

แผนปฏิบัติการจัดการความรู้ระดับมหาวิทยาลัย ประจำปีงบประมาณ พ.ศ. 2569

1. ชื่อโครงการจัดการความรู้: การสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย

2. หน่วยงานที่รับผิดชอบ : ศูนย์คอมพิวเตอร์

3. หลักการและเหตุผล:

ปัจจุบันมหาวิทยาลัยได้ดำเนินการพัฒนาและประยุกต์ใช้เทคโนโลยีดิจิทัลในการสนับสนุนการบริหารจัดการ การเรียนการสอน การวิจัย และการบริการวิชาการอย่างต่อเนื่อง ส่งผลให้คณาจารย์ บุคลากรและนักศึกษา มีการใช้งานระบบสารสนเทศและแพลตฟอร์มดิจิทัลในชีวิตประจำวันเพิ่มมากขึ้น ไม่ว่าจะเป็นระบบอีเมลมหาวิทยาลัย (Email) ระบบสารบรรณอิเล็กทรอนิกส์ ระบบการเรียนการสอนออนไลน์ การใช้ Cloud Service รวมถึงการสื่อสารผ่านสื่อสังคมออนไลน์ อย่างไรก็ตามการใช้งานที่ขยายตัวอย่างกว้างขวางก่อให้เกิดความเสี่ยงด้านภัยคุกคามไซเบอร์ (Cyber Threats) เช่น การโจมตีด้วยมัลแวร์ การฟิชชิ่ง (Phishing) การรั่วไหลของข้อมูลส่วนบุคคล การแอบอ้างตัวตน และการเข้าถึงระบบโดยไม่ได้รับอนุญาต ปัญหาเหล่านี้อาจส่งผลกระทบต่อความมั่นคงปลอดภัยด้านข้อมูลของมหาวิทยาลัย และความเชื่อมั่นในการให้บริการทางดิจิทัล ดังนั้น ศูนย์คอมพิวเตอร์จึงเล็งเห็นถึงความสำคัญในการจัดทำโครงการจัดการความรู้ (KM) เรื่อง การสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย เพื่อสร้างความตระหนักรู้ เสริมสร้างองค์ความรู้พื้นฐาน และถ่ายทอดความรู้ความเข้าใจด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) ที่ถูกต้องให้แก่ผู้ใช้งานภายในมหาวิทยาลัย ให้สามารถใช้งานระบบดิจิทัล ได้อย่างปลอดภัย ลดความเสี่ยงจากภัยคุกคาม และสอดคล้องกับแผนยุทธศาสตร์มหาวิทยาลัย ด้านการบริหารองค์กรที่เป็นเลิศ ตลอดจนสนับสนุนการดำเนินงานตามแผนดิจิทัลของมหาวิทยาลัย

4. วัตถุประสงค์:

- 4.1 เพื่อเสริมสร้างความรู้และความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย
- 4.2 เพื่อสร้างแนวทางป้องกันตนเองจากภัยคุกคามทางไซเบอร์ อาทิ การจัดการรหัสผ่าน การหลีกเลี่ยงฟิชชิ่ง การรักษาความปลอดภัยของอุปกรณ์
- 4.3 เพื่อรวบรวมและถ่ายทอดความรู้ด้าน Cybersecurity ที่เหมาะสมต่อการใช้งาน
- 4.4 เพื่อส่งเสริมวัฒนธรรมการใช้เทคโนโลยีอย่างปลอดภัยและมีความรับผิดชอบ

5. สถานภาพโครงการ: โครงการใหม่

6. การถ่ายทอดแผนสู่การปฏิบัติระดับโครงการตามเกณฑ์ EdPEX:

KM04 การจัดการความรู้ที่สร้างนวัตกรรมและในกระบวนการวางแผนเชิงกลยุทธ์:

7. ระยะเวลาโครงการ: 1 ปี เริ่มต้น ปีงบประมาณ พ.ศ. 2569 สิ้นสุด ปีงบประมาณ พ.ศ. 2569

8. รายละเอียดแผนการดำเนินงานโครงการ:

