

แนวปฏิบัติการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้

ประจำปีงบประมาณ พ.ศ. 2570

ตามที่มหาวิทยาลัยแม่โจ้ได้ประกาศนโยบายการบริหารความเสี่ยง เพื่อให้การบริหารความเสี่ยงของมหาวิทยาลัยและส่วนงาน/หน่วยงานเป็นไปอย่างเป็นระบบ มีมาตรฐานและแนวทางการดำเนินงานที่สอดคล้องกันทั่วทั้งองค์กร และสามารถสนับสนุนการบรรลุวิสัยทัศน์ พันธกิจ เป้าหมายเชิงยุทธศาสตร์ และวัตถุประสงค์ของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ ประกอบกับสภาพแวดล้อมการดำเนินงานมีความไม่แน่นอนและเปลี่ยนแปลงอย่างรวดเร็ว ทั้งด้านเศรษฐกิจ สังคม โครงสร้างประชากร เทคโนโลยีดิจิทัล กฎหมายและกฎระเบียบ ตลอดจนความคาดหวังของผู้มีส่วนได้ส่วนเสีย

เพื่อให้การบริหารความเสี่ยงของมหาวิทยาลัยสามารถรองรับการเปลี่ยนแปลงดังกล่าว และเป็นกลไกสนับสนุนการตัดสินใจ การจัดสรรทรัพยากร การกำกับดูแล และการบรรลุเป้าหมายขององค์กร โดยสอดคล้องกับหลักการบริหารความเสี่ยงตามกรอบ COSO Enterprise Risk Management (COSO ERM) มาตรฐาน ISO 31000:2018 และหลักเกณฑ์ที่เกี่ยวข้อง มหาวิทยาลัยจึงกำหนดแนวปฏิบัติการบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ. 2570 ดังนี้

1. การระบุและพิจารณาประเด็นความเสี่ยง (Risk Identification)

ให้มหาวิทยาลัยและส่วนงาน/หน่วยงานระบุและพิจารณาความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ เป้าหมาย และผลลัพธ์ที่สำคัญ โดยพิจารณาข้อมูลและปัจจัยอย่างน้อย ดังนี้

- สภาพแวดล้อมและปัจจัยทั้งภายในและภายนอกที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์และเป้าหมาย
- วิสัยทัศน์ พันธกิจ ยุทธศาสตร์ เป้าหมายเชิงยุทธศาสตร์ ตัวชี้วัด และแผนปฏิบัติการของมหาวิทยาลัยและส่วนงาน/หน่วยงาน
- ผลการดำเนินงานที่ผ่านมา แนวโน้มของตัวชี้วัด เหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง และประเด็นที่ผลการดำเนินงานไม่เป็นไปตามเป้าหมาย
- ผลการตรวจสอบ ข้อสังเกตและข้อเสนอแนะจากกองตรวจสอบภายใน ผลการประเมินการควบคุมภายใน รวมถึงข้อเสนอแนะจากหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้อง
- ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risks) และแนวโน้มการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อมหาวิทยาลัยในอนาคต เช่น AI และเทคโนโลยีดิจิทัล ภัยคุกคามทางไซเบอร์ การเปลี่ยนแปลงสภาพภูมิอากาศ โครงสร้างประชากร เศรษฐกิจ และภูมิรัฐศาสตร์
- ความเสี่ยงที่มีความเชื่อมโยงหรือส่งผลกระทบต่อกัน (Interdependent Risks) รวมถึงความเสี่ยงที่อาจส่งผลกระทบต่อหลายพันธกิจหรือหลายส่วนงาน

การระบุความเสี่ยงให้มุ่งเน้น **ความไม่แน่นอนที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์** และพิจารณาสาเหตุหรือปัจจัยขับเคลื่อนความเสี่ยง (Risk Drivers) ควบคู่กับเหตุการณ์และผลกระทบ เพื่อให้สามารถกำหนดมาตรการจัดการได้ตรงกับสาเหตุของความเสี่ยง

2. การเชื่อมโยงความเสี่ยงระดับมหาวิทยาลัยสู่ระดับส่วนงาน (Enterprise-to-Unit Risk Alignment)

