ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย

เอกสารนี้ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย จัดทำขึ้นตามประกาศสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๘ ซึ่งกำหนดให้หน่วยงานของรัฐ ต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และกำหนดแนวทางตามที่กฎหมายกำหนด ในการจัดทำโดยละเอียด มีรายละเอียดครอบคลุม ๕ มิติหลัก คือ Identify, Protect, Detect, Respond, Recover โดยแบ่งขอบเขตการดำเนินงานเป็น ๔ ส่วน ดังนี้

ส่วนที่ ๑ การระบุและการบริหารความเสี่ยง (Identify & Governance)

ส่วนที่ ๒ การป้องกัน (Protect)

ส่วนที่ ๓ การตรวจจับและตอบสนอง (Detect & Respond)

ส่วนที่ ๔ การรักษาและฟื้นฟู (Recover)

แต่ละส่วนมีรายละเอียดดังนี้

ส่วนที่ ๑ การระบุและการบริหารความเสี่ยง (Identify & Governance)

ส่วนนี้เป็นกระบวนการพื้นฐานในการกำกับดูแลและบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มหาวิทยาลัยมีความเข้าใจในบริบทของทรัพย์สิน ความเสี่ยง และกฎระเบียบที่เกี่ยวข้อง ก่อนที่จะนำไปสู่การวางมาตรการป้องกันทางเทคนิค

๑.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit)

เพื่อให้มั่นใจว่าระบบสารสนเทศและการดำเนินงานของมหาวิทยาลัยสอดคล้องกับกฎหมาย นโยบาย และมาตรฐานที่กำหนด

ความถี่ในการตรวจสอบ มหาวิทยาลัยกำหนดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ในเดือนกันยายน ก่อนสิ้นปีงบประมาณ หรือเมื่อมีการปรับปรุงระบบอย่างมีนัยสำคัญ

คุณสมบัติผู้ตรวจสอบ มหาวิทยาลัยมอบหมายให้สำนักงานตรวจสอบภายใน เป็นหน่วยงานตรวจสอบภายใน (Internal Audit) ของมหาวิทยาลัย หรืออาจแต่งตั้งผู้ตรวจสอบภายนอกที่มีใบรับรองมาตรฐานวิชาชีพ (เช่น CISA, CISSP) และต้องไม่มีส่วนได้ส่วนเสียกับระบบที่ถูกตรวจสอบ

ขอบเขตการตรวจสอบ ครอบคลุม "บริการที่สำคัญ" (Critical Services) ของมหาวิทยาลัย ประกอบด้วย ระบบทะเบียนนิสิต ระบบบริหารจัดการการเงินการคลัง และระบบการเรียนการสอนออนไลน์ โดยตรวจสอบทั้งด้านเทคนิค (Technical Audit) และด้านกระบวนการ (Process Audit)

การรายงานผล ผู้ตรวจสอบต้องจัดทำรายงานผลการตรวจสอบ ระบุสิ่งที่ตรวจพบ (Findings) ระดับความเสี่ยง และข้อเสนอแนะ เพื่อเสนอต่อผู้บริหารมหาวิทยาลัยและดำเนินการแก้ไข (Remediation) ภายในระยะเวลาที่กำหนด

๑.๒ การประเมินความเสี่ยง (Risk Assessment)

เพื่อให้มหาวิทยาลัยทราบถึงโอกาส ผลกระทบของภัยคุกคาม และจัดลำดับความสำคัญในการจัดสรรงบประมาณและทรัพยากร โดยการประเมินความเสี่ยง ดังนี้

การกำหนดเกณฑ์ความเสี่ยง (Risk Criteria) มหาวิทยาลัย กำหนด "ระดับความเสี่ยงที่ยอมรับได้" (Risk Appetite) เพื่อใช้เป็นเกณฑ์ในการตัดสินใจ โดยระดับความเสี่ยงขึ้นอยู่กับ แนวโน้มหรือโอกาสที่จะเกิดเหตุการณ์ภัยคุกคามกับช่องโหว่ของทรัพย์สิน และผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ภัยคุกคาม ดังตารางที่ ๑ และตารางที่ ๒

ตารางที่ ๑ ระดับแนวโน้มหรือโอกาสที่อาจเกิดขึ้น

ระดับ/ความเสี่ยง	ความถี่	ความน่าจะเป็น (ในการเกิดเหตุการณ์)
สูง	มีแนวโน้มที่จะเกิดขึ้นเป็นประจำหรือบ่อยครั้ง	น่าจะเกิดขึ้น
ปานกลาง	อาจเกิดขึ้นได้ แต่ไม่บ่อยนัก	อาจเกิดขึ้นได้
ต่ำ	เกิดขึ้นได้ยาก ไม่น่าจะเกิดขึ้นมากนัก	ไม่น่าจะเกิดขึ้น

ตารางที่ ๒ ระดับผลกระทบที่อาจเกิดขึ้น

ระดับ/ความเสี่ยง	ผลกระทบทางการเงิน	ผลกระทบจากการดำเนินงาน	ผลกระทบต่อชื่อเสียง	ผลกระทบต่อผู้รับบริการ
สูง	ผลกระทบทางการเงินรุนแรง	มีการหยุดชะงักในการปฏิบัติงานอย่างรุนแรง	มีผลกระทบต่อชื่อเสียงอย่างรุนแรง	มีผลกระทบต่อผู้รับบริการอย่างรุนแรง
ปานกลาง	ผลกระทบทางการเงินปานกลาง	มีการหยุดชะงักในการปฏิบัติงานปานกลาง	มีผลกระทบต่อชื่อเสียงปานกลาง	มีผลกระทบต่อผู้รับบริการปานกลาง
ต่ำ	ผลกระทบทางการเงินน้อยที่สุด	มีการหยุดชะงักในการปฏิบัติงานน้อยที่สุด	มีผลกระทบต่อชื่อเสียงน้อยที่สุด	มีผลกระทบต่อผู้รับบริการน้อยที่สุด

