แบบ RM-1

แบบกำหนดขอบเขตความรับผิดชอบตามประเด็นยุทธศาสตร์
ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

ประเด็นยุทธศาสตร์มหาวิทยาลัย ที่ตอบสนอง	กลยุทธ์/ประเภทความเสี่ยง/ โครงการ/งานประจำ	วัตถุประสงค์	ตัวชี้วัด	เป้าหมาย	ผู้รับผิดชอบ
4. การพัฒนาสู่มหาวิทยาลัยสมรรถนะสูง	4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาล มุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง	เพื่อบำรุงรักษาระบบเครือข่ายให้มีประสิทธิภาพในการให้บริการภายในมหาวิทยาลัยฯ	KPI7 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5) KPI8 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80) KPI9 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80)	(เป้าหมาย คะแนน 5)	ผศ.พรหมเมศ วีระพันธ์ ผศ.ศิลป์ณรงค์ ฉวีพัฒน์

แบบ RM-2

แบบฟอร์มการวิเคราะห์ความเสี่ยง

ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

งานหลักของฝ่าย (1)	ความเสี่ยง (2)	สถานะปัจจุบัน (3)	ปัจจัยเสี่ยง (4)		ผลกระทบ (5)	KPI (6)	โอกาสที่จะเกิด (L) (7)	ผลกระทบ (C) (8)	ระดับความเสี่ยง (9)	ระดับความเสี่ยงที่คาดหวัง (10)	แนวทางการตอบสนอง (11)
			ภายนอก	ภายใน							
งานประจำ (Routine : R)											
4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาลมุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง	O1/การโจมตีความปลอดภัยทางไซเบอร์	1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้	1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผล	1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ 2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึงการสูญหายและความ	1. การหยุดชะงักของระบบสารสนเทศสำคัญของมหาวิทยาลัย (เช่น ระบบทะเบียน การเงิน ระบบการเรียนการสอนออนไลน์) ส่งผลต่อภาพลักษณ์ ความน่าเชื่อถือ และมีค่าใช้จ่ายสูงในการแก้ไขฟื้นฟูระบบ 2. การรั่วไหลของข้อมูลส่วนบุคคลของนักศึกษาและบุคลากร นำไปสู่การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจส่งผลให้มหาวิทยาลัยได้รับบทลงโทษทางกฎหมาย	KPI7 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมายคะแนน 5) KPI8 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80) KPI9 – ร้อยละของนักศึกษา	L2=2	C6=5	10 สูง	ต่ำ	ควบคุมความเสี่ยง

งานหลักของฝ่าย (1)	ความเสี่ยง (2)	สถานะปัจจุบัน (3)	ปัจจัยเสี่ยง (4)		ผลกระทบ (5)	KPI (6)	โอกาสที่จะเกิด (L) (7)	ผลกระทบ (C) (8)	ระดับความเสี่ยง (9)	ระดับความเสี่ยงที่คาดหวัง (10)	แนวทางการตอบสนอง (11)
			ภายนอก	ภายใน							
			ให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้	เสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี		ชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายอย่างน้อยร้อยละ 80)					

แบบ RM 3

แบบแสดงแนวทางตอบสนองความเสี่ยง/แผนบริหารความเสี่ยง
ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (4)	ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5)	ระยะเวลาดำเนินการ (6)
O1/การโจมตีความปลอดภัยทางไซเบอร์	**ภายนอก** 1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้ **ภายใน** 1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ	KPI7 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5) KPI8 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย ร้อยละ 80) KPI9 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80)	ระดับสูง	1. ดำเนินการจัดตั้งคณะทำงานและผู้รับผิดชอบ 2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบายวางแผนการดำเนินงาน 3. จัดอบรมเกี่ยวกับ เรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์ 4. สรุปผลการจัดกิจกรรม 5. จัดทำแผนรักษาความมั่นคงปลอดภัยไซเบอร์ 6. จัดทำแนวปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 7. แบบประเมินความสอดคล้อง ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 8. จัดทำนโยบายการรักษาความมั่นคงปลอดภัย	1. ผศ.พรหมเมศ วีระพันธ์ 2. ผศ.ศิลป์ณรงค์ ฉวีพัฒน์	ปีงบประมาณ 2568

โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (4)	ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5)	ระยะเวลาดำเนินการ (6)
	2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึงการสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี 3. บุคลากรยังขาดความรู้ความเข้าใจในการป้องกันการโจมตีรูปแบบใหม่ผ่านระบบเครือข่ายอินเตอร์เน็ต 4. บุคลากรขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน					