มหาวิทยาลัยกำหนดความเสี่ยงระดับองค์กร (Enterprise Risks) ประจำปีงบประมาณ พ.ศ. 2570 จำนวน 6 ประเด็น เพื่อใช้เป็น กรอบความเสี่ยงร่วมของมหาวิทยาลัย (University Risk Framework) ดังนี้

รหัส	ความเสี่ยงระดับมหาวิทยาลัย	แนวทางการพิจารณาของส่วนงาน
S1	ความสามารถในการแข่งขันด้านการศึกษาและผลกระทบจากการลดลงของจำนวนนักศึกษา	คณะ/วิทยาลัยและส่วนงานที่เกี่ยวข้องควรให้ความสำคัญโดยพิจารณาจำนวนผู้สมัคร นักศึกษาใหม่ อัตราการยืนยันสิทธิ์ การคงอยู่ของนักศึกษา คุณภาพและความสามารถในการแข่งขันของหลักสูตร
O1	ศักยภาพและขีดความสามารถของบุคลากรไม่สอดคล้องกับการเปลี่ยนแปลงในอนาคต (Future Workforce Capability Gap)	ทุกส่วนงานประเมินความเกี่ยวข้อง โดยพิจารณา Competency Gap, Re-skill/Up-skill, AI/Digital Skills, Succession และความเพียงพอของกำลังคน
F1	ความมั่นคงทางการเงินและความยั่งยืนของรายได้	ส่วนงานประเมินตามบทบาทและบริบท โดยเฉพาะส่วนงานที่รับผิดชอบรายได้ งบประมาณ โครงการสร้างรายได้ การบริหารต้นทุน หรือทรัพย์สิน
C1	การปฏิบัติตามกฎหมาย ระเบียบมาตรฐานการกำกับดูแลภาครัฐ และหลักธรรมาภิบาล	ทุกส่วนงานประเมินความเกี่ยวข้องกับกฎหมาย ระเบียบการเงิน พัสดุ บุคลากร จริยธรรม การควบคุมภายใน และธรรมาภิบาล
D1	ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล (Cybersecurity & Personal Data Protection)	ทุกส่วนงานประเมินความเกี่ยวข้อง โดยเฉพาะการใช้ระบบสารสนเทศ ฐานข้อมูล การเข้าถึงข้อมูล และการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
D2	การปรับตัวและใช้ประโยชน์จาก AI และเทคโนโลยีดิจิทัลอย่างเหมาะสมและทันต่อการเปลี่ยนแปลง	ทุกส่วนงานประเมินตามระดับการใช้ AI เทคโนโลยีดิจิทัล ระบบงาน และการเปลี่ยนผ่านสู่ดิจิทัล (Digital Transformation)

ให้ทุกส่วนงาน/หน่วยงานนำความเสี่ยงระดับมหาวิทยาลัยทั้ง 6 ประเด็นไป พิจารณาความเกี่ยวข้อง (Risk Relevance Assessment) กับวัตถุประสงค์ พันธกิจ เป้าหมาย ตัวชี้วัด กระบวนการ โครงการ และบริบทของส่วนงาน โดย มิได้กำหนดให้ทุกส่วนงานต้องนำความเสี่ยงทั้ง 6 ประเด็นไปบรรจุในแผนบริหารความเสี่ยงของส่วนงานทั้งหมด

หากผลการพิจารณาพบว่าความเสี่ยงระดับมหาวิทยาลัยประเด็นใดมีความเกี่ยวข้องและอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการบรรลุเป้าหมายของส่วนงานหรือมหาวิทยาลัย ให้ส่วนงานกำหนดเป็นความเสี่ยงของส่วนงาน โดยปรับถ้อยคำ สาเหตุ ผลกระทบ ตัวชี้วัด และมาตรการจัดการให้สอดคล้องกับบริบทของส่วนงาน พร้อมระบุความเชื่อมโยงกับรหัสความเสี่ยงระดับมหาวิทยาลัยที่เกี่ยวข้อง

ในขณะเดียวกัน ให้ส่วนงานวิเคราะห์ **ความเสี่ยงเฉพาะของส่วนงาน (Unit-specific Risks)** ที่เกิดจาก พันธกิจ กระบวนการ โครงการ ผู้มีส่วนได้ส่วนเสีย และการเปลี่ยนแปลงที่สำคัญเพิ่มเติม โดยไม่จำกัดเฉพาะความเสี่ยงระดับมหาวิทยาลัย เพื่อให้การบริหารความเสี่ยงครอบคลุมทั้ง

