้มีสิทธิ์ต้องการใช้งาน
เป้าหมาย: ลด Downtime และป้องกันเหตุการณ์ที่ทำให้ระบบหยุดทำงาน
ตัวอย่างมาตรการ

- ระบบสำรอง (Backup / Failover / Disaster Recovery)

ตัวอย่างเหตุการณ์ที่กระทบ Availability

- Server ล่มทำให้เว็บไซต์ใช้งานไม่ได้

องค์ประกอบ	คำอธิบาย	ตัวอย่างที่ต้องป้องกัน
C – Confidentiality	ป้องกันข้อมูลรั่วไหล	Data Breach, Password Leak
I – Integrity	ป้องกันข้อมูลถูกแก้ไข	Hacker เปลี่ยนยอดเงิน, Log ถูกลบ
A – Availability	ป้องกันระบบล่ม	DDoS Attack, Server Down

5. ระดับความรุนแรงของเหตุการณ์ (Incident Severity Level)

ระดับ	คำอธิบาย	ตัวอย่าง	การตอบสนอง
Critical	รุนแรงที่สุด มีผลกระทบต่อการดำเนินงานที่สำคัญ เช่น ระบบหลัก (Core System) หยุดทำงานโดยสิ้นเชิง ทำให้ไม่สามารถให้บริการบุคลากรได้	Ransomware ปิดระบบหลัก	แจ้งผู้บริหารทันที, ปิดระบบ
High	กระทบบางระบบหรือข้อมูลสำคัญรั่วไหล	มัลแวร์แพร่กระจายในเครือข่ายบางส่วน, มีช่องโหว่ความปลอดภัยที่สำคัญ ถูกตรวจพบและอยู่ใน	ต้องดำเนินการอย่างเร่งด่วน (Urgent Action) เพื่อป้องกันไม่ให้เหตุการณ์ลุกลาม

ระดับ	คำอธิบาย	ตัวอย่าง	การตอบสนอง
		ระหว่างการถูกใช้โจมตี, Script แปลกปลอม	
Medium	มีผลกระทบต่อการดำเนินงานในระดับจำกัด หรือทำให้เกิดความไม่สะดวกเล็กน้อย แต่ไม่ได้ส่งผลกระทบต่อบริการที่สำคัญของบุคลากรโดยตรง	การพยายามเข้าสู่ระบบที่ไม่สำเร็จหลายครั้ง	ควรมีการสอบสวนและแก้ไขภายในเวลาที่กำหนด
Low	มีผลกระทบเพียงเล็กน้อยหรือไม่ส่งผลกระทบต่อการดำเนินงานขององค์กร	Malware, Phishing, Virus เล็กน้อย, ตรวจพบการพยายามเข้าถึงไฟล์ที่ไม่ได้รับอนุญาต	สามารถดำเนินการแก้ไขได้ตามความสะดวกหรือนำไปบันทึกเป็นข้อมูลเพื่อการเฝ้าระวังในอนาคต

6. แผนการสื่อสาร (Communication Plan)

ประเภทการสื่อสาร	ช่องทาง	ผู้รับผิดชอบ
การแจ้งเหตุภายในองค์กร	Secure Chat, Email ภายใน	Incident Manager
แจ้งผู้บริหาร	โทรศัพท์, รายงานด่วน	Incident Manager
แจ้งหน่วยงานกำกับ (เช่น PDPA Office, ETDA)	เอกสารเป็นทางการ, Secure Email	Legal & Compliance
แจ้งสาธารณะ / ลูกค้า	Facebook, Line Official	ทีมสื่อสาร

ขั้นตอนการสื่อสาร (Communication Flow)

1. ทันทีที่เกิดเหตุ: แจ้งทีมรับมือและผู้บริหารระดับสูงโดยใช้ช่องทางการสื่อสารที่กำหนดไว้
2. ระหว่างการแก้ไข: สื่อสารกับพนักงานอย่างต่อเนื่องเพื่อป้องกันการแพร่กระจาย และเตรียมข้อมูลสำหรับสื่อสารกับลูกค้าหากจำเป็น
3. เมื่อสถานการณ์คลี่คลาย: ออกประกาศหรือคำอธิบายอย่างเป็นทางการเพื่อยืนยันว่าเหตุการณ์ได้ยุติลงแล้ว และชี้แจงมาตรการป้องกันในอนาคต
4. หลังเหตุการณ์: สรุปผลการสื่อสารและทบทวนสิ่งที่ทำได้ดีและควรปรับปรุง

