แผนบริหารความเสี่ยง

คณะสังคมศาสตร์ มหาวิทยาลัยเชียงใหม่
ประจำปีงบประมาณ พ.ศ. 2566

แผนบริหารความเสี่ยงคณะสังคมศาสตร์
ประจำปีงบประมาณ 2566

คณะสังคมศาสตร์ ได้วิเคราะห์เหตุการณ์ในอนาคตที่มีความไม่แน่นอน (Uncertain) มีโอกาสเกิดขึ้น หรือไม่มีโอกาสเกิดขึ้นก็ได้ (Probability/Likelihood) ซึ่งหากเกิดขึ้นแล้วจะส่งผลกระทบเชิงลบ (Impact/Consequence) ก่อให้เกิดความสูญเสีย เสียหาย ล้มเหลว ต่อการบรรลุตามวัตถุประสงค์ (Objectives) และ เป้าหมาย (Target) ของคณะที่กำหนดไว้ ดังนั้นจึงได้กำหนดทิศทางและเป้าหมายในการบริหารความเสี่ยงของคณะไว้ 3 ประการ ประกอบด้วย

1) เพื่อให้คณะฯ ดำรงอยู่ได้อย่างมีคุณค่าและยั่งยืน
2) เพื่อบรรลุพันธกิจ วัตถุประสงค์ และเป้าหมาย ที่สำคัญของคณะฯ อย่างมีคุณภาพ ทั้งในปัจจุบันและในอนาคต ด้วยการบริหารจัดการอย่างมีธรรมาภิบาล
3) เพื่อลดความสูญเสีย และความเสียหายที่อาจเกิดขึ้นในอนาคต เกินกว่าระดับที่คณะฯ ยอมรับได้ ทั้งในด้านการดำเนินงาน ด้านยุทธศาสตร์ ด้านชื่อเสียง ด้านความปลอดภัยในชีวิตและทรัพย์สิน ด้านการเงิน และด้านกฎ ระเบียบ จากการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอก รวมทั้งปัจจัยเสี่ยง/สาเหตุเสี่ยงและ ผลกระทบด้านลบที่จะตามมา

ด้าน	ปัจจัยภายใน	ปัจจัยภายนอก
ยุทธศาสตร์	1. บุคลากรไม่มีความความเชี่ยวชาญตามตำแหน่งงานที่เพียงพอ 2. บุคลากรขาดการพัฒนาทักษะสมรรถนะที่จำเป็นต่อพันกิจ/การปฏิบัติงานแต่หละหน่วยงาน 3. คณะฯ ขาดกระบวนการพัฒนาบุคลากรในรูปแบบรายบุคคลอย่างเป็นรูปธรรม (Individual Development Plan) ที่เป็นรูปธรรมและมีประสิทธิภาพเพียงพอ 4. วัฒนธรรมองค์กรที่ไม่ชอบการเปลี่ยนแปลงหรือความท้าทายใหม่ๆ	1. รูปแบบการทำงานที่เปลี่ยนแปลงไปตามสถานการณ์ปัจจุบันหรืออนาคต 2. การเปลี่ยนแปลงของเทคโนโลยี ความรู้ทักษะที่รวดเร็ว 3. ความเหมาะสมของสัดส่วนอัตรากำลังต่อภาระงานของบุคลากรสายวิชาการ 4. มหาวิทยาลัยมีการกำหนดสมรรถนะประจำตำแหน่ง (Functional Competency) สำหรับบุคลากรสายปฏิบัติเพื่อเป็นเกณฑ์ในการประเมินผลการปฏิบัติงาน
ปฏิบัติงาน	1. ขาดการป้องกันการรักษาความปลอดภัยในเครื่องคอมพิวเตอร์ส่วนบุคคลที่เหมาะสม 2. ผู้ใช้งานและผู้เกี่ยวข้องกับระบบสารสนเทศขาดความรู้ความเข้าใจ ขาดความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ 3. ขาดการป้องกันการรักษาความปลอดภัยในระบบโครงสร้างพื้นฐาน (เครือข่ายและศูนย์ข้อมูล) และระบบสารสนเทศของมหาวิทยาลัย 4. การนำแนวนโยบายและมาตรการการรักษาความปลอดภัยไปสู่การปฏิบัติขาดประสิทธิผล	1. การถูกโจมตีจากบุคคลหรือกลุ่มบุคคล 2. การโจรกรรมข้อมูลที่สำคัญ ผ่านกระบวนการ hacking, compromising หรือ phishing เป็นต้น 3. ภัยคุกคามจากมัลแวร์ ไวรัสคอมพิวเตอร์และการโจมตีในรูปแบบอื่น ๆ