ขั้นตอนการประเมิน

ระบุความเสี่ยง (Identification) ระบุภัยคุกคาม เช่น Ransomware ข้อมูลรั่วไหลที่อาจเกิดกับทรัพย์สินสารสนเทศ

วิเคราะห์ความเสี่ยง (Analysis) ประเมินโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ต่อการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูล

ประเมินค่าความเสี่ยง (Evaluation) จัดลำดับความสำคัญของความเสี่ยงตามระดับความรุนแรง (สูง กลาง ต่ำ)

โดยระดับความเสี่ยงที่มหาวิทยาลัยยอมรับได้ คือระดับต่ำ โดยมีคำอธิบายเกณฑ์ ดังตารางที่ ๓

ตารางที่ ๓ ระดับความเสี่ยงที่ยอมรับได้

ระดับ/ความเสี่ยง	คำอธิบายระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Description)
สูง	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ต้องดำเนินการตามกลยุทธ์การลดความเสี่ยงหรือเลือกโอนความเสี่ยงในทันที
ปานกลาง	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ หน่วยงานควรมีการดำเนินการตอบสนองความเสี่ยงภายใน ๓ - ๖ เดือน
ต่ำ	ความเสี่ยงระดับนี้สามารถยอมรับได้ แต่จะต้องติดตามความเสี่ยงเป็นระยะ เพื่อให้แน่ใจว่า มีการตรวจพบการเปลี่ยนแปลงของสถานการณ์เพื่อที่จะดำเนินการอย่างเหมาะสม

การจัดการความเสี่ยง (Risk Treatment) สำหรับความเสี่ยงที่เกินระดับที่ยอมรับได้ ต้องจัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan) โดยเลือกใช้วิธี ยอมรับ (Accept) หลีกเลี่ยง (Avoid) ถ่ายโอน (Transfer) หรือลดความเสี่ยง (Mitigate)

๑.๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan IRP)

เพื่อให้มีกรอบการทำงานและโครงสร้างการสั่งการที่ชัดเจนเมื่อเกิดเหตุภัยคุกคาม

โครงสร้างทีมตอบสนอง (CIRT Structure) มหาวิทยาลัยจัดตั้งหน่วยประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของมหาวิทยาลัย หรือทีม CIRT ณ ส่วนเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการบำรุงรักษาและปฏิบัติการเกี่ยวกับโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ รวมถึงเครือข่ายและแอปพลิเคชันที่สนับสนุนการทำงานของระบบต่าง ๆ ในมหาวิทยาลัย เป็นที่ปรึกษาให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคแก่หน่วยงาน ผู้บริหารและบุคลากร ในกรณีที่ระบบถูกบุกรุก โครงสร้างทีมตอบสนองได้แก่

๑. ผู้อำนวยการสำนักหอสมุดและเทคโนโลยีสารสนเทศ เป็นผู้บัญชาการเหตุการณ์ (Incident Commander)

๒. ทีมวิเคราะห์ (Analyst) และทีมสื่อสาร (Communication) ประกอบด้วย

(๑) ผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ
(๒) รองผู้อำนวยการส่วนเทคโนโลยีสารสเทศ
(๓) นายศรี แก้วงาม นักวิชาการคอมพิวเตอร์ชำนาญการ
(๔) นายนพดล เพ็ญประชุม นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๕) นายฐิติวัฒน์ หวังสุขใจ นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๖) นายอรรถพล อิ่มวิไลวรรณ นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๗) นายปัญญา นราพันธ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ
(๘) นางสาวณรัชต์หทัย ทองสุข นักวิชาการคอมพิวเตอร์ปฏิบัติการ

กระบวนการแจ้งเหตุ (Reporting) มหาวิทยาลัยกำหนดช่องทางและขั้นตอนการรายงานเหตุผิดปกติ ทั้งจากบุคลากร นิสิต และบุคคลภายนอก รวมถึงกำหนดเกณฑ์การรายงานไปยังหน่วยงานกำกับดูแล เช่น สกมช. กรณีเกิดเหตุร้ายแรง โดยแจ้งเหตุการณ์ที่ส่วนเทคโนโลยีสารสนเทศ ทั้งนี้ส่วนเทคโนโลยีสารสนเทศดำเนินการรายงานผู้บริหารของมหาวิทยาลัยและหน่วยงานกำกับดูแลตามลักษณะเหตุการณ์

ขั้นตอนการปฏิบัติงาน (SOP) ส่วนเทคโนโลยีสารสนเทศ จัดทำคู่มือปฏิบัติงานมาตรฐาน (Standard Operating Procedures) สำหรับรับมือภัยคุกคามแต่ละประเภทที่พบบ่อย อาทิ กรณีติดมัลแวร์ กรณีเว็บถูกโจมตี (Defacement) หรือกรณีข้อมูลส่วนบุคคลรั่วไหล เผยแพร่ไว้ ณ เว็บไซต์ของส่วนงาน

๑.๔ การจัดการทรัพย์สินสารสนเทศ (Asset Management)

