

การประเมินโอกาสและผลกระทบความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง	โอกาสที่จะเกิดความเสียหาย	ผลกระทบความเสียหาย	ระดับความเสี่ยง	ความหมาย	การตอบสนองความเสี่ยง
1. ความเสี่ยงด้านกลยุทธ์					
1 Google ปรับเปลี่ยนนโยบายการให้บริการพื้นที่จัดเก็บข้อมูลบน Google Workspace for Education	4	5	20	สูงมาก	Reduce
2.การเปลี่ยนแปลงนโยบายทางการบริหาร	2	3	6	ต่ำ	Accept
2. ความเสี่ยงด้านการเงิน					
1. ราคาการดูแลระบบมีการปรับราคาสูงเกินงบประมาณที่กำหนดไว้ในโครงการหรืองบประมาณ	4	4	16	สูง	Reduce
2 การเบิกจ่ายงบประมาณไม่ตรงตามแผนที่กำหนด	3	3	9	ปานกลาง	Reduce
3. ความเสี่ยงระเบียบข้อบังคับหรือกฎหมายที่เกี่ยวข้อง					
1. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	3	4	12	สูง	Reduce
2. การร้องเรียนเรื่องการจัดซื้อจัดจ้าง	3	3	9	ปานกลาง	Reduce
4. ความเสี่ยงด้านการปฏิบัติงาน					
1. การแฮกซ์ระบบ และการโจมตีของไวรัส	4	3	12	สูง	Reduce
2. ความเสี่ยงจากการใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	3	4	12	สูง	Reduce

แผนบริหารความเสี่ยง สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีการบริหารความเสี่ยง	การบริหารความเสี่ยง	ผู้รับผิดชอบ
1. Google ปรับเปลี่ยนนโยบายการให้บริการพื้นที่จัดเก็บข้อมูลบน Google Workspace for Education	การหยุดให้บริการ Google workspace เช่น Gmail, Google Drive, Google Photo	สูง	Reduce	<p>1. ทอยย้ายข้อมูลที่จัดเก็บไว้บน Google Drive และบริการอื่น ๆ ของ Google ไปเก็บยัง Local Storage ของแต่ละท่าน หรือ One Drive ของ Microsoft เพื่อให้คงเหลือข้อมูลบนบริการ Google ไม่เกินกำหนดใหม่</p> <p>2. ในกรณีพบว่ามีบัญชีใดมีขนาดพื้นที่เกินกำหนด ทางมหาวิทยาลัยฯ จะดำเนินการระงับบัญชีบัญชีดังกล่าวไว้ก่อน ผู้ที่ถูกระงับการใช้ และให้ทำการติดต่อศูนย์คอมพิวเตอร์และอินเทอร์เน็ตเพื่อดำเนินการ</p> <p>3. ในกรณีไม่ดำเนินใดๆ ทางศูนย์คอมพิวเตอร์และอินเทอร์เน็ตจะขอลบบัญชีที่มีพื้นที่เกินดังกล่าว เพื่อให้การใช้งานส่วนรวมยังดำเนินการต่อไปได้</p>	รองผู้อำนวยการฯ ศูนย์คอมพิวเตอร์ฯ
2. ราคาการดูแลระบบมีการปรับราคาสูงเกิน	ราคาการดูแล และซ่อมบำรุงมีราคาสูงขึ้น ทำให้งบประมาณที่	สูง	Reduce	<p>1. ศึกษาระบบการทำงาน</p> <p>2. ให้บุคลากรประจำสำนัก</p>	รองผู้อำนวยการฯ ศูนย์คอมพิวเตอร์ฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีการบริหารความเสี่ยง	การบริหารความเสี่ยง	ผู้รับผิดชอบ
งบประมาณที่กำหนดไว้ในโครงการหรืองบประมาณ	มีไม่เพียงพอต่อการจ้างบริษัทได้			ทำการดูแล	
3 ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	<ul style="list-style-type: none"> - มัลแวร์ อาจมีแรนซัมแวร์ซึ่งอาจล็อกการเข้าถึงข้อมูลหรือบัญชีผู้ใช้ เว้นแต่จะได้รับค่าไถ่ - ความเสียหายด้านชื่อเสียงและข้อมูล แสกเกอร์อาจทำลายข้อมูลทางธุรกิจและข้อมูลที่สำคัญอื่นๆ - การโจรกรรมอัตลักษณ์บุคคล ข้อมูลอัตลักษณ์บุคคลของคุณ อาจรั่วไหล และถูกแฮกเกอร์นำไปใช้ 	สูง	Reduce	<ol style="list-style-type: none"> 1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2 . การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย 	รองผู้อำนวยการฯ ศูนย์คอมพิวเตอร์ฯ
4. การแฮกซ์ระบบ และการโจมตีของไวรัส	<ol style="list-style-type: none"> 1. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 2. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของสำนักงานฯ 3. ถูกโจรกรรมข้อมูลที่เป็นความลับ 	สูง	Reduce	มีระบบไฟร์วอลล์(Firewall) และระบบป้องกันไวรัส ทำการปรับปรุงค่าด้านมาตรฐานความปลอดภัย	รองผู้อำนวยการฯ ศูนย์คอมพิวเตอร์ฯ
5. ความเสี่ยงจากการใช้คอมพิวเตอร์/	1. เสี่ยงต่อการใช้งานในทางที่ผิด หรือเปล่า	สูง	Reduce	1. การจัดทำข้อมแนะนำเพื่อลดความเสี่ยง	รองผู้อำนวยการฯ ศูนย์คอมพิวเตอร์ฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีการบริหารความเสี่ยง	การบริหารความเสี่ยง	ผู้รับผิดชอบ
เครือข่ายผิดวัตถุประสงค์	<p>ประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ เป็นต้น</p> <p>2. การใช้ Resource ทาผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น</p>			2. กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น	