ด้าน	ปัจจัยภายใน	ปัจจัยภายนอก
กฎระเบียบและข้อบังคับ	1. บุคลากรไม่มีความเข้าใจหรือไม่มีความรู้ในกฎระเบียบที่ต้องปฏิบัติหรือไม่ได้ศึกษาและทำความเข้าใจในเนื้อหาที่เกี่ยวข้อง 2. บุคลากรขาดความตระหนักต่อบทบาทความรับผิดชอบของตนเองต่อสังคม หรือขาดจริยธรรมในการทำงาน 3. บุคลากรมีพฤติกรรมที่ไม่พึงประสงค์ (ติดการพนัน/ติดหนี้นอกระบบ) 4. ระบบปฏิบัติงานเอื้อต่อการทุจริต (การรับเงินสด การตรวจวัสดุคงคลัง) 5. ขาดมาตรการการปกป้องข้อมูลส่วนบุคคลที่เหมาะสม 6. ผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในการขาดความตระหนักความรู้ และทักษะเกี่ยวกับการละเมิดความเป็นส่วนตัว 7. ขาดการป้องกันการรักษาความปลอดภัยในระบบโครงสร้างพื้นฐาน (เครือข่ายและศูนย์ข้อมูล) และระบบสารสนเทศของมหาวิทยาลัย 8. การนำแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลไปสู่การปฏิบัติขาดประสิทธิผล	1. กฎ ระเบียบ มีจำนวนมาก และบางครั้งถูกยกเลิกหรือมีการแก้ไขเพิ่มเติม 2. สภาวะเศรษฐกิจตกต่ำที่กระทบต่อการดำเนินชีวิต 3. การไม่ปฏิบัติตามแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลของบุคคลภายนอกที่เกี่ยวข้อง 4. การถูกโจมตีจากบุคคลหรือกลุ่มบุคคล 5. การโจรกรรมข้อมูลที่สำคัญ ผ่านกระบวนการ Hacking, Compromising หรือ Phishing เป็นต้น 6. ภัยคุกคามจากมัลแวร์ ไวรัสคอมพิวเตอร์ และการโจมตีในรูปแบบอื่น ๆ
ด้านชื่อเสียง	1. เกิดการกระทำความผิดภายในคณะฯ หรือการกระทำใดที่นำไปสู่ความเข้าใจที่ผิด ในเรื่องที่ส่งผลกระทบสำคัญต่อชื่อเสียงและการดำเนินงานของคณะฯ 2. การสื่อสารและการตอบสนองต่อสถานการณ์ที่จะส่งผลกระทบต่อชื่อเสียง ไม่เหมาะสมทั้งด้านช่องทาง และความไม่ทันการณ์ 3. คณะฯ มีบุคลากรที่มีประสบการณ์ต่างกัน ทั้งสายวิชาการและสายปฏิบัติการ และนักศึกษาอาจทำให้มีทัศนคติ มุมมองที่แตกต่างกัน	1. มีสถานการณ์ที่อ่อนไหวในเรื่องที่ส่งผลกระทบสำคัญต่อการดำเนินงานของคณะฯ ซึ่งมีความเสี่ยงต่อการแพร่กระจายข้อมูลและ/หรือ การวิพากษ์ วิจารณ์เป็นวงกว้างในสื่อสังคมออนไลน์ ทำให้มหาวิทยาลัยถูกกล่าวถึงในแง่ลบ 2. มีการใช้สื่อและ social media ในการแพร่กระจายข้อมูล ข่าวสาร โดยไม่ได้มีการกลั่นกรองข้อเท็จจริง (Fake News) และถึงแม้จะได้รับทราบข้อเท็จจริงแล้ว ก็อาจจะไม่ได้มีการแก้ไขในสิ่งที่สื่อสารออกไปแล้ว 3. ความแตกต่างทางความคิดของคนระหว่างกลุ่ม ระหว่างรุ่นที่กระทบต่อการดำเนินงานของคณะฯ

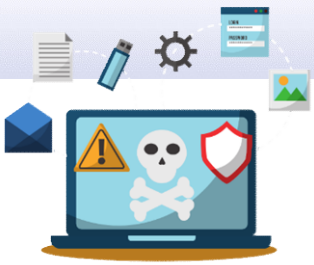
ประเด็นความเสี่ยงที่กำหนดในปีงบประมาณ พ.ศ. 2566

จากการวิเคราะห์ปัจจัยภายในและปัจจัยภายนอก ที่จะส่งผลกระทบต่อการดำเนินงานตามพันธกิจของ คณะสังคมศาสตร์ มหาวิทยาลัยเชียงใหม่ คณะฯ ได้กำหนดประเด็นความเสี่ยงที่สำคัญในปีงบประมาณ พ.ศ. 2566 จำนวน 5 ประเด็น จำนวน 4 ด้าน ได้แก่ ด้านยุทธศาสตร์ (Strategic Risk) ด้านปฏิบัติงาน (Operation Risk) ด้านกฎระเบียบ และข้อบังคับ (Compliance Risk) และด้านชื่อเสียง (Reputation Risk) ดังนี้

ด้านยุทธศาสตร์ (strategic risk)

S1 – บุคลากรขาดทักษะสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์

ด้านปฏิบัติงาน (operation risk)



O1 - ภัยคุกคามด้านเทคโนโลยีสารสนเทศ (cyber attack)

ด้านกฎระเบียบ และข้อบังคับ (compliance risk)

C1 - การไม่ปฏิบัติตามกฎ ระเบียบ ที่เกี่ยวข้องและการทุจริตในหน้าที่

C2 – การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ด้านชื่อเสียง (reputation risk)

R1 - ภาพลักษณ์มหาวิทยาลัยเสียหายหรือถูกลดทอนความน่าเชื่อถือ

ประเด็นความเสี่ยงที่ 1 ด้านยุทธศาสตร์ (strategic risk)

S1 บุคลากรขาดทักษะสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์

สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน

1. บุคลากรไม่มีความความเชี่ยวชาญตามตำแหน่งงานที่เพียงพอ
2. บุคลากรขาดการพัฒนาทักษะสมรรถนะที่จำเป็นต่อพันธกิจ/การปฏิบัติงานแต่ละหน่วยงาน
3. คณะฯ ขาดกระบวนการพัฒนาบุคลากรในรูปแบบรายบุคคลอย่างเป็นรูปธรรม (Individual Development Plan) ที่เป็นรูปธรรมและมีประสิทธิภาพเพียงพอ
4. วัฒนธรรมองค์กรที่ไม่ชอบการเปลี่ยนแปลงหรือความท้าทายใหม่ๆ