แบบติดตามผลการจัดการความเสี่ยง

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
O1/การโจมตีความปลอดภัยทางไซเบอร์	**(ปัจจัยภายนอก)** 1. นโยบายการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ที่ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด 2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรน	**KPI7** – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมายคะแนน5) **KPI8** - ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80)	10 สูง	1. ดำเนินการจัดตั้งคณะทำงานและผู้รับผิดชอบ	ปีงบประมาณ 2568	- รองอธิการบดีฝ่ายวิชาการ - ผอ.สำนักวิทยบริการฯ	**1. จัดตั้งคณะทำงานและผู้รับผิดชอบ** ดังนี้ 1.1 คณะกรรมการดำเนินงานการพัฒนาเว็บไซต์หน่วยงานภายในมหาวิทยาลัยราชภัฏกำแพงเพชร (คณะกรรมการพัฒนาเว็บไซต์ มีหน้าที่ นำข้อมูลและสารสนเทศมาจัดทำเว็บไซต์ให้เหมาะสมกับวัตถุประสงค์การใช้ประโยชน์ พัฒนาเว็บไซต์ รูปแบบภาษาไทยและภาษาอังกฤษ ที่มีคุณภาพ มีความถูกต้องเป็นปัจจุบันและได้รับการปรับปรุงข้อมูลอย่างต่อเนื่อง รองรับการใช้งานได้บนทุกอุปกรณ์ รวมถึงบำรุงรักษาและตรวจตราความปลอดภัยของเว็บไซต์) 1.2 จัดส่งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ให้กับ สกมช.	100	
				2. ประชุมคณะกรรมการดำเนินงาน จัดทำ	ปีงบประมาณ 2568	รอง ผอ. สำนักวิทยบริการฯ	**2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบายวางแผนการดำเนินงาน** เมื่อวันที่ 15 พฤศจิกายน 2567 ประชุมงานพัฒนาเครือข่ายและการสื่อสาร เพื่อชี้แจงนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ของมหาวิทยาลัย และ	100	

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
	ซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้ **(ปัจจัยภายใน)** 1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การ	**KPI9** - ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80)		นโยบาย วาง แผนการดำเนินงาน			สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดังนี้ 2.1 ทบทวนโครงการและตัวชี้วัดที่เกี่ยวข้อง เพื่อนำไปเป็นแนวทางการบริหารและจัดการ มหาวิทยาลัยที่มีการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเป็นสำคัญ 2.2 สำรวจการบริหารจัดการและอุปกรณ์ที่เกี่ยวข้อง อาทิ Firewall, WAP และอื่นๆ 2.3 สำรวจเนื้อหาที่จะให้ความรู้กับบุคลกรเกี่ยวกับการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ อาทิ พรบ.คอมพิวเตอร์, กฎหมายที่เกี่ยวข้อง, ข้อมูลส่วนบุคคล และอื่นๆ 2.4 มอบหมายผู้รับผิดชอบในการขับเคลื่อน รวบรวม จัดทำข้อมูล และรายงานผล 2.5 ตั้งคณะทำงาน 2.6 วางแผนการดำเนินงาน 1) การปรับปรุงอุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) 2) การปรับปรุงเครือข่ายเสมือน (vlan) 3) ปรับปรุงช่องทางการเชื่อมต่อ WiFi 4) อัพเกรดอุปกรณ์เครือข่ายหลัก (Main Switch) 5) อัพเกรดช่องทางการเชื่อมต่อ (โปรโตคอล) เพื่อเพิ่มความเร็วสัญญาณอินเทอรเน็ต 6) อบรมพัฒนาทักษะการบริหารจัดการเครือข่ายเพื่อเสริมสมรรถนะในการทำงานให้กับบุคลากรงานเครือข่าย ฯ 7) อบรมการการตระหนักรู้ภัยคุกคามจากเครือข่าย		

