มาตรฐานการปฏิบัติงาน (Standard Operating Procedure : SOP)

กระบวนงาน การบำรุงรักษาระบบความปลอดภัยไซเบอร์

หน่วยงาน	ผู้เขียน (วัน/เดือน/ปี)	ผู้เห็นชอบ (วัน/เดือน/ปี)	หมายเลข SOP (Version)
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	กฤษฎา พูลยรัตน์ 8 กรกฎาคม 2568		SOP-S2-01 / V1

วัตถุประสงค์

1. เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ระบบสารสนเทศของมหาวิทยาลัยมีความมั่นคงปลอดภัยและเชื่อถือได้
2. เพื่อให้เป็นไปตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
3. เพื่อสนับสนุนการเรียนรู้และการทำงานของบุคลากรโดยไม่เกิดการรบกวนจากเหตุการณ์ทางไซเบอร์

ขอบเขต

1. ระบบเครือข่ายและโครงสร้างพื้นฐาน (Firewall, Switch, Router)
2. ระบบ Server และ ฐานข้อมูล

บทบาทหน้าที่ของผู้เกี่ยวข้อง

- **นักวิชาการคอมพิวเตอร์:** ตรวจสอบและบำรุงรักษาระบบด้านความปลอดภัยตามแผนที่กำหนด
- **หัวหน้างานเทคโนโลยีสารสนเทศ:** วางแผน/อนุมัติแผนการบำรุงรักษาและประเมินความเสี่ยง
- **ผู้ดูแลระบบ (Admin):** ตรวจสอบ Log ความปลอดภัย และดำเนินการอัปเดต Patch ระบบ
- **ผู้อำนวยการสำนักฯและรองผู้อำนวยการสำนักฯ:** กำกับ ติดตาม และรายงานผลการดำเนินงานต่อผู้บริหารระดับมหาวิทยาลัย

มาตรฐานขั้นตอนการปฏิบัติงาน

1. จัดทำแผนการตรวจสอบและบำรุงรักษาด้านความปลอดภัยรายเดือน/ไตรมาส
2. ดำเนินการตามแผน
    - ตรวจสอบระบบและอุปกรณ์เครือข่าย
    - อัปเดตระบบปฏิบัติการและซอฟต์แวร์ทุกครั้งที่มีการประกาศอัปเดต
    - ตรวจสอบเก็บบันทึก Log ตาม พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์
    - จัดทำ Backup และทดสอบการกู้คืนข้อมูลตามแผน Disaster Recovery
3. ตรวจสอบและประเมินผลการดำเนินงาน
4. ปรับปรุงและแก้ไขการดำเนินงาน

กฎหมาย/แนวปฏิบัติที่เกี่ยวข้อง

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. แนวทางปฏิบัติของ NCSA (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)

ตัวชี้วัด

1. ร้อยละของระบบที่ได้รับการบำรุงรักษาด้านความปลอดภัยตามแผน ≥ 95%
2. ร้อยละที่ถูกโจมตีระบบสำเร็จทั้งหมด ≤ 2%
3. ระดับความพึงพอใจของผู้ใช้งานระบบ ≥ 3.51

ขั้นตอนการปฏิบัติงาน (Work Instruction : WI)

กระบวนงาน การบำรุงรักษาระบบความปลอดภัยไซเบอร์

หน่วยงาน	ผู้เขียน (วัน/เดือน/ปี)	ผู้เห็นชอบ (วัน/เดือน/ปี)	หมายเลข WI (Version)
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	22/4/2568		

1. วัตถุประสงค์

1. เพื่อให้การดำเนินงานด้านการตรวจสอบและบำรุงรักษาระบบความปลอดภัยไซเบอร์ เป็นไปอย่างเป็นระบบ สม่ำเสมอ และตรวจสอบได้
2. เพื่อควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในมหาวิทยาลัย
3. เพื่อให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศมีแนวทางปฏิบัติที่ชัดเจน ครอบคลุม สามารถปฏิบัติงานได้อย่างถูกต้องตามมาตรฐานและมีความพร้อมใช้งานอยู่เสมอ สามารถรับมือกับภัยคุกคามไซเบอร์ได้อย่างทันท่วงที

2. ตารางบุคคลที่มีส่วนเกี่ยวข้อง (STAKEHOLDER)