ปัจจัยภายนอก

1. รูปแบบการทำงานที่เปลี่ยนแปลงไปตามสถานการณ์ปัจจุบันหรืออนาคต
2. การเปลี่ยนแปลงของเทคโนโลยี ความรู้ ทักษะที่รวดเร็ว
3. ความเหมาะสมของสัดส่วนอัตรากำลังต่อภาระงานของบุคลากรสายวิชาการ
4. มหาวิทยาลัยมีการกำหนดสมรรถนะประจำตำแหน่ง (Functional Competency) สำหรับบุคลากรสายปฏิบัติเพื่อเป็นเกณฑ์ในการประเมินผลการปฏิบัติงาน

ผลกระทบของความเสี่ยงต่อคณะสังคมศาสตร์

1. บุคลากรที่มีความรู้/ความสามารถ/ความเชี่ยวชาญและทักษะการคิดวิเคราะห์ ที่จำเป็นต่อการบรรลุยุทธศาสตร์
2. ขาดทุนทางปัญญาที่ส่งผลด้านความสามารถในการแข่งขันในยุคเศรษฐกิจฐานความรู้ (Knowledge Based Economy)

ตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI) :

KRI 1 :

จำนวนบุคลากรที่มีองค์ความรู้/ทักษะสำคัญ ในการขับเคลื่อนยุทธศาสตร์

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ (Likelihood & Impact)

1) ค่าโอกาสเกิด (Likelihood)

L1 – ร้อยละของบุคลากรที่มีองค์ความรู้/ทักษะสำคัญ

2) ค่าผลกระทบ (Impact)

I1 – ร้อยละของความสำเร็จของการบรรลุเป้าประสงค์เชิงกลยุทธ์ตามเป้าหมายที่กำหนดในปีงบประมาณ พ.ศ. 2566

ระดับ	โอกาสเกิด (L)	ผลกระทบ (I)
5 (สูงมาก)	> ร้อยละ 40 ของจำนวนบุคลากร มีผลการประเมินสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์ต่ำกว่าเกณฑ์หลังจากได้รับการพัฒนาความรู้ ทักษะ สมรรถนะ	บรรลุเป้าหมายตามยุทธศาสตร์* < ร้อยละ 45
4 (สูง)	ร้อยละ 31 - 40 ของจำนวนบุคลากร มีผลการประเมินสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์ต่ำกว่าเกณฑ์หลังจากได้รับการพัฒนาความรู้ ทักษะ สมรรถนะ	บรรลุเป้าหมายตามยุทธศาสตร์* ร้อยละ 45 -54
3 (ปานกลาง)	ร้อยละ 21 - 30 ของจำนวนบุคลากร มีผลการประเมินสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์ต่ำกว่าเกณฑ์หลังจากได้รับการพัฒนาความรู้ ทักษะ สมรรถนะ	บรรลุเป้าหมายตามยุทธศาสตร์*ร้อยละ 55 – 64
2 (ต่ำ)	ร้อยละ 10 - 20 ของจำนวนบุคลากร มีผลการประเมินสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์ต่ำกว่าเกณฑ์หลังจากได้รับการพัฒนาความรู้ ทักษะ สมรรถนะ	บรรลุเป้าหมายตามยุทธศาสตร์* ร้อยละ 65 -74
1 (ต่ำมาก)	<ร้อยละ 1 0ของจำนวนบุคลากร มีประเมินสมรรถนะที่จำเป็นต่อการบรรลุยุทธศาสตร์ต่ำกว่าเกณฑ์ หลังจากได้รับการพัฒนาความรู้ ทักษะ สมรรถนะผลการ	บรรลุเป้าหมายตามยุทธศาสตร์* > ร้อยละ 75

ระดับความเสี่ยงที่เหลืออยู่ ณ ปัจจุบัน :

ผลกระทบ	โอกาสเกิด				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

ระดับความเสี่ยงที่เหลืออยู่

คะแนน L x I : 2 x 1 = 2 (เสี่ยงต่ำ)

ข้อมูล ณ วันที่ 10 มกราคม 2566

ระดับความเสี่ยงที่ยอมรับได้

คะแนน L x I : 2 x 1 = 2 (เสี่ยงต่ำ)

กิจกรรม/มาตรการควบคุมความเสี่ยง

1. กิจกรรม/โครงการ พัฒนาบุคลากรตามแนวทางการพัฒนาบุคลากรรายบุคคล (Individual Development Plan: IDP)
2. กิจกรรมโครงการ พัฒนาการปฏิบัติงานสู่ความเป็นเลิศ ด้วย Kaizen (Work Improvement by Kaizen Activity)
3. กิจกรรม/โครงการ พัฒนาบุคลากรตามบทบาทหน้าที่ที่รับผิดชอบ

ประเด็นความเสี่ยงที่ 2 ด้านปฏิบัติงาน (operation risk)

O1 ภัยคุกคามด้านเทคโนโลยีสารสนเทศ (cyber attack)

สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน

1. ขาดการป้องกันการรักษาความปลอดภัยในเครื่องคอมพิวเตอร์ส่วนบุคคลที่เหมาะสม
2. ผู้ใช้งานและผู้เกี่ยวข้องกับระบบสารสนเทศขาดความรู้ความเข้าใจ ขาดความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์
3. ขาดการป้องกันการรักษาความปลอดภัยในระบบโครงสร้างพื้นฐาน (เครือข่ายและศูนย์ข้อมูล) และระบบสารสนเทศของมหาวิทยาลัย
4. การนำแนวนโยบายและมาตรการการรักษาความปลอดภัยไปสู่การปฏิบัติขาดประสิทธิผล

ปัจจัยภายนอก

1. การถูกโจมตีจากบุคคลหรือกลุ่มบุคคล
2. การโจรกรรมข้อมูลที่สำคัญ ผ่านกระบวนการ hacking, compromising หรือ phishing เป็นต้น
3. ภัยคุกคามจากมัลแวร์ ไวรัสคอมพิวเตอร์ และการโจมตีในรูปแบบอื่น ๆ

ผลกระทบของความเสี่ยงต่อคณะสังคมศาสตร์

1. ข้อมูลเกิดการสูญหาย การโจรกรรมข้อมูลที่สำคัญ
2. เกิดความเสียหายต่อระบบงาน จนทำให้การปฏิบัติงาน หยุดชะงักหรือล่าช้า
3. สูญเสียเวลา ทรัพย์สิน
4. ภาพลักษณ์ของคณะสังคมศาสตรีเกิดความเสียหาย

ตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI) :

KRI 1 :

1. จำนวนการโจมตี Cyber Attack หรือ ได้รับการแจ้งเตือนเหตุละเมิดความมั่นคงปลอดภัยจากองค์กรภายนอก

2. เครื่องแม่ข่ายที่ระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม

3. จำนวนเว็บไซต์หรือระบบสารสนเทศที่ได้รับผลกระทบจากการโจมตี

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ (Likelihood & Impact)

1) ค่าโอกาสเกิด (Likelihood)

L1 – ร้อยละของการโจมตี

L2 – ร้อยละของเครื่องแม่ข่ายที่ไม่ถูกอัพเดต

2) ค่าผลกระทบ (Impact)

จำนวนเว็บไซต์/ระบบสารสนเทศที่ได้รับผลกระทบจากการโจมตี

ระดับ	โอกาสเกิด (L)		ผลกระทบ (I) จำนวนเว็บไซต์/ระบบสารสนเทศที่ได้รับผลกระทบจากการโจมตี
	L1 ร้อยละของการโจมตี	L2 ร้อยละของเครื่องแม่ข่ายที่ไม่ถูกอัพเดต	
5 (สูงมาก)	การโจมตี มากกว่า 4 ครั้ง/ปี	เครื่องแม่ข่ายที่มีระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม มากกว่าร้อยละ 20	จำนวนเว็บไซต์/ระบบสารสนเทศสำคัญ **ของส่วนงาน** ได้รับผลกระทบจากการโจมตีมากกว่า 3 ระบบ
4 (สูง)	การโจมตี มากกว่าหรือเท่ากับ 4 ครั้ง/ปี	เครื่องแม่ข่ายที่มีระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม มากกว่าร้อยละ 10 แต่ไม่เกินร้อยละ 20	จำนวนเว็บไซต์/ระบบสารสนเทศสำคัญ **ของส่วนงาน** ได้รับผลกระทบจากการโจมตีอย่างน้อย 3 ระบบ
3 (ปานกลาง)	การโจมตี มากกว่าหรือเท่ากับ 3 ครั้ง/ปี	เครื่องแม่ข่ายที่มีระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม มากกว่าร้อยละ 5 แต่ไม่เกินร้อยละ 10	จำนวนเว็บไซต์/ระบบสารสนเทศอื่นๆ **ของส่วนงาน** ได้รับผลกระทบจากการโจมตีอย่างน้อย 2 ระบบ
2 (ต่ำ)	การโจมตี มากกว่าหรือเท่ากับ 2 ครั้ง/ปี	เครื่องแม่ข่ายที่มีระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม ไม่เกินร้อยละ 5	จำนวนเว็บไซต์/ระบบสารสนเทศอื่นๆ **ของส่วนงาน** ได้รับผลกระทบจากการโจมตีอย่างน้อย 1 ระบบ
1 (ต่ำมาก)	การโจมตี มากกว่าหรือเท่ากับ 0 ครั้ง/ปี	ไม่มีเครื่องแม่ข่ายที่มีระบบความปลอดภัยไม่ได้ถูกอัพเดตให้เป็นปัจจุบันในเวลาที่เหมาะสม	ไม่ได้รับผลกระทบ

ระดับความเสี่ยงที่เหลืออยู่ ณ ปัจจุบัน :

ผลกระทบ	โอกาสเกิด				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

ระดับความเสี่ยงที่เหลืออยู่

คะแนน L x I : 2 x 2 = 4 (ความเสี่ยงระดับต่ำมาก)

ข้อมูล ณ กมภาพันธ์ 2566

ระดับความเสี่ยงที่ยอมรับได้

คะแนน L x I : 2 x 2 = 4 (ความเสี่ยงระดับต่ำมาก)