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

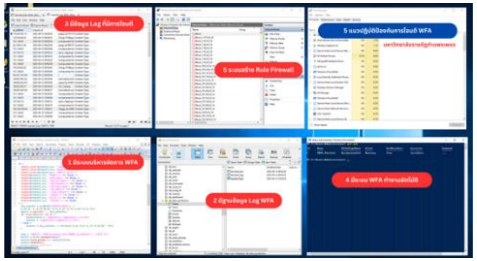
ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
	ใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ 2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึงการสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี						อินเทอร์เน็ต 8) จัดหาอุปกรณ์เพื่อรองรับการใช้บริการ 9) บำรุงรักษาอุปกรณ์งานเครือข่าย   - ประชุมทบทวนแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ (Website Security) - แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์  		
				3. จัดอบรมเกี่ยวกับ เรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากร	ปีงบประมาณ 2568	รอง ผอ. สำนักวิทยบริการฯ	**3. จัดอบรมเกี่ยวกับ เรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์** **3.1 อบรมการใช้งานระบบ MISP (Malware Information Sharing Platform) สำหรับตรวจสอบความปลอดภัยของเว็บไซต์** ซึ่ง MISP เป็นซอฟต์แวร์โอเพ่นซอร์สที่ช่วยในการรวบรวม จัดเก็บ แจกจ่าย และแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ที่เกี่ยวข้องกับการวิเคราะห์	100	

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

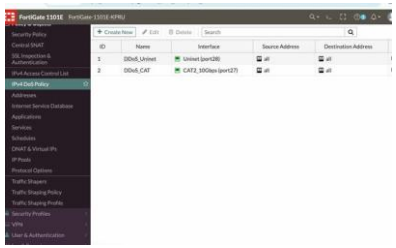
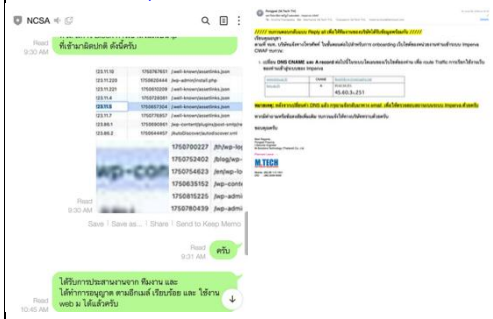
ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
	3. บุคลากรยังขาดความรู้ความเข้าใจในการป้องกันการโจมตีรูปแบบใหม่ผ่านระบบเครือข่ายอินเตอร์เน็ต 4. บุคลากรขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน						เหตุการณ์ความปลอดภัยทางไซเบอร์และมัลแวร์ 2 ครั้ง เมื่อวันที่ 31 มกราคม 2568   และ เมื่อวันที่ 19 มีนาคม 2568   วันที่ 8 กรกฎาคม 2568 ตัวแทนบุคลากรของมหาวิทยาลัยฯ ได้เข้าร่วมกิจกรรมเพื่อสร้างความตระหนักรู้และประชาสัมพันธ์ชี้แจง โครงการบริการระบบตรวจสอบและป้องกันการโจมตีบนเว็บไซต์ API โมบายแอพพลิเคชัน และการปลอมแปลงเว็บที่ใช้ในการหลอกลวงประชาชน นำโดย อาจารย์จตุรงค์ ธงชัย รองผู้อำนวยการฝ่ายพัฒนาสมรรถนะดิจิทัลและภาษาต่างประเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ นายคมกริช กลิ่นอาจ นักวิชาการคอมพิวเตอร์ ชำนาญการ สำนักส่งเสริมวิชาการและงานทะเบียน และนายมนตรี กาไสย นักวิชาการคอมพิวเตอร์ ประจำงานพัฒนาระบบเครือข่ายและการ		

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ ( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย									
ความเสี่ยง (1)	**ปัจจัยเสี่ยง** (2)	KPI (3)	**ระดับความเสี่ยง** (4)	**แผนงาน/กิจกรรม** (5)	**ระยะเวลาดำเนินการ** (6)	**ผู้รับผิดชอบ** (7)	**ผลการดำเนินงานของกิจกรรม** (8)	**ร้อยละความคืบหน้า** (9)	**ปัญหา/อุปสรรค** (10)
							สื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จัดโดย สกมช.  		
				4. สรุปผลการจัดกิจกรรม	ปีงบประมาณ 2568		**4. สรุปผลการดำเนินกิจกรรม KM Website** ประจำปีงบประมาณ 2568 ไว้ที่ https://www.kpru.ac.th/km-web/files/report-webometrics1-10-2025.pdf	100	
				5. จัดทำแนวปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์	ปีงบประมาณ 2568	รอง ผอ. สำนักวิทยบริการฯ	**5. ดำเนินการจัดทำแนวปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้** 5.1 แนวทางปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์มหาวิทยาลัยราชภัฏกำแพงเพชร 5.2 แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยราชภัฏกำแพงเพชร 5.3 แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัยราชภัฏกำแพงเพชร 5.4 แบบประเมินความสอดคล้องของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	100	

