



ประกาศมหาวิทยาลัยนเรศวร

เรื่อง แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร

.....

โดยที่เป็นการสมควรให้ปรับปรุงแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ให้สอดคล้องกับนโยบายและแผนปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อนำไปใช้เป็นแนวปฏิบัติในการป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ในปัจจุบัน และอนาคต เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัยนเรศวร รวมถึงเพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยนเรศวรเป็นไปในทิศทางเดียวกัน และสามารถรองรับการเปลี่ยนแปลงด้านเทคโนโลยีในอนาคตได้อย่างมีประสิทธิภาพและยั่งยืน ประกอบกับมาตรา ๔๓ และ มาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

อาศัยอำนาจตามความในมาตรา ๒๐ มาตรา ๒๑ และมาตรา ๓๗ แห่งพระราชบัญญัติ มหาวิทยาลัยนเรศวร พ.ศ. ๒๕๓๓ ประกอบกับมติคณะกรรมการบริหารมหาวิทยาลัยนเรศวร ในการประชุม ครั้งที่ ๑๕/๒๕๖๙ เมื่อวันที่ ๑ กันยายน ๒๕๖๙ จึงให้กำหนดแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ดังนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศมหาวิทยาลัยนเรศวร เรื่อง แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศมหาวิทยาลัยนเรศวร เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ฉบับลงวันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๖

ข้อ ๔ ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยนเรศวร

“อธิการบดี” หมายความว่า อธิการบดีมหาวิทยาลัยนเรศวร

“คณะ” หมายความว่า คณะ วิทยาลัย บัณฑิตวิทยาลัย สถาบัน สำนัก ศูนย์ หรือส่วนราชการ ที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะทั้งนี้ที่ได้รับการจัดตั้งให้เป็นส่วนราชการมหาวิทยาลัยนเรศวร หรือที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะที่ได้รับการจัดตั้งให้เป็นคณะภายในและมีใช้ส่วนราชการ โดยมติสภามหาวิทยาลัยนเรศวรและให้หมายความรวมถึงสำนักงานอธิการบดีด้วย

“นิสิต” หมายความว่า นิสิตมหาวิทยาลัยนเรศวร

“บุคลากร” หมายความว่า บุคลากรทุกประเภทของมหาวิทยาลัยนเรศวร

ข้อ ๕ ประกาศนี้ให้ใช้บังคับแก่ นิสิต บุคลากรและคณะภายใต้โครงสร้างการบริหารมหาวิทยาลัย

ข้อ ๖ แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มหาวิทยาลัยนเรศวร ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๗ การใดที่อยู่ระหว่างดำเนินการตามประกาศมหาวิทยาลัยนเรศวร เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร ฉบับลงวันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๖ ซึ่งใช้บังคับอยู่ก่อนวันที่ประกาศนี้มีผลบังคับใช้ ให้ดำเนินการตามประกาศฉบับดังกล่าวจนกว่าจะแล้วเสร็จ

ข้อ ๘ ให้อธิการบดีเป็นผู้รักษาการตามประกาศ กรณีมีปัญหาจากการปฏิบัติตามประกาศหรือที่ประกาศนี้ไม่ได้กำหนดไว้ ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๖๙



(รองศาสตราจารย์ ดร.ศรินทร์ทิพย์ แทนธานี)

รักษาราชการแทนอธิการบดีมหาวิทยาลัยนเรศวร

เอกสารแนบท้าย ประกาศมหาวิทยาลัยนเรศวร
เรื่อง แนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยนเรศวร
ฉบับลงวันที่ ๖๐ กันยายน พ.ศ. ๒๕๖๙



สารบัญ

๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์.....	๑
ส่วนที่ ๑ นโยบายและการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Governance)	๓
๑. การกำหนดโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์.....	๓
๒. บทบาทหน้าที่ของผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ	๓
๓. การกำกับดูแลและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์.....	๔
๔. การกำหนดนโยบายด้านสถาปัตยกรรมและการออกแบบความมั่นคงปลอดภัยไซเบอร์.....	๔
๕. การรายงาน การติดตาม และการปรับปรุงอย่างต่อเนื่อง	๔
ส่วนที่ ๒ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management).....	๕
๑. กรอบและกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๕
๒. การระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๖
๓. การจัดทำและบริหารทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์.....	๗
๔. การกำหนดระดับความเสี่ยงที่ยอมรับได้และการจัดการความเสี่ยง.....	๘
๕. การติดตาม รายงาน และการปรับปรุงกระบวนการบริหารความเสี่ยง	๙
ส่วนที่ ๓ มาตรการด้านเทคนิคและการปฏิบัติ (Cybersecurity Controls).....	๑๑
๑. การป้องกัน (Protect).....	๑๑
๒. การตรวจจับ (Detect)	๑๑
ส่วนที่ ๔ การรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response)	๑๔
๑. การจัดทำและทบทวนแผนการรับมือและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan: CIRP).....	๑๔
๒. การฝึกซ้อมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise).....	๑๑
๓. การกำหนดกระบวนการสื่อสารในภาวะวิกฤต (Crisis Communication)	๑๒
๔. การบูรณาการกับแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (Business Continuity Plan: BCP / Disaster Recovery Plan: DRP)	๑๓



สารบัญ

ส่วนที่ ๕ การสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพ (Cybersecurity Awareness and Capability Development).....	๓๖
๑. การจัดให้มีการอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness).....	๓๖
๒. การส่งเสริมการพัฒนาทักษะเฉพาะด้านให้แก่ผู้ดูแลระบบและบุคลากรด้านเทคนิค (Specialized Skill Development)	๓๗
๓. การสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ (Professional Certification and Training Support)	๓๙
๔. การติดตาม ประเมินผล และการปรับปรุงอย่างต่อเนื่อง (Monitoring, Evaluation, and Continuous Improvement)	๔๐



๑. หลักการและเหตุผล

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยมีความเหมาะสม ทันสมัย และสอดคล้องกับสภาพการณ์ภัยคุกคามทางไซเบอร์ที่มีความซับซ้อน ทวีความรุนแรง และเปลี่ยนแปลงอย่างรวดเร็วในปัจจุบัน ซึ่งภัยคุกคามดังกล่าวมิได้จำกัดอยู่เพียงการโจมตีต่อระบบสารสนเทศโดยตรงเท่านั้น หากแต่ยังครอบคลุมถึงความเสี่ยงที่เกิดจากการพึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารในรูปแบบใหม่ อาทิ การใช้ระบบคลาวด์ (Cloud Computing) การเชื่อมต่อระบบจากภายนอกองค์กร (External Connectivity) การนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้ในการดำเนินงาน ตลอดจนความเสี่ยงจากห่วงโซ่อุปทานด้านดิจิทัล (Digital Supply Chain Risk) ซึ่งเกี่ยวข้องกับผู้ให้บริการภายนอก ซอฟต์แวร์ ฮาร์ดแวร์ และบริการเทคโนโลยีสารสนเทศที่มหาวิทยาลัยพึ่งพาในการดำเนินการกิจหลัก

นอกจากนี้ ความก้าวหน้าของเทคโนโลยีควอนตัม (Quantum Technology) โดยเฉพาะการพัฒนาควอนตัมคอมพิวเตอร์ (Quantum Computing) ได้ก่อให้เกิดความท้าทายใหม่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากมีศักยภาพในการส่งผลกระทบต่อความมั่นคงของกลไกการเข้ารหัสข้อมูลและการพิสูจน์ตัวตนที่ใช้อยู่ในปัจจุบัน ซึ่งอาจทำให้มาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เคยมีความเพียงพอไม่สามารถรองรับภัยคุกคามในอนาคตได้อย่างมีประสิทธิภาพ มหาวิทยาลัยจึงจำเป็นต้องตระหนักถึงแนวโน้มดังกล่าว และเตรียมความพร้อมเชิงนโยบายและเชิงบริหาร เพื่อรองรับการเปลี่ยนแปลงด้านเทคโนโลยี และภัยคุกคามในระยะยาว

ประกอบกับการเปลี่ยนแปลงของกรอบกฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับประเทศและระดับสากล ซึ่งกำหนดให้หน่วยงานของรัฐต้องมีระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ครอบคลุมการป้องกัน ตรวจสอบ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ รวมถึงการบริหารจัดการความเสี่ยงด้านเทคโนโลยีเกิดใหม่ (Emerging Technologies Risk) อย่างเหมาะสม โปร่งใส และสามารถตรวจสอบได้

ดังนั้น เพื่อยกระดับการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยให้สอดคล้องกับบริบทเทคโนโลยีและวางแผนรับมือ ป้องกัน ลดความเสี่ยงภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของมหาวิทยาลัย รวมถึงเพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปในทิศทางเดียวกันทั้งมหาวิทยาลัย และสามารถรองรับการเปลี่ยนแปลงด้านเทคโนโลยีในอนาคตได้อย่างมีประสิทธิภาพและยั่งยืน

๒. วัตถุประสงค์

๑) เพื่อยกระดับการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย ให้มีความเหมาะสม ทันสมัย และสอดคล้องกับสภาพการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต รวมถึงภัยคุกคามที่เกิดจากการใช้เทคโนโลยีสารสนเทศและเทคโนโลยีเกิดใหม่

๒) เพื่อกำหนดกรอบมาตรฐานและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน ครอบคลุมการป้องกัน การตรวจสอบ การตอบสนอง และการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ เพื่อให้สามารถนำไปใช้ปฏิบัติได้อย่างเป็นระบบและมีประสิทธิภาพ



๓) เพื่อสร้างความตระหนักรู้ ความเข้าใจ และความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้บริหาร บุคลากร นิสิต นักเรียน และผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๔) เพื่อสนับสนุนและส่งเสริมการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง ทั้งในระดับประเทศและระดับสากลอย่างครบถ้วนและต่อเนื่อง

๕) เพื่อเตรียมความพร้อมของมหาวิทยาลัยในการรองรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดจากเทคโนโลยีเกิดใหม่ อาทิ ระบบคลาวด์ เทคโนโลยีปัญญาประดิษฐ์ และเทคโนโลยีควอนตัม (Quantum Technology) โดยมุ่งเน้นการบริหารจัดการความเสี่ยงในระยะยาวอย่างยั่งยืน



ส่วนที่ ๑

นโยบายและการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Governance)

การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยเป็นไปตามหลักการบริหารจัดการที่ดี มีความโปร่งใส สามารถตรวจสอบได้ และสอดคล้องกับภารกิจหลักของมหาวิทยาลัย โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อการให้บริการ การดำเนินงานทางวิชาการ การวิจัย การบริหารจัดการ และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

แนวทางการปฏิบัติการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๑. การกำหนดโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๑.๑ มีการกำหนดโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ครอบคลุมตั้งแต่ระดับนโยบาย ระดับบริหารจัดการ และระดับปฏิบัติการ เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์มีความต่อเนื่อง เป็นเอกภาพ และสามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

๑.๒ โครงสร้างดังกล่าวต้องแสดงให้เห็นถึงความสัมพันธ์ระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานด้านบริหารความเสี่ยง หน่วยงานตรวจสอบภายใน และหน่วยงานที่รับผิดชอบภารกิจหลักของมหาวิทยาลัย เพื่อให้เกิดการประสานงานและการถ่วงดุลอย่างเหมาะสม

๑.๓ ให้ทุกคณะกำหนดผู้รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ในระดับคณะ เพื่อทำหน้าที่กำกับดูแล ประสานงาน และติดตามการปฏิบัติตามนโยบายและแนวทางที่มหาวิทยาลัยกำหนด

๑.๔ โครงสร้างการกำกับดูแลต้องสามารถรองรับการเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคาม และรูปแบบการให้บริการในอนาคต โดยไม่เป็นอุปสรรคต่อการพัฒนาและนวัตกรรมของมหาวิทยาลัย

๒. บทบาทหน้าที่ของผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๑ ดำเนินการแต่งตั้งผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือ ผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ในลักษณะเดียวกันอย่างเป็นทางการ เพื่อทำหน้าที่เป็นกลไกหลักในการกำหนดทิศทาง นโยบาย และกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๒.๒ ผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีอำนาจหน้าที่ในการเสนอแนะเชิงนโยบายต่อผู้บริหารระดับสูง ประสานงานกับหน่วยงานที่เกี่ยวข้อง และกำกับดูแลให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปตามกรอบที่กำหนด

๒.๓ ผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ ต้องทำหน้าที่เป็นศูนย์กลางในการบูรณาการข้อมูลด้านภัยคุกคาม ความเสี่ยง เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มเทคโนโลยีใหม่ เพื่อสนับสนุนการตัดสินใจเชิงนโยบายของผู้บริหาร

๒.๔ ในระดับคณะ ให้ผู้รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ของคณะทำหน้าที่สนับสนุน และรายงานข้อมูลที่เกี่ยวข้องแก่ผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง



๓. การกำกับดูแลและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๑ นำหลักการ Three Lines of Defense มาเป็นกรอบในการกำหนดบทบาทหน้าที่ของหน่วยงานและบุคลากร เพื่อให้เกิดการควบคุม การกำกับดูแล และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ

๓.๒ ให้มีการบูรณาการแนวคิด Cyber Risk Governance เข้ากับการบริหารความเสี่ยงระดับองค์กร โดยถือว่าความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นความเสี่ยงเชิงกลยุทธ์ที่อาจส่งผลกระทบต่อการบรรลุพันธกิจของมหาวิทยาลัย

๓.๓ การบริหารความเสี่ยงต้องครอบคลุมความเสี่ยงจากระบบสารสนเทศ เทคโนโลยีเกิดใหม่ ผู้ให้บริการภายนอก และความเสี่ยงจากห่วงโซ่อุปทานด้านดิจิทัล (Digital Supply Chain Risk)

๓.๔ ให้มีการติดตาม ทบทวน และรายงานสถานะความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ และนำผลการประเมินไปใช้ในการปรับปรุงนโยบายและมาตรการที่เกี่ยวข้อง

๔. การกำหนดนโยบายด้านสถาปัตยกรรมและการออกแบบความมั่นคงปลอดภัยไซเบอร์

๔.๑ กำหนดนโยบายด้าน Zero Trust Architecture เป็นแนวทางหลักในการออกแบบและบริหารจัดการระบบสารสนเทศที่สำคัญ โดยยึดหลักการตรวจสอบและควบคุมการเข้าถึงอย่างเข้มงวดตามระดับความเสี่ยง

๔.๒ การกำหนดนโยบายดังกล่าวต้องคำนึงถึงการบริหารจัดการตัวตนและสิทธิ์ การแยกส่วนระบบ การตรวจสอบพฤติกรรมการใช้งาน และการป้องกันการเข้าถึงจากแหล่งที่ไม่เชื่อถือ

๔.๓ ให้บูรณาการแนวคิด Security by Design และ Security by Default ในทุกขั้นตอนของการพัฒนา จัดทำ และปรับปรุงระบบสารสนเทศ

๕. การรายงาน การติดตาม และการปรับปรุงอย่างต่อเนื่อง

๕.๑ กำหนดให้มีการรายงานสถานะด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารระดับสูงอย่างสม่ำเสมอ เพื่อให้สามารถกำกับ ติดตาม และตัดสินใจเชิงนโยบายได้อย่างเหมาะสม

๕.๒ รายงานดังกล่าวต้องสะท้อนภาพรวมภัยคุกคาม เหตุการณ์ที่เกิดขึ้น ระดับความเสี่ยง มาตรการควบคุม และข้อเสนอแนะในการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์

๕.๓ นำผลการรายงานและบทเรียนจากเหตุการณ์ที่ผ่านมาเป็นข้อมูลในการพัฒนานโยบาย แผนงาน และมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยอย่างต่อเนื่องและยั่งยืน



ส่วนที่ ๒

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management)

เพื่อกำหนดกรอบและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย ให้เป็นไปอย่างเป็นระบบ สอดคล้องกับภารกิจหลักของมหาวิทยาลัย และสามารถรองรับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนในปัจจุบันและอนาคต รวมถึงเพื่อให้การตัดสินใจด้านการบริหารจัดการความเสี่ยงเป็นไปอย่างเหมาะสม มีเหตุผล และสามารถตรวจสอบได้

แนวทางปฏิบัติการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๑. กรอบและกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๑.๑ กำหนดกรอบ แนวทาง และกระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นมาตรฐานเดียวกันทั่วทั้งมหาวิทยาลัย โดยกำหนดระเบียบวิธี ขั้นตอน เกณฑ์การพิจารณา และรูปแบบเอกสารที่ใช้ในการประเมินความเสี่ยงอย่างชัดเจน ทั้งนี้ เพื่อให้ผลการประเมินความเสี่ยงของทุกคณะ มีความสอดคล้อง เป็นระบบ สามารถเปรียบเทียบและบูรณาการเป็นภาพรวมระดับมหาวิทยาลัยได้ และสามารถนำผลการประเมินไปใช้ประกอบการตัดสินใจเชิงบริหาร การกำหนดนโยบาย การจัดสรรทรัพยากร และการกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพ

๑.๒ ให้คณะดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ ข้อมูล และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบ อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการประเมินเพิ่มเติมเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญซึ่งอาจส่งผลกระทบต่อระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ การเปลี่ยนแปลงอย่างมีนัยสำคัญให้หมายความรวมถึงกรณีการนำระบบสารสนเทศใหม่ มาใช้งาน การเปลี่ยนผู้ให้บริการภายนอก การย้ายหรือปรับเปลี่ยนระบบไปใช้บริการระบบคลาวด์ การเปลี่ยนแปลงสถาปัตยกรรมระบบ หรือการเปลี่ยนแปลงรูปแบบการให้บริการและการเชื่อมต่อระบบ ทั้งนี้ เพื่อให้การประเมินความเสี่ยงสะท้อนสภาพการดำเนินงานจริงและสามารถรองรับภัยคุกคามทางไซเบอร์ ที่อาจเกิดขึ้นได้อย่างทันท่วงที

๑.๓ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ให้พิจารณาครอบคลุมองค์ประกอบหลัก ได้แก่ การระบุทรัพย์สินสารสนเทศที่อยู่ในความรับผิดชอบ การวิเคราะห์ภัยคุกคามที่อาจเกิดขึ้น การพิจารณา ช่องโหว่หรือจุดอ่อนของระบบ การประเมินโอกาสที่จะเกิดเหตุการณ์ และการประเมินผลกระทบที่อาจเกิดขึ้น จากเหตุการณ์ดังกล่าว โดยให้คำนึงถึงหลักการรักษาความมั่นคงปลอดภัยสารสนเทศในด้านความลับ ความถูกต้อง ครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบสารสนเทศเป็นสำคัญ ทั้งนี้ เพื่อให้การประเมินความเสี่ยง มีความรอบด้าน สอดคล้องกับสภาพความเสี่ยงที่แท้จริง และสามารถนำผลการประเมินไปใช้ในการกำหนด มาตรการควบคุมและแนวทางการจัดการความเสี่ยงได้อย่างเหมาะสม



