Bow-Tie Diagram

แบบวิเคราะห์ความเสี่ยง Bow-Tie Diagram

1 ความเสี่ยง

(ไม่ใช่ปัญหาปัจจุบัน)

การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่สามารถให้บริการได้

2 ปัจจัยเสี่ยง - สาเหตุเสี่ยง

ปัจจัยเสี่ยง - สาเหตุเสี่ยง
1. . โปรแกรมหรือข้อมูลถูกทำลาย
2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ
3. การถูกขโมยข้อมูล

3 ผลกระทบของความเสี่ยง

ผลกระทบความเสี่ยง
1. ข้อมูลสูญหาย
2. สูญเสียรายได้

4 วิธีการควบคุม/ลดผลกระทบในปัจจุบัน

สิ่งที่ดำเนินการในปัจจุบัน	ผู้รับผิดชอบ
จัดทำแผนรองรับถานการณ์ฉุกเฉิน ปี 2566	สำนักวิทยบริการฯ
ระบบพิสูจน์ตัวตน ตาม พรบ. คอมพิวเตอร์ 2560	
สำรองข้อมูลเป็นประจำ: เพื่อลดผลกระทบหากเกิดการสูญหายหรือถูกขโมย	

ประเมินความเสี่ยง	
โอกาส × ผลกระทบ	ระดับความเสี่ยง
4×5=20	สูงมาก

5 แผนการจัดการความเสี่ยง

(สิ่งที่จะดำเนินการ +ระยะเวลา+ ผู้รับผิดชอบ)

สิ่งที่จะดำเนินการ	ระยะเวลา	ผู้รับผิดชอบ
1. จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ โดยทำการ Monitor จราจรของระบบเครือข่ายอย่างสม่ำเสมอเพื่อให้สามารถ Blocked การโจมตีได้ทัน	ม.ค. - ก.ย. 68	สำนักวิทยบริการฯ
2. บริหารจัดการสัญญา Maintenance ให้เหมาะสมเพื่อให้ได้ข้อมูลเกี่ยวกับ site ที่ทำการโจมตี Dos ที่ใหม่อยู่เสมอ	ต.ค. 67 - ก.ย. 68	สำนักวิทยบริการฯ
3. ติดตาม Update ฐานข้อมูล Black list ของ Domain ที่เข้าข่ายเป็น Spammer อย่างสม่ำเสมอ	ต.ค. 67 - ก.ย. 68	สำนักวิทยบริการฯ
4. สำรองข้อมูลระบบและสำรองฐานข้อมูลอย่างสม่ำเสมอ (แผนรองรับถานการณ์ฉุกเฉิน ปรับปรุงปี 2566)	ต.ค. 67 - ก.ย. 68	สำนักวิทยบริการฯ

6 ดัชนีชี้วัดความเสี่ยง (KRI) + ค่าเป้าหมาย

(แจ้งเตือนภัยก่อนเกิดเหตุการณ์ความเสี่ยง)

KRI	ค่าเป้าหมาย
ร้อยละผู้ใช้งานรายงานว่าไฟล์สำคัญไม่สามารถเปิดใช้งานได้	ร้อยละ 5
การแจ้งเตือนจาก Firewall, IDS/IPS หรือ Endpoint Security เกี่ยวกับพฤติกรรมที่ผิดปกติ	จำนวน 1 ครั้ง

7 เป้าหมายความเสี่ยงที่ยอมรับได้ (Risk Appetite)

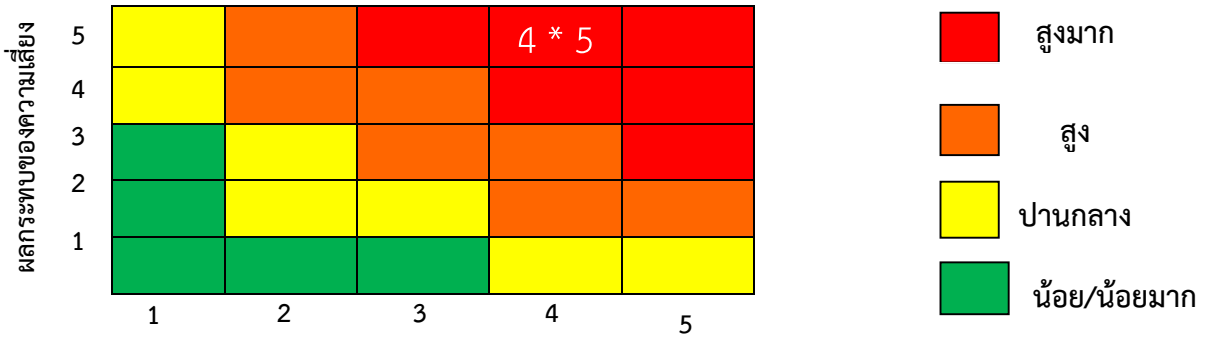
ไม่ควรถูกโจมตีที่สำเร็จ (Successful Attack) เกิน 1 ครั้งต่อปี สำหรับระบบสำคัญ