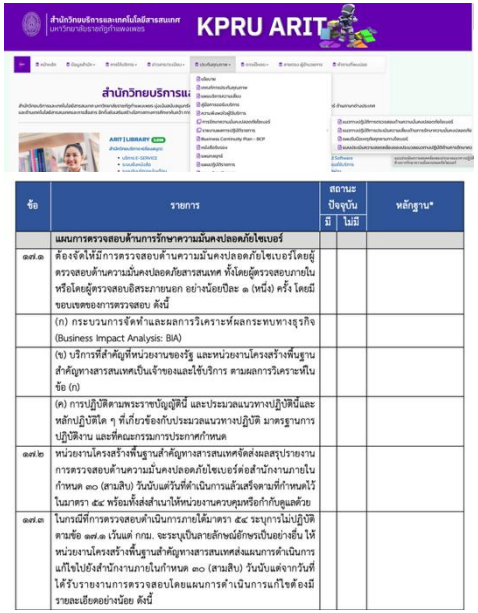
( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
							5.5 ประเมินความพร้อมด้าน Cloud Security ตามประกาศ สกมช. เรื่อง กรอบการทำงานด้านการรักษาความมั่นคง 5.6 แนวปฏิบัติป้องกันการโจมตี WFA		
				6. การนำเทคโนโลยีมาประยุกต์ใช้เพื่อยกระดับการป้องกันความปลอดภัยทางไซเบอร์	ปีงบประมาณ 2568	รอง ผอ. สำนักวิทยบริการฯ	**6. การนำเทคโนโลยีมาประยุกต์ใช้เพื่อยกระดับการป้องกันความปลอดภัยทางไซเบอร์ ดังนี้** 6.1 พัฒนาระบบ WFA (Web Firewall Application) ในการตรวจสอบการโจมตี ดักจับข้อมูลที่เข้ามาแบบปกติ และ ทำการระงับหรือบล็อก การเข้าถึงเครื่องแม่ข่าย  6.2 ระบบ DDOS เฝ้าระวัง ข้อมูลจากภายในและภายนอกที่เข้ามาในเครือข่าย	100	1. การโจมตีในช่วง 18.00 – 06.00 ทำให้บุคลากรต้องเฝ้าระวังตลอดและอาจคลาดเคลื่อนในสถานการณ์ที่โจมตีหนัก 2. จำนวนโดเมนที่ สกมช. ให้สำหรับการป้องมี 1 Website ไม่เพียงพอต่อการป้องกัน

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
							 6.3 ระบบ Imperva CWAF จาก สกมช. สำหรับโดเมน www.kpru.ac.th 		
				7. จัดอบรมเกี่ยวกับเรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์ให้แก่นักศึกษา	ปีงบประมาณ 2568	รอง ผอ. สำนักวิทยบริการฯ	**7. จัดกิจกรรมอบรมการป้องกันภัยอาชญากรรมทางเทคโนโลยี สำหรับนักศึกษา ชั้นปีที่ 1** เมื่อวันที่ 28 พฤษภาคม 2568 ณ ห้องประชุมราชพฤกษ์ ชั้น 3 หอประชุมทีปังกรรัศมีโชติ 	100	

( ) ด้านกลยุทธ์ **(✓) ด้านการปฏิบัติงาน** ( ) ด้านบุคลากร และทรัพยากร ( ) ด้านการเงิน ( ) ด้านการปฏิบัติตามกฎระเบียบ ข้อบังคับ
( ) ด้านนักศึกษา ( ) ด้านสวัสดิภาพและความปลอดภัย

ความเสี่ยง (1)	ปัจจัยเสี่ยง (2)	KPI (3)	ระดับความเสี่ยง (4)	แผนงาน/กิจกรรม (5)	ระยะเวลาดำเนินการ (6)	ผู้รับผิดชอบ (7)	ผลการดำเนินงานของกิจกรรม (8)	ร้อยละความคืบหน้า (9)	ปัญหา/อุปสรรค (10)
				8. แบบประเมินความสอดคล้องของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	ปีงบประมาณ 2568		**8. จัดทำแบบประเมินความสอดคล้องของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** เผยแพร่ไว้ที่เว็บไซต์สำนักวิทยบริการฯ 	100	

ข้อ	รายการ	สถานะปัจจุบัน มี	สถานะปัจจุบัน ไม่มี	หลักฐาน*
	แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑๗.๑	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้			
	(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)			
	(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)			
	(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด			
๑๗.๒	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย			
๑๗.๓	ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้			