๒. การระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒.๑ การระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ดำเนินการระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ครอบคลุมระบบสารสนเทศ ข้อมูล และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบ ทั้งนี้ เพื่อให้สามารถวิเคราะห์ลักษณะของความเสี่ยงได้อย่างชัดเจน กำหนดมาตรการควบคุมและแนวทางการจัดการความเสี่ยงที่เหมาะสมกับระดับและประเภทของความเสี่ยงนั้น ๆ รวมถึงเพื่อให้การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปในทิศทางเดียวกันทั่วทั้งมหาวิทยาลัย

การจำแนกประเภทความเสี่ยงดังกล่าว ให้ใช้เป็นกรอบในการจัดลำดับความสำคัญของความเสี่ยง การกำหนดผู้รับผิดชอบความเสี่ยง และการติดตามประเมินผลการจัดการความเสี่ยงอย่างต่อเนื่อง โดยต้องสามารถเชื่อมโยงกับกระบวนการบริหารความเสี่ยงระดับองค์กรของมหาวิทยาลัยได้อย่างเหมาะสม

๒.๒ ประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องครอบคลุม

การระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ต้องครอบคลุมอย่างน้อย ประเภทความเสี่ยง ดังต่อไปนี้

๒.๒.๑ ความเสี่ยงจากระบบคลาวด์ (Cloud Risk)

ให้พิจารณาความเสี่ยงที่เกิดจากการใช้บริการระบบคลาวด์หรือการนำข้อมูลและระบบสารสนเทศ ไปจัดเก็บหรือประมวลผลบนระบบคลาวด์ ซึ่งรวมถึงความเสี่ยงด้านการควบคุมการเข้าถึงข้อมูล การกำหนดสิทธิ์ผู้ใช้งาน การตั้งค่าความมั่นคงปลอดภัยของระบบ ความพร้อมใช้งานและความต่อเนื่องของบริการ การพึ่งพาผู้ให้บริการระบบคลาวด์ ตลอดจนการเคลื่อนย้ายและการจัดการข้อมูลระหว่างระบบหรือระหว่างผู้ให้บริการ

ทั้งนี้ ให้คณะพิจารณาความเสี่ยงดังกล่าวโดยคำนึงถึงความรับผิดชอบร่วมระหว่างมหาวิทยาลัย และผู้ให้บริการระบบคลาวด์ รวมถึงผลกระทบที่อาจเกิดขึ้นต่อข้อมูลและการให้บริการของมหาวิทยาลัยในกรณีที่เกิดเหตุขัดข้องหรือเหตุภัยคุกคามทางไซเบอร์

๒.๒.๒ ความเสี่ยงจากผู้ให้บริการภายนอกและห่วงโซ่อุปทานด้านดิจิทัล (Third-Party Risk และ Digital Supply Chain Risk)

ให้พิจารณาความเสี่ยงที่เกิดจากการพึ่งพาผู้ให้บริการภายนอก บุคคลหรือนิติบุคคล รวมถึงซอฟต์แวร์ ฮาร์ดแวร์ หรือบริการด้านเทคโนโลยีสารสนเทศจากภายนอกที่มีการเชื่อมต่อหรือสามารถเข้าถึงระบบสารสนเทศ หรือข้อมูลของมหาวิทยาลัย ซึ่งความเสี่ยงดังกล่าวอาจเกิดจากการกำหนดสิทธิ์การเข้าถึงที่ไม่เหมาะสม มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการที่ไม่เพียงพอ หรือความบกพร่องในกระบวนการกำกับดูแล และตรวจสอบผู้ให้บริการภายนอก

ในการพิจารณาความเสี่ยงประเภทนี้ ให้คำนึงถึงความเสี่ยงจากห่วงโซ่อุปทานด้านดิจิทัลที่อาจส่งผลกระทบต่อมหาวิทยาลัย แม้ว่ามหาวิทยาลัยจะมีได้เป็นผู้ควบคุมระบบหรือบริการนั้นโดยตรงก็ตาม

๒.๒.๓ ความเสี่ยงจากภัยคุกคามขั้นสูง (Advanced Cyber Threats)

ให้พิจารณาความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและมีลักษณะการโจมตีแบบเจาะจงเป้าหมาย เช่น การโจมตีด้วยโปรแกรมเรียกค่าไถ่ (Ransomware) การโจมตีแบบต่อเนื่องระยะยาว (Advanced Persistent Threat: APT) และการโจมตีที่มุ่งหวังการเข้าถึงหรือการเปิดเผยข้อมูลสำคัญของมหาวิทยาลัย



การประเมินความเสี่ยงประเภทนี้ ให้คำนึงถึงผลกระทบต่อความต่อเนื่องในการให้บริการ ความเสียหายต่อข้อมูล ระบบสารสนเทศ ชื่อเสียงของมหาวิทยาลัย และผลกระทบที่อาจเกิดขึ้นตามกฎหมายและระเบียบที่เกี่ยวข้อง

๒.๒.๔ ความเสี่ยงจากเทคโนโลยีปัญญาประดิษฐ์และข้อมูลขนาดใหญ่ (Artificial Intelligence and Big Data Risk)

ให้พิจารณาความเสี่ยงที่เกิดจากการนำเทคโนโลยีปัญญาประดิษฐ์หรือการประมวลผลข้อมูลขนาดใหญ่มาใช้ในการดำเนินงาน ซึ่งอาจก่อให้เกิดความเสี่ยงด้านการควบคุมการเข้าถึงข้อมูล การใช้ข้อมูลเกินวัตถุประสงค์ การเชื่อมโยงข้อมูลจากหลายแหล่งจนทำให้สามารถระบุตัวบุคคลได้ รวมถึงความเสี่ยงจากการใช้บริการหรือเครื่องมือด้านปัญญาประดิษฐ์จากภายนอก

ทั้งนี้ ให้คำนึงถึงการกำกับดูแลการใช้ข้อมูล การกำหนดขอบเขตการใช้งาน และการป้องกันการรั่วไหลหรือการนำข้อมูลไปใช้โดยมิชอบ

๒.๓ การพิจารณาความเสี่ยงในมิติที่รอบด้าน

ในการระบุและจำแนกประเภทความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ให้คณะพิจารณาความเสี่ยงควบคู่กันในทุกมิติ ได้แก่ มิติด้านเทคนิค มิติด้านกระบวนการ และมิติด้านบุคลากร เพื่อให้การบริหารความเสี่ยงมีความรอบด้านและลดโอกาสเกิดช่องว่างในการควบคุมความเสี่ยง

ทั้งนี้ ให้คำนึงถึงความเชื่อมโยงระหว่างมิติดังกล่าว และให้ผลการพิจารณาความเสี่ยงสะท้อนถึงสภาพการดำเนินงานจริงของคณะและมหาวิทยาลัยโดยรวม

๓. การจัดทำและบริหารทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๓.๑ จัดทำทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Register) เป็นเอกสารกลางในการรวบรวม บันทึก และบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ ข้อมูล และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่อยู่ในความรับผิดชอบ ทั้งนี้ เพื่อให้การบริหารความเสี่ยงเป็นไปอย่างเป็นระบบ มีความต่อเนื่อง สามารถติดตาม ตรวจสอบ และรายงานสถานะความเสี่ยงได้อย่างชัดเจน รวมถึงสามารถบูรณาการข้อมูลความเสี่ยงของแต่ละคณะเป็นภาพรวมในระดับมหาวิทยาลัย เพื่อใช้ประกอบการกำหนดนโยบาย การวางแผน และการตัดสินใจเชิงบริหารได้อย่างเหมาะสม

๓.๒ ทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต้องจัดทำในรูปแบบและโครงสร้างที่เป็นมาตรฐานเดียวกันทั้งมหาวิทยาลัย และต้องระบุรายละเอียดของความเสี่ยงอย่างน้อย ดังต่อไปนี้

- (๑) รายการความเสี่ยงและคำอธิบายความเสี่ยงที่ชัดเจน ครอบคลุมลักษณะ สาเหตุ และขอบเขตของความเสี่ยงนั้น
- (๒) สาเหตุและปัจจัยเสี่ยงที่อาจก่อให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- (๓) ผลกระทบที่อาจเกิดขึ้นต่อข้อมูล ระบบสารสนเทศ การให้บริการ ภารกิจหลัก ชื่อเสียง หรือการปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง
- (๔) ระดับความเสี่ยงก่อนการควบคุมและระดับความเสี่ยงหลังการควบคุม โดยอาศัยเกณฑ์การประเมินความเสี่ยงที่มหาวิทยาลัยกำหนด



(๕) มาตรการควบคุมที่มีอยู่ในปัจจุบัน และมาตรการเพิ่มเติมที่จำเป็นต้องดำเนินการเพื่อปรับลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(๖) ระยะเวลาดำเนินการ แผนงาน หรือกิจกรรมที่เกี่ยวข้องกับการจัดการความเสี่ยง รวมถึงสถานะความคืบหน้าในการดำเนินการดังกล่าว

ทั้งนี้ ทะเบียนความเสี่ยงต้องได้รับการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ และต้องสะท้อนสถานการณ์ความเสี่ยงที่แท้จริงของระบบและการดำเนินงานในแต่ละช่วงเวลา

๓.๓ กำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) อย่างชัดเจนสำหรับความเสี่ยงแต่ละรายการ โดยผู้รับผิดชอบความเสี่ยงมีหน้าที่กำกับ ติดตาม ควบคุม และรายงานความคืบหน้าในการจัดการความเสี่ยงตามแผนที่กำหนด รวมถึงประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อดำเนินมาตรการควบคุมและปรับปรุงแก้ไขอย่างเหมาะสม ทั้งนี้ เพื่อให้เกิดความรับผิดชอบที่ชัดเจน และให้การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพและตรวจสอบได้

๔. การกำหนดระดับความเสี่ยงที่ยอมรับได้และการจัดการความเสี่ยง

๔.๑ กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเสี่ยงที่สามารถยอมรับได้ในทางปฏิบัติ (Risk Tolerance) ด้านความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน โดยให้สอดคล้องกับแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทั้งนี้ เพื่อใช้เป็นกรอบในการพิจารณา ตัดสินใจ และกำหนดทิศทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยอย่างเป็นระบบและมีมาตรฐานเดียวกัน

การกำหนด Risk Appetite และ Risk Tolerance ดังกล่าว ต้องคำนึงถึงระดับความสำคัญของระบบสารสนเทศ ข้อมูล และภารกิจหลักของมหาวิทยาลัย รวมถึงผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงาน ความเชื่อมั่น และการปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง

๔.๒ ในการกำหนดและประเมินระดับความเสี่ยง ให้ใช้เกณฑ์การประเมินตามระดับความรุนแรงของความเสี่ยง โดยอาศัยผลการพิจารณาจากโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ตามแนวทางที่สกมช. กำหนด ซึ่งสามารถจำแนกระดับความเสี่ยงออกเป็นระดับต่าง ๆ ดังต่อไปนี้

๔.๒.๑ ความเสี่ยงระดับต่ำ (Low Risk)

หมายถึง ความเสี่ยงที่มีโอกาสเกิดและผลกระทบอยู่ในระดับต่ำ ไม่ส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือภารกิจหลักของมหาวิทยาลัย ความเสี่ยงในระดับนี้สามารถยอมรับได้ โดยให้มีการติดตามและควบคุมตามมาตรการปกติ

๔.๒.๒ ความเสี่ยงระดับปานกลาง (Medium Risk)

หมายถึง ความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานหรือการให้บริการในบางส่วน หากเกิดขึ้นอาจต้องใช้ทรัพยากรในการแก้ไขในระดับหนึ่ง ความเสี่ยงในระดับนี้สามารถยอมรับได้ภายใต้เงื่อนไขที่มีมาตรการควบคุมที่เหมาะสม และต้องมีการติดตามทบทวนอย่างสม่ำเสมอ

๔.๒.๓ ความเสี่ยงระดับสูง (High Risk)

หมายถึง ความเสี่ยงที่มีโอกาสเกิดหรือผลกระทบในระดับสูง ซึ่งอาจส่งผลกระทบต่อภารกิจหลัก ความต่อเนื่องในการให้บริการ หรือข้อมูลสำคัญของมหาวิทยาลัย ความเสี่ยงในระดับนี้ไม่ควรยอมรับโดยไม่มีการเพิ่มเติม และต้องกำหนดแผนการจัดการความเสี่ยงเพื่อลดระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้



๔.๒.๔ ความเสี่ยงระดับสูงมากหรือวิกฤต (Very High / Critical Risk)

หมายถึง ความเสี่ยงที่อาจส่งผลกระทบรุนแรงต่อการดำเนินงานในภาพรวม ความมั่นคงปลอดภัยของข้อมูล หรือก่อให้เกิดผลกระทบด้านกฎหมาย ชื่อเสียง หรือความเชื่อมั่นของมหาวิทยาลัย ความเสี่ยงในระดับนี้ไม่สามารถยอมรับได้ และต้องเร่งดำเนินการจัดการความเสี่ยงโดยทันที รวมถึงรายงานต่อผู้บริหารระดับสูงเพื่อพิจารณากำหนดมาตรการและแนวทางแก้ไขอย่างเร่งด่วน

๔.๓ การเลือกแนวทางการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ให้พิจารณาให้เหมาะสมกับระดับความเสี่ยงที่ประเมินได้ โดยอาจใช้แนวทางการจัดการความเสี่ยงตามหลักสากลและแนวทางของ สกมช. ได้แก่

๔.๓.๑ การลดความเสี่ยง (Risk Mitigation) โดยการกำหนดหรือปรับปรุงมาตรการควบคุมด้านเทคนิค ด้านกระบวนการ หรือด้านบุคลากร

๔.๓.๒ การโอนย้ายความเสี่ยง (Risk Transfer) เช่น การทำประกันภัยไซเบอร์ หรือการกำหนดความรับผิดชอบในสัญญากับผู้ให้บริการภายนอก

๔.๓.๓ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) โดยการยกเลิกหรือปรับเปลี่ยนกิจกรรมหรือระบบที่ก่อให้เกิดความเสี่ยงในระดับที่ไม่สามารถยอมรับได้

๔.๓.๔ การยอมรับความเสี่ยง (Risk Acceptance) ในกรณีที่ความเสี่ยงอยู่ในระดับที่ยอมรับได้และมีเหตุผลเชิงบริหารรองรับ ทั้งนี้ ต้องได้รับการพิจารณาและอนุมัติตามระดับอำนาจหน้าที่ที่มหาวิทยาลัยกำหนด

๔.๔ การตัดสินใจด้านการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ต้องคำนึงถึงผลกระทบต่อภารกิจหลักของมหาวิทยาลัย ความต่อเนื่องในการให้บริการ ความคุ้มค่าในการใช้ทรัพยากร งบประมาณ ความพร้อมด้านบุคลากร ตลอดจนความสอดคล้องกับกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง ทั้งนี้ เพื่อให้การจัดการความเสี่ยงเป็นไปอย่างสมดุล เหมาะสม และสนับสนุนการดำเนินงานของมหาวิทยาลัยอย่างยั่งยืน

๕. การติดตาม รายงาน และการปรับปรุงกระบวนการบริหารความเสี่ยง

๕.๑ ดำเนินการติดตาม ตรวจสอบ และรายงานสถานะความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ โดยให้รายงานต่อผู้บริหารระดับสูงและคณะกรรมการที่เกี่ยวข้อง ตามรอบระยะเวลาที่มหาวิทยาลัยกำหนด ทั้งนี้ เพื่อให้ผู้บริหารสามารถรับทราบสถานการณ์ความเสี่ยง ภาพรวมภัยคุกคามทางไซเบอร์ และความคืบหน้าในการดำเนินมาตรการจัดการความเสี่ยง รวมถึงสามารถใช้ข้อมูลดังกล่าวประกอบการกำหนดนโยบาย การตัดสินใจเชิงบริหาร และการจัดสรรทรัพยากรได้อย่างเหมาะสมและทันทั่วถึง

การรายงานสถานะความเสี่ยงดังกล่าว ควรครอบคลุมสาระสำคัญ เช่น ระดับความเสี่ยงที่สำคัญหรือมีนัยสำคัญต่อมหาวิทยาลัย ความเสี่ยงที่ยังอยู่ในระดับสูงหรือสูงมาก ผลการดำเนินมาตรการควบคุมความคืบหน้าของแผนจัดการความเสี่ยง และประเด็นที่ต้องการการตัดสินใจหรือการสนับสนุนจากผู้บริหาร

๕.๒ ดำเนินการนำข้อมูลจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นจริง ผลการตรวจประเมินด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งจากการตรวจประเมินภายในและภายนอก ตลอดจนบทเรียนที่ได้รับจากการรับมือเหตุการณ์ดังกล่าว มาใช้เป็นข้อมูลประกอบในการทบทวน วิเคราะห์ และปรับปรุงกระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง



ทั้งนี้ การทบทวนและปรับปรุงดังกล่าว ควรครอบคลุมการปรับปรุงกรอบการประเมินความเสี่ยง เกณฑ์การประเมินระดับความเสี่ยง มาตรการควบคุม แผนการจัดการความเสี่ยง และแนวทางปฏิบัติที่เกี่ยวข้อง เพื่อให้สามารถรองรับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ

๕.๓ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยถือเป็นกระบวนการต่อเนื่อง มิใช่การดำเนินการเป็นครั้งคราว และต้องบูรณาการเข้ากับระบบบริหารความเสี่ยงองค์กรของมหาวิทยาลัย ในภาพรวม โดยให้ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของความเสี่ยงองค์กรที่ต้องได้รับการกำกับดูแล ติดตาม และรายงานในระดับเดียวกับความเสี่ยงด้านอื่น ๆ ที่มีผลต่อการบรรลุพันธกิจและเป้าหมายเชิงยุทธศาสตร์ของมหาวิทยาลัย

ทั้งนี้ เพื่อให้การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สนับสนุนการดำเนินงานของมหาวิทยาลัยอย่างมีประสิทธิภาพ สามารถรักษาความต่อเนื่องในการให้บริการ ลดโอกาสและผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยอย่างยั่งยืน



ส่วนที่ ๓

มาตรการด้านเทคนิคและการปฏิบัติ (Cybersecurity Controls)

๑. การป้องกัน (Protect)

มาตรการด้านการป้องกัน มีวัตถุประสงค์เพื่อป้องกัน ลดโอกาส และลดความเสี่ยงจากการเข้าถึง การใช้งาน การเปิดเผย หรือการเปลี่ยนแปลงข้อมูลและระบบสารสนเทศโดยมิชอบ รวมถึงเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยในเชิงป้องกันเชิงรุก โดยให้คณะถือปฏิบัติตามมาตรการดังต่อไปนี้

๑.๑ การควบคุมการเข้าถึงแบบหลายปัจจัย (Multi-Factor Authentication : MFA)

๑.๑.๑ หลักการและวัตถุประสงค์

กำหนดให้มีการใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication : MFA) เป็น มาตรการพื้นฐานในการควบคุมการเข้าถึงระบบสารสนเทศที่มีความสำคัญ ทั้งนี้ เพื่อเสริมสร้างความมั่นคง ปลอดภัยในการพิสูจน์ตัวตนของผู้ใช้งาน ลดความเสี่ยงจากการถูกขโมยรหัสผ่าน การโจมตีแบบฟิชซิง การเข้าถึง ระบบโดยมิได้รับอนุญาต และการใช้บัญชีผู้ใช้งานในทางที่ไม่เหมาะสม อันอาจส่งผลกระทบต่อข้อมูล ระบบสารสนเทศ และภารกิจหลักของมหาวิทยาลัย

