แผนการบริหารความเสี่ยงมหาวิทยาลัยเทคโนโลยีสุรนารี ประจำปีงบประมาณ พ.ศ. 2564

ส่วนที่ 1

ความเสี่ยง	สาเหตุความเสี่ยง	การประเมินค่าความเสี่ยงก่อนมีกิจกรรมควบคุม			ระดับความเสี่ยงที่ยอมรับได้			วิธีการจัดการความเสี่ยง	สัญญาณเตือนภัย
		L	I	R1	L	I	R2		
ด้านสารสนเทศ : ความไม่ปลอดภัยของข้อมูลส่วนบุคคล	มหาวิทยาลัยยังไม่มีนโยบายที่ชัดเจนเพื่อรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล PDPA (Personal Data Protection Act)	4	4	**16 (E)**	2	2	**4 (M)**	1. CEO มอบหมายนโยบาย แนวปฏิบัติ โดยสร้างกฎ Policy เพื่อควบคุมข้อมูลไม่ให้รั่วไหล 2. ประชุมหารือหน่วยงานที่เกี่ยวข้องกับการเก็บข้อมูลส่วนบุคคล เพื่อรับทราบนโยบายและแนวปฏิบัติเดียวกัน 3. หน่วยงานต้องออบแบบกระบวนการดำเนินงานเกี่ยวกับการรักษาข้อมูลส่วนบุคคล 3.1 การเก็บข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากผู้รับบริการ 3.2 ต้องมีกระบวนการเก็บรักษาข้อมูลไม่ให้รั่วไหล-สูญหาย 3.3 มีช่องทางให้ผู้รับบริการสามารถตรวจสอบได้	ข้อมูลส่วนบุคคลที่เป็นข้อมูล sensitive ถูกเผยแพร่ทาง Internet

ส่วนที่ 2

ประเภทความเสี่ยง	ตัวชี้วัด	เป้าหมายตัวชี้วัด				หน่วยนับ
		ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4	
ความเสี่ยงด้านปฏิบัติงาน (Operational Risk)	**ตัวชี้วัดกิจกรรมควบคุม:** - ระดับความสำเร็จของการสร้างกระบวนการป้องกันข้อมูลส่วนบุคคลรั่วไหล **รายละเอียดขั้นตอนกิจกรรมควบคุม โปรดระบุใน Milestone**	1	2	3	5	คะแนน
	ตัวชี้วัดความเสี่ยง (KRI): 1. จำนวนข้อร้องเรียนเกี่ยวกับการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต 2. ความสำเร็จการป้องกัน/แก้ไข การ hack ระบบสารสนเทศของมหาวิทยาลัย ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลสำเร็จ 3. ความสำเร็จการกู้คืนข้อมูล ระบบสารสนเทศของมหาวิทยาลัย ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายในเวลา 6 ชั่วโมง	0 100 100	0 100 100	0 100 100	0 100 100	ครั้ง ร้อยละ ร้อยละ

ระดับขั้นของความสำเร็จ Milestone

ส่วนที่ 3

ตัวชี้วัดกิจกรรมควบคุม : ระดับความสำเร็จของการสร้างกระบวนการป้องกันข้อมูลส่วนบุคคลรั่วไหล

น้ำหนัก : ร้อยละ

คำอธิบาย :

กำหนดเป็นระดับขั้นของความสำเร็จ (Milestone) แบ่งเกณฑ์การให้คะแนนเป็น 5 ระดับ พิจารณาจากความก้าวหน้าของขั้นตอนการดำเนินงานตามเป้าหมายแต่ละระดับ ดังนี้ โดยที่ :

ข้อที่ 1

ขั้นตอนที่	รายละเอียดผลงานของแต่ละขั้นตอน	คะแนน
1	มหาวิทยาลัย -หน่วยงานที่เกี่ยวข้อง มีนโยบายที่ชัดเจนเพื่อรองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล PDPA (Personal Data Protection Act)	1
2	มหาวิทยาลัย-หน่วยงานที่เกี่ยวข้อง มีกระบวนการดำเนินงานเกี่ยวกับการรักษาข้อมูลส่วนบุคคล	2
3	มหาวิทยาลัย-หน่วยงานที่เกี่ยวข้อง มีกระบวนการเก็บรักษาข้อมูลไม่ให้รั่วไหล-สูญหาย	3
4	มหาวิทยาลัย-หน่วยงานที่เกี่ยวข้อง มีช่องทางให้ผู้รับบริการสามารถตรวจสอบได้	4
5	สรุปผลการดำเนินงานต่อผู้บริหาร	5

ขั้นที่ 2

ระดับความสำเร็จของ Milestone	ระดับคะแนน				
	1 คะแนน	2 คะแนน	3 คะแนน	4 คะแนน	5 คะแนน
ขั้นตอนที่ 1	✓	✓	✓	✓	✓
ขั้นตอนที่ 2		✓	✓	✓	✓
ขั้นตอนที่ 3			✓	✓	✓
ขั้นตอนที่ 4				✓	✓
ขั้นตอนที่ 5					✓

ขั้นที่ 3

ตัวบ่งชี้	หน่วยนับ	เกณฑ์การให้คะแนน				
		1	2	3	4	5
จำนวนขั้นตอนการดำเนินการที่แล้วเสร็จ	ขั้นตอน	ขั้นตอน 1	ขั้นตอน 2	ขั้นตอน 3	ขั้นตอน 4	ขั้นตอน 5

ผลการประเมิน : ..... คะแนน