เพื่อให้ทราบสถานะและตำแหน่งของทรัพย์สินสารสนเทศทั้งหมด ซึ่งเป็นพื้นฐานสำคัญของการป้องกัน

ทะเบียนทรัพย์สิน (Asset Inventory) ส่วนเทคโนโลยีสารสนเทศ ประสานกองพัสดุและทรัพย์สินในการจัดทำฐานข้อมูลทรัพย์สินสารสนเทศที่ครอบคลุม ฮาร์ดแวร์ (Server PC) ซอฟต์แวร์ (License Version) และข้อมูล (Data) ตามมาตรฐานทะเบียนทรัพย์สินของมหาวิทยาลัย

การจัดลำดับความสำคัญ (Classification)) ส่วนเทคโนโลยีสารสนเทศ ประสานกองพัสดุและทรัพย์สินในการจัดกลุ่มทรัพย์สินตามระดับความสำคัญต่อพันธกิจของมหาวิทยาลัย (Criticality) และตามชั้นความลับของข้อมูล (Data Classification) เพื่อกำหนดมาตรการป้องกันที่เหมาะสมกับแต่ละระดับ

การทบทวน (Review)) ส่วนเทคโนโลยีสารสนเทศ ประสานกองพัสดุและทรัพย์สินในการดำเนินการตรวจสอบความถูกต้องของทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน

๑.๕ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment & Penetration Testing)

เพื่อค้นหาจุดอ่อนทางเทคนิคในเชิงรุก ก่อนที่จะถูกผู้ไม่หวังดีใช้ประโยชน์

การประเมินช่องโหว่ (Vulnerability Assessment) ส่วนเทคโนโลยีสารสนเทศดำเนินการสแกนหาช่องโหว่ของระบบปฏิบัติการ ซอฟต์แวร์ และอุปกรณ์เครือข่าย อย่างสม่ำเสมอ ทุกไตรมาส และหรือทุกครั้งที่มีการติดตั้งระบบใหม่ เพื่อระบุและจัดการ Patch ความปลอดภัย

การทดสอบเจาะระบบ (Penetration Testing) ส่วนเทคโนโลยีสารสนเทศประสานดำเนินการทดสอบเจาะระบบสำหรับ "บริการที่สำคัญ" และระบบที่เชื่อมต่อกับอินเทอร์เน็ตสาธารณะ อย่างน้อยปีละ ๑ ครั้ง โดยผู้เชี่ยวชาญที่มีคุณสมบัติเหมาะสม เพื่อจำลองสถานการณ์การโจมตีเสมือนจริง

การแก้ไขและติดตามผล (Remediation) เมื่อพบช่องโหว่ ส่วนเทคโนโลยีสารสนเทศนำเข้าสู่กระบวนการจัดการความเสี่ยงและดำเนินการแก้ไขตามกรอบเวลาที่กำหนดตามระดับความรุนแรง

๑.๖ การจัดการผู้ให้บริการภายนอก (Third-Party Management)

เนื่องจากมหาวิทยาลัยมีการใช้บริการจากภายนอก (Outsource/Cloud) จึงต้องมีการบริหารจัดการความเสี่ยงที่เกี่ยวข้อง ๓ ประการ คือ

การคัดเลือกและประเมิน (Due Diligence) ก่อนการจัดจ้าง ต้องประเมินความมั่นคงปลอดภัยของผู้ให้บริการ ว่ามีมาตรฐานสอดคล้องกับนโยบายของมหาวิทยาลัยหรือไม่

ข้อตกลงระดับการให้บริการ (SLA & Contracts) ต้องระบุเงื่อนไขด้านความมั่นคงปลอดภัยในสัญญาจ้าง หรือข้อตกลงการใช้บริการ (TOR) ได้แก่ การรักษาความลับข้อมูลนิสิต การแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล และสิทธิของมหาวิทยาลัยในการตรวจสอบ (Audit Rights)

การควบคุมการเข้าถึง (Access Control) หากผู้ให้บริการจำเป็นต้องเข้าถึงระบบภายในมหาวิทยาลัย ต้องจำกัดสิทธิการเข้าถึงเท่าที่จำเป็น (Least Privilege) มีการกำหนดระยะเวลาเข้าถึงที่ชัดเจน และมีการบันทึกตรวจสอบการทำงาน (Log) ของผู้ให้บริการอย่างเคร่งครัด

ส่วนที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

มหาวิทยาลัย วางมาตรการควบคุมทางเทคนิคและกระบวนการปฏิบัติงาน เพื่อลดช่องทางที่ผู้ไม่หวังดีใช้เป็นช่องทางในการโจมตี (Attack Surface) และปกป้องทรัพย์สินสารสนเทศของมหาวิทยาลัยจากการเข้าถึงโดยไม่ได้รับอนุญาต ได้แก่ การจัดการการควบคุมการเข้าถึง การทำระบบให้มีความแข็งแกร่ง การจัดการการเชื่อมต่อระยะไกล การจัดการสื่อเก็บข้อมูลแบบถอดได้ และการแบ่งปันข้อมูล

๒.๑ การจัดการการควบคุมการเข้าถึง (Access Control)

เพื่อให้มั่นใจว่าเฉพาะผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงระบบสารสนเทศและข้อมูลสำคัญของมหาวิทยาลัยได้ จึงกำหนดการจัดการการควบคุมการเข้าถึงตามหลักการสิทธิเท่าที่จำเป็น การพิสูจน์ตัวตนแบบหลายปัจจัย การบริหารจัดการบัญชีผู้ใช้งาน และนโยบายรหัสผ่าน