การกำหนดใช้ MFA ถือเป็นมาตรการเชิงป้องกันเชิงรุกที่ช่วยเพิ่มระดับความมั่นคงปลอดภัยไซเบอร์ โดยอาศัยการพิสูจน์ตัวตนมากกว่าหนึ่งปัจจัย อันได้แก่ สิ่งที่คุณรู้ (Knowledge Factor) สิ่งที่คุณมี (Possession Factor) และสิ่งที่เป็นลักษณะเฉพาะของคุณ (Inherence Factor)

๑.๑.๒ ขอบเขตการบังคับใช้

กำหนดให้มีการใช้ MFA อย่างน้อยในกรณีดังต่อไปนี้

(๑) บัญชีผู้ดูแลระบบ (Administrator หรือ Privileged Account) ทุกประเภท

(๒) บัญชีผู้ใช้งานที่สามารถเข้าถึงข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลที่อยู่ภายใต้การคุ้มครองตาม กฎหมาย

(๓) ระบบสารสนเทศหลักหรือระบบที่สนับสนุนภารกิจสำคัญของมหาวิทยาลัย

(๔) ระบบที่สามารถเข้าถึงจากเครือข่ายภายนอกหรือผ่านเครือข่ายอินเทอร์เน็ต

(๕) การเข้าถึงระบบจากระยะไกล (Remote Access) เช่น VPN, Remote Desktop, Cloud Console

(๖) ระบบที่มีการเชื่อมต่อกับระบบภายนอกหรือผู้ให้บริการภายนอก

ทั้งนี้ คณะอาจกำหนดให้มีการขยายการใช้ MFA ไปยังระบบหรือกลุ่มผู้ใช้งานอื่นเพิ่มเติมตามระดับความ เสี่ยงที่ประเมินได้

๑.๑.๓ แนวทางการเลือกวิธีการพิสูจน์ตัวตนแบบหลายปัจจัย

ในการกำหนดวิธีการพิสูจน์ตัวตนแบบหลายปัจจัย ให้พิจารณาเลือกวิธีการที่เหมาะสมกับระดับความเสี่ยง ลักษณะการใช้งาน และความพร้อมของระบบ โดยอาจใช้วิธีการหนึ่งหรือหลายวิธีร่วมกัน เช่น

(๑) รหัสผ่านร่วมกับรหัสยืนยันแบบใช้ครั้งเดียว (One-Time Password: OTP)

(๒) แอปพลิเคชันยืนยันตัวตน (Authenticator Application)



(๓) อุปกรณ์ยืนยันตัวตนทางกายภาพ (Hardware Token หรือ Security Key)

(๔) ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

(๕) ชีวมิติ (Biometric) ในกรณีที่มีความเหมาะสมและได้รับการรับรองด้านความปลอดภัย

ทั้งนี้ ให้หลีกเลี่ยงการใช้วิธีการพิสูจน์ตัวตนที่มีความเสี่ยงสูง หรือไม่สอดคล้องกับแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ในปัจจุบัน

๑.๑.๔ ขั้นตอนปฏิบัติในการนำ MFA ไปใช้

ให้คณะดำเนินการตามขั้นตอนดังต่อไปนี้

(๑) การระบุระบบและบัญชีผู้ใช้งานที่ต้องใช้ MFA

ให้คณะสำรวจและจัดทำบัญชีรายชื่อระบบสารสนเทศและบัญชีผู้ใช้งานที่อยู่ในขอบเขตการบังคับใช้ MFA ตามที่มหาวิทยาลัยกำหนด โดยให้จัดลำดับความสำคัญตามระดับความเสี่ยง

(๒) การกำหนดนโยบายและการตั้งค่า MFA

กำหนดนโยบายการใช้ MFA ที่ชัดเจน ครอบคลุมเงื่อนไขการบังคับใช้ วิธีการพิสูจน์ตัวตน การจัดการกรณีอุปกรณ์สูญหาย และการยกเว้นการใช้งานในกรณีจำเป็น โดยต้องได้รับการอนุมัติตามสายการบังคับบัญชา

(๓) การดำเนินการติดตั้งและเปิดใช้ MFA

ดำเนินการติดตั้งหรือกำหนดค่าระบบ MFA ให้สอดคล้องกับระบบสารสนเทศที่ใช้งานอยู่ ทั้งระบบภายในและระบบคลาวด์ พร้อมทั้งทดสอบการทำงานก่อนเปิดใช้งานจริง

(๔) การสื่อสารและสร้างความเข้าใจแก่ผู้ใช้งาน

ดำเนินการแจ้งแนวทางการใช้ MFA แก่ผู้ใช้งานอย่างชัดเจน รวมถึงการจัดทำคู่มือหรือแนวทางปฏิบัติ เพื่อให้ผู้ใช้งานสามารถปฏิบัติตามได้อย่างถูกต้องและลดผลกระทบต่อการใช้งาน

(๕) การบริหารจัดการกรณีฉุกเฉินหรือข้อยกเว้น

กำหนดกระบวนการรองรับกรณีผู้ใช้งานไม่สามารถใช้ MFA ได้ชั่วคราว เช่น อุปกรณ์สูญหาย หรือระบบขัดข้อง โดยต้องมีการบันทึก ตรวจสอบ และอนุมัติเป็นรายการกรณี

๑.๑.๕ การติดตาม ทบทวน และปรับปรุง

ดำเนินการติดตามและทบทวนการใช้ MFA อย่างสม่ำเสมอ เพื่อประเมินประสิทธิภาพ ความเหมาะสม และปัญหาอุปสรรคในการใช้งาน ทั้งนี้ ให้ใช้ผลการติดตามดังกล่าวในการปรับปรุงนโยบาย วิธีการพิสูจน์ตัวตน และขั้นตอนการปฏิบัติให้สอดคล้องกับระดับความเสี่ยงและสภาพการณ์ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป

๑.๒ การจัดการตัวตนและสิทธิ์การเข้าถึง (Identity and Access Management: IAM / Privileged Access Management: PAM)

๑.๒.๑ หลักการและวัตถุประสงค์

กำหนดนโยบายและแนวทางการบริหารจัดการตัวตนและสิทธิ์การเข้าถึงระบบสารสนเทศอย่างเป็นระบบ ครอบคลุมระบบสารสนเทศ ข้อมูล และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศทั้งหมดที่อยู่ในความรับผิดชอบของมหาวิทยาลัย ทั้งนี้ เพื่อให้การเข้าถึงและการใช้งานระบบเป็นไปตามหน้าที่ความรับผิดชอบของผู้ใช้งาน แต่ละรายอย่างเหมาะสม ลดความเสี่ยงจากการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต การใช้สิทธิ์เกินความจำเป็น และการกระทำโดยมิชอบซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย



การบริหารจัดการตัวตนและสิทธิ์ การเข้าถึงให้ยึดหลักการให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติหน้าที่ (Least Privilege) และหลักการแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) เป็นสำคัญ เพื่อให้เกิดการถ่วงดุล ลดความเสี่ยงจากความผิดพลาดหรือการทุจริต และเพิ่มความสามารถในการตรวจสอบย้อนหลัง

๑.๒.๒ ขอบเขตการบังคับใช้

ดำเนินการบริหารจัดการตัวตนและสิทธิ์การเข้าถึงครอบคลุมอย่างน้อย ดังต่อไปนี้

- (๑) บัญชีผู้ใช้งานทั่วไปของบุคลากร นิสิต และผู้ใช้งานที่เกี่ยวข้อง
- (๒) บัญชีผู้ดูแลระบบหรือบัญชีที่มีสิทธิ์พิเศษ (Privileged Accounts)
- (๓) บัญชีผู้ใช้งานของผู้ให้บริการภายนอกหรือผู้รับจ้าง (Vendor / Outsource Accounts)
- (๔) บัญชีระบบหรือบัญชีบริการ (Service Accounts)
- (๕) การเข้าถึงระบบสารสนเทศทั้งภายในและภายนอกเครือข่ายของมหาวิทยาลัย

๑.๒.๓ แนวทางการบริหารจัดการตัวตนและสิทธิ์การเข้าถึง

(๑) การบริหารจัดการวงจรชีวิตบัญชีผู้ใช้งาน (User Account Lifecycle Management)

๑. ดำเนินการบริหารจัดการบัญชีผู้ใช้งานอย่างเป็นระบบตลอดวงจรชีวิตการใช้งาน โดยครอบคลุมขั้นตอน ดังต่อไปนี้การสร้างบัญชีผู้ใช้งาน (User Provisioning)

การสร้างบัญชีผู้ใช้งานต้องเป็นไปตามคำร้องขอที่ได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้มีอำนาจ โดยกำหนดสิทธิ์การเข้าถึงให้สอดคล้องกับบทบาทหน้าที่ของผู้ใช้งาน และต้องบันทึกข้อมูลการอนุมัติไว้เป็นหลักฐาน

๒. การกำหนดและปรับเปลี่ยนสิทธิ์การเข้าถึง (Access Granting and Modification)

การกำหนดหรือปรับเปลี่ยนสิทธิ์การเข้าถึงต้องพิจารณาตามหลัก Least Privilege และ Segregation of Duties และต้องดำเนินการตามขั้นตอนที่กำหนด พร้อมบันทึกเหตุผลและการอนุมัติทุกครั้ง

๓. การยกเลิกหรือเพิกถอนสิทธิ์การเข้าถึง (De-provisioning)

เมื่อผู้ใช้งานพ้นสภาพการเป็นบุคลากร นิสิต หรือสิ้นสุดหน้าที่ หรือไม่มีความจำเป็นต้องเข้าถึงระบบแล้ว ให้ดำเนินการยกเลิกหรือเพิกถอนสิทธิ์การเข้าถึงโดยทันที เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) การจัดการบัญชีที่มีสิทธิ์พิเศษ (Privileged Access Management: PAM)

กำหนดมาตรการควบคุมบัญชีที่มีสิทธิ์พิเศษอย่างเข้มงวด เนื่องจากบัญชีดังกล่าวมีความเสี่ยงสูง และอาจก่อให้เกิดผลกระทบในวงกว้าง หากถูกใช้งานโดยมิชอบมาตรการดังกล่าวให้ครอบคลุมอย่างน้อย ดังต่อไปนี้

๑. การจำกัดจำนวนบัญชีที่มีสิทธิ์พิเศษให้เท่าที่จำเป็น
๒. การแยกบัญชีผู้ใช้งานทั่วไปออกจากบัญชีผู้ดูแลระบบ
๓. การใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (MFA) สำหรับบัญชีที่มีสิทธิ์พิเศษ
๔. การบันทึกและติดตามการใช้งานบัญชีที่มีสิทธิ์พิเศษ (Logging and Monitoring)
๕. การกำหนดระยะเวลาการให้สิทธิ์แบบชั่วคราวในกรณีจำเป็น และการเพิกถอนสิทธิ์เมื่อสิ้นสุดภารกิจ



(๓) การทบทวนสิทธิ์การเข้าถึงและการตรวจสอบ

ดำเนินการทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ เพื่อยืนยันว่าการให้สิทธิ์ยังมีความเหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบ

ทั้งนี้ ให้ใช้ผลการทบทวนสิทธิ์เป็นข้อมูลในการปรับปรุงทะเบียนบัญชีผู้ใช้งาน การเพิกถอนสิทธิ์ที่ไม่จำเป็น และการเสริมสร้างมาตรการควบคุมให้มีประสิทธิภาพยิ่งขึ้น

๑.๒.๔ ขั้นตอนปฏิบัติในการดำเนินการด้าน IAM / PAM

ให้คณะดำเนินการตามขั้นตอนปฏิบัติ ดังต่อไปนี้

- (๑) จัดทำและปรับปรุงบัญชีรายชื่อผู้ใช้งานและบัญชีที่มีสิทธิ์พิเศษให้เป็นปัจจุบัน
- (๒) กำหนดบทบาทและสิทธิ์การเข้าถึงตามหน้าที่ (Role-Based Access Control)
- (๓) จัดทำแบบคำร้องและขั้นตอนการอนุมัติการให้สิทธิ์และปรับเปลี่ยนสิทธิ์
- (๔) บูรณาการการใช้ MFA และการบันทึกการใช้งานกับบัญชีที่มีความเสี่ยงสูง
- (๕) ดำเนินการทบทวนสิทธิ์และรายงานผลต่อผู้บังคับบัญชาหรือคณะกรรมการที่เกี่ยวข้องตามรอบที่กำหนด

๑.๒.๕ การติดตามและปรับปรุง

ดำเนินการติดตาม ประเมินผล และปรับปรุงการดำเนินการด้านการจัดการตัวตนและสิทธิ์การเข้าถึงอย่างต่อเนื่อง โดยพิจารณาจากผลการตรวจประเมิน เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และการเปลี่ยนแปลงด้านเทคโนโลยีและภัยคุกคาม เพื่อให้มาตรการด้าน IAM และ PAM มีความเหมาะสมทันสมัย และสอดคล้องกับระดับความเสี่ยงที่เปลี่ยนแปลงไป

๑.๓ การกำหนดค่าความมั่นคงปลอดภัยของระบบและการเสริมความแข็งแกร่งของระบบ (Secure Configuration and System Hardening)

๑.๓.๑ หลักการและวัตถุประสงค์

กำหนดมาตรฐานและแนวทางการตั้งค่าความมั่นคงปลอดภัยของระบบสารสนเทศ อุปกรณ์เครือข่าย ระบบปฏิบัติการ และแอปพลิเคชันอย่างเหมาะสมและเป็นระบบ โดยมุ่งลดจุดอ่อนด้านความมั่นคงปลอดภัยที่อาจถูกใช้เป็นช่องทางในการโจมตีหรือก่อให้เกิดเหตุภัยคุกคามทางไซเบอร์ ทั้งนี้ เพื่อยกระดับความมั่นคงปลอดภัยของระบบตั้งแต่ระดับโครงสร้างพื้นฐานจนถึงระดับแอปพลิเคชัน และเพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีความพร้อมใช้งาน มีความมั่นคงปลอดภัย และสามารถรองรับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ

การกำหนดค่าความมั่นคงปลอดภัยของระบบและการเสริมความแข็งแกร่งของระบบให้ถือเป็นมาตรการพื้นฐานที่ต้องดำเนินการอย่างต่อเนื่อง ควบคู่กับมาตรการด้านอื่น ๆ เพื่อป้องกันการโจมตีที่อาศัยช่องโหว่จากการตั้งค่าระบบที่ไม่เหมาะสมหรือการใช้งานค่าตั้งต้นที่ไม่ปลอดภัย



๑.๓.๒ ขอบเขตการบังคับใช้

กำหนดค่าความมั่นคงปลอดภัยของระบบและการเสริมความแข็งแกร่งของระบบ ครอบคลุมอย่างน้อยในระบบและองค์ประกอบดังต่อไปนี้

- (๑) ระบบปฏิบัติการของเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่าย
- (๒) แอปพลิเคชัน ระบบฐานข้อมูล และระบบสารสนเทศของมหาวิทยาลัย
- (๓) อุปกรณ์เครือข่ายและอุปกรณ์ความมั่นคงปลอดภัย เช่น Firewall, Router, Switch, Wireless Access Point

- (๔) ระบบสารสนเทศที่เชื่อมต่อกับเครือข่ายภายนอกหรือระบบคลาวด์
- (๕) ระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลสำคัญหรือข้อมูลที่อยู่ภายใต้การคุ้มครองตามกฎหมาย

๑.๓.๓ แนวทางการกำหนดค่าความมั่นคงปลอดภัยและการเสริมความแข็งแกร่งของระบบ

(๑) การกำหนดมาตรฐานการตั้งค่าความมั่นคงปลอดภัย (Secure Configuration Baseline)

ดำเนินการจัดทำและกำหนดมาตรฐานการตั้งค่าความมั่นคงปลอดภัยขั้นต่ำ (Secure Configuration Baseline) สำหรับระบบและอุปกรณ์แต่ละประเภท โดยอ้างอิงแนวปฏิบัติที่เป็นที่ยอมรับ เช่น มาตรฐานสากลหรือแนวทางของหน่วยงานภาครัฐ ทั้งนี้ เพื่อให้การตั้งค่าระบบมีความสอดคล้อง เป็นมาตรฐานเดียวกัน และลดความเสี่ยงจากการตั้งค่าที่ไม่เหมาะสม

มาตรฐานดังกล่าวควรครอบคลุมการตั้งค่าความปลอดภัยเริ่มต้น การกำหนดนโยบายรหัสผ่าน การควบคุมการเข้าถึง การตั้งค่าการบันทึกเหตุการณ์ และการจำกัดการใช้งานฟังก์ชันหรือบริการที่ไม่จำเป็น

(๒) การปิดหรือจำกัดการใช้งานบริการที่ไม่จำเป็น

ให้คณะดำเนินการตรวจสอบและปิด หรือจำกัดการใช้งานบริการ พอร์ต ฟังก์ชัน หรือซอฟต์แวร์ที่ไม่จำเป็นต่อการใช้งานหรือภารกิจของระบบนั้น ๆ เพื่อลดพื้นที่การโจมตี (Attack Surface) และลดโอกาสที่ผู้ไม่หวังดีจะใช้เป็นช่องทางในการเข้าถึงหรือโจมตีระบบ

ทั้งนี้ การเปิดใช้งานบริการเพิ่มเติมต้องได้รับการพิจารณาและอนุมัติตามขั้นตอนที่มหาวิทยาลัยกำหนด และต้องมีการบันทึกไว้เป็นหลักฐาน

(๓) การอัปเดตแพตช์และซอฟต์แวร์อย่างสม่ำเสมอ

กำหนดกระบวนการบริหารจัดการแพตช์และการอัปเดตซอฟต์แวร์ (Patch Management) อย่างเป็นระบบ โดยให้ดำเนินการติดตาม แจ้งเตือน และติดตั้งแพตช์หรืออัปเดตด้านความมั่นคงปลอดภัยตามระดับความสำคัญของช่องโหว่และความเสี่ยง

ทั้งนี้ ให้กำหนดระยะเวลาในการติดตั้งแพตช์ที่เหมาะสมตามระดับความรุนแรงของช่องโหว่ และให้มีการทดสอบแพตช์ก่อนนำไปใช้งานจริงในระบบสำคัญ เพื่อป้องกันผลกระทบต่อการให้บริการ

(๔) การตรวจสอบและประเมินการตั้งค่าความมั่นคงปลอดภัยเป็นระยะ

ให้คณะดำเนินการตรวจสอบและประเมินการตั้งค่าความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ เพื่อยืนยันว่าการตั้งค่าระบบยังคงเป็นไปตามมาตรฐานที่กำหนด และไม่มีการเปลี่ยนแปลงหรือเบี่ยงเบนจากค่าที่ปลอดภัยโดยไม่ได้รับอนุญาต



การตรวจสอบดังกล่าวอาจดำเนินการผ่านการตรวจประเมินภายใน การใช้เครื่องมือสแกนช่องโหว่ หรือการตรวจสอบจากหน่วยงานที่เกี่ยวข้อง ทั้งนี้ ให้บันทึกผลการตรวจสอบและนำผลดังกล่าวไปใช้ในการปรับปรุงแก้ไขการตั้งค่าระบบอย่างเหมาะสม

