วิทยาลัยนวัตกรรม
สื่อสารสังคม
มหาวิทยาลัยศรีนครินทรวิโรฒ

คู่มือปฏิบัติงาน
การจัดการ Cybersecurity

วิทยาลัยนวัตกรรมสื่อสารสังคม

มหาวิทยาลัยศรีนครินทรวิโรฒ

กฎเกณฑ์การปฏิบัติงานด้านไอทีและความมั่นคงปลอดภัยไซเบอร์

ฝ่ายไอที วิทยาลัยนวัตกรรมสื่อสารสังคม มหาวิทยาลัยศรีนครินทรวิโรฒ

(อ้างอิงตาม NIST Cybersecurity Framework 2.0)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการปฏิบัติงานของฝ่ายไอที วิทยาลัยนวัตกรรมสื่อสารสังคม (COSCI) มหาวิทยาลัยศรีนครินทรวิโรฒ ในการบริหารจัดการระบบสารสนเทศ ทรัพยากรด้านไอที และความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับ NIST Cybersecurity Framework 2.0 อันประกอบด้วย 5 องค์ประกอบหลัก ได้แก่ Identify, Protect, Detect, Respond และ Recover

2. ขอบเขต

กฎเกณฑ์ฉบับนี้ครอบคลุมการดูแลระบบสารสนเทศ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และเครือข่ายของวิทยาลัยนวัตกรรมสื่อสารสังคม โดยมีรายละเอียดทรัพยากรหลัก ดังนี้

- ฮาร์ดแวร์: Server ระบบสารสนเทศ 3 เครื่อง, NAS Server 1 เครื่อง, คอมพิวเตอร์ห้องปฏิบัติการ 295 เครื่อง, คอมพิวเตอร์บุคลากร 70 เครื่อง
- ซอฟต์แวร์: ระบบยืมคืนครุภัณฑ์ ระบบฝึกงาน ระบบ KPIs และระบบสารสนเทศอื่นๆ
- ข้อมูล: ข้อมูลนิสิต 500 คน ข้อมูลบุคลากร 70 คน ข้อมูลครุภัณฑ์ ข้อมูลการฝึกงาน ข้อมูล KPIs

3. ผู้รับผิดชอบ

นักวิชาการคอมพิวเตอร์ ฝ่ายไอที วิทยาลัยนวัตกรรมสื่อสารสังคม เป็นผู้รับผิดชอบหลักในการดำเนินการตามกฎเกณฑ์ฉบับนี้ และรายงานต่อผู้ช่วยคณบดีฝ่ายเทคโนโลยีสารสนเทศ

4. มาตรการความมั่นคงปลอดภัยไซเบอร์ตามกรอบ NIST CSF 2.0

รายละเอียดมาตรการที่ฝ่ายไอทีต้องปฏิบัติแยกตามองค์ประกอบของ NIST Cybersecurity Framework 2.0 แสดงในตารางต่อไปนี้