หลักการสิทธิเท่าที่จำเป็น (Least Privilege) มหาวิทยาลัยออกประกาศกำหนดสิทธิการใช้งานระบบสารสนเทศให้แก่บุคลากรและนิสิต ตามความจำเป็นของหน้าที่ความรับผิดชอบเท่านั้น ห้ามมิให้สิทธิเกินความจำเป็น

การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) มหาวิทยาลัยออกประกาศบังคับใช้ MFA สำหรับการเข้าถึงระบบที่สำคัญ (Critical Services) และสำหรับบัญชีผู้ดูแลระบบ (Administrator) เพื่อป้องกันการถูกขโมยรหัสผ่าน

การบริหารจัดการบัญชีผู้ใช้งาน (User Access Management) ต้องมีกระบวนการสร้าง ปรับปรุง และยกเลิกสิทธิ (Joiners Movers Leavers) ที่รวดเร็ว โดยเฉพาะเมื่อบุคลากรลาออกหรือนิสิตพ้นสภาพ โดยกำหนดให้ผู้ดูแลระบบทบทวนสิทธิการใช้งาน (Access Review) อย่างน้อยปีละ ๑ ครั้ง เพื่อเพิกถอนสิทธิที่ไม่จำเป็น

นโยบายรหัสผ่าน (Password Policy) กำหนดความยาวและความซับซ้อนของรหัสผ่านตามมาตรฐานสากล และห้ามใช้รหัสผ่านที่คาดเดาได้ง่าย

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

เพื่อลดช่องโหว่ของอุปกรณ์และซอฟต์แวร์ที่ใช้ในมหาวิทยาลัย โดยการปิดจุดอ่อนที่มาพร้อมกับการตั้งค่าเริ่มต้น

กำหนดมาตรฐานการตั้งค่า (Security Baseline) มหาวิทยาลัยต้องจัดทำมาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำสำหรับระบบปฏิบัติการ (OS) เว็บเซิร์ฟเวอร์ และอุปกรณ์เครือข่าย โดยอ้างอิงมาตรฐานสากล เช่น CIS Benchmarks หรือ NIST

การปิดบริการที่ไม่จำเป็น ดำเนินการปิดพอร์ต (Port) บริการ (Services) และบัญชีผู้ใช้เริ่มต้น (Default Accounts) ที่ไม่ได้ใช้งานออกจากระบบ เพื่อลดโอกาสในการถูกโจมตี

การจัดการแพตช์ (Patch Management) ต้องดำเนินการติดตั้งแพตช์ความมั่นคงปลอดภัยให้กับระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ โดยเฉพาะแพตช์ระดับวิกฤต (Critical) ต้องดำเนินการภายในระยะเวลาที่กำหนด เช่น ภายใน ๔๘ ชั่วโมง หรือ ๗ วัน ตามระดับความเสี่ยง

๒.๓ การจัดการการเชื่อมต่อระยะไกล (Remote Connection)

เพื่อรองรับการทำงานและการเรียนการสอนจากนอกสถานที่ (Work from Home / Remote Learning) อย่างปลอดภัย

ช่องทางเชื่อมต่อที่ปลอดภัย (Secure Channel) การเข้าถึงระบบภายในมหาวิทยาลัยจากภายนอก ต้องทำผ่านช่องทางที่มีการเข้ารหัส เช่น VPN (Virtual Private Network) หรือเทคโนโลยี Zero Trust

การตรวจสอบอุปกรณ์ (Endpoint Compliance) ก่อนอนุญาตให้เชื่อมต่อ ต้องมีการตรวจสอบความปลอดภัยของอุปกรณ์ปลายทาง เช่น ต้องติดตั้ง Antivirus และอัปเดต OS เป็นเวอร์ชันปัจจุบัน

การควบคุมอุปกรณ์ส่วนตัว (BYOD) หากอนุญาตให้ใช้อุปกรณ์ส่วนตัวของบุคลากรหรือนิสิตเข้าถึงระบบสำคัญ ต้องมีมาตรการควบคุม เช่น การแยกเครือข่ายสำหรับ BYOD หรือการใช้เทคโนโลยี Virtual Desktop Infrastructure (VDI)

๒.๔ การจัดการสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

เพื่อป้องกันมัลแวร์ที่แพร่กระจายผ่าน USB Drive และป้องกันข้อมูลรั่วไหล

การสแกนความปลอดภัย ส่วนเทคโนโลยีสารสนเทศกำหนดให้ผู้ใช้มีการสแกนไวรัสและมัลแวร์ในสื่อบันทึกข้อมูลแบบถอดได้ เช่น Flash Drive External HDD ทุกครั้งก่อนใช้งานกับคอมพิวเตอร์ของมหาวิทยาลัย

การปิดระบบเล่นอัตโนมัติ (Disable Auto-run) ส่วนเทคโนโลยีสารสนเทศแนะนำให้ผู้ใช้ตั้งค่าเครื่องคอมพิวเตอร์ในสำนักงานและห้องปฏิบัติการให้ปิดการทำงานของ Auto-run/Auto-play เพื่อป้องกันการรันสคริปต์อันตรายโดยอัตโนมัติ

การเข้ารหัสข้อมูล (Encryption) หากจำเป็นต้องบันทึกข้อมูลความลับหรือข้อมูลส่วนบุคคลลงในสื่อแบบถอดได้ ส่วนเทคโนโลยีสารสนเทศแนะนำให้ผู้ใช้ต้องดำเนินการเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันกรณีอุปกรณ์สูญหาย

๒.๕ การแบ่งปันข้อมูล (Information Sharing)

เพื่อสร้างความร่วมมือและแลกเปลี่ยนข้อมูลภัยคุกคามกับเครือข่ายภายนอก เช่น เครือข่ายมหาวิทยาลัย Uni-CERT หรือ สกมช.