๑.๓.๔ ขั้นตอนปฏิบัติในการดำเนินการ

ให้คณะดำเนินการตามขั้นตอนปฏิบัติ ดังต่อไปนี้

- (๑) สำรวจและจัดทำบัญชีรายชื่อระบบ อุปกรณ์ และแอปพลิเคชันที่อยู่ในความรับผิดชอบ
- (๒) กำหนดหรือปรับปรุงค่าการตั้งค่าความมั่นคงปลอดภัยให้เป็นไปตามมาตรฐานที่มหาวิทยาลัยกำหนด
- (๓) ปิดหรือจำกัดการใช้งานบริการและฟังก์ชันที่ไม่จำเป็น
- (๔) ดำเนินการอัปเดตแพตช์และซอฟต์แวร์ตามรอบระยะเวลาที่กำหนด
- (๕) ตรวจสอบและบันทึกผลการตั้งค่าและการเปลี่ยนแปลงทุกครั้ง
- (๖) รายงานผลการดำเนินการและประเมินความเสี่ยงที่พบต่อผู้บังคับบัญชาหรือหน่วยงานที่รับผิดชอบ

ตามสายการบังคับบัญชา

๑.๓.๕ การติดตามและปรับปรุง

ดำเนินการติดตาม ทบทวน และปรับปรุงมาตรฐานและแนวทางการกำหนดค่าความมั่นคงปลอดภัยของระบบอย่างต่อเนื่อง โดยพิจารณาจากผลการตรวจประเมิน เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป เพื่อให้มาตรการด้าน Secure Configuration และ System Hardening มีความเหมาะสม ทันสมัย และสามารถรองรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

๑.๔ การพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure Software Development Life Cycle: Secure SDLC)

๑.๔.๑ หลักการและวัตถุประสงค์

กำหนดให้การพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุง แก้ไข และต่อเติมระบบสารสนเทศเดิม ต้องดำเนินการตามแนวคิดการพัฒนาระบบอย่างมั่นคงปลอดภัย (Secure Software Development Life Cycle: Secure SDLC) โดยบูรณาการมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เข้าไปในทุกขั้นตอนของวงจรการพัฒนาระบบ ตั้งแต่การวิเคราะห์ความต้องการ การออกแบบ การพัฒนา การทดสอบ การนำระบบไปใช้งาน และการบำรุงรักษา

ทั้งนี้ เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นจากกระบวนการพัฒนาระบบที่ไม่รัดกุม และเพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีความมั่นคงปลอดภัยตั้งแต่ต้นทาง (Security by Design และ Security by Default) พร้อมทั้งสนับสนุนการดำเนินงานอย่างมีประสิทธิภาพ และต่อเนื่อง



๑.๔.๒ ขอบเขตการบังคับใช้

ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย ต้องดำเนินการตามแนวคิด Secure SDLC ครอบคลุมระบบสารสนเทศทุกประเภทที่พัฒนา ใช้งานให้กับมหาวิทยาลัย หรือพัฒนา ใช้งานให้หน่วยงานภายนอกมหาวิทยาลัย รวมถึงระบบเว็บแอปพลิเคชัน ระบบฐานข้อมูล ระบบบริการอิเล็กทรอนิกส์ ระบบที่เชื่อมต่อกับระบบภายนอก ระบบที่มีการจ้างพัฒนาจากผู้ให้บริการภายนอก และระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลสำคัญหรือข้อมูลส่วนบุคคล การดำเนินงานปรับปรุงระบบเดิม การพัฒนาเพิ่มเติม (Enhancement) และการบำรุงรักษาระบบในระยะยาว

๑.๔.๓ แนวทางการดำเนินการตาม Secure SDLC ในแต่ละขั้นตอน

(๑) ขั้นตอนการวิเคราะห์ความต้องการ (Requirement Analysis)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย พิจารณาและระบุข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของความต้องการของระบบ โดยต้องคำนึงถึงประเภทข้อมูล ความสำคัญของระบบ ความเสี่ยงด้านความมั่นคงปลอดภัย และข้อกำหนดตามกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง รวมถึงการกำหนดระดับการคุ้มครองข้อมูลและความต้องการด้านการควบคุมการเข้าถึงอย่างเหมาะสม

(๒) ขั้นตอนการออกแบบระบบ (System Design)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย ดำเนินการออกแบบสถาปัตยกรรมระบบโดยคำนึงถึงหลักการด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การแยกส่วนของระบบ การควบคุมการเข้าถึง การป้องกันข้อมูล การบันทึกเหตุการณ์ และการรองรับการตรวจสอบย้อนหลัง ทั้งนี้ เพื่อป้องกันความเสี่ยงจากช่องโหว่เชิงโครงสร้าง และสนับสนุนการป้องกันภัยคุกคามทางไซเบอร์ในระยะยาว

(๓) ขั้นตอนการพัฒนา (Development)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย ปฏิบัติตามแนวทางการพัฒนาโปรแกรมอย่างมั่นคงปลอดภัย (Secure Coding Practices) โดยหลีกเลี่ยงการใช้รูปแบบการเขียนโปรแกรมที่อาจก่อให้เกิดช่องโหว่ด้านความมั่นคงปลอดภัย และให้มีการตรวจสอบคุณภาพและความปลอดภัยของโค้ดอย่างเหมาะสมระหว่างการพัฒนา

(๔) ขั้นตอนการทดสอบ (Testing)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย ดำเนินการทดสอบระบบด้านความมั่นคงปลอดภัย ก่อนนำระบบไปใช้งานจริง โดยครอบคลุมการทดสอบช่องโหว่ การทดสอบการตั้งค่าความมั่นคงปลอดภัย และการทดสอบการควบคุมการเข้าถึง ทั้งนี้ เพื่อยืนยันว่าระบบเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้

(๕) ขั้นตอนการนำระบบไปใช้งาน (Deployment)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย ดำเนินการตรวจสอบความพร้อมด้านความมั่นคงปลอดภัยของระบบก่อนเปิดใช้งานจริง โดยต้องมั่นใจว่าการตั้งค่าระบบเป็นไปตามมาตรฐาน การเข้าถึงได้รับการควบคุมอย่างเหมาะสม และมีมาตรการรองรับเหตุการณ์ด้านความมั่นคงปลอดภัย



(๖) ขั้นตอนการบำรุงรักษาและปรับปรุงระบบ (Maintenance)

ให้ผู้พัฒนาระบบสารสนเทศของมหาวิทยาลัย มีการติดตาม ตรวจสอบ และปรับปรุงระบบอย่างต่อเนื่อง รวมถึงการแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยที่ตรวจพบ การอัปเดตซอฟต์แวร์ และการทบทวนมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับสภาพการณ์ภัยคุกคามที่เปลี่ยนแปลงไป

๑.๔.๔ ขั้นตอนปฏิบัติในการดำเนินการตาม Secure SDLC

ให้คณะดำเนินการตามขั้นตอนปฏิบัติ ดังต่อไปนี้

- (๑) กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของเอกสารความต้องการระบบ
- (๒) จัดให้มีการทบทวนการออกแบบระบบด้านความมั่นคงปลอดภัยก่อนการพัฒนา
- (๓) ตรวจสอบความมั่นคงปลอดภัยของโค้ดและระบบระหว่างการพัฒนาและก่อนนำไปใช้งาน
- (๔) บันทึกและติดตามการแก้ไขช่องโหว่ที่ตรวจพบจนกว่าจะแล้วเสร็จ
- (๕) จัดทำเอกสารและคู่มือด้านความมั่นคงปลอดภัยประกอบระบบสารสนเทศ
- (๖) รายงานผลการดำเนินการและประเมินความเสี่ยงต่อผู้บังคับบัญชาหรือหน่วยงานที่เกี่ยวข้อง

๑.๔.๕ การติดตามและปรับปรุง

ให้คณะดำเนินการติดตาม ทบทวน และปรับปรุงแนวทางการดำเนินการตาม Secure SDLC อย่างต่อเนื่อง โดยอาศัยผลการตรวจประเมิน เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มภัยคุกคามใหม่ ๆ เพื่อให้กระบวนการพัฒนาระบบสารสนเทศของมหาวิทยาลัยมีความมั่นคงปลอดภัย ทันสมัย และสอดคล้องกับมาตรฐานและแนวปฏิบัติที่เหมาะสม

๑.๕ การเข้ารหัสข้อมูลขณะจัดเก็บและขณะรับส่ง (Data Encryption at Rest and in Transit)

๑.๕.๑ หลักการและวัตถุประสงค์

กำหนดให้มีการเข้ารหัสข้อมูลที่มีความสำคัญ หรือข้อมูลที่อยู่ภายใต้การคุ้มครองตามกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง ทั้งในขณะจัดเก็บ (Data at Rest) และในขณะรับส่งผ่านเครือข่าย (Data in Transit) เพื่อป้องกันการเข้าถึง การเปิดเผย การดักจับ หรือการนำข้อมูลไปใช้โดยมิได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย ผู้ใช้บริการ หรือผู้มีส่วนได้ส่วนเสีย

การเข้ารหัสข้อมูลถือเป็นมาตรการพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ช่วยลดความเสี่ยง และผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การรั่วไหลของข้อมูล การโจมตีระบบจัดเก็บข้อมูล หรือการดักฟังข้อมูลระหว่างการสื่อสาร รวมทั้งสนับสนุนการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูล และมาตรฐานที่เกี่ยวข้อง

๑.๕.๒ ขอบเขตการบังคับใช้

ให้การเข้ารหัสข้อมูลครอบคลุมอย่างน้อยในกรณีดังต่อไปนี้

- (๑) ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว และข้อมูลที่อยู่ภายใต้การคุ้มครองตามกฎหมาย
- (๒) ข้อมูลสำคัญด้านการบริหาร การเงิน การศึกษา การวิจัย และข้อมูลเชิงยุทธศาสตร์
- (๓) ระบบฐานข้อมูล ระบบจัดเก็บข้อมูล สื่อบันทึกข้อมูล และระบบสำรองข้อมูล
- (๔) การรับส่งข้อมูลผ่านเครือข่ายภายใน เครือข่ายภายนอก และเครือข่ายอินเทอร์เน็ต
- (๕) ระบบสารสนเทศที่เชื่อมต่อกับระบบคลาวด์หรือผู้ให้บริการภายนอก



๑.๕.๓ แนวทางการดำเนินการด้านการเข้ารหัสข้อมูล

(๑) การเข้ารหัสข้อมูลขณะจัดเก็บ (Data Encryption at Rest)

ดำเนินการเข้ารหัสข้อมูลที่จัดเก็บอยู่ในระบบฐานข้อมูล ระบบไฟล์ ระบบจัดเก็บข้อมูลส่วนกลาง ระบบสำรองข้อมูล และสื่อบันทึกข้อมูลทุกประเภท โดยเลือกใช้กลไกการเข้ารหัสที่เหมาะสมกับประเภทและระดับความสำคัญของข้อมูล ทั้งนี้ เพื่อป้องกันการเข้าถึงข้อมูลในกรณีที่ระบบหรืออุปกรณ์ถูกโจมตี สูญหาย ถูกขโมย หรือถูกเข้าถึงโดยมิได้รับอนุญาต

(๒) การเข้ารหัสข้อมูลขณะรับส่ง (Data Encryption in Transit)

กำหนดให้มีการเข้ารหัสข้อมูลในระหว่างการรับส่งผ่านเครือข่าย โดยใช้โปรโตคอลและกลไกการสื่อสารที่มีความมั่นคงปลอดภัย เพื่อป้องกันการดักฟัง การแก้ไข หรือการปลอมแปลงข้อมูลระหว่างการสื่อสารระหว่างผู้ใช้งาน ระบบสารสนเทศ และผู้ให้บริการภายนอก

(๓) การเลือกใช้อัลกอริทึมและมาตรฐานการเข้ารหัส

การเลือกใช้อัลกอริทึมและกลไกการเข้ารหัสต้องเป็นไปตามมาตรฐานที่ยอมรับในปัจจุบัน และสอดคล้องกับแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม โดยต้องหลีกเลี่ยงการใช้อัลกอริทึมที่ล้าสมัย หรือมีความเสี่ยงสูง และต้องมีการทบทวน ปรับปรุง หรือเปลี่ยนแปลงการใช้งานให้ทันสมัยอย่างสม่ำเสมอ

(๔) การบริหารจัดการกุญแจเข้ารหัส (Key Management)

กำหนดกระบวนการบริหารจัดการกุญแจเข้ารหัสอย่างเป็นระบบ ครอบคลุมการสร้าง การจัดเก็บ การใช้งาน การหมุนเวียน การสำรอง และการเพิกถอนกุญแจเข้ารหัส โดยต้องกำหนดสิทธิ์การเข้าถึงกุญแจเข้ารหัสอย่างเหมาะสม จำกัดเฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง และต้องมีการบันทึกและตรวจสอบการใช้งานกุญแจเข้ารหัส เพื่อให้สามารถตรวจสอบย้อนหลังได้

๑.๕.๔ ขั้นตอนปฏิบัติในการดำเนินการ

ให้คณะดำเนินการตามขั้นตอนปฏิบัติ ดังต่อไปนี้

- (๑) จำแนกประเภทข้อมูลและกำหนดระดับความสำคัญของข้อมูลที่อยู่ในความรับผิดชอบ
- (๒) กำหนดวิธีการและกลไกการเข้ารหัสที่เหมาะสมกับประเภทข้อมูลและระบบสารสนเทศ
- (๓) ดำเนินการเข้ารหัสข้อมูลทั้งในขณะจัดเก็บและขณะรับส่งตามมาตรฐานที่มหาวิทยาลัยกำหนด
- (๔) จัดให้มีระบบหรือกระบวนการบริหารจัดการกุญแจเข้ารหัสอย่างเหมาะสม
- (๕) กำหนดสิทธิ์การเข้าถึงข้อมูลและกุญแจเข้ารหัสตามหลักการให้สิทธิ์เท่าที่จำเป็น
- (๖) ตรวจสอบและทบทวนการใช้งานการเข้ารหัสและกุญแจเข้ารหัสอย่างสม่ำเสมอ
- (๗) บันทึกและรายงานเหตุการณ์ที่เกี่ยวข้องกับการเข้ารหัสหรือการจัดการกุญแจเข้ารหัสตามกระบวนการที่กำหนด

๑.๕.๕ การติดตามและปรับปรุง

ดำเนินการติดตาม ประเมินผล และปรับปรุงแนวทางการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสอย่างต่อเนื่อง โดยพิจารณาจากผลการตรวจประเมิน เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และการเปลี่ยนแปลงด้านเทคโนโลยีและมาตรฐานการเข้ารหัส เพื่อให้มาตรการด้านการเข้ารหัสข้อมูลมีความเหมาะสม ทันสมัย และสามารถรองรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ



๑.๖ การเตรียมความพร้อมด้านการเข้ารหัสสำหรับยุคควอนตัม (Post-Quantum Cryptography)

๑.๖.๑ หลักการและวัตถุประสงค์

กำหนดนโยบายและแนวทางในการเตรียมความพร้อมรองรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดจากการพัฒนาของเทคโนโลยีควอนตัม ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของกลไกการเข้ารหัส การพิสูจน์ตัวตน และการแลกเปลี่ยนกุญแจที่ใช้อยู่ในปัจจุบัน โดยเฉพาะระบบและข้อมูลที่ต้องการการคุ้มครองในระยะยาว

การเตรียมความพร้อมดังกล่าวมีวัตถุประสงค์เพื่อให้มหาวิทยาลัยสามารถบริหารจัดการความเสี่ยงเชิงคาดการณ์ (Forward-Looking Risk Management) ลดผลกระทบจากการเปลี่ยนแปลงทางเทคโนโลยีในอนาคต และรักษาความเชื่อมั่นด้านความมั่นคงปลอดภัยไซเบอร์ของข้อมูลและระบบสารสนเทศอย่างต่อเนื่องและยั่งยืน

๑.๖.๒ ขอบเขตการดำเนินการเชิงนโยบาย

ดำเนินการเตรียมความพร้อมด้าน Post-Quantum Cryptography ดำเนินการในเชิงนโยบาย และการบริหารจัดการความเสี่ยง โดยครอบคลุมอย่างน้อย ดังต่อไปนี้

- (๑) ระบบสารสนเทศและโครงสร้างพื้นฐานที่ใช้กลไกการเข้ารหัสหรือการพิสูจน์ตัวตน
- (๒) ข้อมูลสำคัญหรือข้อมูลที่ต้องการการคุ้มครองในระยะยาว เช่น ข้อมูลส่วนบุคคล ข้อมูลวิจัย ข้อมูลเชิงยุทธศาสตร์

(๓) ระบบที่มีอายุการใช้งานยาวนานหรือยากต่อการปรับเปลี่ยนในระยะสั้น

(๔) ระบบที่มีการเชื่อมต่อกับหน่วยงานหรือผู้ให้บริการภายนอก

๑.๖.๓ แนวทางการเตรียมความพร้อมด้าน Post-Quantum Cryptography

(๑) การติดตามแนวโน้มและมาตรฐานที่เกี่ยวข้อง

ดำเนินการติดตามพัฒนาการ แนวโน้ม และมาตรฐานด้านการเข้ารหัสสำหรับยุคควอนตัมจากหน่วยงานที่เกี่ยวข้องทั้งในระดับประเทศและระดับสากล รวมถึงแนวปฏิบัติที่เป็นที่ยอมรับ เพื่อใช้เป็นข้อมูลประกอบการกำหนดทิศทางเชิงนโยบายและการวางแผนในระยะยาว

(๒) การสำรวจและประเมินผลกระทบต่อระบบและข้อมูล

ดำเนินการสำรวจระบบสารสนเทศ กลไกการเข้ารหัส และการพิสูจน์ตัวตนที่ใช้ในปัจจุบัน เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการพัฒนาของเทคโนโลยีควอนตัม โดยให้ความสำคัญกับระบบและข้อมูลที่ต้องการการคุ้มครองในระยะยาว หรือมีผลกระทบสูงหากเกิดการละเมิดความมั่นคงปลอดภัย

(๓) การบูรณาการ Post-Quantum Risk เข้ากับการบริหารความเสี่ยงองค์กร

ดำเนินการนำประเด็นความเสี่ยงจากเทคโนโลยีควอนตัมมาบูรณาการเป็นส่วนหนึ่งของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงองค์กร โดยพิจารณาในเชิงการวางแผนระยะยาวและการเตรียมความพร้อมเชิงกลยุทธ์

(๔) การวางแผนการเปลี่ยนผ่านเชิงนโยบาย (Migration Planning)

ดำเนินการจัดทำแผนการเตรียมความพร้อมและการเปลี่ยนผ่านกลไกการเข้ารหัสในระยะยาว โดยมุ่งเน้นการกำหนดหลักการ แนวทาง และลำดับความสำคัญของระบบที่ควรได้รับการปรับปรุงก่อน ทั้งนี้ การเปลี่ยนผ่านให้ดำเนินการอย่างเป็นขั้นตอน และคำนึงถึงความต่อเนื่องในการให้บริการและความคุ้มค่าในการใช้ทรัพยากร