คุณสมบัติ	มาตรการ	ผู้รับผิดชอบ
Identify (ระบุ)	1. จัดทำและปรับปรุงทะเบียนทรัพย์สินด้านไอที (Asset Inventory) • ฮาร์ดแวร์: Server ระบบสารสนเทศ 3 เครื่อง, NAS Server 1 เครื่อง, คอมพิวเตอร์ห้องปฏิบัติการ 295 เครื่อง, คอมพิวเตอร์บุคลากร 70 เครื่อง • ซอฟต์แวร์: ระบบยืมคืนครุภัณฑ์ ระบบฝึกงาน ระบบ KPIs และระบบสารสนเทศอื่นๆ ของวิทยาลัย • ข้อมูล: ข้อมูลส่วนตัวนิสิต 500 คน ข้อมูลบุคลากร 70 คน ข้อมูลครุภัณฑ์ ข้อมูลการฝึกงาน ข้อมูล KPIs ของบุคลากร 2. ประเมินความเสี่ยงด้านไซเบอร์ของระบบสารสนเทศและทรัพย์สินทุกรายการอย่างน้อยปีละ 1 ครั้ง 3. จัดทำแผนผังเครือข่าย (Network Diagram) และผังการไหลของข้อมูล (Data Flow Diagram) ให้เป็นปัจจุบัน 4. ระบุบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์	นักวิชาการคอมพิวเตอร์
Protect (ป้องกัน)	1. ควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) แบ่งสิทธิ์ตามบทบาทหน้าที่ (Role-based Access Control) 2. ป้องกันข้อมูลด้วยการเข้ารหัส (Encryption) • ระบบสารสนเทศที่พัฒนาขึ้นมีการเข้ารหัสผ่านแบบ Hashing ด้วยอัลกอริทึม Bcrypt ผสม salt แบบสุ่ม • ระบบสารสนเทศที่เผยแพร่ใช้งานผ่านอินเทอร์เน็ตในรูปแบบเว็บแอปพลิเคชันต้องเข้ารหัสผ่าน SSL/TLS 3. ติดตั้งและปรับปรุงโปรแกรมป้องกันมัลแวร์ (Antivirus/Endpoint Protection) บนเครื่องคอมพิวเตอร์ทุกเครื่อง 4. ปรับปรุงแพตช์ของระบบปฏิบัติการและซอฟต์แวร์ (Patch Management) อย่างสม่ำเสมอ 5. กำหนดนโยบายรหัสผ่าน (Password Policy) ขั้นต่ำ 8 ตัวอักษร ผสมตัวอักษรใหญ่ เล็ก ตัวเลข และเปลี่ยนทุก 6 เดือน	นักวิชาการคอมพิวเตอร์

คุณสมบัติ	มาตรการ	ผู้รับผิดชอบ
	6. จัดอบรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรอย่างน้อยปีละ 1 ครั้ง	
Detect (ตรวจจับ)	1. รวบรวมและตรวจสอบเหตุการณ์ที่เกิดขึ้นจาก Server โดยดูจาก log ไฟล์ 2. ตั้งค่า Alert ผ่านอีเมลเมื่อมีการ login ผิดปกติในจำนวนครั้งมากกว่า 5 ครั้ง 3. ตรวจสอบการใช้งานทรัพยากร CPU, RAM, Disk และเครือข่ายของ Server อย่างต่อเนื่อง 4. ตรวจสอบการเข้าถึงระบบสารสนเทศจาก IP ที่ผิดปกติหรือพื้นที่ที่ไม่ได้รับอนุญาต 5. จัดทำรายงานเหตุการณ์ที่ตรวจพบเสนอผู้บริหารทุก 1 เดือน	นักวิชาการคอมพิวเตอร์
Respond (ตอบสนอง)	ขั้นตอนการตอบสนองเหตุการณ์ภัยคุกคามไซเบอร์: 1. ระบุและจำแนกประเภทภัยคุกคาม (Threat Identification & Classification) 2. แยกระบบที่ถูกโจมตีออกจากเครือข่าย (Containment & Isolation) 3. แจ้งผู้เกี่ยวข้องและผู้บริหารโดยทันที พร้อมจัดทำบันทึกเหตุการณ์ 4. เริ่มกระบวนการกู้คืนข้อมูลและระบบ 5. วิเคราะห์สาเหตุของเหตุการณ์ (Root Cause Analysis) และจัดทำรายงานสรุป	นักวิชาการคอมพิวเตอร์
Recover (กู้คืน)	การกู้คืนและสำรองข้อมูลจากส่วนฐานข้อมูลของระบบสารสนเทศ และไฟล์เอกสาร โดยจัดเก็บ 3 รูปแบบ: 1) Cloud-based ผ่าน Google Drive ในรูปแบบฐานข้อมูลและไฟล์เอกสารแบบ Google Business Standard licensed โดเมน cosciswu.com 2) NAS Server ของวิทยาลัยฯ สำหรับเก็บในรูปแบบฐานข้อมูลและไฟล์เอกสาร 3) Portable HD drive สำหรับเก็บไฟล์เอกสารรายบุคคล เนื่องจากไฟล์ฐานข้อมูลมีขนาดไม่ใหญ่มาก จึงเลือกจัดเก็บแบบ Full backup เก็บทั้งหมด และ Incremental backup เฉพาะส่วนที่มีการเปลี่ยนแปลง 4. ทดสอบการกู้คืนข้อมูล (Restore Test) อย่างน้อยปีละ 2 ครั้ง เพื่อยืนยันความถูกต้องของข้อมูลสำรอง 5. ปรับปรุงแผนการกู้คืน (Disaster Recovery Plan) เมื่อมีการเปลี่ยนแปลงระบบหรือมีเหตุการณ์สำคัญ	นักวิชาการคอมพิวเตอร์