ลำดับที่	ผู้เกี่ยวข้อง	หน้าที่ความรับผิดชอบ	คำอธิบาย
1	ผู้อำนวยการสำนักวิทยบริการฯ	กำกับ ติดตาม และให้ข้อเสนอแนะเชิงนโยบาย	เป็นผู้บริหารสูงสุดของหน่วยงาน มีหน้าที่กำกับทิศทางและให้การอนุมัตินโยบายด้านความมั่นคงปลอดภัยไซเบอร์
2	หัวหน้างานระบบเครือข่าย	วางแผน อนุมัติ และตรวจสอบการดำเนินงานบำรุงรักษาระบบ	เป็นผู้ควบคุมแผนงานในเชิงเทคนิค ให้คำแนะนำแก่เจ้าหน้าที่ และประเมินผลการดำเนินงานตามแผนบำรุงรักษา
3	เจ้าหน้าที่เทคโนโลยีสารสนเทศ	ปฏิบัติงานตรวจสอบ บำรุงรักษา แก้ไข และรายงานผล	เป็นผู้ปฏิบัติงานตามแผน มีหน้าที่ตรวจสอบระบบ เช่น Firewall, Antivirus, Backup, Patch Update และจัดทำรายงานสรุปต่อผู้บังคับบัญชา
4	เจ้าหน้าที่ Helpdesk/Support	ประสานงาน รับแจ้งปัญหา และส่งต่อให้ทีมผู้รับผิดชอบ	เป็นด่านแรกในการรับเรื่องและจัดลำดับความสำคัญในการแก้ไขปัญหา รวมถึงอัพเดตสถานะให้กับผู้ใช้งาน
5	ผู้ใช้งานระบบ (บุคลากรภายใน มจษ.)	แจ้งเหตุขัดข้อง ร่วมมือในการตรวจสอบ และปฏิบัติตามมาตรการความปลอดภัยที่กำหนด	มีหน้าที่แจ้งปัญหาที่พบ และปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ เช่น ไม่ใช้รหัสผ่านซ้ำ ไม่เปิดไฟล์แนบที่ไม่รู้แหล่งที่มา เป็นต้น

3. วัสดุและอุปกรณ์ ทรัพยากรที่เกี่ยวข้อง

ประเภท	รายการ / ทรัพยากรที่ใช้	รายละเอียดเพิ่มเติม
ซอฟต์แวร์	ระบบป้องกันไวรัส	ตรวจสอบมัลแวร์ และภัยคุกคามในเครื่องปลายทาง
	ระบบ IDS/IPS	ตรวจจับและป้องกันการโจมตีในเครือข่าย
	ระบบอัปเดตเวอร์ชัน อัตโนมัติ	สำหรับอัปเดตซอฟต์แวร์ OS และแอปพลิเคชันเพื่ออุดช่องโหว่
	ระบบจัดการบันทึก Log	ติดตามกิจกรรมต้องสงสัย วิเคราะห์ภัยคุกคาม
ฮาร์ดแวร์	เครื่องแม่ข่าย (Server) ที่ให้บริการหลัก	เช่น Web Server, DB Server, Authentication Server
	อุปกรณ์ Firewall	สำหรับควบคุมการเข้า-ออกของข้อมูลเครือข่าย
	อุปกรณ์กระจายสัญญาณ	Router, Switch
	อุปกรณ์สำรองไฟ (UPS)	เพื่อป้องกันระบบล่มจากไฟตก/ไฟดับ
เอกสาร/แผนงาน	แผนงานบำรุงรักษาประจำปี	ใช้กำหนดรอบเวลาและรายการที่ต้องตรวจสอบ
	แบบฟอร์ม Checklist การตรวจสอบ	ใช้ในการบันทึกผลการดำเนินงานและการประเมิน
บุคลากรเฉพาะทาง	เจ้าหน้าที่ IT / Security Admin	ต้องมีความรู้ด้าน Cybersecurity พอสมควร
	ผู้ตรวจสอบภายใน (Internal Auditor)	ใช้ในการทบทวนระบบเพื่อความโปร่งใสและตรวจสอบย้อนหลัง