๑.๖.๔ ขั้นตอนปฏิบัติในการดำเนินการ

ให้คณะดำเนินการตามขั้นตอนปฏิบัติ ดังต่อไปนี้

- (๑) รวบรวมข้อมูลระบบและกลไกการเข้ารหัสที่ใช้อยู่ในความรับผิดชอบ
- (๒) จำแนกระบบและข้อมูลตามระดับความสำคัญและอายุการคุ้มครองของข้อมูล
- (๓) ประเมินความเสี่ยงและผลกระทบจากเทคโนโลยีควอนตัมในเชิงนโยบาย
- (๔) บันทึกประเด็นความเสี่ยงด้าน Post-Quantum Cryptography ไว้ในทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- (๕) เสนอแนะแผนการเตรียมความพร้อมหรือแผนการเปลี่ยนผ่านต่อผู้บริหารตามสายการบังคับบัญชา
- (๖) ติดตามและทบทวนสถานการณ์และแนวโน้มอย่างสม่ำเสมอ

๑.๖.๕ การติดตามและทบทวน

ดำเนินการติดตามและทบทวนแนวทางการเตรียมความพร้อมด้าน Post-Quantum Cryptography อย่างต่อเนื่อง โดยพิจารณาจากการเปลี่ยนแปลงของเทคโนโลยี มาตรฐาน และระดับความเสี่ยง เพื่อปรับปรุงนโยบายและแผนการดำเนินงานให้มีความเหมาะสมและทันสมัยอยู่เสมอ

๒. การตรวจจับ (Detect)

มาตรการด้านการตรวจจับ มีวัตถุประสงค์เพื่อให้มหาวิทยาลัยสามารถตรวจพบเหตุผิดปกติ เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ก่อนที่จะก่อให้เกิดผลกระทบต่อข้อมูล ระบบสารสนเทศ และภารกิจหลักของมหาวิทยาลัย ทั้งนี้ การตรวจจับที่มีประสิทธิภาพต้องอาศัยระบบเฝ้าระวังอย่างต่อเนื่อง การวิเคราะห์ข้อมูลเชิงลึก และการใช้ข้อมูลข่าวกรองด้านภัยคุกคามทางไซเบอร์เพื่อประกอบการตัดสินใจ

๒.๑ ระบบเฝ้าระวังและตรวจจับเหตุผิดปกติ (Security Information and Event Management: SIEM / Security Operations Center: SOC)

๒.๑.๑ หลักการและวัตถุประสงค์

จัดให้มีระบบหรือกลไกในการเฝ้าระวัง ตรวจจับ วิเคราะห์ และแจ้งเตือนเหตุผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่องและเป็นระบบ โดยอาศัยระบบบริหารจัดการและวิเคราะห์ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Information and Event Management: SIEM) และ/หรือการดำเนินงานของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Security Operations Center: SOC)

ทั้งนี้ เพื่อให้มหาวิทยาลัยสามารถตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันท่วงที ลดระยะเวลาในการตรวจจับ (Mean Time to Detect: MTTD) และสนับสนุนการตอบสนองต่อเหตุการณ์อย่างเหมาะสม ก่อนที่เหตุการณ์ดังกล่าวจะก่อให้เกิดผลกระทบต่อข้อมูล ระบบสารสนเทศ การให้บริการ และภารกิจหลักของมหาวิทยาลัย

การดำเนินการดังกล่าวอาจอยู่ในรูปแบบการดำเนินการภายในมหาวิทยาลัย การใช้บริการจากผู้ให้บริการภายนอก หรือการดำเนินการในรูปแบบผสมผสาน ทั้งนี้ ให้พิจารณาตามความเหมาะสมของบริบท ความเสี่ยง และทรัพยากรของมหาวิทยาลัย



๒.๑.๒ ขอบเขตและคุณลักษณะของระบบ SIEM / SOC

ระบบเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติต้องมีความสามารถในการรวบรวม วิเคราะห์ เชื่อมโยง และจัดเก็บข้อมูลเหตุการณ์ (Event) และข้อมูลจราจรทางคอมพิวเตอร์จากแหล่งต่าง ๆ อย่างครบถ้วน และต่อเนื่อง โดยครอบคลุมอย่างน้อย ดังต่อไปนี้

- (๑) ระบบเครือข่ายและอุปกรณ์เครือข่าย
- (๒) เครื่องแม่ข่าย ระบบปฏิบัติการ และระบบฐานข้อมูล
- (๓) แอปพลิเคชันและระบบสารสนเทศของมหาวิทยาลัย
- (๔) ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น Firewall, IDS/IPS, Endpoint Security
- (๕) ระบบคลาวด์และบริการจากผู้ให้บริการภายนอก

ทั้งนี้ ระบบต้องสามารถวิเคราะห์พฤติกรรมที่ผิดปกติ การพยายามบุกรุก การละเมิดนโยบาย ด้านความมั่นคงปลอดภัยไซเบอร์ และเหตุการณ์ที่อาจเป็นภัยคุกคามทางไซเบอร์ รวมถึงสามารถจัดลำดับความสำคัญของเหตุการณ์ตามระดับความรุนแรงและผลกระทบได้อย่างเหมาะสม

๒.๑.๓ แนวทางการดำเนินการและการกำกับดูแลเชิงระบบ

กำหนดโครงสร้างการกำกับดูแลการดำเนินงานด้าน SIEM / SOC อย่างชัดเจน โดยกำหนดบทบาทหน้าที่ ความรับผิดชอบ และบุคลากรที่เกี่ยวข้อง เพื่อให้การเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติเป็นไปอย่างต่อเนื่อง ตรวจสอบได้ และสามารถบูรณาการกับกระบวนการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

๒.๑.๔ แนวทางการปฏิบัติ

(๑) การกำหนดขอบเขตระบบและแหล่งข้อมูล

กำหนดขอบเขตของระบบ แหล่งข้อมูล และอุปกรณ์ที่ต้องส่งข้อมูลเหตุการณ์หรือ Log เข้าสู่ระบบ SIEM อย่างชัดเจน โดยพิจารณาจากระดับความสำคัญของระบบ ความเสี่ยง และผลกระทบที่อาจเกิดขึ้น ทั้งนี้ ให้จัดทำบัญชีแหล่งข้อมูลและทบทวนขอบเขตดังกล่าวอย่างสม่ำเสมอ เพื่อให้การเฝ้าระวังครอบคลุมระบบสำคัญอย่างแท้จริง

(๒) การกำหนดกรณีเหตุการณ์ผิดปกติและรูปแบบพฤติกรรมที่ต้องเฝ้าระวัง

กำหนดกรณีเหตุการณ์ผิดปกติ รูปแบบพฤติกรรม และเหตุการณ์ที่ต้องเฝ้าระวัง (Use Case / Detection Scenario) ตามระดับความเสี่ยงของระบบและข้อมูล เช่น การพยายามเข้าสู่ระบบผิดพลาดซ้ำ ๆ การเข้าถึงระบบจากตำแหน่งที่ผิดปกติ การใช้สิทธิ์เกินขอบเขต หรือการเปลี่ยนแปลงการตั้งค่าระบบโดยมิได้รับอนุญาต

ทั้งนี้ ให้มีการจัดลำดับความสำคัญของกรณีเฝ้าระวัง เพื่อให้สามารถใช้ทรัพยากรในการวิเคราะห์และตอบสนองได้อย่างเหมาะสม

(๓) การกำหนดกระบวนการแจ้งเตือนและการประสานงาน

กำหนดกระบวนการแจ้งเตือน (Alert) เมื่อระบบตรวจพบเหตุการณ์ผิดปกติ โดยระบุเงื่อนไข ระดับความรุนแรง ช่องทางการแจ้งเตือน และผู้รับผิดชอบอย่างชัดเจน รวมถึงกำหนดแนวทางการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อให้สามารถดำเนินการตรวจสอบและตอบสนองต่อเหตุการณ์ได้อย่างทันทั่วทั้งที่



(๔) การติดตาม วิเคราะห์ และยกระดับเหตุการณ์

มีการติดตาม วิเคราะห์ และประเมินเหตุการณ์ที่ตรวจพบอย่างเป็นระบบ โดยพิจารณาระดับความรุนแรง ผลกระทบ และแนวโน้มการขยายตัวของเหตุการณ์ ทั้งนี้ ให้สามารถยกระดับเหตุการณ์ไปยังหน่วยงาน หรือผู้มีอำนาจตัดสินใจตามระดับความรุนแรง เพื่อรองรับการตอบสนองในระดับที่เหมาะสม

(๕) การทบทวนและปรับปรุงกฎการตรวจจับอย่างต่อเนื่อง

ดำเนินการทบทวน ประเมิน และปรับปรุงกฎการตรวจจับ (Detection Rules / Correlation Rules) และแนวทางการเฝ้าระวังอย่างสม่ำเสมอ โดยอาศัยผลการตรวจพบเหตุการณ์จริง บทเรียนที่ได้รับ เหตุการณ์ ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา และแนวโน้มภัยคุกคามใหม่ ๆ เพื่อเพิ่มประสิทธิภาพในการตรวจจับ และลดการแจ้งเตือนที่ไม่จำเป็น

๒.๑.๕ การเชื่อมโยงกับกระบวนการอื่น

ให้การดำเนินงานด้าน SIEM / SOC เชื่อมโยงกับกระบวนการด้านการบริหารความเสี่ยง การตอบสนอง เหตุการณ์ การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และการรายงานต่อผู้บริหาร เพื่อให้การเฝ้าระวัง และตรวจจับเหตุผิดปกติเป็นส่วนหนึ่งของระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์แบบครบวงจร ของมหาวิทยาลัย

๒.๒ การจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์และ Log ตามกฎหมาย

๒.๒.๑ หลักการและวัตถุประสงค์

ดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และข้อมูลเหตุการณ์ของระบบสารสนเทศ อย่างครบถ้วน ถูกต้อง เป็นระบบ และเป็นไปตามกฎหมาย ระเบียบ ประกาศ และแนวทางที่เกี่ยวข้อง ทั้งนี้ เพื่อใช้เป็นหลักฐานในการตรวจสอบ วิเคราะห์ และสืบสวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึง เพื่อสนับสนุนการดำเนินการทางกฎหมาย การรายงานต่อหน่วยงานที่เกี่ยวข้อง และการพิสูจน์ข้อเท็จจริงในกรณีที่เกิดเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์

การจัดเก็บและวิเคราะห์ข้อมูล Log ต้องดำเนินการโดยคำนึงถึงความครบถ้วน ความถูกต้อง ความน่าเชื่อถือ ความสามารถในการตรวจสอบย้อนหลัง และการคุ้มครองข้อมูลส่วนบุคคล โดยต้องมีการกำหนด มาตรการควบคุมการเข้าถึง การรักษาความมั่นคงปลอดภัยของข้อมูล Log และการกำหนดระยะเวลาการจัดเก็บ ข้อมูลอย่างเหมาะสมและสมดุลระหว่างความจำเป็นด้านความมั่นคงปลอดภัยและการคุ้มครองสิทธิของบุคคล

๒.๒.๒ ขอบเขตและประเภทของข้อมูล Log

ดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และ Log ครอบคลุมระบบสารสนเทศและองค์ประกอบ ที่อยู่ในความรับผิดชอบของมหาวิทยาลัยอย่างเหมาะสม โดยให้พิจารณาจัดเก็บข้อมูล Log อย่างน้อยในประเภท ดังต่อไปนี้

- (๑) Log การเข้าใช้งานและการพิสูจน์ตัวตนของผู้ใช้งาน (Authentication / Access Log)
- (๒) Log ของระบบปฏิบัติการ เครื่องแม่ข่าย และระบบฐานข้อมูล
- (๓) Log ของอุปกรณ์เครือข่ายและระบบรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น Firewall, IDS/IPS
- (๔) Log ของแอปพลิเคชันและระบบสารสนเทศที่ให้บริการแก่ผู้ใช้งาน
- (๕) Log ของระบบคลาวด์หรือบริการจากผู้ให้บริการภายนอกที่เชื่อมต่อกับระบบของมหาวิทยาลัย



ทั้งนี้ ให้พิจารณาระดับความสำคัญของระบบและข้อมูลประกอบการกำหนดประเภทและรายละเอียดของ Log ที่ต้องจัดเก็บ เพื่อให้สอดคล้องกับระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

๒.๒.๓ แนวทางการจัดเก็บข้อมูล Log ตามกฎหมาย

กำหนดแนวทางการจัดเก็บข้อมูล Log ให้เป็นไปตามกฎหมายและประกาศที่เกี่ยวข้อง โดยคำนึงถึงสาระสำคัญอย่างน้อย ดังต่อไปนี้

(๑) การกำหนดระยะเวลาการจัดเก็บข้อมูล Log

ดำเนินการกำหนดระยะเวลาการจัดเก็บข้อมูล Log ให้สอดคล้องกับข้อกำหนดตามกฎหมายที่เกี่ยวข้อง และวัตถุประสงค์ในการใช้งาน โดยต้องกำหนดระยะเวลาอย่างชัดเจน แยกตามประเภทของ Log และระดับความสำคัญของระบบ

(๒) ความถูกต้องและความครบถ้วนของข้อมูล Log

ดำเนินการกำหนดมาตรการเพื่อรับรองว่าข้อมูล Log ที่จัดเก็บมีความถูกต้อง ครบถ้วน และสะท้อนเหตุการณ์ที่เกิดขึ้นจริง เช่น การตั้งค่าเวลาให้ตรงกัน (Time Synchronization) การจัดเก็บข้อมูลอย่างต่อเนื่อง และการตรวจสอบความสมบูรณ์ของข้อมูล Log อย่างสม่ำเสมอ

(๓) การป้องกันการแก้ไขหรือทำลายข้อมูล Log

ดำเนินการกำหนดมาตรการป้องกันมิให้ข้อมูล Log ถูกแก้ไข เปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยไม่ได้รับอนุญาต โดยอาจใช้มาตรการด้านเทคนิคและกระบวนการควบคุม เช่น การกำหนดสิทธิ์การเข้าถึง การแยกหน้าที่ความรับผิดชอบ และการจัดเก็บข้อมูล Log ในระบบที่มีความมั่นคงปลอดภัยเหมาะสม

๒.๒.๔ แนวทางการวิเคราะห์และการใช้ประโยชน์จากข้อมูล Log

ดำเนินการนำข้อมูล Log ที่จัดเก็บสามารถนำมาวิเคราะห์และใช้ประโยชน์อย่างเป็นระบบ สนับสนุนการตรวจจับและจัดการภัยคุกคามทางไซเบอร์ โดยให้พิจารณาดำเนินการดังต่อไปนี้

(๑) การวิเคราะห์เหตุผิดปกติและเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

ดำเนินการนำข้อมูล Log มาวิเคราะห์เพื่อระบุเหตุผิดปกติ พฤติกรรมที่เบี่ยงเบนจากปกติ การพยายามบุกรุก การละเมิดนโยบาย และเหตุการณ์ที่อาจเป็นภัยคุกคามทางไซเบอร์ ทั้งนี้ เพื่อสนับสนุนการตรวจจับและการตอบสนองต่อเหตุการณ์ได้อย่างทันทั่วทั้ง

(๒) การวิเคราะห์แนวโน้มและช่องโหว่ของระบบ

ให้นำข้อมูล Log มาวิเคราะห์แนวโน้มภัยคุกคาม รูปแบบการโจมตี และจุดอ่อนของระบบสารสนเทศ เพื่อใช้ประกอบการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดมาตรการควบคุมเพิ่มเติม และการบริหารความเสี่ยงในระยะยาว

๒.๒.๕ แนวทางการปฏิบัติ

(๑) กำหนดประเภทและแหล่งที่มาของ Log ที่ต้องจัดเก็บให้ชัดเจนและเป็นมาตรฐานเดียวกัน

(๒) กำหนดระยะเวลาการจัดเก็บ Log ให้สอดคล้องกับกฎหมายและวัตถุประสงค์ในการใช้งาน

(๓) จัดให้มีระบบและมาตรการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย Log โดยมิได้รับอนุญาต

(๔) กำหนดสิทธิ์ผู้มีอำนาจเข้าถึง Log อย่างชัดเจน และบันทึกการเข้าถึงทุกครั้งเพื่อให้สามารถตรวจสอบย้อนหลังได้



(๕) นำข้อมูล Log มาวิเคราะห์อย่างสม่ำเสมอ เพื่อระบุเหตุผิดปกติ แนวโน้มภัยคุกคาม และช่องโหว่ของระบบ

(๖) จัดให้มีการรายงานผลการวิเคราะห์ Log ต่อหน่วยงานหรือผู้บริหารที่เกี่ยวข้องตามรอบระยะเวลาที่กำหนด

(๗) บูรณาการข้อมูล Log เข้ากับระบบเฝ้าระวังและตรวจจับเหตุผิดปกติ เช่น SIEM หรือ SOC

๒.๒.๖ การกำกับดูแลและการทบทวน

ดำเนินการกำกับดูแล ติดตาม และทบทวนการจัดเก็บและวิเคราะห์ข้อมูล Log อย่างสม่ำเสมอ เพื่อให้การดำเนินการเป็นไปตามกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง และให้สามารถปรับปรุงแนวทางปฏิบัติให้สอดคล้องกับสภาพการณ์ภัยคุกคาม เทคโนโลยี และข้อกำหนดทางกฎหมายที่เปลี่ยนแปลงไป

๒.๓ การใช้ข้อมูลข่าวกรองด้านภัยคุกคามและตัวบ่งชี้การโจมตี (Threat Intelligence และ Indicators of Compromise: IoC)

๒.๓.๑ หลักการและวัตถุประสงค์

ดำเนินการนำข้อมูลข่าวกรองด้านภัยคุกคาม (Threat Intelligence) และตัวบ่งชี้การโจมตี (Indicators of Compromise: IoC) มาใช้เป็นส่วนหนึ่งของกระบวนการเฝ้าระวัง ตรวจจับ วิเคราะห์ และประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ เพื่อเพิ่มขีดความสามารถในการระบุเหตุการณ์ที่อาจเป็นการโจมตีการบุกรุกระบบ หรือกิจกรรมที่มีความเสี่ยงได้อย่างรวดเร็ว แม่นยำ และสอดคล้องกับสถานการณ์ภัยคุกคามในปัจจุบัน

การใช้ข้อมูล Threat Intelligence และ IoC ช่วยสนับสนุนการตรวจจับเชิงรุก (Proactive Detection) ลดระยะเวลาในการตรวจพบเหตุการณ์ (Mean Time to Detect: MTTD) และช่วยให้มหาวิทยาลัยสามารถเตรียมความพร้อม ปรับมาตรการควบคุม และตอบสนองต่อภัยคุกคามได้อย่างเหมาะสมก่อนที่จะเกิดผลกระทบในวงกว้าง

๒.๓.๒ ขอบเขตและแหล่งที่มาของข้อมูลข่าวกรอง

ใช้ข้อมูลข่าวกรองด้านภัยคุกคามจากแหล่งข้อมูลที่เชื่อถือได้และเหมาะสมกับบริบทของหน่วยงาน โดยอาจประกอบด้วย

(๑) ข้อมูลจากหน่วยงานภาครัฐหรือหน่วยงานกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ข้อมูลจากหน่วยงานหรือเครือข่ายความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์

(๓) ข้อมูลจากแหล่งสาธารณะที่ได้รับการยอมรับ (Open-source Threat Intelligence)

(๔) ข้อมูลจากผู้ให้บริการเชิงพาณิชย์ด้าน Threat Intelligence ตามความเหมาะสม

(๕) ข้อมูลจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นภายในมหาวิทยาลัยเอง