7. เครื่องมือและระบบสนับสนุน

1. เครื่องมือสำหรับการจัดการและประสานงาน (Management & Coordination Tools)
   - ระบบที่ช่วยประสานงานและทำให้กระบวนการรับมือเป็นอัตโนมัติ (Automate) ช่วยให้ทีมรับมือไม่ต้องเสียเวลาไปกับงานที่ต้องทำซ้ำ ๆ และสามารถตอบสนองได้อย่างรวดเร็วยิ่งขึ้น
   - ระบบที่ใช้ในการ บันทึก ติดตาม และจัดการ เหตุการณ์ที่เกิดขึ้น ทำให้สามารถตรวจสอบสถานะของแต่ละเหตุการณ์ได้อย่างชัดเจน
2. เครื่องมือสำหรับการตรวจจับและวิเคราะห์ (Detection & Analysis Tools)

   2.1 เครื่องมือหรือวิธีการคำนวณความน่าจะเป็น (Likelihood)

   หน้าที่ของ Likelihood Calculator : เพื่อวิเคราะห์และประเมินความเสี่ยงของเหตุการณ์หรือช่องโหว่

   1. Discoverability (การค้นพบได้ง่าย)

   ความหมาย: ระดับความง่ายหรือยากในการ ค้นพบช่องโหว่ (Vulnerability) หรือปัญหาโดยบุคคลภายนอกหรือผู้โจมตี

   - ถ้าช่องโหว่ ค้นพบได้ง่าย = ความเสี่ยงสูง เพราะแฮกเกอร์สามารถหาพบได้เร็ว
   - ถ้าช่องโหว่ซ่อนอยู่ลึกและยากต่อการสังเกต = ความเสี่ยงจะลดลง

ระดับ	คำอธิบาย
High (สูง)	สามารถค้นหาได้ง่าย เช่น scan ด้วยเครื่องมือทั่วไปก็พบ
Medium (กลาง)	ต้องมีความรู้เฉพาะด้านหรือขั้นตอนซับซ้อนจึงจะเจอ
Low (ต่ำ)	แทบไม่สามารถค้นพบได้ เว้นแต่เข้าถึงระบบภายใน

2. Exploitability (ความสามารถในการโจมตี)

ความหมาย: ความง่ายหรือยากในการ ใช้ประโยชน์จากช่องโหว่ เพื่อโจมตีระบบ

ระดับ	คำอธิบาย
High (สูง)	โจมตีได้ง่าย เช่น ใช้เครื่องมือสำเร็จรูป, ไม่มีการป้องกัน
Medium (กลาง)	ต้องมีความรู้หรือเตรียมตัวก่อนโจมตี
Low (ต่ำ)	ต้องใช้ทรัพยากรสูงมากหรือโอกาสโจมตีสำเร็จต่ำ

3. Reproducibility (การทำซ้ำได้)

ความหมาย: ความสามารถในการ **ทำให้ปัญหาเกิดซ้ำได้** ทุกครั้งที่มีการทดลอง

ระดับ	คำอธิบาย
High (สูง)	ทำซ้ำได้ 100% ตามขั้นตอนที่ชัดเจน
Medium (กลาง)	ทำซ้ำได้บ่อยครั้ง แต่ไม่ 100%
Low (ต่ำ)	เกิดขึ้นแบบสุ่ม ยากต่อการทำซ้ำ

4. Likelihood (โอกาสที่จะเกิดขึ้น)

ความหมาย: ความน่าจะเป็นที่ ช่องโหว่จะถูกค้นพบและโจมตีจริง โดยรวม Discoverability + Exploitability + Reproducibility เข้าด้วยกัน

สูตรตัวอย่าง

$$\text{Likelihood} = \frac{\text{Discoverability} + \text{Exploitability} + \text{Reproducibility}}{3}$$

ระดับ	คำอธิบาย
High (สูง)	มีโอกาสเกิดขึ้นบ่อยมาก
Medium (กลาง)	มีโอกาสเกิดเป็นบางครั้ง
Low (ต่ำ)	โอกาสเกิดต่ำมาก

