



ประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
เรื่อง นโยบายการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ
และความเสี่ยงด้านภัยคุกคามไซเบอร์

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม ตระหนักถึงความสำคัญของการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) และการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) เพื่อให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ โดยใช้เทคโนโลยีสารสนเทศให้สอดรับกับหลักการดำเนินงานของสำนักวิทยบริการฯ สามารถวางแผนควบคุมและแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ และมีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป รวมทั้งป้องกันปัญหาและภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้น จึงขอกำหนดนโยบายการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงด้านภัยคุกคามไซเบอร์ เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสที่จะเกิดความเสียหาย มีความมั่นคงปลอดภัยของสารสนเทศ ดังนี้

๑. ให้มีคณะกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตัวแทนจากทางหน่วยงานหลักของมหาวิทยาลัยที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และจากสำนักวิทยบริการฯ และให้กำหนดหน้าที่ความรับผิดชอบพร้อมทั้งวิธีการบริหารจัดการ

๒. พัฒนาและรักษาการอบรมการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล และติดตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง และพิจารณาการปฏิบัติตามให้สอดคล้อง

๓. ให้มีการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ โดยการประเมินจากภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) ความเป็นไปได้ (Likelihoods) และผลกระทบ (Impact) ต่อหน่วยงาน รวมทั้งให้มีการจัดการความเสี่ยง ที่มีความสอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กร อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง

๔. สื่อความและจดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อสร้างความตระหนักรู้ ความรับผิดชอบ และความเข้าใจการรับมือกับภัยคุกคามทางไซเบอร์ให้กับบุคลากรอย่างน้อยปีละ ๑ ครั้ง

๕. ให้มีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ ให้ครอบคลุมระบบสารสนเทศของสำนักวิทยบริการฯ พร้อมทั้งจัดให้มีการเฝ้าระวัง และให้หน่วยงานที่มีหน้าที่รับผิดชอบ เกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ ต้องรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างน้อย ไตรมาสละครั้ง

๖. ให้จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งลดผลกระทบต่อกระบวนการให้บริการที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนการตอบสนองฯ อย่างน้อยปีละ ๒ ครั้ง

๗. ให้จัดทำแผนพื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อกระบวนการให้บริการ ของหน่วยงานที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนพื้นฟูฯ เพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน อย่างน้อยปีละ ๑ ครั้ง

๘. ให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากการภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

จึงประกาศมาเพื่อให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๔

นาย

(ผู้ช่วยศาสตราจารย์ ดร.บัญชา ศรีสมบัติ)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