กิจกรรม/มาตรการควบคุมความเสี่ยง

1. ตรวจสอบป้องกันภัยจากคุกคามทางด้านไซเบอร์ รวมถึงการบำรุงดูแลรักษาระบบให้อยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพ อย่างน้อย ไตรมาสละ 1 ครั้ง
2. ปรับปรุงนโยบายและมาตรการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐานและระบบสารสนเทศตามสถานการณ์อย่างเหมาะสม
3. การจัดทำแผนรองรับสถานการณ์ฉุกเฉินในกรณีที่ระบบเกิดความเสียหาย (Academic Continuity Plan: ACP) และซ้อมรับสถานการณ์สม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
4. พัฒนาบุคลากร รวมถึงสร้างความตระหนักรู้ภัยไซเบอร์อย่างน้อย ไตรมาสละ 1 ครั้ง รวมถึงมีการแจ้งข่าวสารให้ความรู้ที่จำเป็นแก่ผู้เกี่ยวข้องทุกเดือน โดยคำนึงถึงความต่างระหว่างช่วงวัย
5. ดำเนินการทดสอบระบบความปลอดภัยด้วยการทดสอบการเจาะระบบ (penetration test) ที่ครอบคลุมช่องโหว่ของระบบโครงสร้างพื้นฐานและระบบสารสนเทศสำคัญ อย่างน้อยปีละ 1 ครั้ง

ประเด็นความเสี่ยงที่ 3 ด้านกฎระเบียบ และข้อบังคับ (compliance risk)
C1 - การไม่ปฏิบัติตามกฎ ระเบียบ ที่เกี่ยวข้อง และการทุจริตในหน้าที่

สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน

1. บุคลากรไม่มีความเข้าใจหรือไม่มีความรู้ในกฎระเบียบที่ต้องปฏิบัติ หรือไม่ได้ศึกษาและทำความเข้าใจในเนื้อหาที่เกี่ยวข้อง
2. บุคลากรขาดความตระหนักต่อบทบาทความรับผิดชอบของตนเองต่อสังคม หรือขาดจริยธรรมในการทำงาน
3. บุคลากรมีพฤติกรรมที่ไม่พึงประสงค์ (ติดการพนัน/ติดหนี้นอกระบบ)
4. ระบบปฏิบัติงานเอื้อต่อการทุจริต (การรับเงินสด การตรวจวัสดุคงคลัง)

ปัจจัยภายนอก

1. กฎ ระเบียบ มีจำนวนมาก และบางครั้งถูกยกเลิกหรือมีการแก้ไขเพิ่มเติม
2. สภาวะเศรษฐกิจตกต่ำที่กระทบต่อการดำเนินชีวิต

ผลกระทบของความเสี่ยงต่อคณะสังคมศาสตร์

ผลกระทบต่อระดับความโปร่งใส ชื่อเสียง และความเชื่อมั่นต่อคณะสังคมศาสตร์

ตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI) :

KRI 1: จำนวนข้อตรวจพบการไม่ปฏิบัติตามกฎระเบียบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน

KRI 2: จำนวนการสอบสวนความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง)

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ (Likelihood & Impact)

1) ค่าโอกาสเกิด (Likelihood)

L1 – จำนวนข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน

L2 –จำนวนการสอบสวนความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง)

2) ค่าผลกระทบ (Impact)

I1 – ผลกระทบด้านชื่อเสียง

I2 – มูลค่าความเสียหายต่อองค์กรหรือบุคคลภายนอก หรือเทียบเท่าความเสียหาย

ระดับ	โอกาสเกิด (L)		ผลกระทบ (I)	
	L1 จำนวนข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน (ใช้ข้อมูลสะสมทั้งปี)	L2 จำนวนการสอบสวนความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง) (ใช้ข้อมูลสะสมทั้งปี)	I1 ด้านชื่อเสียง	I2 มูลค่าความเสียหายต่อองค์กรหรือบุคคลภายนอก หรือเทียบเท่าความเสียหาย
5 (สูงมาก)	มีข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน จำนวนมากกว่า 20 เรื่องขึ้นไป	มีจำนวนการสอบสวนในความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง) จำนวน 5 เรื่องขึ้นไป	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและมหาวิทยาลัย	มูลค่าความเสียหายเกิน 1,000,000 บาทขึ้นไป
4 (สูง)	มีข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน จำนวน 15 - 20 เรื่อง	มีจำนวนการสอบสวนในความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง) จำนวน 4 เรื่องขึ้นไป	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและส่วนงาน	มูลค่าความเสียหายตั้งแต่ 500,001 – 1,000,000 บาท
3 (ปานกลาง)	มีข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน จำนวน 10 - 14 เรื่อง	มีจำนวนการสอบสวนในความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง) จำนวน 3 เรื่อง	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและหน่วยงาน	มูลค่าความเสียหายตั้งแต่ 100,001 – 500,000 บาท
2 (ต่ำ)	มีข้อตรวจพบ ที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน จำนวน 5 - 9 เรื่อง	มีจำนวนการสอบสวนในความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง) ไม่เกิน 2 เรื่อง	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคล	มูลค่าความเสียหายหรือไม่เกิน 100,000 บาท
1 (ต่ำมาก)	มีข้อตรวจพบที่เป็นระดับสีส้มและสีแดง จากสำนักงานการตรวจสอบภายใน จำนวน 0 - 4 เรื่อง	ไม่มีจำนวนการสอบสวนในความผิดการทุจริตในหน้าที่ (วินัยร้ายแรง)	ไม่มีการเสียชื่อเสียง	ไม่มีมูลค่าความเสียหาย

ระดับความเสี่ยงที่เหลืออยู่ ณ ปัจจุบัน :

ผลกระทบ	โอกาสเกิด				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

ระดับความเสี่ยงที่เหลืออยู่

คะแนน L x I : 4 x 1 = 4 (ระดับความเสี่ยงต่ำ)