ทั้งนี้ มหาวิทยาลัยจะดำเนินการพิจารณาความเหมาะสม ความคุ้มค่า และความสอดคล้องกับระดับความเสี่ยงในการเลือกใช้แหล่งข้อมูลดังกล่าว



๒.๓.๓ แนวทางการใช้ Threat Intelligence และ IoC ในการตรวจจับภัยคุกคาม

(๑) การคัดเลือกและประเมินความน่าเชื่อถือของแหล่งข้อมูล

กำหนดแนวทางในการคัดเลือกและประเมินความน่าเชื่อถือของแหล่งข้อมูล Threat Intelligence โดยพิจารณาจากความถูกต้อง ความทันสมัย ความสอดคล้องกับบริบทของมหาวิทยาลัย และประวัติความน่าเชื่อถือของแหล่งข้อมูล ทั้งนี้ เพื่อป้องกันการนำข้อมูลที่ไม่ถูกต้องหรือไม่เหมาะสมมาใช้ ซึ่งอาจก่อให้เกิดการแจ้งเตือนที่คลาดเคลื่อนหรือส่งผลกระทบต่อการทำงาน

(๒) การนำ IoC มาประยุกต์ใช้กับระบบเฝ้าระวัง

ดำเนินการนำตัวบ่งชี้การโจมตี (IoC) เช่น หมายเลขไอพี ชื่อโดเมน URL ค่าแฮชของไฟล์ ลายเซ็นของมัลแวร์ หรือรูปแบบพฤติกรรมที่ผิดปกติ มาประยุกต์ใช้กับระบบเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติ เช่น ระบบ SIEM ระบบตรวจจับการบุกรุก หรือระบบรักษาความมั่นคงปลอดภัยอื่น เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามที่อาจเกิดขึ้นกับระบบของมหาวิทยาลัย

(๓) การปรับปรุงและอัปเดตข้อมูล IoC อย่างต่อเนื่อง

ดำเนินการจัดให้มีการปรับปรุงและอัปเดตข้อมูล IoC อย่างสม่ำเสมอ เพื่อให้ข้อมูลที่ใช้ทำงานมีความทันสมัย และสามารถสะท้อนรูปแบบภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา ทั้งนี้ ให้กำหนดกระบวนการจัดการวงจรชีวิตของ IoC ตั้งแต่การรับข้อมูล การนำไปใช้งาน การทบทวน และการยกเลิกการใช้งานเมื่อข้อมูลหมดความเหมาะสม

(๔) การวิเคราะห์ความเกี่ยวข้องของ IoC กับบริบทของมหาวิทยาลัย

ก่อนดำเนินการตอบสนองต่อ IoC ที่ตรวจพบ ควรมีการวิเคราะห์ความเกี่ยวข้องและผลกระทบต่อระบบและบริบทของมหาวิทยาลัย โดยพิจารณาจากประเภทของระบบ ความสำคัญของข้อมูล ลักษณะการใช้งาน และประวัติการใช้งานที่ผ่านมา ทั้งนี้ เพื่อหลีกเลี่ยงการตอบสนองที่ไม่จำเป็นหรือเกินความเหมาะสม และเพื่อให้งานจัดการเหตุการณ์เป็นไปอย่างมีประสิทธิภาพ

(๕) การใช้ Threat Intelligence ในการปรับปรุงมาตรการตรวจจับและป้องกัน

ดำเนินการนำข้อมูล Threat Intelligence มาใช้ประกอบการปรับปรุงกฎการตรวจจับ (Detection Rules) มาตรการป้องกัน และแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยให้ข้อมูลดังกล่าวเป็นฐานในการพัฒนามาตรการเชิงป้องกันและเชิงตรวจจับให้สอดคล้องกับภัยคุกคามที่เกิดขึ้นจริง

๒.๓.๔ แนวทางการปฏิบัติ

(๑) กำหนดแหล่งข้อมูล Threat Intelligence ที่จะนำมาใช้งานอย่างเป็นทางการ

(๒) กำหนดกระบวนการรับ ตรวจสอบ และบูรณาการข้อมูล IoC เข้ากับระบบ SIEM หรือระบบเฝ้าระวัง

(๓) กำหนดผู้รับผิดชอบในการบริหารจัดการ Threat Intelligence และ IoC อย่างชัดเจน

(๔) จัดให้มีการทบทวนความเหมาะสมของ IoC และข้อมูลข่าวกรองอย่างสม่ำเสมอ

(๕) บันทึกและจัดเก็บข้อมูล Threat Intelligence และ IoC เพื่อใช้ในการวิเคราะห์ย้อนหลัง และการพัฒนาแนวทางปฏิบัติ

(๖) เชื่อมโยงการใช้ Threat Intelligence กับกระบวนการตอบสนองเหตุการณ์และการบริหารความเสี่ยง

(๗) รายงานผลการใช้ข้อมูล Threat Intelligence และแนวโน้มภัยคุกคามต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องตามรอบระยะเวลาที่กำหนด



๒.๓.๕ การกำกับดูแลและการปรับปรุง

ดำเนินการกำกับดูแล ติดตาม และประเมินผลการใช้ข้อมูล Threat Intelligence และ IoC อย่างต่อเนื่อง โดยพิจารณาจากประสิทธิภาพในการตรวจจับเหตุการณ์ ความเหมาะสมของแหล่งข้อมูล และผลกระทบต่อ การดำเนินงาน เพื่อนำผลการประเมินดังกล่าวไปปรับปรุงแนวทางการปฏิบัติให้มีความเหมาะสม ทันสมัย และสอดคล้องกับระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๒.๔ การบูรณาการและการปรับปรุงอย่างต่อเนื่อง

๒.๔.๑ หลักการและวัตถุประสงค์

ดำเนินการบูรณาการมาตรการด้านการตรวจจับเหตุผิดปกติและภัยคุกคามทางไซเบอร์เข้ากับมาตรการ ด้านการป้องกัน การตอบสนอง และการฟื้นฟูจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อให้การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างครบวงจร มีความต่อเนื่อง และสามารถ ลดผลกระทบต่อข้อมูล ระบบสารสนเทศ และภารกิจหลักของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

การบูรณาการดังกล่าวมีวัตถุประสงค์เพื่อให้ข้อมูลจากกระบวนการตรวจจับถูกนำไปใช้ประโยชน์ ในการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ทั้งในเชิงเทคนิค เชิงกระบวนการ และเชิงการบริหารจัดการความเสี่ยง เพื่อให้มหาวิทยาลัยสามารถรองรับภัยคุกคาม เทคโนโลยี และความเสี่ยง ที่เปลี่ยนแปลงไปได้อย่างเหมาะสมและยั่งยืน

๒.๔.๒ แนวทางการบูรณาการเชิงระบบ

ดำเนินการจัดให้มีการเชื่อมโยงข้อมูล กระบวนการ และบทบาทหน้าที่ระหว่างมาตรการด้านการตรวจจับ (Detect) มาตรการด้านการป้องกัน (Protect) มาตรการด้านการตอบสนอง (Respond) และมาตรการด้าน การฟื้นฟู (Recover) อย่างชัดเจน โดยกำหนดแนวทางและขั้นตอนการดำเนินงานที่สอดคล้องกัน เพื่อให้ การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปในทิศทางเดียวกันทั่วทั้งมหาวิทยาลัย

ทั้งนี้ การบูรณาการดังกล่าวควรครอบคลุมการแลกเปลี่ยนข้อมูล การแจ้งเตือน การตัดสินใจ และการรายงานผลในทุกระดับที่เกี่ยวข้อง

๒.๔.๓ แนวทางการดำเนินการและการปรับปรุงอย่างต่อเนื่อง

(๑) การเชื่อมโยงข้อมูลจากการตรวจจับสู่การป้องกัน

ดำเนินการนำข้อมูลและผลการตรวจจับเหตุผิดปกติจากระบบเฝ้าระวัง เช่น การนำ SIEM / SOC มาใช้ในการ ปรับปรุงมาตรการด้านการป้องกัน เช่น การปรับปรุงนโยบายการเข้าถึง การเสริมมาตรการควบคุมทางเทคนิค การปรับค่าการตั้งค่าความมั่นคงปลอดภัยของระบบ และการปรับปรุงกฎหรือกลไกการป้องกัน เพื่อป้องกันไม่ให้เกิดเหตุการณ์ในลักษณะเดียวกันเกิดขึ้นซ้ำ

(๒) การบูรณาการการตรวจจับกับการตอบสนองเหตุการณ์

ดำเนินการให้ข้อมูลจากการตรวจจับถูกนำไปใช้เป็นข้อมูลตั้งต้นในกระบวนการตอบสนองเหตุการณ์ ด้านความมั่นคงปลอดภัยไซเบอร์ โดยให้มีการกำหนดจุดเชื่อมต่อที่ชัดเจนระหว่างระบบเฝ้าระวังและกระบวนการ ตอบสนอง เพื่อให้การยืนยันเหตุการณ์ การยกระดับ การสั่งการ และการดำเนินการแก้ไขเป็นไปอย่างรวดเร็ว และเหมาะสมตามระดับความรุนแรงของเหตุการณ์



(๓) การนำบทเรียนจากเหตุการณ์มาใช้ในการฟื้นฟูและปรับปรุง

มีการนำบทเรียนที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ผลการวิเคราะห์เหตุการณ์ และผลการทดสอบหรือซ้อมแผน มาใช้ในการปรับปรุงมาตรการด้านการตรวจจับ การป้องกัน การตอบสนอง และการฟื้นฟู ทั้งนี้ เพื่อยกระดับความพร้อมและลดความเสี่ยงในระยะยาว

(๔) การทบทวนและพัฒนาระบบการตรวจจับอย่างต่อเนื่อง

ดำเนินการทบทวนและประเมินประสิทธิภาพของระบบการตรวจจับอย่างสม่ำเสมอ โดยพิจารณาจากตัวชี้วัดที่เหมาะสม เช่น ระยะเวลาในการตรวจจับ ความแม่นยำของการแจ้งเตือน และความสามารถในการตรวจจับภัยคุกคามรูปแบบใหม่ เพื่อนำผลการประเมินไปใช้ในการพัฒนา ปรับปรุง และเพิ่มประสิทธิภาพของระบบการตรวจจับให้สอดคล้องกับสภาพการณ์ที่เปลี่ยนแปลงไป

๒.๔.๔ แนวทางการปฏิบัติ

- (๑) กำหนดกระบวนการแลกเปลี่ยนข้อมูลระหว่างระบบตรวจจับ ระบบป้องกัน และกระบวนการตอบสนอง
- (๒) กำหนดบทบาทและความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้องอย่างชัดเจน
- (๓) จัดให้มีการทบทวนและปรับปรุงกฎการตรวจจับและมาตรการที่เกี่ยวข้องตามรอบระยะเวลาที่กำหนด
- (๔) นำผลการตรวจจับและบทเรียนจากเหตุการณ์มาประกอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(๕) รายงานผลการดำเนินงานด้านการตรวจจับและการปรับปรุงต่อผู้บริหารและคณะกรรมการที่เกี่ยวข้อง

- (๖) บูรณาการการดำเนินงานด้านการตรวจจับเข้ากับระบบบริหารความเสี่ยงองค์กรและการวางแผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ

๒.๔.๕ การกำกับดูแลและการพัฒนาอย่างยั่งยืน

ดำเนินการกำกับดูแล ติดตาม และประเมินผลการบูรณาการและการปรับปรุงมาตรการด้านการตรวจจับอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการดังกล่าวมีความเหมาะสม ทันสมัย และสามารถรองรับการเปลี่ยนแปลงของภัยคุกคาม เทคโนโลยี และความเสี่ยงได้อย่างยั่งยืน



ส่วนที่ ๔

การรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response)

การรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นกระบวนการสำคัญในการลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับข้อมูล ระบบสารสนเทศ และการให้บริการของมหาวิทยาลัย ทั้งนี้ เพื่อให้สามารถควบคุมสถานการณ์ แก้ไขปัญหา และฟื้นฟูการดำเนินงานให้กลับสู่สภาวะปกติได้อย่างรวดเร็วและเหมาะสม

๑. การจัดทำและทบทวนแผนการรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan: CIRP)

๑.๑ หลักการและวัตถุประสงค์

ดำเนินการจัดทำแผนการรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศ ข้อมูล และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศของมหาวิทยาลัย

แผนรับมือฯ ดังกล่าวควรมีวัตถุประสงค์เพื่อให้การดำเนินการรับมือเหตุการณ์เป็นไปอย่างมีระบบ เป็นเอกภาพ และสามารถดำเนินการได้อย่างทันท่วงที ลดความเสียหาย ลดผลกระทบต่อการกิจหลัก ความต่อเนื่องในการให้บริการ และชื่อเสียงของมหาวิทยาลัย รวมทั้งสนับสนุนการรายงานและการดำเนินการตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

๑.๒ ขอบเขตและองค์ประกอบของแผน CIRP

แผนรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ต้องครอบคลุมอย่างน้อยในประเด็นดังต่อไปนี้

(๑) ประเภทและระดับของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เช่น เหตุการณ์รั่วไหลของข้อมูล การโจมตีระบบ การดักจับข้อมูลหรือแรนซัมแวร์ การโจมตีแบบปฏิเสธการให้บริการ และเหตุการณ์อื่นที่มีผลกระทบต่อระบบหรือข้อมูล

(๒) ขั้นตอนการดำเนินงานตั้งแต่การตรวจพบและแจ้งเหตุ การประเมินสถานการณ์ การควบคุมและจำกัดขอบเขตความเสียหาย การแก้ไขและกู้คืนระบบ การสื่อสารและการรายงาน รวมถึงการทบทวนหลังเหตุการณ์

(๓) บทบาทหน้าที่ ความรับผิดชอบ และสายการบังคับบัญชาของหน่วยงานและบุคลากรที่เกี่ยวข้องอย่างชัดเจน

(๔) แนวทางการประสานงานกับหน่วยงานภายใน หน่วยงานภายนอก และผู้ให้บริการที่เกี่ยวข้อง

(๕) การเชื่อมโยงกับแผนความต่อเนื่องทางธุรกิจ (BCP) และแผนกู้คืนระบบ (DRP)



๑.๓ การจัดทำและการทบทวนแผน

ดำเนินการจัดทำ ทบทวน และปรับปรุงแผน CIRP อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงระบบสารสนเทศ โครงสร้างองค์กร เทคโนโลยี รูปแบบการให้บริการ หรือแนวโน้มภัยคุกคามทางไซเบอร์ เพื่อให้แผนมีความทันสมัย สอดคล้องกับสภาพแวดล้อมและความเสี่ยงในปัจจุบัน และสามารถนำไปใช้ปฏิบัติได้จริง

การทบทวนแผนต้องคำนึงถึงบทเรียนที่ได้รับจากเหตุการณ์ที่ผ่านมา ผลการฝึกซ้อม และผลการตรวจประเมิน เพื่อให้เกิดการปรับปรุงอย่างต่อเนื่อง

๑.๔ แนวทางการปฏิบัติ

๑.๔.๑ การจัดทำแผน CIRP ให้ครอบคลุมเหตุการณ์ในระดับต่าง ๆ

ดำเนินการกำหนดระดับความรุนแรงของเหตุการณ์ (Severity Level) อย่างชัดเจน พร้อมแนวทางการดำเนินการที่เหมาะสมกับแต่ละระดับ เพื่อให้การตอบสนองเป็นไปอย่างสอดคล้องกับผลกระทบและความเร่งด่วนของเหตุการณ์

๑.๔.๒ การกำหนดขั้นตอนการรายงานและการยกระดับเหตุการณ์

ดำเนินการกำหนดขั้นตอน ช่องทาง และระยะเวลาในการรายงานเหตุการณ์อย่างชัดเจน รวมถึงเกณฑ์การยกระดับเหตุการณ์ไปยังผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง เพื่อให้การตัดสินใจเป็นไปอย่างรวดเร็วและเหมาะสม

๑.๔.๓ การระบุช่องทางการประสานงานภายในและภายนอก

ดำเนินการกำหนดช่องทางการประสานงานระหว่างหน่วยงานภายในมหาวิทยาลัย และช่องทางการติดต่อกับหน่วยงานภายนอก เช่น ผู้ให้บริการระบบ หน่วยงานกำกับดูแล หรือหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การดำเนินการแก้ไขและการรายงานเป็นไปอย่างรวดเร็ว

๑.๔.๔ การจัดทำบัญชีผู้ติดต่อในกรณีฉุกเฉิน

ดำเนินการจัดทำและปรับปรุงบัญชีรายชื่อผู้ติดต่อในกรณีฉุกเฉินอย่างสม่ำเสมอ โดยระบุบทบาทหน้าที่ และช่องทางการติดต่อ เพื่อให้สามารถเรียกใช้ทรัพยากรและประสานงานได้ทันทีเมื่อเกิดเหตุการณ์

๑.๔.๕ การทบทวนและการทดสอบแผน

ดำเนินการจัดให้มีการทดสอบแผน CIRP ผ่านการฝึกซ้อมหรือการจำลองสถานการณ์อย่างสม่ำเสมอ เพื่อประเมินความพร้อมของบุคลากร กระบวนการ และระบบ และนำผลการทดสอบมาปรับปรุงแผนให้มีประสิทธิภาพยิ่งขึ้น

๑.๔.๖ การบันทึกและการรายงานหลังเหตุการณ์

ดำเนินการจัดทำรายงานสรุปเหตุการณ์ (Post-Incident Report) เพื่อวิเคราะห์สาเหตุ ผลกระทบ การตอบสนอง และบทเรียนที่ได้รับ และนำผลดังกล่าวไปใช้ในการปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงในภาพรวม



๒. การฝึกซ้อมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๒.๑ หลักการและวัตถุประสงค์

ดำเนินการจัดให้มีการฝึกซ้อมการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ เพื่อทดสอบความพร้อมของบุคลากร กระบวนการ และระบบสารสนเทศในการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ทั้งในมิติด้านเทคนิค ด้านการบริหารจัดการ และด้านการสื่อสาร

การฝึกซ้อมดังกล่าวมีวัตถุประสงค์เพื่อประเมินประสิทธิภาพของแผนการรับมือและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CIRP) ความชัดเจนของบทบาทหน้าที่ การประสานงานระหว่างหน่วยงาน และความพร้อมในการตัดสินใจภายใต้สถานการณ์วิกฤต รวมถึงเพื่อสร้างความตระหนักรู้และเสริมสร้างขีดความสามารถของบุคลากรทุกระดับที่เกี่ยวข้อง

๒.๒ ประเภทและรูปแบบของการฝึกซ้อม

ดำเนินการฝึกซ้อมในรูปแบบที่หลากหลายและเหมาะสมกับบริบทและระดับความเสี่ยงของมหาวิทยาลัย โดยอย่างน้อยต้องครอบคลุมรูปแบบดังต่อไปนี้

๒.๒.๑ การฝึกซ้อมเชิงเทคนิค (Technical Exercise)

เป็นการฝึกซ้อมที่มุ่งทดสอบความสามารถด้านเทคนิคของผู้ปฏิบัติงาน เช่น การตรวจจับ วิเคราะห์ การควบคุม และการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการใช้งานเครื่องมือ ระบบเฝ้าระวัง และระบบสนับสนุนการตอบสนองเหตุการณ์

๒.๒.๒ การฝึกซ้อมเชิงบริหารหรือเชิงสถานการณ์ (Management / Tabletop Exercise)

