รายงานผลการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

มหาวิทยาลัยราชภัฏมหาสารคาม

ปีงบประมาณ พ.ศ. 2568 – 2569

---

1. บทนำ

มหาวิทยาลัยราชภัฏมหาสารคามได้ให้ความสำคัญกับการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อรองรับภัยคุกคามที่มีแนวโน้มเพิ่มขึ้นทั้งในเชิงปริมาณและความซับซ้อน โดยมุ่งเน้นการยกระดับศักยภาพขององค์กรให้สามารถ **ป้องกัน (Prevention) ตรวจจับ (Detection) และตอบสนอง (Response)** ต่อภัยคุกคามได้อย่างมีประสิทธิภาพ การดำเนินงานในปีงบประมาณ พ.ศ. 2568 – 2569 ครอบคลุม 3 มิติสำคัญ ได้แก่

1. การพัฒนาบุคลากร (People)
2. การพัฒนาเทคโนโลยีและโครงสร้างพื้นฐาน (Technology)
3. การพัฒนากระบวนการเฝ้าระวังและบริหารจัดการความมั่นคงปลอดภัย (Process)

2. ผลการดำเนินงานที่สำคัญ

2.1 การพัฒนาโครงสร้างพื้นฐานด้านไซเบอร์ (Server, SOC และ DR Site)

มหาวิทยาลัยได้ดำเนินการปรับปรุงระบบโครงสร้างพื้นฐานด้านสารสนเทศให้ทันสมัย รองรับการใช้งานในยุคดิจิทัล พร้อมยกระดับความมั่นคงปลอดภัย ดังนี้

(1) การพัฒนาเครื่องแม่ข่าย (Server Modernization)

- รองรับเทคโนโลยี Virtualization, Cloud Integration และ Container (เช่น Docker)
- เพิ่มประสิทธิภาพด้านการประมวลผลและการจัดเก็บข้อมูล
- ยกระดับความเสถียรและความพร้อมใช้งานของระบบ

(2) การใช้ระบบเฝ้าระวังความปลอดภัย (SOC: Security Operations Center)

- เฝ้าระวังเหตุการณ์ผิดปกติแบบ 24x7
- ตรวจจับพฤติกรรมเสี่ยง เช่น การเข้าถึงโดยไม่ได้รับอนุญาต และ Anomaly Detection
- แจ้งเตือนเหตุการณ์แบบ Real-time และสนับสนุน Incident Response
- จัดทำรายงานสถานะความปลอดภัยอย่างต่อเนื่อง

(3) การจัดตั้งศูนย์สำรองข้อมูล (Disaster Recovery Site: DR Site)

- สำรองข้อมูลและทำ Data Replication ไปยังศูนย์สำรอง
- รองรับการกู้คืนระบบ (Failover) ในกรณีเกิดเหตุขัดข้องหรือภัยพิบัติ
- กำหนดค่า RTO และ RPO สำหรับระบบสำคัญ

ผลลัพธ์:

เพิ่มความต่อเนื่องในการให้บริการ (Business Continuity) และลดความเสี่ยงจากการหยุดชะงักของระบบ

2.2 การติดตั้งระบบป้องกันภัยคุกคาม (WAF และ SOC)

มหาวิทยาลัยได้ติดตั้งระบบ **Web Application Firewall (WAF)** ควบคู่กับการใช้บริการ SOC เพื่อป้องกันภัยคุกคามที่เกิดกับเว็บไซต์และระบบสารสนเทศ

ขอบเขตการป้องกัน

- ป้องกันการโจมตี เช่น SQL Injection, Cross-site Scripting (XSS), Remote Code Execution
- ปกป้องระบบสำคัญ ได้แก่ เว็บไซต์มหาวิทยาลัย ระบบทะเบียน ระบบบุคลากร และระบบ MIS
- ตรวจจับและกรอง Traffic ที่เป็นอันตราย

การเพิ่มประสิทธิภาพระบบ

- ลดความเสี่ยงจากการโจมตีแบบ DDoS (ในระดับหนึ่ง)
- เพิ่มความพร้อมใช้งานของระบบ (Availability)
- เก็บ Log และนำไปใช้วิเคราะห์เหตุการณ์ด้านความปลอดภัย

การรองรับมาตรฐาน

- OWASP / OWASP Top 10
- ISO/IEC 27001

ผลลัพธ์:

ลดความเสี่ยงจากการโจมตีทางไซเบอร์ และเพิ่มประสิทธิภาพในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย

2.3 การพัฒนาศักยภาพบุคลากรด้านไซเบอร์

มหาวิทยาลัยได้ดำเนินการพัฒนาบุคลากรทั้งในเชิงเทคนิคและเชิงกฎหมาย เพื่อเสริมสร้างความพร้อมขององค์กร

(1) การอบรมด้าน Incident Response (ร่วมกับ สกมช.)