ข้อมูล ณ กมภาพันธ์ 2566

ระดับความเสี่ยงที่ยอมรับได้

คะแนน L x I : 2 x 1 = 2 (ความเสี่ยงระดับต่ำ)

กิจกรรม/มาตรการควบคุมความเสี่ยง

1. พัฒนาระบบการรับข้อร้องเรียนและการจัดการข้อร้องเรียน
2. มีการตรวจสอบภายในและรายงานผลอย่างเป็นระบบและสม่ำเสมอ
3. เพิ่มมาตรการควบคุมภายในและใช้เทคโนโลยีในการจัดการทางการเงินเพื่อความถูกต้อง
4. อบรมสัมมนา/ ซักซ้อมทำความเข้าใจ/ ให้ความรู้ เกี่ยวกับข้อกฎหมาย และระเบียบข้อบังคับที่ผิดพลาดบ่อย ๆ พร้อมทั้งมีช่องทางให้คำปรึกษา เช่น การเบิกจ่ายเงินอุดหนุนทั่วไป
5. มีระบบการตักเตือน ลงโทษที่เหมาะสม
6. ส่งเสริมการสร้างจิตสำนึกด้านจริยธรรมและความโปร่งใส (ITA)
7. แผนป้องกันการทุจริต

ประเด็นความเสี่ยงที่ 4 ด้านกฎระเบียบ และข้อบังคับ (compliance risk)
C2 – การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน

1. ขาดมาตรการการปกป้องข้อมูลส่วนบุคคลที่เหมาะสม
2. ผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในการขาดความตระหนัก ความรู้ และทักษะเกี่ยวกับการละเมิดความเป็นส่วนตัว
3. ขาดการป้องกันการรักษาความปลอดภัยในระบบโครงสร้างพื้นฐาน (เครือข่ายและศูนย์ข้อมูล) และระบบสารสนเทศของมหาวิทยาลัย
4. การนำแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลไปสู่การปฏิบัติขาดประสิทธิผล

ปัจจัยภายนอก

1. การไม่ปฏิบัติตามแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลของบุคคลภายนอกที่เกี่ยวข้อง
2. การถูกโจมตีจากบุคคลหรือกลุ่มบุคคล
3. การโจรกรรมข้อมูลที่สำคัญ ผ่านกระบวนการ Hacking, Compromising หรือ Phishing เป็นต้น
4. ภัยคุกคามจากมัลแวร์ ไวรัสคอมพิวเตอร์ และการโจมตีในรูปแบบอื่น ๆ

ผลกระทบของความเสี่ยงต่อคณะสังคมศาสตร์

1. ข้อมูลส่วนบุคคลของนักศึกษาหรือบุคลากรถูกละเมิดก่อให้เกิดอันตรายทั้งทางร่างกายหรือต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล
2. ภาพลักษณ์ของคณะสังคมศาสตร์เกิดความเสียหาย
3. เกิดการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง

ตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI) :

KRI 1:

1. จำนวนเหตุละเมิดข้อมูลส่วนบุคคล (ค่า L)

2. ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคลจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล (ค่า I)

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ (Likelihood & Impact)

1) ค่าโอกาสเกิด (Likelihood)

L1 – จำนวนเหตุละเมิดข้อมูลส่วนบุคคล

2) ค่าผลกระทบ (Impact)

I1 – ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคล จากสำนักงานคุ้มครองข้อมูลส่วนบุคคล

ระดับ	โอกาสเกิด (L)	ผลกระทบ (I)
5 (สูงมาก)	เกิดเหตุละเมิดข้อมูลส่วนบุคคล มากกว่า 12 ครั้งต่อปี	ข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวจำนวนมากถูกละเมิดและก่อให้เกิดอันตรายทั้งทางร่างกายหรือต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล และนำมาซึ่งการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง
4 (สูง)	เกิดเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 9-12 ครั้งต่อปี	ข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวถูกละเมิดและก่อให้เกิดอันตรายทั้งทางร่างกายหรือต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล และนำมาซึ่งการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง
3 (ปานกลาง)	เกิดเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 5-8 ครั้งต่อปี	ข้อมูลส่วนบุคคลจำนวนมากถูกละเมิดแต่ไม่ก่อให้เกิดอันตรายทั้งทางร่างกายหรือต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล
2 (ต่ำ)	เกิดเหตุละเมิดข้อมูลส่วนบุคคล จำนวน 2-4 ครั้งต่อปี	ข้อมูลส่วนบุคคลถูกละเมิดแต่ไม่ก่อให้เกิดอันตรายทั้งทางร่างกายหรือต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล ไม่ต้องแจ้งเหตุละเมิดไปยังสำงานคุ้มครองข้อมูลส่วนบุคคล
1 (ต่ำมาก)	เกิดเหตุละเมิดข้อมูลส่วนบุคคล ไม่เกิน 1 ครั้งต่อปี	ไม่ได้รับผลกระทบ

ระดับความเสี่ยงที่เหลืออยู่ ณ ปัจจุบัน :

ผลกระทบ	โอกาสเกิด				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

ระดับความเสี่ยงที่เหลืออยู่

คะแนน L x I : 1 x 1 = 1 (ความเสี่ยงระดับต่ำมาก)

ข้อมูล ณ กมภาพันธ์ 2566

ระดับความเสี่ยงที่ยอมรับได้

คะแนน L x I : 2 x 1 = 2 (ความเสี่ยงระดับต่ำมาก)