เป็นการฝึกซ้อมที่มุ่งทดสอบกระบวนการตัดสินใจ การสื่อสาร การประสานงาน และการบริหารจัดการ ภายใต้สถานการณ์วิกฤต โดยมีผู้บริหารและหน่วยงานสนับสนุนเข้าร่วม เพื่อประเมินความพร้อมในระดับนโยบาย และการบริหาร

๒.๓ การออกแบบสถานการณ์จำลอง

การฝึกซ้อมต้องจัดทำสถานการณ์จำลองที่สะท้อนภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้และใกล้เคียงกับสถานการณ์จริงของมหาวิทยาลัย โดยพิจารณาจากผลการประเมินความเสี่ยง ลักษณะระบบสารสนเทศ และข้อมูลสำคัญของมหาวิทยาลัย

สถานการณ์จำลองอาจครอบคลุมเหตุการณ์ เช่น การโจมตีด้วยมัลแวร์หรือแรนซัมแวร์ การรั่วไหลของข้อมูล การโจมตีระบบบริการหลัก หรือเหตุการณ์ที่มีผลกระทบต่อการให้บริการในวงกว้าง เพื่อให้การฝึกซ้อมสามารถทดสอบทั้งด้านเทคนิค ด้านกระบวนการ และด้านการบริหารได้อย่างครบถ้วน

๒.๔ แนวทางการปฏิบัติ

๒.๔.๑ การกำหนดประเภทและความถี่ของการฝึกซ้อม

ดำเนินการกำหนดประเภท ความถี่ และขอบเขตของการฝึกซ้อมให้เหมาะสมกับระดับความเสี่ยงและความพร้อมของมหาวิทยาลัย โดยควรมีการฝึกซ้อมอย่างน้อยปีละ ๑ ครั้ง และอาจจัดเพิ่มเติมในกรณีที่มีการเปลี่ยนแปลงระบบหรือมีเหตุการณ์สำคัญเกิดขึ้น

๒.๔.๒ การจัดทำสถานการณ์จำลองที่สอดคล้องกับความเสี่ยง

ดำเนินการจัดทำสถานการณ์จำลองบนพื้นฐานของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การฝึกซ้อมสะท้อนจุดเสี่ยงและผลกระทบที่แท้จริงของมหาวิทยาลัย



๒.๔.๓ การบันทึกผลการฝึกซ้อมและบทเรียนที่ได้รับ

ดำเนินการบันทึกผลการฝึกซ้อมอย่างเป็นระบบ โดยระบุขั้นตอนการดำเนินการ ปัญหา อุปสรรค จุดแข็ง จุดอ่อน และข้อเสนอแนะ เพื่อใช้เป็นข้อมูลประกอบการปรับปรุงแผนและกระบวนการ

๒.๔.๔ การนำผลการฝึกซ้อมไปใช้ปรับปรุงแผน CIRP และกระบวนการที่เกี่ยวข้อง

ดำเนินการนำผลการฝึกซ้อมและบทเรียนที่ได้รับมาใช้ในการทบทวนและปรับปรุงแผน CIRP ขั้นตอนการตอบสนองเหตุการณ์ และการประสานงานระหว่างหน่วยงาน เพื่อยกระดับความพร้อมและประสิทธิภาพในการรับมือเหตุการณ์จริง

๒.๔.๕ การรายงานผลการฝึกซ้อมต่อผู้บริหาร

ดำเนินการจัดทำรายงานสรุปผลการฝึกซ้อมเสนอผู้บริหารและคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ประกอบการตัดสินใจเชิงนโยบาย การจัดสรรทรัพยากร และการกำหนดมาตรการปรับปรุงเพิ่มเติม

๒.๔.๖ การบูรณาการการฝึกซ้อมกับแผนและกระบวนการอื่น

ดำเนินการฝึกซ้อมเชื่อมโยงกับแผนการสื่อสารในภาวะวิกฤต แผนความต่อเนื่องทางธุรกิจ (BCP) และแผนกู้คืนระบบ (DRP) เพื่อทดสอบความสอดคล้องของแผนในภาพรวม

๓. การกำหนดกระบวนการสื่อสารในภาวะวิกฤต (Crisis Communication)

๓.๑ หลักการและวัตถุประสงค์

ดำเนินการกำหนดกระบวนการสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อให้การสื่อสารทั้งภายในและภายนอกมหาวิทยาลัยเป็นไปอย่างถูกต้อง เหมาะสม ทันเวลา และสอดคล้องกับสถานการณ์ ทั้งนี้ เพื่อป้องกันความสับสน การเผยแพร่ข้อมูลที่คลาดเคลื่อน หรือการสื่อสารที่อาจก่อให้เกิดผลกระทบเพิ่มเติมต่อการดำเนินงาน ความเชื่อมั่น และภาพลักษณ์ของมหาวิทยาลัย

กระบวนการสื่อสารในภาวะวิกฤตมีวัตถุประสงค์เพื่อสนับสนุนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ ช่วยให้ผู้บริหารสามารถตัดสินใจได้อย่างเหมาะสม และสร้างความเข้าใจที่ถูกต้องแก่ผู้มีส่วนได้ส่วนเสียทุกกลุ่ม

๓.๒ ขอบเขตและหลักการสำคัญของการสื่อสารในภาวะวิกฤต

การสื่อสารในภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ต้องยึดหลักความถูกต้อง ความจำเป็น ความเหมาะสม และความรับผิดชอบ โดยคำนึงถึงประเด็นด้านกฎหมาย การคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยของข้อมูล และผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือของมหาวิทยาลัย

ทั้งนี้ การสื่อสารต้องอยู่ภายใต้การกำกับดูแลของผู้มีอำนาจตามที่มหาวิทยาลัยกำหนด โดยสอดคล้องกับแผนการรับมือและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CIRP) และแผนอื่นที่เกี่ยวข้อง

๓.๓ โครงสร้างการกำกับดูแลและบทบาทหน้าที่

ดำเนินการกำหนดโครงสร้างการกำกับดูแลการสื่อสารในภาวะวิกฤตอย่างชัดเจน โดยระบุบทบาทหน้าที่ของผู้บริหาร หน่วยงาน และบุคลากรที่เกี่ยวข้อง เช่น ผู้มีอำนาจในการอนุมัติการสื่อสาร ผู้รับผิดชอบด้านการสื่อสาร ผู้ให้ข้อมูลด้านเทคนิค และผู้ประสานงานกับหน่วยงานภายนอก เพื่อให้การสื่อสารเป็นไปในทิศทางเดียวกันและลดความเสี่ยงจากการสื่อสารที่ไม่เหมาะสม



๓.๔ แนวทางการปฏิบัติ

๓.๔.๑ การกำหนดผู้รับผิดชอบด้านการสื่อสารในภาวะวิกฤต

ดำเนินการกำหนดผู้รับผิดชอบหรือคณะทำงานด้านการสื่อสารในภาวะวิกฤตอย่างชัดเจน โดยระบุอำนาจหน้าที่ ความรับผิดชอบ และสายการบังคับบัญชา เพื่อให้การสื่อสารเป็นไปอย่างมีเอกภาพและสามารถตัดสินใจได้อย่างทันทั่วถึง

๓.๔.๒ การกำหนดช่องทางการสื่อสารภายในและภายนอก

ดำเนินการกำหนดช่องทางการสื่อสารที่เหมาะสมสำหรับการสื่อสารภายในมหาวิทยาลัยและการสื่อสารกับหน่วยงานภายนอก ผู้ให้บริการ สื่อมวลชน หรือสาธารณชน โดยคำนึงถึงความรวดเร็ว ความถูกต้อง และความปลอดภัยของข้อมูล

๓.๔.๓ การจัดเตรียมแนวทางหรือแม่แบบข้อความสำหรับการสื่อสาร

ดำเนินการจัดเตรียมแนวทางหรือแม่แบบข้อความ (Communication Template) สำหรับการสื่อสารในสถานการณ์ต่าง ๆ เช่น การแจ้งเหตุเบื้องต้น การอัปเดตสถานการณ์ การชี้แจงข้อเท็จจริง และการสื่อสารหลังการแก้ไขเหตุการณ์ เพื่อให้การสื่อสารมีความสอดคล้อง ลดความคลาดเคลื่อน และสามารถดำเนินการได้อย่างรวดเร็ว

๓.๔.๔ การประสานงานกับหน่วยงานที่เกี่ยวข้องก่อนการสื่อสาร

ก่อนดำเนินการสื่อสารในภาวะวิกฤต ให้มีการประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานด้านเทคนิค หน่วยงานด้านกฎหมาย หน่วยงานด้านคุ้มครองข้อมูล และผู้บริหาร เพื่อพิจารณาความถูกต้อง ความเหมาะสม และผลกระทบของเนื้อหาที่จะสื่อสาร

๓.๔.๕ การควบคุมและการอนุมัติการสื่อสาร

ดำเนินการกำหนดกระบวนการควบคุมและอนุมัติการสื่อสารอย่างชัดเจน โดยเฉพาะการสื่อสารภายนอก เพื่อป้องกันการเผยแพร่ข้อมูลที่ไม่ถูกต้อง ไม่ครบถ้วน หรืออาจก่อให้เกิดผลกระทบทางกฎหมายหรือภาพลักษณ์

๓.๔.๖ การบันทึกและการติดตามการสื่อสาร

ดำเนินการบันทึกการสื่อสารในภาวะวิกฤตทุกขั้นตอน เพื่อใช้เป็นหลักฐานในการตรวจสอบย้อนหลัง การประเมินผล และการปรับปรุงกระบวนการสื่อสารในอนาคต

๓.๔.๗ การทบทวนและปรับปรุงแผนการสื่อสารอย่างสม่ำเสมอ

ดำเนินการทบทวนและปรับปรุงกระบวนการและแผนการสื่อสารในภาวะวิกฤตอย่างสม่ำเสมอ โดยอาศัยผลจากการฝึกซ้อม เหตุการณ์จริง และบทเรียนที่ได้รับ เพื่อให้กระบวนการสื่อสารมีความเหมาะสม ทันสมัย และสอดคล้องกับบริบทที่เปลี่ยนแปลงไป

๔. การบูรณาการกับแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (Business Continuity Plan: BCP / Disaster Recovery Plan: DRP)

๔.๑ หลักการและวัตถุประสงค์

ดำเนินการบูรณาการแผนการรับมือและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) เข้ากับแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนกู้คืนระบบ (Disaster Recovery Plan: DRP) เพื่อให้การรับมือกับเหตุการณ์ไซเบอร์



เป็นไปอย่างสอดคล้อง เป็นเอกภาพ และสนับสนุนการดำเนินงานตามภารกิจหลักของมหาวิทยาลัยอย่างต่อเนื่อง แม้จะอยู่ภายใต้สถานการณ์ฉุกเฉินหรือภาวะวิกฤต

การบูรณาการดังกล่าวมีวัตถุประสงค์เพื่อให้มหาวิทยาลัยสามารถควบคุมผลกระทบจากเหตุการณ์ไซเบอร์ ลดระยะเวลาในการหยุดชะงักของระบบและบริการ และฟื้นฟูการดำเนินงานให้กลับสู่สภาวะปกติได้อย่างเหมาะสมตามระดับความเสี่ยงและทรัพยากรที่มีอยู่

๔.๒ ขอบเขตและองค์ประกอบของการบูรณาการ

การบูรณาการ CIRP กับ BCP และ DRP ต้องครอบคลุมระบบสารสนเทศ กระบวนการทางธุรกิจ และบริการที่มีความสำคัญต่อภารกิจหลักของมหาวิทยาลัย โดยต้องพิจารณาองค์ประกอบอย่างน้อย ดังต่อไปนี้

- (๑) ลำดับความสำคัญของระบบและบริการที่ต้องได้รับการฟื้นฟูเป็นลำดับแรก
- (๒) ระยะเวลาการกู้คืนที่ยอมรับได้ (Recovery Time Objective: RTO) และระดับการสูญเสียข้อมูลที่ยอมรับได้ (Recovery Point Objective: RPO)
- (๓) ทรัพยากรที่จำเป็นในการฟื้นฟูระบบและบริการ
- (๔) บทบาทหน้าที่และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้อง
- (๕) แนวทางการประสานงานระหว่างหน่วยงานด้านเทคนิค หน่วยงานด้านการบริหาร และหน่วยงานสนับสนุน

๔.๓ แนวทางการบูรณาการเชิงกระบวนการ

๔.๓.๑ การเชื่อมโยงขั้นตอนการดำเนินงาน

ดำเนินการกำหนดจุดเชื่อมโยงระหว่างขั้นตอนของแผน CIRP กับขั้นตอนของแผน BCP และ DRP อย่างชัดเจน ตั้งแต่การตรวจพบเหตุการณ์ การประเมินผลกระทบ การตัดสินใจด้านการกู้คืนระบบ การสื่อสาร และการฟื้นฟูการดำเนินงาน เพื่อให้การดำเนินการในแต่ละแผนเป็นไปในทิศทางเดียวกันและไม่ซ้ำซ้อน

๔.๓.๒ การกำหนดลำดับความสำคัญของระบบและบริการ

ดำเนินการกำหนดลำดับความสำคัญของระบบและบริการที่จำเป็นต่อภารกิจหลัก โดยอาศัยผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อให้สามารถจัดสรรทรัพยากร และดำเนินการฟื้นฟูได้อย่างเหมาะสมภายใต้ข้อจำกัดด้านเวลาและทรัพยากร

๔.๓.๓ การกำหนดเกณฑ์ด้านระยะเวลาการกู้คืน

ดำเนินการกำหนดค่า RTO และ RPO สำหรับระบบและบริการแต่ละประเภทอย่างชัดเจน และให้ค่าเหล่านี้สอดคล้องกับระดับความเสี่ยง ผลกระทบ และความคาดหวังของผู้มีส่วนได้ส่วนเสีย เพื่อใช้เป็นกรอบในการตัดสินใจ และการดำเนินการกู้คืนระบบ

๔.๔ แนวทางการปฏิบัติ

๔.๔.๑ การเชื่อมโยงขั้นตอน CIRP กับ BCP และ DRP

ดำเนินการจัดทำแผนผังหรือแนวทางการเชื่อมโยงขั้นตอนการดำเนินงานของ CIRP, BCP และ DRP เพื่อให้ผู้ปฏิบัติงานเข้าใจบทบาทหน้าที่และลำดับการดำเนินการอย่างชัดเจน



๔.๔.๒ การกำหนดลำดับความสำคัญของระบบและบริการ

ดำเนินการจัดทำบัญชีระบบและบริการที่สำคัญ พร้อมกำหนดระดับความสำคัญและแนวทางการฟื้นฟูในแต่ละกรณี เพื่อสนับสนุนการตัดสินใจในภาวะฉุกเฉิน

๔.๔.๓ การทดสอบความสอดคล้องของแผนอย่างสม่ำเสมอ

ดำเนินการจัดให้มีการทดสอบหรือฝึกซ้อมแผน CIRP, BCP และ DRP ในลักษณะที่เชื่อมโยงกัน เพื่อประเมินความสอดคล้องและความพร้อมของแผนในภาพรวม

๔.๔.๔ การปรับปรุงแผนตามผลการทดสอบและเหตุการณ์จริง

ดำเนินการนำผลจากการทดสอบ การฝึกซ้อม และเหตุการณ์ที่เกิดขึ้นจริงมาวิเคราะห์และใช้ในการปรับปรุงแผนให้มีความเหมาะสมและทันสมัย

๔.๔.๕ การรายงานผลการทดสอบและการฟื้นฟูต่อผู้บริหาร

ดำเนินการจัดทำรายงานสรุปผลการทดสอบและการดำเนินการฟื้นฟูระบบเสนอผู้บริหาร และคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ประกอบการตัดสินใจเชิงนโยบายและการจัดสรรทรัพยากรในอนาคต

๔.๔.๖ การบูรณาการกับการบริหารความเสี่ยงองค์กร

ดำเนินการนำผลการบูรณาการและบทเรียนจากเหตุการณ์ไซเบอร์ไปใช้ประกอบการปรับปรุงการบริหารความเสี่ยงองค์กรและการวางแผนเชิงยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ

๔.๕ การกำกับดูแลและการปรับปรุงอย่างต่อเนื่อง

ดำเนินการกำกับดูแล ติดตาม และทบทวนการบูรณาการแผน CIRP, BCP และ DRP อย่างต่อเนื่อง เพื่อให้แผนมีความสอดคล้อง เหมาะสม และสามารถรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและยั่งยืน



ส่วนที่ ๕

การสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพ (Cybersecurity Awareness and Capability Development)

การสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร และผู้มีส่วนได้ส่วนเสีย เป็นปัจจัยสำคัญในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยในระยะยาว ทั้งนี้ เพื่อให้บุคลากรทุกระดับมีความเข้าใจบทบาทและหน้าที่ของตนเอง สามารถปฏิบัติงานได้อย่างถูกต้อง ปลอดภัย และสอดคล้องกับนโยบายและมาตรฐานที่กำหนด

๑. การจัดให้มีการอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๑.๑ หลักการและวัตถุประสงค์

ดำเนินการจัดให้มีการอบรมและกิจกรรมสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่องแก่ผู้บริหาร บุคลากร นิสิต และผู้ที่เกี่ยวข้อง เพื่อเสริมสร้างความรู้พื้นฐาน ความเข้าใจ และทัศนคติ ที่ถูกต้องเกี่ยวกับภัยคุกคามทางไซเบอร์ แนวทางการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัย ตลอดจน ความรับผิดชอบตามนโยบาย ระเบียบ และกฎหมายที่เกี่ยวข้อง

การสร้างความตระหนักดังกล่าวมีวัตถุประสงค์เพื่อให้ผู้ใช้งานทุกระดับสามารถตระหนักถึงบทบาท ของตนเองในการป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ลดโอกาสเกิดเหตุจากความผิดพลาด ของมนุษย์ (Human Error) และสนับสนุนการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร อย่างยั่งยืน

๑.๒ ขอบเขตและกลุ่มเป้าหมาย

การอบรมและกิจกรรมสร้างความตระหนักต้องครอบคลุมกลุ่มเป้าหมายอย่างน้อย ดังต่อไปนี้

- (๑) ผู้บริหารระดับสูงและผู้บริหารคณะ
- (๒) บุคลากรสายวิชาการและสายสนับสนุน
- (๓) นิสิตและผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัย
- (๔) ผู้ปฏิบัติงานภายนอกหรือผู้ให้บริการที่มีการเข้าถึงระบบหรือข้อมูลของมหาวิทยาลัย

ทั้งนี้ มหาวิทยาลัยจะดำเนินการพิจารณาในการปรับระดับเนื้อหา ความลึก และรูปแบบการสื่อสาร ให้เหมาะสมกับบทบาท หน้าที่ และระดับความเสี่ยงของแต่ละกลุ่มเป้าหมาย

๑.๓ แนวทางการออกแบบและการจัดการอบรม

การอบรมด้าน Cybersecurity Awareness ต้องออกแบบให้มีความเหมาะสม ทันสมัย และสอดคล้องกับ สภาพการณ์ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอยู่ตลอดเวลา โดยต้องมุ่งเน้นการนำไปใช้ปฏิบัติได้จริง และสร้าง การมีส่วนร่วมของผู้เข้าร่วมอบรม