แบบ RM-5

แบบสรุปผลการประเมินความเสี่ยงภายหลังการดำเนินการตามแผนบริหารความเสี่ยง

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI ประจำปี 2568 รอบ 12 เดือน				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
O1/การโจมตีความปลอดภัยทางไซเบอร์	2 (L2)	5 (C6)	10 สูง	2 (L2)	4 (C6)	8 ปานกลาง	ลดลง	**KPI7** – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์	คะแนน 5	- ผอ.สำนักวิทยบริการฯ	☑ บรรลุ ☐ ไม่บรรลุ ผลดำเนินงาน ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ มีการดำเนินการทั้ง 5 ระดับ ดังนี้ 1-มีการระบุความเสี่ยงภัยคุกคามทางไซเบอร์ 2-มีมาตรการป้องกันความเสี่ยงภัยคุกคามทางไซเบอร์ 3-มีมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ 4-มีมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ 5-มีมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	ถึงแม้ว่าความเสี่ยงจะลดลง แต่ยังคงต้องดำเนินการจัดการความเสี่ยงประเด็นนี้ต่อไป เพื่อให้ระบบสารสนเทศและเว็บไซต์มีความปลอดภัย

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI ประจำปี 2568 รอบ 12 เดือน				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
							ลดลง	**KPI8** - ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์	ร้อยละ 80	- ผอ.สำนักวิทยบริการฯ	☑ บรรลุ ☐ ไม่บรรลุ ผลดำเนินงาน **1. อบรมการใช้งานระบบ MISP (Malware Information Sharing Platform) สำหรับตรวจสอบความปลอดภัยของเว็บไซต์** ให้กับผู้ดูแลเว็บไซต์หน่วยงานภายในมหาวิทยาลัย จำนวน 2 ครั้ง เมื่อวันที่ 31 มกราคม 2568  และ เมื่อวันที่ 19 มีนาคม 2568  **2. ส่งตัวแทนบุคลากรของมหาวิทยาลัยฯ เข้าร่วมกิจกรรมเพื่อสร้างความตระหนักรู้และประชาสัมพันธ์ชี้แจง โครงการบริการระบบตรวจสอบและป้องกันการโจมตีบนเว็บไซต์ API โมบายแอพพลิเคชัน และการปลอมแปลงเว็บที่ใช้ในการหลอกลวงประชาชน** เมื่อวันที่ 8 กรกฎาคม 2568 ณ ห้องอัศวิน แกรนด์บอลรูม เอ ชั้น 4 โรงแรมอัศวิน แกรนด์ คอนเวนชัน แจ้งวัฒนะ กรุงเทพฯ จัดโดย	- อบรมส่งเสริมความรู้ความเข้าใจการรับมือเหตุภัยคุกคามทางไซเบอร์เพื่อให้บุคลากรของหน่วยงานสามารถรับมือกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ได้

ความเสี่ยง	ระดับความเสี่ยง						การเปลี่ยนแปลงระดับความเสี่ยง (ลดลง/ เท่าเดิม/ เพิ่มขึ้น)	ผลการบริหารความเสี่ยงตาม KPI ประจำปี 2568 รอบ 12 เดือน				แนวทางดำเนินงานปีถัดไป
	ก่อนการประเมิน			หลังการประเมิน				KPI	เป้าหมาย	ผู้รับผิดชอบ	ผลลัพธ์	
											สกมช. ผู้เข้าร่วมอบรม ได้แก่ อาจารย์จตุรงค์ ธงชัย รองผู้อำนวยการฝ่ายพัฒนาสมรรถนะดิจิทัลและภาษาต่างประเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ นายคมกริช กลิ่นอาจ นักวิชาการคอมพิวเตอร์ ชำนาญการ สำนักส่งเสริมวิชาการและงานทะเบียน และนายมนตรี กาไสย นักวิชาการคอมพิวเตอร์ ประจำงานพัฒนาระบบเครือข่ายและการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ  	
							ลดลง	KPI9 - ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์	ร้อยละ 80	- ผอ.สำนักวิทยบริการฯ	☑ บรรลุ ☐ ไม่บรรลุ <u>ผลดำเนินงาน</u> จัดกิจกรรมอบรมการป้องกันภัยอาชญากรรมทางเทคโนโลยี สำหรับนักศึกษา ชั้นปีที่ 1 เมื่อวันที่ 28 พฤษภาคม 2568 ณ ห้องประชุมราชพฤกษ์ชั้น 3 หอประชุมทีปังกรรัศมีโชติ  	จัดกิจกรรมอบรมสำหรับนักศึกษาต่อเนื่องในปีถัดไปเพื่อให้รู้เท่าทันภัยอาชญากรรมทางเทคโนโลยี