แบบฟอร์มการประเมินตนเอง เพื่อการป้องกันและปราบปรามการทุจริตมหาวิทยาลัยเทคโนโลยีสุรนารี

ประเภทความเสี่ยงด้านอาชญากรรมทางไซเบอร์ (Cyber Crime)

แบบ C-1

หน่วยงาน :ศูนย์คอมพิวเตอร์

งานหลัก	งานย่อย	เหตุการณ์หลัก	เหตุการณ์สุ่มเสี่ยง	☑ เลือกตัวเลือกที่ตรงกับหน่วยงานของท่าน
งานหลัก : 1. งานบริการระบบ internet data Center	**งานย่อย :** 1. งานดูแลระบบสารสนเทศ 2. งานดูแลระบบบัญชีผู้ใช้งานส่วนกลาง มหาวิทยาลัย	1. การยักยอก (Asset Misappropriation Fraud)	1.1 ปลอมแปลงเอกสารเบิกเงิน	
			1.2 เบิกค่าใช้จ่ายสูงเกินจริง	
			1.3 เซ็นต์รับงานที่ยังไม่เสร็จ	
			1.4 จ่ายเงินเดือน / ค่าแรงให้พนักงานที่ไม่มีตัวตน	
			1.5 นำเอกสารมาเบิกเงินซ้ำ	
			1.6 ปลอมแปลงลายเซ็นผู้อนุมัติจ่ายเงิน	
			1.7 ขายเป็นเงินสดแต่บันทึกเป็นลูกหนี้ นำเงินสดเข้ากระเป๋า	
			1.8 นำเงินสดย่อยไปหมุนใช้ส่วนตัว	
			1.9 อื่นๆ โปรดระบุ.....	
		2. ทุจริตด้านจัดซื้อ (Procurement Fraud)	2.1 มีความสัมพันธ์ส่วนตัวกับผู้ขาย	
			2.2 ผู้ขายที่เสนอราคาไม่มีตัวตนจริง	
			2.3 ราคาขาย/ค่าบริการของผู้ขายสูงเกินจริงและสูงกว่าราคาตลาด	
			2.4 อื่นๆ โปรดระบุ.....	
		3. การติดสินบน และการคอร์รัปชั่น (Bribery & Corruption)	3.1 การติดสินบน	
			3.2 การให้หรือรับเงินใต้โต๊ะ	
			3.3 การคอร์รัปชั่น	
			3.4 การกรรโชกทรัพย์	
			3.5 การหลอกลวง	

งานหลัก	งานย่อย	เหตุการณ์หลัก	เหตุการณ์สุ่มเสี่ยง	☑ เลือกตัวเลือกที่ตรงกับหน่วยงานของท่าน
			3.6 การสมรู้ร่วมคิด	
			3.7 การฟอกเงิน	
			3.8 อื่นๆ โปรดระบุ.....	
		4. อาชญากรรมทางไซเบอร์ (Cyber Crime)	4.1 การแฮกเข้าสู่ระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลส่วนบุคคล	✓
			4.2 การนำ User / Password ของผู้อื่นไปใช้เพื่อประโยชน์ส่วนตัว	
			4.3 อื่นๆ โปรดระบุ.....	
		5. Fraudulent Financial Reporting (การตบแต่งรายงานทางการเงิน)	5.1 รับรู้รายได้ไม่ถูกต้อง	
			5.2 รับรู้รายการบัญชีไม่ถูกหมวดบัญชี	
			5.3 ไม่รับรู้หนี้สินที่เกิดขึ้น	
			5.4 ไม่รับรู้ค่าใช้จ่ายที่เกิดขึ้น	
			5.5 บันทึกบัญชีผิดงวด	
			5.6 ประเมินทรัพย์สินไม่เหมาะสม (อายุการใช้งาน มูลค่าซาก)	
			5.7 อื่นๆ โปรดระบุ.....	

✸ **ข้อแนะนำในการจัดทำ แบบ C-1 :**

1) งานหลักและงานย่อย คืองานตามภารกิจหรือพันธกิจของหน่วยงานและต้องระบุรายละเอียดลงไปกับลงมือปฏิบัติการ
2) เหตุการณ์หลัก คือ การเลือกเหตุการณ์จากแนวคิด 5 ประเภทการทุจริตและความเสี่ยงที่จะเกิดการทุจริต
3) เลือกเหตุการณ์สุ่มเสี่ยงที่สอดคล้องกับพันธกิจและกระบวนการปฏิบัติงานของหน่วยงานของท่าน แล้วนำเหตุการณ์สุ่มเสี่ยงที่เลือกไปจัดทำกิจกรรมควบคุมตามแบบฟอร์ม C-2 ต่อไป

แบบกำหนดรายละเอียดการประเมินตนเองเพื่อการป้องกันและปราบปรามการทุจริต ปีงบประมาณ พ.ศ. 2566

แบบ C-2

งานหลัก	งานย่อย	ประเภทความเสี่ยง/เหตุการณ์สุ่มเสี่ยง (ตามแบบ C-1)	ระบุลักษณะงานที่มีโอกาสเกิดการทุจริต	ประเมินค่าความเสี่ยงก่อนมีกิจกรรมควบคุม				รหัสกิจกรรมควบคุม	กิจกรรมควบคุม	ระดับความเสี่ยงที่ยอมรับได้			
				L	I	T1	ระบุเกณฑ์ผลกระทบ			L	I	T1	ระบุเกณฑ์ผลกระทบ
งานหลัก : **1.**งานบริการระบบ internet data Center	**งานย่อย :** 1. งานดูแลระบบสารสนเทศ 2. งานดูแลระบบบัญชีผู้ใช้งานส่วนกลางมหาวิทยาลัย คอมพิวเตอร์และอุปกรณ์ต่อพ่วง	**ประเภท :** ทุจริตอาชญากรรมทางไซเบอร์ (Cyber Crime) เหตุการณ์สุ่มเสี่ยง : 1. การแฮกเข้าสู่ระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลส่วนบุคคล	1.อาจมีการ hack ระบบสารสนเทศเพื่อเข้าถึง หรือเปลี่ยนแปลงแก้ไขข้อมูล - ข้อมูลส่วนบุคคล	3	2	6 (M)	ด้านภาพลักษณ์และชื่อเสียงของหน่วยงาน/ด้านความน่าเชื่อมั่นต่อระบบของมหาวิทยาลัย	C	1. กำหนดให้มีกระบวนการตรวจสอบการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลบนระบบสารสนเทศ 2. กำหนดให้มีการปรับปรุงระบบสารสนเทศ ที่มีข้อมูลส่วนบุคคล ที่อยู่ในความดูแลของศูนย์คอมพิวเตอร์ ให้มีความปลอดภัยตาม penetration testing	2	2	4 (L)	ด้านภาพลักษณ์และชื่อเสียงของหน่วยงาน/ด้านความน่าเชื่อมั่นต่อระบบของมหาวิทยาลัย

แบบฟอร์มรายละเอียดการกำหนดกิจกรรมรายเดือนเพื่อการป้องกันและปราบปรามการทุจริต

แบบ C-3

กิจกรรมควบคุม	การดำเนินตามกิจกรรมควบคุม				รายละเอียดการดำเนินงาน (โปรดระบุ)
	ไตรมาส 1	**ไตรมาส 2**	**ไตรมาส 3**	**ไตรมาส 4**	
1. กำหนดให้มีกระบวนการตรวจสอบ การเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลบนระบบสารสนเทศ	25	50	75	100	ปรับปรุงระบบสารสนเทศให้รองรับกระบวนการตรวจสอบ การเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคล บนระบบสารสนเทศ
2. กำหนดให้มีการปรับปรุงระบบสารสนเทศ ที่มีข้อมูลส่วนบุคคล ที่อยู่ในความดูแลของศูนย์คอมพิวเตอร์ ให้มีความปลอดภัยตาม penetration testing	25	50	75	100	ปรับปรุงระบบสารสนเทศ โดยอุดช่องโหว่ของระบบตามที่ได้มีการจัดทำ penetration testing