กำหนดชั้นความลับข้อมูล (Traffic Light Protocol - TLP) ใช้มาตรฐาน TLP (Red Amber Green Clear) ในการระบุขอบเขตการเผยแพร่ข้อมูลภัยคุกคาม เพื่อให้ผู้รับข้อมูลทราบว่าสามารถส่งต่อข้อมูลได้แค่ไหน

การปกป้องข้อมูลอ่อนไหว ก่อนแบ่งปันข้อมูลภัยคุกคาม (Threat Intelligence) ออกสู่ภายนอก ต้องดำเนินการลบหรือปกปิดข้อมูลส่วนบุคคล (PII) หรือข้อมูลความลับของมหาวิทยาลัย (Anonymization) ออกก่อน

ช่องทางการแบ่งปัน กำหนดช่องทางและผู้รับผิดชอบในการรับ-ส่งข้อมูลภัยคุกคามกับหน่วยงานภายนอกอย่างเป็นทางการ เพื่อความรวดเร็วในการรับมือเหตุการณ์

ส่วนที่ ๓ การตรวจจับและตอบสนอง (Detect & Respond)

มหาวิทยาลัยให้ความสำคัญอย่างยิ่งในการตรวจจับและตอบสนอง มีความ "รู้ตัว" เมื่อถูกโจมตี และสามารถ "สื่อสาร" เพื่อควบคุมสถานการณ์ รวมถึง "ฝึกซ้อม" เพื่อเตรียมความพร้อมอยู่เสมอ โดยกำหนด

มาตรการติดตามเฝ้าระวังภัยคุกคาม การจัดทำกระบวนการสื่อสารในภาวะวิกฤติ และการฝึกซ้อมความปลอดภัยไซเบอร์

๓.๑ การสร้างมาตรการเฝ้าติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Monitoring & Detection)

เพื่อให้มหาวิทยาลัยมีกลไกในการตรวจจับความผิดปกติที่เกิดขึ้นกับระบบสารสนเทศและบริการที่สำคัญได้ทันท่วงที โดย

การบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ (Log Management) ได้แก่

การเก็บรักษา (Logging) ส่วนเทคโนโลยีสารสนเทศกำหนดแนวทางปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files) จากอุปกรณ์แม่ข่าย (Server) อุปกรณ์เครือข่าย (Network Device) และ applications สำคัญ ให้ครบถ้วนตามกฎหมายและมาตรฐานความปลอดภัย อย่างน้อย ๙๐ วัน

การรวมศูนย์ข้อมูล (Centralized Log) ส่วนเทคโนโลยีสารสนเทศกำหนดแนวทางปฏิบัติในการนำ Log จากระบบที่สำคัญมารวมศูนย์ที่ระบบบริหารจัดการข้อมูล เพื่อให้ง่ายต่อการวิเคราะห์และป้องกันการถูกลบทำลายโดยผู้โจมตี

การเฝ้าระวังเหตุการณ์ (Security Monitoring) ได้แก่

เครื่องมือตรวจจับ (Detection Tools) ส่วนเทคโนโลยีสารสนเทศดำเนินการติดตั้งและเปิดใช้งานระบบตรวจจับการบุกรุก (IDS/IPS) และระบบป้องกันมัลแวร์ (Anti-malware) ที่ทันสมัย เพื่อดักจับภัยคุกคามที่รู้จัก (Known Threats)

ศูนย์เฝ้าระวัง (SOC) จัดให้มีเจ้าหน้าที่หรือศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operations Center SOC) ทำหน้าที่เฝ้าระวังและวิเคราะห์การแจ้งเตือน (Alerts) ตลอด ๒๔ ชั่วโมง หรือในช่วงเวลาทำการตามความเหมาะสมของความเสี่ยง

กระบวนการคัดแยกเหตุการณ์ (Incident Triage) กำหนดกระบวนการวิเคราะห์เพื่อแยกแยะระหว่าง "เหตุการณ์ทั่วไป" (Event) กับ "ภัยคุกคามทางไซเบอร์" (Incident) เพื่อลดการแจ้งเตือนที่ผิดพลาด (False Positive) และส่งต่อเรื่องให้ทีมตอบสนองได้ถูกต้อง

๓.๒ การจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

เพื่อให้การสื่อสารในช่วงเวลาวิกฤตเป็นไปอย่างมีเอกภาพ ลดความสับสน ข่าวลือ และความตื่นตระหนกของนิสิต บุคลากร และสาธารณชน

ทีมสื่อสารภาวะวิกฤต (Crisis Communication Team) แต่งตั้งทีมงานเฉพาะกิจประกอบด้วย ผู้บริหารฝ่ายสื่อสารองค์กร ฝ่ายกฎหมาย ฝ่ายไอที และผู้บริหารระดับสูง เพื่อร่วมกันกำหนดทิศทางการสื่อสาร