แบบ SNRU-ERM 1

แบบกำหนดเกณฑ์มาตรฐานการประเมินความเสี่ยง

ความเสี่ยง (1)	ระดับ	เกณฑ์โอกาส (2)		เกณฑ์ผลกระทบ (3)		
		โอกาสที่จะเกิด	คำอธิบาย	ระดับ	ผลกระทบ	คำอธิบาย
การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่สามารถให้บริการได้	5	สูงมาก	ค่อนข้างแน่นอนคาดหมายว่าจะเกิดขึ้นในสถานการณ์ส่วนใหญ่	**5**	**รุนแรงที่สุด**	**ระบบสารสนเทศ ทั้งหมดหยุดชะงัก ส่งผลกระทบมหาวิทยาลัย และมีผลกระทบต่อชื่อเสียงมหาวิทยาลัยอย่างรุนแรง**
	4	**สูง**	**เป็นไปได้มาก คาดหมายว่าจะเกิดขึ้นค่อนข้างบ่อย**	4	ค่อนข้างรุนแรง	ระบบสารสนเทศหยุดทำงานบางส่วน แต่ยังมีวิธีการให้บริการทางเลือก เกิดความล่าช้าในการให้บริการ
	3	ปานกลาง	เป็นไปได้ เกิดขึ้นบางครั้ง	3	ปานกลาง	ระบบที่ไม่สำคัญถูกโจมตี และไม่ส่งผลกระทบโดยตรงต่อการดำเนินงานหลัก
	2	น้อย	อาจจะเกิดขึ้นน้อยมาก	2	น้อย	มีความไม่สะดวกต่อผู้ใช้งานภายใน หรือการดำเนินงานในบางส่วนราชการ
	1	น้อยมาก	อาจเกิดขึ้นเฉพาะในสถานการณ์ที่ไม่ปกติบางกรณี	1	น้อยมาก	เกิดการหยุดชะงักในระบบที่ไม่มีความสำคัญ และสามารถแก้ไขได้อย่างรวดเร็ว

เกณฑ์มาตรฐานระดับความเสี่ยง (Degree of Risk/Risk Matrix)



แบบ SNRU-ERM 2

แผนบริหารความเสี่ยงมหาวิทยาลัยราชภัฏสกลนคร ประจำปีงบประมาณ พ.ศ. 2568

สอดคล้องกับภารกิจมหาวิทยาลัย ☐ 1. ด้านการเรียนการสอน ☐ 2. ด้านวิจัย ☑ 3. ด้านบริการวิชาการ ☐ 4. ด้านทะนุบำรุงศิลปวัฒนธรรม ☐ 5. ด้านบริหารจัดการ

ด้านของความเสี่ยง : ☐ กลยุทธ์ (S) ☐ การปฏิบัติงาน (O) ☑ การเงิน (F) ☐ กฎหมายและข้อกำหนดผูกพันองค์กร (C) ☐ อื่น ๆ .....

ความเสี่ยง (1)	ปัจจัยความเสี่ยง/สาเหตุความเสี่ยง (2)	แหล่งที่มา (3)		กลยุทธ์/แนวทางการจัดการความเสี่ยง (4)	โครงการ/กิจกรรม (5)	งบประมาณ (บาท) (6)	ระยะเวลา ผู้กำกับดูแล/ผู้รับผิดชอบ (7)
		ภายใน	ภายนอก				
1. การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่สามารถให้บริการได้	1. โปรแกรมหรือข้อมูลถูกทำลาย		✓	จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ โดยทำการ Monitor จราจรของระบบเครือข่ายอย่างสม่ำเสมอเพื่อให้สามารถ Blocked การโจมตีได้ทัน	โครงการจัดหาอุปกรณ์รักษาความปลอดภัย Firewall (Next Generation Firewall)	2,000,000 (รออนุมัติ)	**ระยะเวลา :** 1 ต.ค. 67 – 30 ก.ย. 68 **ผู้กำกับดูแล :** ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยี **ผู้รับผิดชอบ:** 1. หัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน 2. หัวหน้างานพัฒนาระบบสารสนเทศ
	2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ	✓	✓	ติดตาม Update ฐานข้อมูล Black list ของ Domain ที่เข้าข่ายเป็น Spammer อย่างสม่ำเสมอ	โครงการบริหารความมั่นคงของข้อมูลและการจัดการความเสี่ยง	100,000	
	3. การถูกขโมยข้อมูล		✓	1. สำรองข้อมูลระบบและสำรองฐานข้อมูลอย่างสม่ำเสมอ (แผนรองรับถานการณ์ฉุกเฉิน ปรับปรุงปี 2566) 2. บริหารจัดการสัญญา Maintenance ให้เหมาะสมเพื่อให้ได้ข้อมูลเกี่ยวกับ site ที่ทำการโจมตี Dos ที่ใหม่อยู่เสมอ	โครงการเช่าวงจรอินเทอร์เน็ตเพื่อทำระบบวงจรสื่อสารสำรอง (Backup Link)	240,000	