กิจกรรม/มาตรการควบคุมความเสี่ยง

1. จัดทำมาตรการ และแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคล รวมถึงการทบทวนมาตรการและแนวปฏิบัติอย่างสม่ำเสมอ
2. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิดการตระหนัก มีความรู้ และทักษะในการจัดการข้อมูลส่วนบุคคล
3. จัดให้มีการซ้อมกระบวนการตอบสนอง ในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น อย่างน้อย 1 ครั้งต่อปี

ประเด็นความเสี่ยงที่ 5 ด้านชื่อเสียง (reputation risk)

R1 – ภาพลักษณ์คณะสังคมศาสตร์เสียหายหรือถูกลดทอนความน่าเชื่อถือ

สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน

1. เกิดการกระทำความผิดภายในคณะฯ หรือการกระทำใดที่นำไปสู่ความเข้าใจที่ผิดในเรื่องที่ส่งผลกระทบสำคัญต่อชื่อเสียงและการดำเนินงานของคณะฯ
2. การสื่อสารและการตอบสนองต่อสถานการณ์ที่จะส่งผลกระทบต่อชื่อเสียง ไม่เหมาะสมทั้งด้านช่องทาง และความไม่ทันการณ์
3. คณะฯ มีบุคลากรที่มีประสบการณ์ต่างกัน ทั้งสายวิชาการและสายปฏิบัติการ และนักศึกษา อาจทำให้มีทัศนคติ มุมมองที่แตกต่างกัน

ปัจจัยภายนอก

1. มีสถานการณ์ที่อ่อนไหวในเรื่องที่ส่งผลกระทบสำคัญต่อการดำเนินงานของคณะฯ ซึ่งมีความเสี่ยงต่อการแพร่กระจายข้อมูล และ/หรือ การวิพากษ์ วิจารณ์เป็นวงกว้างในสื่อสังคมออนไลน์ ทำให้คณะสังคมศาสตร์ถูกกล่าวถึงในแง่ลบ
2. มีการใช้สื่อและ social media ในการแพร่กระจายข้อมูล ข่าวสาร โดยไม่ได้มีการกลั่นกรองข้อเท็จจริง (Fake News) และถึงแม้จะได้รับทราบข้อเท็จจริงแล้วก็อาจจะไม่ได้มีการแก้ไขในสิ่งที่สื่อสารออกไปแล้ว
3. ความแตกต่างทางความคิดของคนระหว่างกลุ่ม ระหว่างรุ่นที่กระทบต่อการดำเนินงานของคณะฯ

ผลกระทบของความเสี่ยงต่อคณะสังคมศาสตร์

1. ผลกระทบต่อชื่อเสียง หรือความน่าเชื่อถือของคณะสังคมศาสตร์
2. ผลกระทบต่อความร่วมมือระหว่างแหล่งทุน และผู้มีส่วนได้ส่วนเสียกับคณะสังคมศาสตร์

ตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI) :

KRI 1 : ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment เกินเกณฑ์ที่กำหนด

KRI 2 : กระทู้เชิงลบที่ส่งผลต่อภาพลักษณ์ของคณะสังคมศาสตร์และเกิดการขยายวง

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ (Likelihood & Impact)

1) ค่าโอกาสเกิด (Likelihood)

L1 – ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment เกินเกณฑ์ที่กำหนด

2) ค่าผลกระทบ (Impact)

I1 – ระดับผลกระทบต่อภาพลักษณ์ของคณะฯ

ระดับ	โอกาสเกิด (L) L1 ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment เกินเกณฑ์ที่กำหนด	ผลกระทบ (I)
5 (สูงมาก)	ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment จากโพสต์ที่เกี่ยวข้องกับคณะฯ บ่อยครั้ง โดยโอกาสเกิดมากกว่า 90% หรือเกิดทุกสัปดาห์	มีผลกระทบ **ในระดับนานาชาติ** หรือมีการยกเลิกการดำเนินการใด ๆ กับคณะฯ อันเกิดจากข่าวสารเชิงลบ
4 (สูง)	ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment จากโพสต์ที่เกี่ยวข้องกับคณะฯ โดยโอกาสเกิดมากกว่า 50% หรือเกิดทุกเดือน	มีผลกระทบ**ในระดับประเทศ** หรือมีการชะลอการดำเนินการใด ๆ กับคณะฯ เกิดจากข่าวสารเชิงลบ
3 (ปานกลาง)	ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment จากโพสต์ที่เกี่ยวข้องกับคณะฯ ที่เคยเกิดขึ้นแล้ว โดยโอกาสเกิดมากกว่า 10% หรือเกิดทุก 3 เดือน	มีผลกระทบ**ในระดับภูมิภาค** หรือมีผลกระทบบางประการต่อการดำเนินการใด ๆกับคณะฯ อันเกิดจากข่าวสารเชิงลบ
2 (ต่ำ)	ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment จากโพสต์ที่เกี่ยวข้องกับคณะฯ ที่ไม่เคยเกิดขึ้น โดยโอกาสเกิดมากกว่า 1% หรือเกิดทุก 6 เดือน	มีผลกระทบ ภายในคณะฯ ที่สามารถจัดการได้
1 (ต่ำมาก)	ผลรายงาน Social Media Analytics แสดงค่า Negative Sentiment จากโพสต์ที่เกี่ยวข้องกับคณะฯ เป็นเหตุการณ์ไม่ปกติโดยโอกาสเกิดน้อยกว่า 1% หรือเกิดในทุก 1 ปี	**ไม่มีผลกระทบ** กับคณะฯ