- **Top-down Risks** — ความเสี่ยงที่ถ่ายทอดหรือเชื่อมโยงจากระดับมหาวิทยาลัยสู่ส่วนงาน
- **Bottom-up Risks** — ความเสี่ยงที่ค้นพบจากบริบทและกระบวนการของส่วนงาน และอาจยกระดับเข้าสู่การพิจารณาเป็นความเสี่ยงระดับมหาวิทยาลัยเมื่อมีนัยสำคัญ

หลักการเชื่อมโยง

Enterprise Risk → Risk Relevance Assessment → วิเคราะห์ตามบริบทส่วนงาน → ประเมินระดับความเสี่ยง → บรรจุใน Risk Register เมื่อมีนัยสำคัญ → กำหนดมาตรการและ KRI → ติดตามและรายงาน → เชื่อมโยง/ยกระดับกลับสู่ระดับมหาวิทยาลัย

3. ประเภทและขอบเขตของความเสี่ยง

ให้มหาวิทยาลัยและส่วนงาน/หน่วยงานพิจารณาความเสี่ยงให้ครอบคลุมประเภทหลัก ดังนี้

(1) **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** ความเสี่ยงที่เกี่ยวข้องกับการกำหนดหรือการขับเคลื่อน ยุทธศาสตร์ นโยบาย เป้าหมาย หรือทิศทางการดำเนินงาน ซึ่งอาจส่งผลให้ไม่สามารถบรรลุเป้าหมายเชิง ยุทธศาสตร์ภายใต้บริบทและการเปลี่ยนแปลงที่เกิดขึ้น

(2) **ความเสี่ยงด้านการดำเนินงาน (Operational Risk)** ความเสี่ยงจากกระบวนการปฏิบัติงาน บุคลากร ระบบงาน โครงสร้างพื้นฐาน หรือเหตุการณ์ภายในและภายนอกที่อาจส่งผลกระทบต่อประสิทธิภาพ ประสิทธิผล คุณภาพ และความต่อเนื่องของการดำเนินงาน

(3) **ความเสี่ยงด้านการเงิน (Financial Risk)** ความเสี่ยงที่เกี่ยวข้องกับรายได้ งบประมาณ ค่าใช้จ่าย สภาพคล่อง กระแสเงินสด การจัดสรรและใช้ทรัพยากรทางการเงิน ตลอดจนความมั่นคงและความยั่งยืนทางการเงิน

(4) **ความเสี่ยงด้านการปฏิบัติตามกฎหมายและธรรมาภิบาล (Compliance & Governance Risk)** ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ นโยบาย มติ มาตรฐาน หรือหลักเกณฑ์ ที่เกี่ยวข้อง รวมถึงความเสี่ยงด้านการกำกับดูแล ธรรมาภิบาล จริยธรรม ความโปร่งใส และการควบคุมภายใน

(5) **ความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Technology Risk)** ความเสี่ยงจากการใช้หรือการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล ระบบสารสนเทศ AI ข้อมูล ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล เทคโนโลยีที่เกิดขึ้นใหม่ รวมถึงความพร้อมของโครงสร้างพื้นฐานและการปรับตัวต่อ Digital Transformation

นอกจากนี้ ให้ **ทุกส่วนงาน/หน่วยงานประเมินความเสี่ยงด้านการทุจริต (Fraud Risk)** ให้ครอบคลุม กระบวนการที่มีโอกาสเกิดการทุจริตหรือการประพฤติมิชอบ เช่น การใช้อำนาจโดยมิชอบ การเรียกรับหรือให้ผลประโยชน์ ผลประโยชน์ทับซ้อน การจัดซื้อจัดจ้าง การบริหารงบประมาณและทรัพย์สิน การรับ-จ่ายเงิน การเบิกจ่าย ตลอดจนกระบวนการอื่นตามลักษณะและบริบทของส่วนงาน โดยเชื่อมโยงผลการประเมินกับระบบ ควบคุมภายในและมาตรการป้องกันการทุจริตที่เกี่ยวข้อง