- พัฒนาศักยภาพในการจัดทำ Cyber Incident Response Plan
- ครอบคลุมการบริหารจัดการเหตุการณ์ในทุกระดับ
- จัดทำแผนรับมือภัยคุกคามไซเบอร์ของมหาวิทยาลัยสำเร็จ

(2) การอบรมด้านกฎหมายไซเบอร์

- อบรมบุคลากรจำนวน 600 คน
- ครอบคลุม PDPA และ พ.ร.บ.คอมพิวเตอร์

ผลลัพธ์:

- บุคลากรมี Cybersecurity Awareness สูงขึ้น
- ลดความเสี่ยงด้านกฎหมายและการละเมิดข้อมูล
- สนับสนุนการกำกับดูแลด้าน IT Governance

2.4 การเข้าร่วมโครงการ Government Web Protection (GWP)

มหาวิทยาลัยได้เข้าร่วมโครงการ **Government Web Protection (GWP)** เพื่อยกระดับความปลอดภัยของเว็บไซต์ตามมาตรฐานภาครัฐ

- นำระบบและเว็บไซต์เข้าร่วมจำนวน 5 ระบบ
- ได้รับการป้องกันและเฝ้าระวังภัยคุกคาม เช่น DDoS และ Web Attack
- มีระบบแจ้งเตือนและวิเคราะห์ภัยคุกคามแบบเชิงรุก

ผลลัพธ์:

- เพิ่มระดับความมั่นคงปลอดภัยเว็บไซต์
- ลดความเสี่ยงจากภัยคุกคาม
- สอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ภาครัฐ

2.5 การพัฒนาระบบตรวจสอบช่องโหว่เว็บไซต์ (OWASP-based System)

ศูนย์เทคโนโลยีดิจิทัลและนวัตกรรมได้พัฒนาระบบตรวจสอบช่องโหว่เว็บไซต์ เพื่อสนับสนุนผู้ดูแลระบบและนักพัฒนา

คุณสมบัติของระบบ

- สแกนช่องโหว่อัตโนมัติ (Automated Vulnerability Scanning)
- Dashboard แสดงสถานะความเสี่ยง
- ระบบแจ้งเตือนแบบ Real-time
- รายงานช่องโหว่ตามมาตรฐาน OWASP และ MITRE CWE

ผลลัพธ์:

- ลดระยะเวลาในการตรวจสอบและแก้ไขช่องโหว่
- เพิ่มความปลอดภัยของเว็บไซต์
- รองรับการตรวจประเมินมาตรฐานระดับประเทศ

3. สรุปภาพรวม

จากการดำเนินงานในปีงบประมาณ พ.ศ. 2568 – 2569 มหาวิทยาลัยราชภัฏมหาสารคามมีการพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์อย่างครอบคลุมในทุกมิติ โดยสามารถสรุปได้ดังนี้

- **ด้านบุคลากร (People):** มีความรู้ ความตระหนัก และความสามารถในการรับมือภัยไซเบอร์เพิ่มขึ้น
- **ด้านกระบวนการ (Process):** มีแผนและระบบการตอบสนองเหตุการณ์ที่ชัดเจน
- **ด้านเทคโนโลยี (Technology):** มีระบบป้องกัน เฝ้าระวัง และตรวจสอบที่ทันสมัย

ส่งผลให้มหาวิทยาลัยสามารถ

- ป้องกันและลดความเสี่ยงจากภัยคุกคามไซเบอร์
- เพิ่มความต่อเนื่องและความน่าเชื่อถือของระบบสารสนเทศ
- รองรับการพัฒนา “มหาวิทยาลัยดิจิทัล” ได้อย่างมั่นคงและยั่งยืน