ประกาศกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง นโยบายบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy)

.....

ตามที่ กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการจัดทำระบบความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 : 2022 เพื่อความปลอดภัย ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อเป็นไปตามตัวชี้วัด 9.1 ระบบการบริหารจัดการด้าน IT ที่ได้มาตรฐานสากล นั้น

กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้จัดทำนโยบายบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ โดยยึดหลักการ **"การกำกับดูแล และบริหารจัดการด้านเทคโนโลยีสารสนเทศในมหาวิทยาลัยนเรศวร ด้วยความปลอดภัยอย่างมืออาชีพ CITCOMS : The Professional Information Technology Governance for the Naresuan University"** ดังนี้

ISMS Policy Abbreviation	**รายละเอียดการดำเนินการตาม นโยบายบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ**
C - Confidentiality (การรักษาความลับ)	- ปกป้องข้อมูลสำคัญจากการเข้าถึงโดยไม่ได้รับอนุญาต - จัดระดับชั้นความลับของข้อมูลและควบคุมการเข้าถึงตามความเหมาะสม - ไม่เปิดเผยข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล, ข้อมูลรหัสผ่าน, IP ของระบบเครือข่าย
I - Integrity (ความถูกต้องสมบูรณ์)	- รักษาความถูกต้องและความสมบูรณ์ของข้อมูลในระบบสารสนเทศ - ตรวจสอบคำขอใช้งาน ประวัติการเข้าใช้งาน (Log) และความผิดปกติที่เกิดขึ้นเพื่อป้องกันการแก้ไขข้อมูลโดยผู้ใช้งานที่ไม่ได้รับอนุญาต
T - Transparency (ความโปร่งใส)	- สื่อสารนโยบายและขั้นตอนด้านความมั่นคงปลอดภัยสารสนเทศให้ผู้เกี่ยวข้องทราบอย่างชัดเจน และเปิดเผยข้อมูลแนวปฏิบัติเพื่อป้องกันภัยคุกคามทางไซเบอร์ ตลอดจนกฎหมายที่เกี่ยวข้อง - กำหนดให้มีการตรวจสอบ (Audit) เพื่อทวนสอบว่ามีการดำเนินงานเป็นไปตามขั้นตอนการปฏิบัติที่ได้รับการอนุมัติไว้อย่างถูกต้อง และมีประสิทธิภาพ
C - Compliance (การปฏิบัติตามกฎระเบียบ)	- ปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง กับความปลอดภัยของข้อมูล - ดำเนินการตามระเบียบปฏิบัติ และคู่มือตามมาตรฐาน ISO 27001 อย่างเคร่งครัด
O - Optimization (การปรับปรุงอย่างต่อเนื่อง)	- ปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างสม่ำเสมอ - ส่งเสริมวัฒนธรรมการปรับปรุงอย่างต่อเนื่องในองค์กร
M – Monitoring (การเฝ้าระวัง)	- ตรวจสอบเฝ้าระวังระบบสารสนเทศอย่างต่อเนื่องเพื่อตรวจจับภัยคุกคาม และความผิดปกติ - บันทึกและวิเคราะห์เหตุการณ์ด้านความปลอดภัยเพื่อป้องกันและแก้ไขปัญหาไม่ให้เกิดขึ้น
S - Security Awareness (การสร้างความตระหนัก)	- จัดอบรมและให้ความรู้ด้านความปลอดภัยแก่บุคลากรทุกระดับอย่างสม่ำเสมอ - ส่งเสริมวัฒนธรรมความปลอดภัยในองค์กร

ประกาศ ณ วันที่ 2 ธันวาคม 2567

(รองศาสตราจารย์ ดร.พงศ์พันธ์ กิจสนาโยธิน)
รักษาการในตำแหน่ง ผู้อำนวยการ
กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร