

รายงานผลการดำเนินงานตามแผนการบริหารความเสี่ยง “ระดับหน่วยงาน”

1. ความเสี่ยงระดับหน่วยงาน: อุปกรณ์ดาต้าเซ็นเตอร์เสียหายจากไฟฟ้าตก/กระชาก	
สาเหตุความเสี่ยง :	เนื่องจากปัจจุบันเกิดปัญหาสินค้า IT ขาดแคลน (Shortage) ทำให้หากเกิดเหตุการณ์ไฟฟ้าดับจนอุปกรณ์เสียหายอาจทำให้การหาอุปกรณ์ทดแทนในระยะยาวเกิดความล่าช้า
วิธีการจัดการความเสี่ยง :	<ol style="list-style-type: none"> <li>1. จัดทำแผนสำรองสำหรับอุปกรณ์ทดแทนในแต่ละพีเจอร์ เช่น หากเกิดเหตุการณ์อุปกรณ์ Router เสียหาย ให้สลับไปใช้พีเจอร์ของไฟลว์อัลแทน</li> <li>2. จัดทำการ Backup Config อุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้การเปลี่ยนอุปกรณ์นั้นทำได้ราบรื่นไร้ปัญหา</li> </ol>
ตัวชี้วัดกิจกรรมควบคุม:	<ol style="list-style-type: none"> <li>1. จำนวนอุปกรณ์กรณีเครือข่ายหลักที่มีการจัดทำ Backup Config</li> <li>2. มีแผนการสำรองสำหรับอุปกรณ์เครือข่ายที่สำคัญเพื่อแก้ไขปัญหาฉุกเฉิน</li> </ol>
<b>รายงานตามตัวชี้วัด</b> <ol style="list-style-type: none"> <li>1. จำนวนอุปกรณ์เครือข่ายหลักที่มีการจัดทำ Backup Config</li> <li>2. Downtime ระบบเครือข่ายไม่เกิน 8 ชม./วัน</li> </ol>	<b>ผลการดำเนินงาน ณ สิ้นไตรมาส 2/2566</b> <ol style="list-style-type: none"> <li>1. จำนวนอุปกรณ์เครือข่ายหลักที่มีการจัดทำ Backup Config ดังนี้ <ul style="list-style-type: none"> <li>-อุปกรณ์ Backbone Switch Cisco-6807</li> <li>-อุปกรณ์ Firewall Fortigate-600E</li> <li>-อุปกรณ์ Firewall Fortigate-3200D</li> <li>-อุปกรณ์ Router Gateway ASA</li> <li>-อุปกรณ์ Switch ประจำอาคาร Cisco 9300</li> <li>-อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย รุ่น 1700 1800 2700 2800</li> </ul> </li> <li>2. ระยะเวลา Downtime ไตรมาส2 <ul style="list-style-type: none"> <li>-ไม่มี Downtime</li> </ul> </li> </ol>

2. ความเสี่ยงระดับหน่วยงาน : อุปกรณ์เครือข่ายประจำอาคารปฏิบัติการด้านดิจิทัลไม่มีไฟฟ้าสำรองในกรณีไฟดับไฟกระชาก	
สาเหตุความเสี่ยง :	เนื่องจากปัจจุบันอาคารปฏิบัติการด้านดิจิทัลไม่มีระบบไฟฟ้าสำรอง สำหรับป้องกันในกรณีไฟดับ ไฟกระชาก ทำให้ส่งผลกระทบต่อการเรียนการสอน และอุปกรณ์เครือข่ายประจำอาคาร อาจก่อให้เกิดความเสียหายได้
วิธีการจัดการความเสี่ยง :	1. จัดหาระบบไฟฟ้าสำรองให้กับระบบเครือข่ายภายในอาคารปฏิบัติการด้านดิจิทัล เพื่อป้องกันความเสียหายของอุปกรณ์เครือข่าย
ตัวชี้วัดกิจกรรมควบคุม:	1. มีระบบไฟฟ้าสำรองครอบคลุมอุปกรณ์เครือข่ายประจำอาคารปฏิบัติการด้านเทคโนโลยีดิจิทัล
<b>รายงานตามตัวชี้วัด</b> 1. มีระบบไฟฟ้าสำรองครอบคลุมอุปกรณ์เครือข่ายประจำอาคารปฏิบัติการด้านเทคโนโลยีดิจิทัล	<b>ผลการดำเนินงาน ณ สิ้นไตรมาส 2/2566</b> 1. จัดทำรายการค่าของงบประมาณกลางปี (2566) เพื่อจัดซื้อระบบสำรองไฟฟ้า สำหรับอุปกรณ์เครือข่าย ประจำอาคารปฏิบัติการด้านเทคโนโลยีดิจิทัล 2. จัดทำ BOQ งานจ้างเดินสายระบบไฟฟ้ารับรองการติดตั้งระบบสำรองไฟฟ้า สำหรับอุปกรณ์เครือข่าย ประจำอาคารปฏิบัติการด้านเทคโนโลยีดิจิทัล

3. ความเสี่ยงระดับหน่วยงาน : คอมพิวเตอร์ในห้องปฏิบัติการคอมพิวเตอร์ อาจทำงานผิดปกติจากการติดตั้งโปรแกรมเพิ่มเติม	
สาเหตุความเสี่ยง :	ในระหว่างการเรียนการสอนอาจมีการขอติดตั้งโปรแกรมต่าง ๆ เพิ่มเติม ซึ่งจำเป็นต้องใช้บัญชีและรหัสผ่านที่มีสิทธิ์เป็น Administrator ทำให้มีโอกาสถูกติดตั้งโปรแกรมที่ไม่พึงประสงค์ มีผลให้คอมพิวเตอร์ทำงานผิดปกติ หรือประสิทธิภาพการทำงานลดลง
วิธีการจัดการความเสี่ยง :	<ol style="list-style-type: none"> <li>1. จำกัดเวลาของการใช้งานบัญชีผู้ที่มีสิทธิ์การติดตั้งโปรแกรมตามความจำเป็นในการใช้งาน</li> <li>2. เปลี่ยนรหัสผ่านบัญชีผู้ใช้ที่มีสิทธิ์การติดตั้งโปรแกรมเป็นระยะ</li> </ol>
ตัวชี้วัดกิจกรรมควบคุม:	<ol style="list-style-type: none"> <li>1. จำกัดเวลาของการใช้งานบัญชีผู้ที่มีสิทธิ์การติดตั้งโปรแกรมตามความจำเป็นในการใช้งาน</li> <li>2. เปลี่ยนรหัสผ่านบัญชีผู้ใช้ที่มีสิทธิ์การติดตั้งโปรแกรมเป็นระยะ</li> </ol>
รายงานตามตัวชี้วัด <ol style="list-style-type: none"> <li>1. จำกัดเวลาของการใช้งานบัญชีผู้ที่มีสิทธิ์การติดตั้งโปรแกรมตามความจำเป็นในการใช้งาน</li> <li>2. เปลี่ยนรหัสผ่านบัญชีผู้ใช้ที่มีสิทธิ์การติดตั้งโปรแกรมเป็นระยะ</li> </ol>	<b>ผลการดำเนินงาน ณ สิ้นไตรมาส 2/2566</b> <ol style="list-style-type: none"> <li>1. ควบคุมเวลาในการใช้งาน User ที่มีสิทธิ์ Administrator ทำให้ยังไม่พบความผิดปกติของเครื่องคอมพิวเตอร์</li> </ol>

รายงานผลการดำเนินงานตามแผนปฏิบัติการด้านการป้องกันและปราบปรามการทุจริต  
“ระดับหน่วยงาน”

