นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

สำนักนวัตกรรมดิจิทัลและระบบอัจฉริยะ กำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ มหาวิทยาลัยสงขลานครินทร์ โดยกำหนดให้มีมาตรฐาน (Standard) ระเบียบปฏิบัติ (Procedure) ให้ครอบคลุมการรักษาความมั่นคงปลอดภัยสารสนเทศและป้องกันภัยคุกคามต่าง ๆ รวมถึงภัยคุกคามทางไซเบอร์ สอดคล้องกับกฎหมาย กฎระเบียบ โดยยึดหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) และความปลอดภัย (Safety) มีรายละเอียด ดังนี้

1. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การควบคุมการเข้าถึงและใช้งานทางกายภาพและสภาพแวดล้อมของพื้นที่ศูนย์ข้อมูลซึ่งมีระบบสารสนเทศที่สำคัญของมหาวิทยาลัย เพื่อให้บริการได้อย่างต่อเนื่องและปลอดภัย

2. กำหนดแผนระบบสารสนเทศสำรองที่สมบูรณ์และพร้อมใช้งาน พร้อมมีแผนดำเนินงานอย่างต่อเนื่องในสภาวะวิกฤต (Business Continuity Plan: BCP) เพื่อให้บริการได้อย่างต่อเนื่องและปลอดภัย

3. กำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการตรวจสอบ ประเมิน และรายงานเหตุการณ์ที่เกิดขึ้นและความเสี่ยงทางกายภาพและความมั่นคงปลอดภัยสารสนเทศ อย่างสม่ำเสมอ ดำเนินมาตรการป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีระบบตรวจจับและตอบสนองต่อเหตุการณ์ความปลอดภัย

4. เผยแพร่นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักฯ ได้รับทราบ

5. จัดทำเอกสารและคู่มือเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และจัดอบรมให้กับบุคลากรเป็นประจำ

6. กำหนดระเบียบปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักฯ อ้างอิงตามมาตรฐาน ISO/IEC 27001:2022 และปฏิบัติตามอย่างเคร่งครัด

7. ดำเนินการป้องกัน ตรวจจับ และประเมินผลการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นประจำ เพื่อให้มั่นใจว่าระบบมีความปลอดภัยเพียงพอ

8. มุ่งมั่นในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และดำเนินการปรับปรุงแก้ไขอย่างต่อเนื่อง เพื่อให้สอดคล้องกับเทคโนโลยีใหม่ ๆ และภัยคุกคามที่เกิดขึ้น ทบทวนอย่างน้อยปีละ 1 ครั้ง