ระดับความเสี่ยงที่เหลืออยู่ ณ ปัจจุบัน :

ผลกระทบ	โอกาสเกิด				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

ระดับความเสี่ยงที่เหลืออยู่

คะแนน L x I : 1 x 1 = 1 (ความเสี่ยงระดับต่ำมาก)

ข้อมูล ณ กมภาพันธ์ 2566

ระดับความเสี่ยงที่ยอมรับได้

คะแนน L x I : 2 x 2 = 4 (ความเสี่ยงระดับต่ำ)

กิจกรรม/มาตรการควบคุมความเสี่ยง

1. ใช้เครื่องมือ Social Analytics วิเคราะห์เหตุการณ์ ควบคุมและวางแผนจัดการความเสี่ยง

   1.1 มีการจัดทำข้อมูลรายวันในภาพรวมของคณะฯ เพื่อประเมินสถานการณ์โดยใช้เครื่องมือ Trend View ของ Social media monitoring

   1.2 มีการตอบสนองต่อเหตุการณ์อย่างเหมาะสมและทันเวลา

2. จัดแนวปฏิบัติเพื่อรับมือกับข่าวปลอม (fake news) ที่เกิดขึ้น (strategic responses) โดยจัดทำแผนการตอบสนองเพื่อรับมือกับข่าวปลอมที่เกิดขึ้นและข่าวที่ส่งผลกระทบแง่ลบต่อภาพลักษณ์หรือชื่อเสียงของคณะฯ (crisis communication management) ที่ครอบคลุมสายการบังคับบัญชา (chain of command) และผู้รับผิดชอบดำเนินการ (accountability) ที่ชัดเจน เพื่อการตอบสนองเชิงกลยุทธ์ที่รวดเร็ว และมีการถ่ายทอดแผนให้ผู้เกี่ยวข้องภายในหน่วยงาน
3. ใช้ระบบรับฟังเสียงผู้รับบริการและผู้มีส่วนได้ส่วนเสีย (VOC) จัดทำแนวปฏิบัติและแผนบริหารงานเฝ้าระวังและบริหารจัดการในภาวะวิกฤต และมีช่องทางรับฟังเสียงผู้รับบริการผ่านทางระบบออนไลน์ https://voc.cmu.ac.th จดหมาย และการร้องเรียนด้วยตนเอง โดยส่วนใหญ่เป็นช่องทางสื่อสังคมออนไลน์ Facebook Page ของคณะฯ ซึ่งมีการกำหนดแนวทางปฏิบัติ และหากพบว่าเป็นข้อมูลที่มีผลกระทบต่อภาพลักษณ์และชื่อเสียงของคณะฯ จะมีการรายงานให้ผู้บริหารที่กำกับดูแลงานด้านสื่อสารทราบทันที
4. จัดตั้งทีมปฏิบัติการด้านข่าวสาร (Information Operation: IO) เพื่อตอบสนองต่อข่าวด้านลบทาง Social Media ที่มีต่อมหาวิทยาลัย และเปิดพื้นที่ทั้งสาธารณะและ (virtual platform) การแสดงความคิดเห็น
5. จัดทำแนวทางการสื่อสารเชิงรุก สำหรับข้อมูลเชิงบวก เพื่อสร้างความเข้มแข็งของภาพลักษณ์ที่ดีของคณะฯ

การถ่ายทอดแผนบริหารความเสี่ยงระดับคณะสู่ส่วนงาน

เพื่อให้การบริหารความเสี่ยงของคณะสังคมศาสตร์ มหาวิทยาลัยเป็นไปในทิศทางเดียวกัน กำหนดให้ส่วนงานภายในคณะสังคมศาสตร์ทุกส่วนงาน จัดทำแผนควบคุมภายในที่สอดคล้องกับนโยบายบริหารความเสี่ยงของคณะฯ โดยคณะอนุกรรมการบริหารความเสี่ยงฯ จะพิจารณาประเด็นความเสี่ยงที่ส่วนงานจะต้องเลือกนำไปจัดทำเป็นแผนปฏิบัติงาน ที่สอดคล้องกับนโยบายมหาวิทยาลัยและบริบทของแต่ละส่วนงานต่อไป โดยต้องผ่านความเห็นชอบจากคณะกรรมการบริหารประจำคณะฯ และคณะกรรมการอำนวยการประจำคณะฯ และรายงานผลการบริหารความเสี่ยงต่อมหาวิทยาลัยทราบทุกปี

การติดตามและประเมินผลแผนบริหารความเสี่ยง

กำหนดให้ส่วนงานภายในคณะฯ ติดตามรายงานผลการดำเนินงานทุกไตรมาสผ่านระบบ CMU-RM และคณะอนุกรรมการบริหารความเสี่ยงพิจารณา หากมีความเสี่ยงใดที่มีระดับสูงให้พิจารณากิจกรรมควบคุมความเสี่ยงเพิ่มเติมเพื่อลดหรือควบคุมความเสี่ยงนั้นให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ และรวบรวมสรุปข้อมูลรายงานต่อคณะกรรมการบริหารประจำคณะ/คณะกรรมการอำนวยการ ทุก 6 เดือน ทั้งนี้หากเกิดเหตุการณ์ไม่ปกติและเป็นความเสี่ยงสำคัญใหม่ๆ คณะฯ จะต้องทบทวนแผนได้ทันที