5. Impact (ผลกระทบ)

ความหมาย: ระดับความเสียหาย **ถ้าช่องโหว่ถูกโจมตีสำเร็จ** เช่น ระบบล่ม, ข้อมูลรั่วไหล, เสียชื่อเสียงองค์กร

ระดับ	ตัวอย่างผลกระทบ
High (สูง)	ระบบหลักล่ม, ข้อมูลสำคัญรั่วไหล, สูญเสียรายได้สูง
Medium (กลาง)	กระทบผู้ใช้บางส่วน, มี downtime ชั่วคราว
Low (ต่ำ)	ผลกระทบเล็กน้อย, ไม่กระทบต่อธุรกิจโดยรวม

6. Risk Level (ระดับความเสี่ยง)

ความหมาย: เป็นค่ารวมจาก **Likelihood × Impact** เพื่อวัดความเสี่ยงโดยรวม

สูตรตัวอย่าง

$$\text{Risk Level} = \text{Likelihood} \times \text{Impact}$$

Risk Level	ความหมาย
High (สูง)	ต้องแก้ไขทันที / P1 Critical
Medium (กลาง)	วางแผนแก้ไขในระยะสั้น / P2
Low (ต่ำ)	เฝ้าติดตามได้ / P3-P4

8. Checklist สำหรับการทบทวนแผน Incident Response ประจำปี

1. การทบทวนนโยบายและเอกสาร (Policy & Documentation Review)
   - นโยบายการรับมือ (Incident Response Policy): ตรวจสอบว่านโยบายยังคงสอดคล้องกับวัตถุประสงค์ทางธุรกิจและกฎหมายที่เกี่ยวข้องหรือไม่ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)
   - แผนการรับมือ (Incident Response Plan): ทบทวนแต่ละขั้นตอนของแผนว่ายังคงใช้งานได้จริงหรือไม่
   - แผนการสื่อสาร (Communication Plan): ตรวจสอบรายชื่อผู้ติดต่อทั้งภายในและภายนอกว่าเป็นปัจจุบันหรือไม่
2. การทบทวนทีมและบทบาท (Team & Roles Review)
   - รายชื่อทีมรับมือ: ปรับปรุงแก้ไขรายชื่อและข้อมูลติดต่อของสมาชิกในทีมทุกคน รวมถึงบทบาทและหน้าที่ที่รับผิดชอบ
   - การฝึกอบรม (Training): ตรวจสอบว่าสมาชิกในทีมทุกคนได้รับการฝึกอบรมที่จำเป็นหรือไม่ เช่น การวิเคราะห์หลักฐานทางดิจิทัล หรือการรับมือกับ Ransomware
   - การกำหนดผู้รับผิดชอบ (Role Clarity): ยืนยันว่าทุกคนในทีมเข้าใจบทบาทและหน้าที่ของตนเองอย่างชัดเจน
3. การทบทวนเครื่องมือและเทคโนโลยี (Tools & Technology Review)
   - ระบบและเครื่องมือ: ตรวจสอบว่าเครื่องมือที่ใช้ในการรับมือ ยังทำงานได้อย่างถูกต้องและมีประสิทธิภาพหรือไม่
   - ซอฟต์แวร์และ Patch: ตรวจสอบว่าระบบปฏิบัติการและซอฟต์แวร์ที่สำคัญได้รับการอัปเดต Patch ความปลอดภัยล่าสุดอยู่เสมอ
   - การสำรองข้อมูล (Backup): ตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลสำรอง และทดสอบกระบวนการกู้คืนข้อมูล (Restore) เป็นประจำ
4. การทบทวนจากการฝึกซ้อม (Exercise & Drill Review) และเหตุการณ์จริง
   - วิเคราะห์และจัดทำรายงานสรุปจากผลการฝึกซ้อมจำลองสถานการณ์ เพื่อระบุจุดอ่อนของแผนและนำไปสู่การปรับปรุงแก้ไข
   - รวบรวมข้อมูลและจัดทำรายงานหลังเกิดเหตุการณ์ (Post-Incident Report) จากเหตุการณ์จริงที่เกิดขึ้น เพื่อนำบทเรียนที่ได้ไปปรับปรุงแผนการรับมือ

ประกาศ ณ วันที่

นายธรรมนูญ น่วมอนงค์
ผู้อำนวยการกองทรัพยากรทุนมนุษย์