4. การวิเคราะห์ ประเมิน และจัดการความเสี่ยง

ให้ส่วนงาน/หน่วยงานวิเคราะห์และประเมินความเสี่ยงโดยใช้เกณฑ์ที่มหาวิทยาลัยกำหนด เพื่อให้สามารถเปรียบเทียบและรายงานผลในมาตรฐานเดียวกัน โดยพิจารณาอย่างน้อย ดังนี้

1. โอกาสเกิด (Likelihood: L) — ความเป็นไปได้หรือความถี่ของการเกิดเหตุการณ์ความเสี่ยง
 2. ผลกระทบ (Impact: I) — ระดับความรุนแรงของผลกระทบต่อวัตถุประสงค์ ยุทธศาสตร์ การดำเนินงาน การเงิน บุคลากร ผู้มีส่วนได้ส่วนเสีย กฎหมาย ธรรมชาติ ชีวเสี่ยง และความต่อเนื่องขององค์กร
 3. ประเมิน ระดับความเสี่ยงก่อนการจัดการ (Inherent Risk) และพิจารณามาตรการควบคุมที่มีอยู่ (Existing Controls)
 4. ประเมิน ระดับความเสี่ยงคงเหลือ (Residual Risk) ภายหลังพิจารณาประสิทธิผลของมาตรการควบคุม
 5. เปรียบเทียบระดับความเสี่ยงกับ Risk Appetite (RA) และ Risk Tolerance (RT) ตามเกณฑ์ที่มหาวิทยาลัยหรือส่วนงานกำหนด
 6. สำหรับความเสี่ยงที่สูงกว่า RA/RT หรือมีระดับสูงและสูงมาก ให้จัดทำมาตรการจัดการความเสี่ยงเพิ่มเติม (Additional Controls/Action Plan) พร้อมกำหนดเจ้าของความเสี่ยง ผู้รับผิดชอบ ระยะเวลา และผลลัพธ์ที่คาดหวัง
 7. กำหนด Key Risk Indicators (KRI) และสัญญาณเตือนภัยล่วงหน้า (Early Warning Signals: EWS) ตามความเหมาะสม เพื่อใช้ติดตามการเปลี่ยนแปลงของความเสี่ยงและสนับสนุนการดำเนินการเชิงรุก
- การกำหนดมาตรการจัดการความเสี่ยงให้มุ่งจัดการที่ สาเหตุและปัจจัยขับเคลื่อนความเสี่ยง (Root Causes & Risk Drivers) และพิจารณาประสิทธิผลของมาตรการมากกว่าการติดตามเพียงความก้าวหน้าของกิจกรรม

5. การติดตามและรายงานผลการบริหารความเสี่ยง

ให้ส่วนงาน/หน่วยงานติดตาม ผลการดำเนินงานตามมาตรการ ผลของ KRI สัญญาณเตือนภัย ระดับความเสี่ยงคงเหลือ และประสิทธิผลของมาตรการจัดการความเสี่ยง พร้อมวิเคราะห์สาเหตุเมื่อผลการดำเนินงานไม่เป็นไปตาม RA/RT หรือเป้าหมายที่กำหนด และรายงานต่อมหาวิทยาลัยตามรอบ ดังนี้

รอบการรายงาน	ระยะเวลาสะสมของผลการดำเนินงาน	กำหนดส่งรายงาน
รอบ 6 เดือน	1 ตุลาคม – 31 มีนาคม	เมษายน
รอบ 9 เดือน	1 ตุลาคม – 30 มิถุนายน	กรกฎาคม
รอบ 12 เดือน	1 ตุลาคม – 30 กันยายน	ตุลาคม
จัดทำแผนบริหารความเสี่ยงปีถัดไป	ทบทวนและจัดทำในช่วงตุลาคม-ธันวาคม	ธันวาคม

หมายเหตุ: รอบ 9 เดือนและรอบ 12 เดือนควรรายงานผลแบบสะสมตั้งแต่ต้นปีงบประมาณ มิใช่เฉพาะผลของเดือนเมษายน-มิถุนายน หรือกรกฎาคม-กันยายน เพื่อให้สามารถเปรียบเทียบแนวโน้มของ KRI และระดับความเสี่ยงได้อย่างถูกต้อง