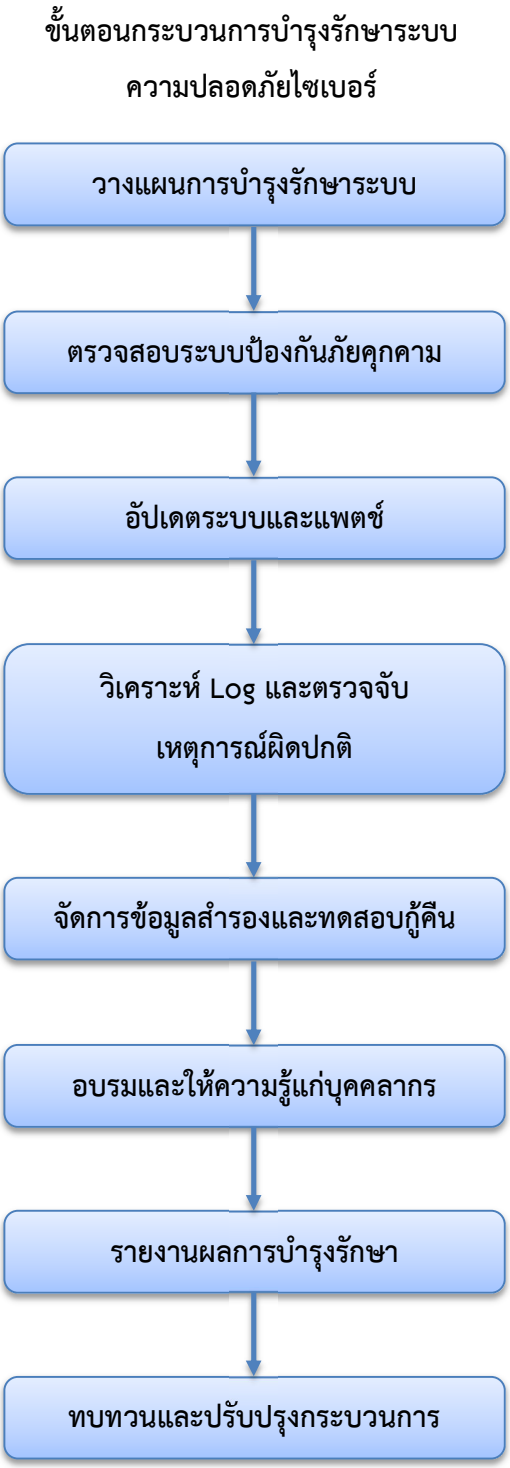
4. ข้อพิจารณาด้านคุณภาพ

ประเด็นด้านคุณภาพ	รายละเอียด
ความครบถ้วนของการตรวจสอบ	ตรวจสอบระบบที่อยู่ในแผนบำรุงรักษาทุกระบบตามรอบที่กำหนด โดยใช้ Checklist ที่กำหนดไว้เท่านั้น
ความถูกต้องของรายงานผล	รายงานการตรวจสอบต้องแสดงข้อมูลจริง ตรวจสอบได้ และมีหลักฐานประกอบ เช่น Screenshot หรือ Log file
ความรวดเร็วในการตอบสนองเหตุการณ์ผิดปกติ	มีการตรวจสอบในตอนเช้าของทุกวัน เมื่อตรวจพบภัยคุกคามหรือระบบผิดปกติ ต้องมีการตอบสนองเบื้องต้นภายใน 1 ชั่วโมง และแก้ไขภายใน 4 ชั่วโมง
ความปลอดภัยของกระบวนการดำเนินงาน	เข้าถึงระบบต้องผ่านการยืนยันตัวตน และใช้บัญชีเฉพาะ มีการจำกัดสิทธิการเข้าถึงระบบ
การปฏิบัติงานตามกฎหมาย/ระเบียบที่เกี่ยวข้อง	มีการอัปเดตแนวปฏิบัติให้สอดคล้องกับ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ 2562 และ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
ความพร้อมใช้งานของระบบ (Availability)	มีระบบสำรองข้อมูลและแผนการฟื้นฟูเมื่อเกิด Downtime ให้ระบบกลับมาใช้งานได้ภายในระยะเวลาที่กำหนดไว้

5. เอกสารอ้างอิง

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. คู่มือแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (DGA)

6. ขั้นตอน (Work Flow)



ขั้นตอนกระบวนงาน การบำรุงรักษาระบบความปลอดภัยไซเบอร์

ลำดับ	ขั้นตอน	ระยะเวลา (วัน)	หน่วยงานผู้รับผิดชอบ	ผู้บริหารที่เกี่ยวข้อง
1	จัดทำแผนบำรุงรักษาระบบความปลอดภัยรายปีและรายไตรมาส	15 วันทำการต้นปีงบประมาณ	หัวหน้างานระบบเครือข่าย, นักวิชาการคอมพิวเตอร์	ผู้อำนวยการสำนักฯ
2	ตรวจสอบและอัปเดตระบบ Firewall, Antivirus, IDS/IPS	ทุกเดือน (ภายใน 3 วันทำการต้นเดือน)	นักวิชาการคอมพิวเตอร์	หัวหน้างานระบบเครือข่าย
3	อัปเดตเวอร์ชัน ระบบปฏิบัติการและซอฟต์แวร์	ภายใน 7 วันหลังจากมีประกาศอัปเดต	นักวิชาการคอมพิวเตอร์ / Admin	หัวหน้างานระบบเครือข่าย
4	ตรวจสอบ Log ความปลอดภัยและวิเคราะห์เหตุการณ์	ทุกสัปดาห์	Admin ระบบ	หัวหน้างานระบบเครือข่าย
5	ทำ Backup ข้อมูล และทดสอบการกู้คืน (Disaster Recovery)	ทุกเดือน	นักวิชาการคอมพิวเตอร์	หัวหน้างานระบบเครือข่าย
6	เข้าอบรมและเผยแพร่ให้ความรู้ภัยคุกคามไซเบอร์แก่บุคลากร	ปีละ 1 ครั้ง	นักวิชาการคอมพิวเตอร์ / วิทยากรภายนอก	ผู้อำนวยการสำนักฯ
7	สรุปผลการตรวจสอบและจัดทำรายงานส่งผู้บริหาร	ทุกไตรมาส	หัวหน้างานระบบเครือข่าย	ผู้อำนวยการสำนักฯ / รองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ
8	ทบทวนและปรับปรุงแผนงานตามข้อเสนอแนะหรือเหตุการณ์สำคัญ	ปีละ 1 ครั้ง (ปลายปีงบประมาณ)	หัวหน้างานระบบเครือข่าย, เจ้าหน้าที่ IT	ผู้อำนวยการสำนักฯ / อธิการบดี (หากมีการเปลี่ยนแปลงนโยบายระดับมหาวิทยาลัย)