โฆษกประจำเหตุการณ์ (Spokesperson) กำหนดตัวบุคคล ได้แก่รองอธิการบดีฝ่ายประชาสัมพันธ์และเผยแผ่ ซึ่งกำกับดูแลงานด้านเทคโนโลยีสารสนเทศ ให้ทำหน้าที่เป็นผู้ให้ข่าวสารอย่างเป็นทางการ เพื่อความถูกต้องและน่าเชื่อถือของข้อมูล

ช่องทางการสื่อสาร (Communication Channels) ได้แก่

ภายใน กำหนดช่องทางแจ้งเตือนบุคลากรและนิสิต ผ่านสื่อภายในของมหาวิทยาลัย

ภายนอก กำหนดช่องทางแถลงข่าวต่อสื่อมวลชนและสาธารณะ ผ่านเว็บไซต์หลักและ Social Media ทางการของมหาวิทยาลัย

การเตรียมข้อความ (Prepared Messages) จัดทำร่างแถลงการณ์ (Templates) สำหรับสถานการณ์ต่าง ๆ ไว้ล่วงหน้า เช่น กรณีระบบล่ม กรณีข้อมูลรั่วไหล เพื่อความรวดเร็วในการสื่อสารเมื่อเกิดเหตุจริง

๓.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

เพื่อให้มั่นใจว่าบุคลากรเข้าใจบทบาทหน้าที่ และแผนงานที่วางไว้สามารถนำมาปฏิบัติได้จริงเมื่อเกิดเหตุ

ความถี่ในการฝึกซ้อม มหาวิทยาลัยกำหนดจัดให้มีการฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละ ๑ ครั้ง

รูปแบบการฝึกซ้อม

การฝึกซ้อมบนโต๊ะ (Tabletop Exercise - TTX) เน้นการอภิปรายจำลองสถานการณ์ร่วมกันระหว่างผู้บริหารและหัวหน้างาน เพื่อทดสอบกระบวนการตัดสินใจและการประสานงาน

การฝึกซ้อมเสมือนจริง (Drill/Functional Exercise) เน้นการปฏิบัติทางเทคนิคของเจ้าหน้าที่ไอที เช่น การกู้คืนระบบจาก Backup การตัดการเชื่อมต่อเครือข่ายเมื่อพบมัลแวร์

การประเมินและปรับปรุง (Evaluation & Improvement) หลังการฝึกซ้อม ต้องมีการสรุปผล (After Action Review) เพื่อถอดบทเรียน (Lessons Learned) และนำข้อบกพร่องไปปรับปรุงแผนการรักษาความมั่นคงปลอดภัยให้ดียิ่งขึ้น

ส่วนที่ ๔ การรักษาและฟื้นฟู (Recover)

ส่วนนี้มุ่งเน้นกระบวนการกู้คืนระบบและบริการให้กลับสู่สภาวะปกติ (Resilience) โดยมีหัวใจสำคัญอยู่ที่การวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อลดผลกระทบต่อพันธกิจหลักของมหาวิทยาลัย

๔.๑ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis BIA)

ก่อนที่จะสร้างแผนฟื้นฟู มหาวิทยาลัยต้องทราบก่อนว่าระบบใด "ล่มไม่ได้" หรือ "ล่มได้นานแค่ไหน" เพื่อจัดลำดับความสำคัญในการกู้คืน

การระบุกระบวนการสำคัญ (Critical Business Functions) มหาวิทยาลัยกำหนดให้กระบวนการที่ส่งผลกระทบสูงหากหยุดชะงัก ประกอบด้วย การลงทะเบียนเรียน การประกาศเกรด การเบิกจ่ายงบประมาณ และการเรียนการสอนออนไลน์

การกำหนดค่าเป้าหมาย (Recovery Metrics) สำหรับแต่ละกระบวนการสำคัญ ต้องกำหนดค่าชี้วัด ๒ ประการ คือ

ระยะเวลาเป้าหมายในการกู้คืน (Recovery Time Objective - RTO) ระยะเวลาที่ยอมให้ระบบหยุดทำงานได้ โดยต้องกู้คืนภายใน ๘ ชั่วโมง

เป้าหมายจุดของข้อมูลที่ยอมรับให้สูญหายได้ (Recovery Point Objective - RPO) ปริมาณข้อมูลที่ยอมรับให้สูญหายย้อนหลังได้เมื่อต้องกู้คืนข้อมูล โดย ฐานข้อมูลเกรด ต้องไม่สูญหายเกิน ๑ ชั่วโมงล่าสุด หรือ Zero Data Loss

๔.๒ การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan - BCP)

เพื่อให้มหาวิทยาลัยมีขั้นตอนปฏิบัติที่ชัดเจนในการดำเนินงานต่อ ในขณะที่ระบบหลักยังไม่สามารถใช้งานได้

โครงสร้างทีมกอบกู้สถานการณ์ (Business Continuity Team) ระบุรายชื่อและเบอร์ติดต่อของคณะทำงานที่มีอำนาจตัดสินใจประกาศใช้แผน BCP (Activation) และทีมงานภาคสนามที่จะดำเนินการกู้ระบบ

กลยุทธ์ความต่อเนื่อง (Continuity Strategies) กำหนดวิธีการสำรองเมื่อเกิดวิกฤต เช่น

กรณีระบบลงทะเบียนล่ม เปิดช่องทางลงทะเบียนสำรองผ่าน Google Form หรือใช้ระบบ Manual ที่จุดบริการ One Stop Service

กรณีระบบเครือข่ายล่ม แจ้งข่าวผ่านช่องทางสื่อสารของมหาวิทยาลัย ถึงเหตุขัดข้องและประมาณการระยะเวลาในการแก้ไขปรับปรุง