เป้าหมายโครงการ/ตัวชี้วัด	หน่วยนับ	แผนปีงบประมาณ พ.ศ.				
		2569				
		รวม	Q1	Q2	Q3	Q4
<p>เป้าหมายโครงการ : เพื่อสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) ให้แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย</p> <p>ตัวชี้วัด :</p> <ol style="list-style-type: none"> ระดับความสำเร็จของการจัดการความรู้เพื่อสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) ให้แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย การจัดกิจกรรมแลกเปลี่ยนเรียนรู้ ทดสอบการหลอกลวง (Phishing Attack) โดยกำหนดให้มีผู้ที่ไม่ตกเป็นเหยื่อการทดสอบมากกว่า 90% การเผยแพร่ความรู้/สื่อประชาสัมพันธ์ ด้าน Cybersecurity 	คะแนน	5	1	2	4	5
ครั้ง	1	-	-	1	1	
ครั้ง	1	-	-	-	1	
ครั้ง	4	1	2	3	4	

9. ตัวชี้วัดความสำเร็จแบบ Milestone : ระดับความสำเร็จของการจัดการความรู้เพื่อสร้างความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) ให้แก่ผู้ใช้งานทั่วไปภายในมหาวิทยาลัย

9.1 รายละเอียดผลงานของแต่ละขั้นตอน

ขั้นตอน	KM Process	รายละเอียดผลงานของแต่ละขั้นตอน
1	การกำหนดประเด็นการจัดการความรู้และนิยามความรู้ที่บ่งชี้ (Knowledge Identification)	จัดการประชุมคณะทำงานการจัดการความรู้ประจำศูนย์คอมพิวเตอร์ ระดมความคิด กำหนดขอบเขต ระบุประเด็นความรู้ที่จำเป็นด้าน Cybersecurity สำหรับผู้ใช้งานทั่วไป เช่น รหัสผ่าน ป้องกันฟิชชิ่ง การรักษาข้อมูล
2	การสร้างและแสวงหาความรู้ (Knowledge Creation and Acquisition)	ศึกษาและสรรหาข้อมูลจากแหล่งความรู้หรือผู้เชี่ยวชาญทั้งภายในและภายนอกมหาวิทยาลัย และศึกษาและรวบรวมข้อมูลจากมาตรฐานสากล และคู่มือจากสำนักงานพัฒนารัฐบาลดิจิทัล (DGA)

ขั้นตอน	KM Process	รายละเอียดผลงานของแต่ละขั้นตอน
3	การจัดความรู้ให้เป็นระบบ (Knowledge Organization)	จัดเตรียมข้อมูลที่ได้จากการสรรหาจากแหล่งความรู้หรือผู้เชี่ยวชาญ และจัดเก็บหมวดหมู่ความรู้เป็น เช่น ความรู้พื้นฐาน แนวทางป้องกันเบื้องต้นจากภัยคุกคามทางไซเบอร์ ให้เป็นระบบ
4	การประมวลและกลั่นกรองความรู้ (Knowledge Codification and Refinement)	กลั่นกรองข้อมูลเพื่อตรวจสอบความถูกต้อง ปรับปรุงเนื้อหาให้ง่ายต่อการเข้าใจของผู้ใช้งานทั่วไป พร้อมตัวอย่างและภาพประกอบ
5	การเข้าถึงความรู้ (Knowledge Access)	จัดเก็บข้อมูลเป็นลายลักษณ์อักษร เพื่ออ้างอิงและเผยแพร่ผ่านเว็บไซต์ของศูนย์คอมพิวเตอร์ ระบบอีเมลกลาง และเพจ Facebook หน่วยงาน
6	การแบ่งปันแลกเปลี่ยนความรู้ (Knowledge Sharing)	จัดกิจกรรมแลกเปลี่ยนเรียนรู้ตามแผนปฏิบัติการการจัดการความรู้ เพื่อแลกเปลี่ยนความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity 101) ให้กับผู้ใช้งานภายในมหาวิทยาลัย
7	การเรียนรู้ (Learning)	ประเมินผลการนำไปใช้หลังกิจกรรมแลกเปลี่ยนเรียนรู้ เช่น ทดสอบสถานการณ์จำลอง (Phishing Simulation) เพื่อนำผลมาปรับปรุงเนื้อหาและพัฒนากระบวนการอย่างต่อเนื่อง

9.2 เกณฑ์การให้คะแนนตัวบ่งชี้

ตัวบ่งชี้	หน่วยนับ	เกณฑ์การให้คะแนน				
		1	2	3	4	5
จำนวนขั้นตอนการดำเนินการที่แล้วเสร็จ	ขั้นตอน	ขั้นตอน ...1...	ขั้นตอน ..1-2..	ขั้นตอน ..1-4..	ขั้นตอน ..1-6..	ขั้นตอน ...1-7.