กรณีพบว่า KRI เกิน Risk Tolerance ความเสี่ยงเพิ่มขึ้นอย่างมีนัยสำคัญ เกิดเหตุการณ์ร้ายแรง หรือ อาจส่งผลกระทบต่อมหาวิทยาลัยในวงกว้าง ให้ส่วนงานรายงานและยกระดับประเด็น (Risk Escalation) ต่อผู้บริหารหรือมหาวิทยาลัยโดยไม่ต้องรอรอบการรายงานปกติ พร้อมกำหนดมาตรการแก้ไขหรือมาตรการตอบสนองที่เหมาะสม

6. การทบทวน ปรับปรุง และยกระดับความเสี่ยง

ให้มหาวิทยาลัยและส่วนงาน/หน่วยงานทบทวนประเด็นความเสี่ยง ปัจจัยขับเคลื่อน ระดับความเสี่ยง RA/RT, KRI, EWS และมาตรการจัดการอย่างสม่ำเสมอ รวมทั้งทบทวนเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงยุทธศาสตร์ นโยบาย โครงสร้างองค์กร กฎหมาย เทคโนโลยี เศรษฐกิจ สังคม สิ่งแวดล้อม หรือ เกิดเหตุการณ์สำคัญที่อาจกระทบต่อการบรรลุวัตถุประสงค์

หากส่วนงานพบความเสี่ยงที่มีระดับสูงมาก มีผลกระทบข้ามส่วนงาน มีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญ หรือส่วนงานไม่สามารถบริหารจัดการได้ภายใต้อำนาจและทรัพยากรที่มีอยู่ ให้เสนอประเด็นดังกล่าวต่อมหาวิทยาลัยเพื่อพิจารณากระดับเป็นความเสี่ยงระดับมหาวิทยาลัยหรือกำหนดมาตรการร่วมในระดับองค์กร ทั้งนี้ ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการบริหารงานตามปกติ (Embedded Risk Management) และเป็นความรับผิดชอบร่วมกันของผู้บริหารและบุคลากรทุกระดับ เพื่อส่งเสริมวัฒนธรรมการบริหารความเสี่ยง (Risk Culture) และให้ข้อมูลความเสี่ยงถูกนำไปใช้ประกอบการวางแผน การตัดสินใจ การจัดสรรทรัพยากร และการปรับปรุงการดำเนินงานอย่างต่อเนื่อง อันจะนำไปสู่ การสร้างคุณค่า การปกป้องคุณค่า และความยั่งยืนของมหาวิทยาลัย

หลักการสำคัญสำหรับส่วนงาน ปีงบประมาณ พ.ศ. 2570

“ทุกส่วนงานต้องพิจารณาความเสี่ยงระดับมหาวิทยาลัยทั้ง 6 ประเด็น แต่ไม่จำเป็นต้องนำทั้ง 6 ประเด็นไปเป็นความเสี่ยงของส่วนงาน”

ให้เลือกเฉพาะประเด็นที่ **เกี่ยวข้องและมีนัยสำคัญต่อวัตถุประสงค์หรือเป้าหมายของส่วนงาน** มาจัดทำ Risk Register พร้อมทั้งค้นหาความเสี่ยงเฉพาะของส่วนงานเพิ่มเติม เพื่อให้เกิดการบริหารความเสี่ยงแบบ **Top-down + Bottom-up** และเชื่อมโยงความเสี่ยงตั้งแต่ระดับส่วนงานถึงระดับมหาวิทยาลัยอย่างเป็นระบบ

แนวปฏิบัติการบริหารความเสี่ยง มหาวิทยาลัยแม่โจ้ ประจำปีงบประมาณ พ.ศ. 2570 ได้ผ่านการพิจารณาและให้ความเห็นชอบจาก คณะกรรมการบริหารจัดการความเสี่ยงและการควบคุมภายใน มหาวิทยาลัยแม่โจ้ ในคราวประชุมครั้งที่ 1/2569 เมื่อวันที่ 17 สิงหาคม 2569 และผ่านการพิจารณาและให้ความเห็นชอบจาก คณะกรรมการบริหารมหาวิทยาลัย ในคราวประชุมครั้งที่ 14/2569 เมื่อวันที่ 26 สิงหาคม 2569 เพื่อใช้เป็นกรอบและแนวทางในการบริหารความเสี่ยงของมหาวิทยาลัยและส่วนงาน/หน่วยงาน ประจำปีงบประมาณ พ.ศ. 2570 ให้เป็นไปในทิศทางเดียวกันอย่างเป็นระบบและมีประสิทธิภาพ