แผนการกู้คืนระบบสารสนเทศ (Disaster Recovery Plan - DRP) ซึ่งเป็นส่วนย่อยของ BCP ที่เน้นด้านเทคนิค ระบุขั้นตอนทางเทคนิคในการนำระบบ Server และ Network กลับมาทำงาน (Start-up sequence) การตั้งค่า IP Address ใหม่ และการตรวจสอบความถูกต้องของข้อมูลหลังกู้คืน

๔.๓ การจัดการการสำรองข้อมูล (Backup Management)

ถือเป็นปราการด่านสุดท้ายในการกู้คืนข้อมูลหากเกิดเหตุการณ์ Ransomware หรือภัยพิบัติทางกายภาพ

หลักการสำรองข้อมูล (Backup Strategy) มหาวิทยาลัยใช้หลักการ **๓-๒-๑** ในการสำรองข้อมูลสำคัญ โดย จัดเก็บข้อมูลอย่างน้อย **๓** ชุด (ต้นฉบับ ๑ + สำรอง ๒)

เก็บในสื่อบันทึกข้อมูลต่างชนิดกันอย่างน้อย **๒** รูปแบบ (เช่น Disk และ Cloud)

เก็บข้อมูลสำรองอย่างน้อย **๑** ชุด ไว้สถานที่อื่น (Off-site) หรือในระบบที่ไม่สามารถแก้ไขได้ (Immutable Backup) เพื่อป้องกัน Ransomware

ความถี่ในการสำรองข้อมูล กำหนดรอบการสำรองข้อมูล (Daily Weekly Monthly) ให้สอดคล้องกับค่า RPO

การเข้ารหัสข้อมูลสำรอง ข้อมูลสำรองที่เก็บไว้นอกสถานที่หรือบน Cloud ต้องได้รับการเข้ารหัส (Encryption) เพื่อป้องกันข้อมูลรั่วไหลหากสื่อบันทึกข้อมูลสูญหาย

๔.๔ การทดสอบและปรับปรุงแผน (Testing and Maintenance)

เพื่อให้มั่นใจว่าแผนที่เขียนไว้สามารถใช้งานได้จริงเมื่อเกิดเหตุ (ไม่ใช่แค่กระดาษ)

การทดสอบกู้คืนข้อมูล (Restore Test) ฝ่ายไอทีต้องทำการสุ่มทดสอบการกู้คืนข้อมูลจากสื่อบันทึกข้อมูลสำรอง (Backup Media) อย่างน้อยทุก ๖ เดือน เพื่อตรวจสอบว่าไฟล์ Backup ไม่เสียหายและสามารถนำกลับมาใช้งานได้จริง

การซ้อมแผน BCP จัดให้มีการซ้อมแผนความต่อเนื่องทางธุรกิจร่วมกับหน่วยงานเจ้าของข้อมูล (Business Units) อย่างน้อยปีละ ๑ ครั้ง เพื่อดูความพร้อมของคนและกระบวนการ

การทบทวนแผน ปรับปรุงแผน BCP และบัญชีรายชื่อผู้ติดต่อให้เป็นปัจจุบันทันทีที่มีการเปลี่ยนแปลงบุคลากร หรือมีการเปลี่ยนแปลงระบบงานใหม่

ภาคผนวก

ตารางสรุปรายการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ การระบุและบริหารจัดการ (Identify & Governance)

เป้าหมาย เพื่อให้ทราบสถานะทรัพย์สิน ความเสี่ยง และการกำกับดูแล

ลำดับ	รายการตรวจสอบ (Checklist Item)	สถานะ (✓/✗)	อ้างอิง/ หมายเหตุ
๑.๑	การตรวจสอบ (Audit) มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบอิสระ (Internal/External) อย่างน้อยปีละ ๑ ครั้ง		
๑.๒	การประเมินความเสี่ยง (Risk Assessment) มีการประเมินความเสี่ยงประจำปี และรายงานผลต่อผู้บริหารระดับสูง		
๑.๓	ทะเบียนทรัพย์สิน (Asset Inventory) มีบัญชีรายชื่อ Hardware Software และ Data ที่เป็นปัจจุบัน และระบุผู้รับผิดชอบชัดเจน		
๑.๔	บริการที่สำคัญ (Critical Services) มีการระบุระบบที่สำคัญยิ่งยวด (เช่น ระบบทะเบียน, ระบบการเงิน) อย่างชัดเจน		
๑.๕	การประเมินช่องโหว่ (VA) มีการสแกนช่องโหว่ระบบปฏิบัติการและอุปกรณ์เครือข่ายอย่างสม่ำเสมอ		
๑.๖	การทดสอบเจาะระบบ (Pentest) มีการจ้างผู้เชี่ยวชาญทำ Penetration Testing ระบบสำคัญที่เชื่อมต่ออินเทอร์เน็ต อย่างน้อยปีละ ๑ ครั้ง		
๑.๗	ผู้ให้บริการภายนอก (Third-party) สัญญาจ้าง (TOR/SLA) มีข้อกำหนดด้านความปลอดภัยและสิทธิในการตรวจสอบ		

ส่วนที่ ๒ การป้องกัน (Protect)