๑.๔ แนวทางการปฏิบัติ

๑.๔.๑ การกำหนดหลักสูตรหรือหัวข้อการอบรมให้เหมาะสมกับกลุ่มเป้าหมาย

ดำเนินการกำหนดหลักสูตรหรือหัวข้อการอบรมด้าน Cybersecurity Awareness โดยพิจารณา จากบทบาทหน้าที่ ระดับความเสี่ยง และลักษณะการใช้งานระบบสารสนเทศของแต่ละกลุ่มเป้าหมาย



เช่น การตระหนักรู้ด้านฟิชซิง การตั้งรหัสผ่านที่มั่นคงปลอดภัย การใช้งานอุปกรณ์ส่วนบุคคลอย่างปลอดภัย และความรับผิดชอบด้านข้อมูลส่วนบุคคล

๑.๔.๒ การจัดให้มีการอบรมอย่างสม่ำเสมอและการทบทวนเนื้อหา

ดำเนินการจัดอบรมด้าน Cybersecurity Awareness อย่างสม่ำเสมอ ตามรอบระยะเวลาที่เหมาะสม และต้องมีการทบทวน ปรับปรุง และอัปเดตเนื้อหาให้ทันต่อรูปแบบภัยคุกคามทางไซเบอร์ รวมไปถึงเทคโนโลยี และกฎหมายที่เปลี่ยนแปลงไป เพื่อให้การอบรมมีความทันสมัยและสอดคล้องกับความเสี่ยงในปัจจุบัน

๑.๔.๓ การใช้รูปแบบการอบรมและการสื่อสารที่หลากหลาย

ดำเนินการใช้รูปแบบการอบรมและการสื่อสารที่หลากหลายและเหมาะสม เช่น การบรรยาย การเรียนรู้ผ่านระบบออนไลน์ การจัดกิจกรรมรณรงค์ การเผยแพร่สื่อประชาสัมพันธ์ การทดสอบจำลองสถานการณ์ หรือการสื่อสารผ่านช่องทางภายใน เพื่อเพิ่มประสิทธิภาพในการสื่อสารและการจดจำของผู้เข้าร่วม

๑.๔.๔ การประเมินผลการอบรมและระดับความตระหนักรู้

ดำเนินการประเมินผลการอบรมและระดับความตระหนักรู้ของผู้เข้าร่วม เช่น การทดสอบความรู้ก่อนและหลังการอบรม การประเมินพฤติกรรมการใช้งานระบบ หรือการสำรวจความคิดเห็น เพื่อใช้เป็นข้อมูลประกอบการปรับปรุงหลักสูตรและแนวทางการอบรมในอนาคต

๑.๔.๕ การบันทึกและรายงานผลการดำเนินงานด้านการอบรม

ดำเนินการบันทึกข้อมูลการจัดอบรม ผลการประเมิน และข้อเสนอแนะอย่างเป็นระบบ และจัดทำรายงานสรุปผลการดำเนินงานด้าน Cybersecurity Awareness เสนอผู้บริหารและคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ประกอบการกำหนดนโยบาย การจัดสรรทรัพยากร และการปรับปรุงแผนงานด้านความมั่นคงปลอดภัยไซเบอร์

๑.๔.๖ การเชื่อมโยงกับนโยบายและมาตรการอื่นของมหาวิทยาลัย

ดำเนินการจัดอบรมและกิจกรรมสร้างความตระหนักรู้เชื่อมโยงกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ นโยบายการคุ้มครองข้อมูลส่วนบุคคล และมาตรการด้านเทคนิคและการบริหารอื่น ๆ เพื่อให้ผู้เข้าร่วมเห็นภาพรวมและความสำคัญของการปฏิบัติตามนโยบายอย่างเป็นรูปธรรม

๒. การส่งเสริมการพัฒนาทักษะเฉพาะด้านให้แก่ผู้ดูแลระบบและบุคลากรด้านเทคนิค (Specialized Skill Development)

๒.๑ หลักการและวัตถุประสงค์

ดำเนินการส่งเสริมและสนับสนุนการพัฒนาทักษะเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้ดูแลระบบ ผู้พัฒนาระบบ และบุคลากรด้านเทคนิคที่เกี่ยวข้อง เพื่อเสริมสร้างขีดความสามารถในการออกแบบ พัฒนา ดูแล ป้องกัน ตรวจสอบ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ สอดคล้องกับบทบาทหน้าที่ ความรับผิดชอบ และระดับความเสี่ยงของระบบสารสนเทศที่อยู่ในความดูแล

การพัฒนาทักษะดังกล่าวมีวัตถุประสงค์เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย ลดความเสี่ยงจากการขาดทักษะหรือความเชี่ยวชาญเฉพาะด้าน และสร้างความพร้อมรองรับเทคโนโลยี และภัยคุกคามรูปแบบใหม่ในปัจจุบันและอนาคต



๒.๒ ขอบเขตและกลุ่มเป้าหมาย

การพัฒนาทักษะเฉพาะด้านต้องครอบคลุมบุคลากรด้านเทคนิคอย่างน้อย ดังต่อไปนี้

- (๑) ผู้ดูแลระบบและเครือข่าย
- (๒) ผู้พัฒนาระบบและแอปพลิเคชัน
- (๓) บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
- (๔) บุคลากรที่ปฏิบัติงานด้านระบบคลาวด์ ระบบฐานข้อมูล และโครงสร้างพื้นฐานสำคัญ
- (๕) บุคลากรด้านการตรวจสอบ วิเคราะห์ และตอบสนองเหตุการณ์ด้านไซเบอร์

ทั้งนี้ มหาวิทยาลัยจะดำเนินการพิจารณาในการปรับระดับความลึกของทักษะให้เหมาะสมกับหน้าที่ และระดับความรับผิดชอบของแต่ละตำแหน่งงาน

๒.๓ แนวทางการกำหนดทักษะและสมรรถนะ

ดำเนินการกำหนดกรอบทักษะและสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์สำหรับตำแหน่งงาน ด้านเทคนิคอย่างชัดเจน โดยพิจารณาจากบทบาทหน้าที่ ความรับผิดชอบ ลักษณะงาน และระดับความเสี่ยง ของระบบที่ดูแล เพื่อใช้เป็นแนวทางในการพัฒนาบุคลากรและประเมินความพร้อมของทรัพยากรบุคคล ด้านไซเบอร์

๒.๔ แนวทางการปฏิบัติ

๒.๔.๑ การระบุทักษะและสมรรถนะที่จำเป็นสำหรับตำแหน่งงานต่าง ๆ

ดำเนินการระบุทักษะด้านเทคนิคและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นสำหรับ แต่ละตำแหน่งงาน เช่น ความรู้ด้านระบบเครือข่าย ความมั่นคงปลอดภัยของระบบปฏิบัติการ การพัฒนาโปรแกรม อย่างมั่นคงปลอดภัย การตรวจจับและตอบสนองเหตุการณ์ และการบริหารจัดการระบบคลาวด์

๒.๔.๒ การจัดทำแผนพัฒนาบุคลากรด้านไซเบอร์อย่างเป็นระบบ

ดำเนินการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในระยะสั้น ระยะกลาง และระยะยาว โดยกำหนดเป้าหมาย ตัวชี้วัด และแนวทางการพัฒนาอย่างชัดเจน เพื่อให้การพัฒนาบุคลากร เป็นไปอย่างต่อเนื่องและมีทิศทางเดียวกัน

๒.๔.๓ การส่งเสริมการอบรมเชิงลึก การฝึกปฏิบัติ และการแลกเปลี่ยนความรู้

ดำเนินการส่งเสริมการอบรมเชิงลึก การฝึกปฏิบัติจริง (Hands-on Training) การจัดเวทีแลกเปลี่ยน ความรู้ และการเรียนรู้จากประสบการณ์ เพื่อเสริมสร้างความเข้าใจและทักษะที่สามารถนำไปใช้ปฏิบัติได้จริง ในสถานการณ์ต่างๆ

๒.๔.๔ การสนับสนุนการเข้าร่วมกิจกรรมฝึกซ้อมหรือการแข่งขันด้านไซเบอร์

ดำเนินการสนับสนุนบุคลากรเข้าร่วมกิจกรรมฝึกซ้อม การทดสอบระบบ หรือการแข่งขันด้านความมั่นคง ปลอดภัยไซเบอร์ เพื่อพัฒนาทักษะการคิดวิเคราะห์ การแก้ไขปัญหา และการทำงานเป็นทีมในสถานการณ์ ที่ใกล้เคียงกับเหตุการณ์จริง

๒.๔.๕ การประเมินและติดตามผลการพัฒนาทักษะของบุคลากร

ดำเนินการประเมินและติดตามผลการพัฒนาทักษะของบุคลากรอย่างสม่ำเสมอ โดยพิจารณาจาก ผลการอบรม การทดสอบ การปฏิบัติงานจริง และการประเมินสมรรถนะ เพื่อใช้เป็นข้อมูลในการปรับปรุง แผนพัฒนาบุคลากรและการจัดสรรทรัพยากรในอนาคต



๒.๔.๖ การเชื่อมโยงการพัฒนาทักษะกับเส้นทางความก้าวหน้าในสายงาน

ดำเนินการเชื่อมโยงการพัฒนาทักษะเฉพาะด้านกับเส้นทางความก้าวหน้าในสายงานและการประเมินผล การปฏิบัติงาน เพื่อสร้างแรงจูงใจและรักษาบุคลากรที่มีความสามารถด้านไซเบอร์ไว้กับองค์กร

๓. การสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ (Professional Certification and Training Support)

๓.๑ หลักการและวัตถุประสงค์

ดำเนินการสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ แก่บุคลากรที่เกี่ยวข้องอย่างเป็นระบบ เพื่อยกระดับความรู้ ความสามารถ และความเชี่ยวชาญเฉพาะด้าน ให้เป็นไปตามแนวปฏิบัติที่เป็นที่ยอมรับในระดับสากล และเสริมสร้างมาตรฐานการปฏิบัติงานด้านความมั่นคง ปลอดภัยไซเบอร์ของมหาวิทยาลัยให้มีความน่าเชื่อถือและเป็นที่ยอมรับ

การสนับสนุนดังกล่าวมีวัตถุประสงค์เพื่อให้บุคลากรสามารถนำความรู้และทักษะที่ได้รับจากการอบรม และการรับรองมาตรฐานมาประยุกต์ใช้ในการพัฒนาระบบ มาตรการ และกระบวนการด้านความมั่นคงปลอดภัย ไซเบอร์ของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ และสอดคล้องกับบทบาทหน้าที่ ความรับผิดชอบ และระดับ ความเสี่ยงของงานที่ปฏิบัติ

๓.๒ ขอบเขตและกลุ่มเป้าหมาย

การสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพต้องครอบคลุมบุคลากรที่ปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคลากรที่มีบทบาทในการกำกับดูแล วางนโยบาย หรือบริหารจัดการความเสี่ยงด้านไซเบอร์ ทั้งนี้ ให้พิจารณาความเหมาะสมของประเภทการอบรม และการรับรองมาตรฐานให้สอดคล้องกับตำแหน่งงานและระดับความรับผิดชอบของแต่ละบุคลากร

๓.๓ แนวทางการกำหนดกรอบการสนับสนุน

ดำเนินการกำหนดกรอบ หลักเกณฑ์ และแนวทางการสนับสนุนการอบรมและการรับรองมาตรฐาน วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน โดยคำนึงถึงความจำเป็น ความคุ้มค่า ประโยชน์ที่ได้รับ ต่อองค์กร และความสอดคล้องกับยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ของมหาวิทยาลัย

๓.๔ แนวทางการปฏิบัติ

๓.๔.๑ การกำหนดหลักเกณฑ์และแนวทางการสนับสนุน

ดำเนินการกำหนดหลักเกณฑ์และเงื่อนไขในการสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพ เช่น ประเภทของหลักสูตรหรือการรับรองที่ให้การสนับสนุน หลักเกณฑ์การคัดเลือกผู้เข้าร่วม ระยะเวลาการผูกพัน การปฏิบัติงาน และแนวทางการประเมินผลหลังการอบรม เพื่อให้การสนับสนุนเป็นไปอย่างโปร่งใสและเป็นธรรม

๓.๔.๒ การส่งเสริมการเข้าร่วมอบรมและสอบรับรองให้สอดคล้องกับบทบาทหน้าที่

ดำเนินการส่งเสริมการเข้าร่วมอบรมและการสอบรับรองมาตรฐานที่สอดคล้องกับบทบาทหน้าที่ ความรับผิดชอบ และทักษะที่จำเป็นของแต่ละตำแหน่งงาน เพื่อให้ความรู้และทักษะที่ได้รับสามารถนำไปใช้ ประโยชน์ในการปฏิบัติงานจริงได้อย่างเหมาะสม



๓.๔.๓ การจัดสรรงบประมาณและทรัพยากรสนับสนุน

ดำเนินการจัดสรรงบประมาณหรือทรัพยากรสนับสนุนการอบรมและการรับรองมาตรฐานวิชาชีพตามความเหมาะสมและความจำเป็น โดยคำนึงถึงความคุ้มค่าและผลลัพธ์ที่มหาวิทยาลัยจะได้รับในระยะยาว

๓.๔.๔ การส่งเสริมการถ่ายทอดความรู้และประสบการณ์หลังการอบรม

ดำเนินการส่งเสริมให้บุคลากรที่ได้รับการอบรมหรือการรับรองมาตรฐานถ่ายทอดความรู้ ประสบการณ์ และแนวปฏิบัติที่ได้รับให้แก่บุคลากรอื่นในมหาวิทยาลัย เพื่อขยายผลการพัฒนาความรู้และยกระดับความสามารถขององค์กรโดยรวม

๓.๔.๕ การบันทึกและติดตามผลการรับรองมาตรฐานวิชาชีพของบุคลากร

ดำเนินการบันทึกข้อมูลการอบรมและการรับรองมาตรฐานวิชาชีพของบุคลากรอย่างเป็นระบบ และติดตามผลการนำความรู้ไปใช้ในการปฏิบัติงาน รวมถึงการต่อยอดหรือการพัฒนาความรู้เพิ่มเติม เพื่อให้สามารถประเมินประสิทธิผลของการสนับสนุนได้อย่างเหมาะสม

๓.๔.๖ การเชื่อมโยงกับการพัฒนาสายอาชีพและการประเมินผลการปฏิบัติงาน

ดำเนินการเชื่อมโยงการอบรมและการรับรองมาตรฐานวิชาชีพกับการพัฒนาสายอาชีพ การประเมินผลการปฏิบัติงาน และการวางแผนกำลังคนด้านไซเบอร์ เพื่อสร้างแรงจูงใจและรักษาบุคลากรที่มีความเชี่ยวชาญไว้กับมหาวิทยาลัย

๔. การติดตาม ประเมินผล และการปรับปรุงอย่างต่อเนื่อง (Monitoring, Evaluation, and Continuous Improvement)

๔.๑ หลักการและวัตถุประสงค์

ดำเนินการติดตาม ประเมินผล และปรับปรุงการดำเนินงานด้านการสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อให้การพัฒนาบุคลากรมีความเหมาะสม ทันสมัย และสอดคล้องกับความเสี่ยง ภัยคุกคาม และความต้องการของมหาวิทยาลัยในระยะยาว

การดำเนินการดังกล่าวมีวัตถุประสงค์เพื่อให้มหาวิทยาลัยสามารถประเมินประสิทธิผลของกิจกรรมการอบรมและการพัฒนาศักยภาพ ตรวจสอบความเพียงพอของทักษะและสมรรถนะของบุคลากร และนำผลการประเมินไปใช้ในการปรับปรุงนโยบาย แผนงาน และแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ

๔.๒ ขอบเขตการติดตามและประเมินผล

การติดตามและประเมินผลต้องครอบคลุมองค์ประกอบสำคัญอย่างน้อย ดังต่อไปนี้

- (๑) ผลการอบรมและกิจกรรมสร้างความตระหนัก
- (๒) ระดับความรู้ ความเข้าใจ และทักษะของบุคลากร
- (๓) การนำความรู้และทักษะไปใช้ในการปฏิบัติงานจริง
- (๔) ประสิทธิภาพของมาตรการและกิจกรรมด้านการพัฒนาศักยภาพ
- (๕) ความสอดคล้องกับนโยบาย แผน และมาตรฐานที่เกี่ยวข้อง



๔.๓ แนวทางการปฏิบัติ

๔.๓.๑ การกำหนดตัวชี้วัดและเกณฑ์การประเมินผล

ดำเนินการกำหนดตัวชี้วัดและเกณฑ์การประเมินผลการดำเนินงานด้านการสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพอย่างชัดเจน เช่น อัตราการเข้าร่วมอบรม ระดับความรู้ก่อนและหลังการอบรม ผลการประเมินทักษะ และความพึงพอใจของผู้เข้าร่วม เพื่อใช้เป็นเครื่องมือในการติดตามและประเมินผลอย่างเป็นระบบ

๔.๓.๒ การรวบรวมและวิเคราะห์ข้อมูลอย่างเป็นระบบ

ดำเนินการรวบรวมข้อมูลจากผลการอบรม การประเมินทักษะ การทดสอบ การสำรวจความคิดเห็น และข้อมูลอื่นที่เกี่ยวข้องอย่างเป็นระบบ และนำข้อมูลดังกล่าวมาวิเคราะห์เพื่อประเมินจุดแข็ง จุดอ่อน และช่องว่างในการพัฒนาศักยภาพของบุคลากร

๔.๓.๓ การใช้บทเรียนที่ได้รับในการปรับปรุงการดำเนินงาน

ดำเนินการนำบทเรียนที่ได้รับจากการอบรม การฝึกซ้อม และเหตุการณ์ที่เกี่ยวข้อง มาใช้ในการทบทวน และปรับปรุงเนื้อหา วิธีการอบรม และแนวทางการพัฒนาศักยภาพ เพื่อให้การดำเนินงานมีประสิทธิภาพ และตอบสนองต่อความเสี่ยงที่เปลี่ยนแปลงไป

๔.๓.๔ การรายงานผลและการสื่อสารต่อผู้บริหาร

ดำเนินการจัดทำรายงานสรุปผลการติดตามและประเมินผลเสนอผู้บริหารและคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ประกอบการตัดสินใจเชิงนโยบาย การจัดสรรทรัพยากร และการกำหนดทิศทางการพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ในอนาคต

๔.๓.๕ การปรับปรุงแผนและแนวทางการพัฒนาอย่างต่อเนื่อง

ดำเนินการปรับปรุงแผนงาน หลักสูตร และกิจกรรมด้านการสร้างความรู้ ความตระหนัก และการพัฒนาศักยภาพอย่างต่อเนื่อง โดยอาศัยผลการประเมิน ข้อมูลเชิงประจักษ์ และแนวโน้มภัยคุกคามและเทคโนโลยี เพื่อให้การพัฒนาบุคลากรมีความเหมาะสมและทันสมัย

๔.๓.๖ การบูรณาการกับการบริหารความเสี่ยงและยุทธศาสตร์องค์กร

ดำเนินการนำผลการติดตามและประเมินผลไปบูรณาการกับกระบวนการบริหารความเสี่ยงองค์กร และการวางแผนเชิงยุทธศาสตร์ของมหาวิทยาลัย เพื่อให้การพัฒนาศักยภาพด้านไซเบอร์สนับสนุนเป้าหมาย และภารกิจของมหาวิทยาลัยอย่างยั่งยืน