5. ตารางสรุปกิจกรรมและความถี่ในการปฏิบัติงาน

เพื่อให้การดำเนินงานเป็นไปอย่างต่อเนื่องและตรวจสอบได้

ฝ่ายไอทีกำหนดกิจกรรมหลักและความถี่การปฏิบัติงาน ดังนี้

ลำดับ	กิจกรรม / มาตรการ	ความถี่	เอกสาร / หลักฐาน
1	ปรับปรุงทะเบียนทรัพย์สินด้านไอที (ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล)	ทุก 6 เดือน	ทะเบียนทรัพย์สินไอที
2	ประเมินความเสี่ยงด้านไซเบอร์ของระบบสารสนเทศ	ปีละ 1 ครั้ง	รายงานการประเมินความเสี่ยง
3	ปรับปรุงแพตช์ระบบปฏิบัติการและซอฟต์แวร์	ทุกเดือน	บันทึก Patch Log
4	ตรวจสอบ log ไฟล์ Server และตั้งค่า Alert	ทุกวัน	Log file & Alert report
5	สำรองข้อมูล Full backup	ทุกสัปดาห์	บันทึก Backup Log
6	สำรองข้อมูล Incremental backup	ทุกวัน	บันทึก Backup Log
7	ทดสอบการกู้คืนข้อมูล (Restore Test)	ปีละ 2 ครั้ง	รายงานผลการทดสอบ
8	ตรวจสอบและทบทวนสิทธิ์การเข้าถึงระบบ (Access Review)	ทุก 6 เดือน	รายงาน Access Review
9	อบรมให้ความรู้ด้านไซเบอร์แก่บุคลากร	ปีละ 1 ครั้ง	เอกสารการอบรม
10	ทบทวนแผนกู้คืนระบบ (DRP)	ปีละ 1 ครั้ง	เอกสาร DRP ฉบับล่าสุด
11	รายงานสถานะความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหาร	ทุกเดือน	รายงานเสนอผู้บริหาร

6. การรายงานและการทบทวน

- นักวิชาการคอมพิวเตอร์ต้องจัดทำรายงานสถานะระบบไอทีและเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์เสนอผู้บริหารทุกเดือน

- ทบทวนกฎเกณฑ์ฉบับนี้อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ เช่น การเปลี่ยนระบบสารสนเทศ การเกิดเหตุการณ์ภัยคุกคามที่กระทบต่อระบบ
- เก็บบันทึกหลักฐานการปฏิบัติงานทุกกิจกรรมเป็นระยะเวลาอย่างน้อย 3 ปี เพื่อใช้ในการตรวจประเมินคุณภาพและตรวจสอบภายใน

7. บทลงโทษและการบังคับใช้

กรณีที่นักวิชาการคอมพิวเตอร์ไม่สามารถปฏิบัติตามกฎเกณฑ์ฉบับนี้ได้ ให้รายงานเหตุผลและแนวทางแก้ไขต่อผู้ช่วยคณบดีฝ่ายเทคโนโลยีสารสนเทศโดยทันที เพื่อพิจารณาแนวทางและทรัพยากรเพิ่มเติม การไม่ปฏิบัติตามโดยไม่มีเหตุอันควร อาจส่งผลต่อการประเมิน KPIs ตามระเบียบของวิทยาลัยและมหาวิทยาลัย

ลงชื่อ .....

(**สิทธิชัย วรโชติกำจร**)

ผู้ช่วยคณบดีฝ่ายเทคโนโลยีสารสนเทศ

วันที่ 8 / 5 / 69