เป้าหมาย เพื่อสร้างเกราะป้องกันทางเทคนิคและลดโอกาสถูกโจมตี

ลำดับ	รายการตรวจสอบ (Checklist Item)	สถานะ (✓/✗)	อ้างอิง/ หมายเหตุ
๒.๑	การยืนยันตัวตน (MFA) บังคับใช้ Multi-Factor Authentication สำหรับผู้ดูแลระบบและระบบสำคัญ		
๒.๒	สิทธิเท่าที่จำเป็น (Least Privilege) มีการจำกัดสิทธิการเข้าถึงข้อมูลตามความจำเป็น และทบทวนสิทธิเมื่อพนักงานลาออก/ย้ายงาน		
๒.๓	ความแข็งแกร่งของระบบ (Hardening) มีการตั้งค่า Security Baseline เช่น ปิดพอร์ตที่ไม่ใช้ เปลี่ยนรหัสผ่าน Default เป็นต้น		
๒.๔	การจัดการแพตช์ (Patch Mgt) มีนโยบายติดตั้ง Patch ความปลอดภัยภายในระยะเวลาที่กำหนด (โดยเฉพาะ Critical Patch)		
๒.๕	การเชื่อมต่อระยะไกล (Remote Access) การเข้าถึงระบบจากภายนอก (WFH) ต้องผ่าน VPN หรือช่องทางที่เข้ารหัสเท่านั้น		
๒.๖	อุปกรณ์พกพา (Removable Media) มีการสแกนไวรัสสื่อบันทึกข้อมูล (USB) ก่อนใช้งานกับเครื่องคอมพิวเตอร์มหาวิทยาลัย		
๒.๗	การแบ่งปันข้อมูล (Info Sharing) มีการกำหนดชั้นความลับข้อมูล (TLP) ก่อนส่งต่อข้อมูลภัยคุกคามให้หน่วยงานภายนอก		

ส่วนที่ ๓ การตรวจจับและตอบสนอง (Detect & Respond)

เป้าหมาย เพื่อให้รู้ตัวเมื่อเกิดเหตุและระงับเหตุได้ทันท่วงที

ลำดับ	รายการตรวจสอบ (Checklist Item)	สถานะ (✓/✗)	อ้างอิง/ หมายเหตุ
๓.๑	การเก็บ Logs มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ครบถ้วนตามกฎหมาย และเก็บรักษาอย่างน้อย ๙๐ วัน		
๓.๒	ศูนย์เฝ้าระวัง (Monitoring) มีระบบแจ้งเตือนความผิดปกติ (Alert) หรือศูนย์ SOC ที่เฝ้าระวังภัยคุกคาม		
๓.๓	ทีมตอบสนอง (CIRT) มีคำสั่งแต่งตั้งทีมตอบสนองเหตุการณ์ (Incident Response Team) พร้อมเบอร์ติดต่อฉุกเฉิน		
๓.๔	แผนรับมือ (IR Plan) มีแผนปฏิบัติการเมื่อเกิดเหตุภัยคุกคาม (Playbook) ที่เป็นลายลักษณ์อักษร		
๓.๕	การสื่อสารวิกฤต (Crisis Comm) มีการกำหนด "โฆษก" และร่างแถลงการณ์เตรียมพร้อมสำหรับภาวะวิกฤต		
๓.๖	การฝึกซ้อม (Exercise) มีการซ้อมแผนรับมือภัยคุกคาม (Tabletop หรือ Drill) อย่างน้อยปีละ ๑ ครั้ง		

ส่วนที่ ๔ การรักษาและฟื้นฟู (Recover)

เป้าหมาย เพื่อให้การเรียนการสอนและการบริหารงานดำเนินต่อได้

ลำดับ	รายการตรวจสอบ (Checklist Item)	สถานะ (✓/✗)	อ้างอิง/หมายเหตุ
๔.๑	วิเคราะห์ผลกระทบ (BIA) มีการประเมิน RTO (เวลาที่ยอมให้ระบบล่ม) และ RPO (ข้อมูลที่ยอมให้หาย) สำหรับระบบสำคัญ		
๔.๒	แผนความต่อเนื่อง (BCP) มีแผน BCP ที่ระบุขั้นตอนการทำงานสำรอง (Manual/Alternate Site) เมื่อระบบหลักล่ม		
๔.๓	การสำรองข้อมูล (Backup) มีการสำรองข้อมูลตามหลัก ๓-๒-๑ (มี ๓ ชุด, ๒ สื่อ, ๑ นอกสถานที่)		
๔.๔	ทดสอบกู้คืน (Restore Test) มีการทดสอบกู้คืนข้อมูลจาก Backup อย่างน้อยทุก ๖ เดือน เพื่อมั่นใจว่าข้อมูลไม่เสียหาย		
๔.๕	การปรับปรุงแผน มีการทบทวนและปรับปรุงแผน BCP หลังการฝึกซ้อม หรือเมื่อมีการเปลี่ยนแปลงระบบ		

📝 ข้อแนะนำในการนำไปใช้

การประเมิน ให้บุคลากร ส่วนเทคโนโลยีสารสนเทศ ประเมินเบื้องต้น แล้วประธานคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ตรวจสอบ โดยทำเครื่องหมาย ✅ หรือ ❌ ตามความเป็นจริง

แผนปรับปรุง รายการใดที่ได้ ❌ ให้ระบุในช่องหมายเหตุว่า "จะดำเนินการแก้ไขเมื่อไหร่" และ "ใครรับผิดชอบ"

การรายงาน นำผลสรุปจากตารางนี้รายงานต่ออธิการบดี เพื่อขออนุมัติทรัพยากรในการปิดช่องโหว่ต่อไป