1. แผนการป้องกันและปราบปรามการทุจริตมหาวิทยาลัยเทคโนโลยีสุรนารี ประเภทความเสี่ยงด้านการจัดซื้อ (Procurement Fraud)	
งานหลัก :	งานจัดซื้อจัดจ้าง
ประเภทความเสี่ยง:	ทุจริตด้านจัดซื้อ (Procurement Fraud)
กิจกรรมควบคุม :	<ol style="list-style-type: none"> <li>1. การกำหนดเกณฑ์ในการแต่งตั้งกรรมการจัดทำร่างขอบเขตของงาน (TOR) วงเงินเกิน 500,000 บาท <ol style="list-style-type: none"> <li>1.1 การกำหนดเกณฑ์การจัดทำร่างขอบเขตของงาน (TOR) ของหน่วยงาน ให้แต่งตั้งคณะกรรมการจัดทำ TOR ภายในหน่วยงาน หากวงเงินไม่เกิน 500,000 บาท</li> <li>1.2 การจัดทำร่างขอบเขตของงาน (TOR) ให้ยึดหลักตามข้อกำหนดของกระทรวงดิจิทัล</li> </ol> </li> <li>2. การขอใบเสนอราคา <ol style="list-style-type: none"> <li>2.1 รวบรวมรายชื่อบริษัทที่ขึ้นทะเบียนกับกระทรวงพาณิชย์และประชาสัมพันธ์ ให้ลงชื่อเข้าในรายชื่อผู้ค้ากับศูนย์คอมพิวเตอร์</li> <li>2.2 แจ้งให้บริษัทที่อยู่ในรายชื่อผู้ค้าทราบ ให้บริษัทที่สนใจส่งใบเสนอราคาเข้า email: <a href="mailto:procurement@sut.ac.th">procurement@sut.ac.th</a></li> <li>2.3 คัดเลือกบริษัทที่เสนอราคาต่ำสุดจำนวน 3 ราย เพื่อส่งให้พัสดุดำเนินการต่อไป</li> </ol> </li> </ol>
รายงานตามตัวชี้วัดกิจกรรมควบคุม	<p><b>ผลการดำเนินงาน ณ สิ้นไตรมาส 2</b></p> <ol style="list-style-type: none"> <li>1. จัดซื้อจัดจ้างวงเงินงบประมาณเกิน 500,000 บาท <ul style="list-style-type: none"> <li>- ไม่มีการจัดซื้อจัดจ้าง</li> </ul> </li> <li>2. จัดซื้อจัดจ้างวงเงินงบประมาณไม่เกิน 500,000 บาท <ul style="list-style-type: none"> <li>● จัดจ้าง จ้างเดินสายสัญญาณระบบเครือข่ายคอมพิวเตอร์ บริเวณหอพักนักศึกษา 1 ระบบ วงเงินไม่เกิน 500,000 บาท</li> <li>● จัดจ้างเช่าใช้บริการอินเทอร์เน็ตบ้านพักบุคลากร 1 ระบบ วงเงินไม่เกิน 180,000 บาท</li> <li>● จัดซื้อระบบรักษาความปลอดภัยห้องจัดเก็บครุภัณฑ์ รับประกันสินค้า 3 ปี 1 ระบบ ราคา 37,500 บาท</li> <li>● ขอให้จัดซื้อ ตลับลูกปืนเครื่องพิมพ์ จำนวน 1 ตัว @750 บาท</li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>● จัดจ้างซ่อมสายเคเบิลใยแก้วนำแสง (Fiber Optic) อาคารเทวรัตนวิทยารักษ์ ศูนย์เครื่องมือวิทยาศาสตร์และเทคโนโลยี (F12) วงเงินไม่เกิน 18,404 บาท</li> <li>● จัดจ้างปรับปรุงสายเคเบิลโทรศัพท์ต่อนนอก กลุ่มหอพักนักศึกษา S7-13 และสำนักงานประชา ส่วนอาคารสถานที่ (ประตู 4) 1 ระบบ วงเงินไม่เกิน 70,000 บาท</li> <li>● จัดซื้อหน่วยจัดเก็บข้อมูล (Hard Disk) จำนวน 2 ตัว@ 2,250 บาท รวม 4,500 บาท</li> </ul>
--	--

<b>2. แผนป้องกันและปราบปรามการทุจริตมหาวิทยาลัยเทคโนโลยีสุรนารี ประเภทความเสี่ยงด้านอาชญากรรมทางไซเบอร์ (Cyber Crime)</b>	
งานหลัก:	งานบริการระบบ Internet Data Center
ประเภทความเสี่ยง:	อาชญากรรมทาง ไซเบอร์ (Cyber Crime)
กิจกรรมควบคุม :	<ol style="list-style-type: none"> <li>1. กำหนดให้มีกระบวนการตรวจสอบ การเปลี่ยนแปลง แก้ไขข้อมูล ส่วนบุคคลบนระบบสารสนเทศ</li> <li>2.กำหนดให้มีการปรับปรุงระบบสารสนเทศ ที่มีข้อมูลส่วนบุคคล ที่ อยู่ในความดูแลของศูนย์คอมพิวเตอร์ ให้มีความปลอดภัยตาม Penetration Testing</li> </ol>
รายงานตามตัวชี้วัดกิจกรรมควบคุม	<p><b>ผลการดำเนินการ ณ สิ้นไตรมาส 2</b></p> <ol style="list-style-type: none"> <li>1. ดำเนินการปรับปรุงการจัดเก็บข้อมูล Query log MySQL Server เพื่อให้สามารถตรวจสอบ การเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคล ที่อยู่ใน Webhosting ของมหาวิทยาลัย</li> <li>2.จัดสรร Certificate SSL สำหรับการใช้งานเว็บไซต์ภายในมหาวิทยาลัย</li> <li>3.ทำการปรับปรุงแก้ไขระบบสารสนเทศของศูนย์คอมพิวเตอร์ ตาม Penetration Testing <ul style="list-style-type: none"> <li>● ปรับปรุงระบบ sutmail.sut.ac.th (patch ระบบปฏิบัติการ)</li> <li>● ปรับปรุงระบบขอ account online (เข้ารหัส field ที่สำคัญในฐานข้อมูล)</li> <li>● ตรวจสอบข้อมูลส่วนบุคคลในระบบฐานข้อมูล ที่ควรได้รับการเข้ารหัสข้อมูล</li> </ul> </li> </ol>