แผนบริหารความเสี่ยงของมหาวิทยาลัยราชภัฏเพชรบุรี
ประจำปีงบประมาณ พ.ศ. 2569

ผ่านการอนุมัติเห็นชอบตามมติที่ประชุมสภามหาวิทยาลัยราชภัฏเพชรบุรี ครั้งที่ 6/2569
เมื่อวันที่ 15 มิถุนายน พ.ศ. 2569

แผนบริหารความเสี่ยงของมหาวิทยาลัยราชภัฏเพชรบุรี ประจำปีงบประมาณ พ.ศ. 2569

ลำดับที่	ประเด็นความเสี่ยง	การประเมินความเสี่ยง		
		โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ความไม่ปลอดภัยจากสภาวะวิกฤตฉุกเฉิน	4	3	12 (สูง)
2	การหยุดชะงักและการรั่วไหลของข้อมูลในระบบสารสนเทศ	3	3	9 (สูง)

<u>ประเด็นความเสี่ยงที่ 1 : ความไม่ปลอดภัยจากสภาวะวิกฤตฉุกเฉิน</u>

1.1 ยุทธศาสตร์ 6 การขับเคลื่อนมหาวิทยาลัยสู่ความเป็นดิจิทัล และยกระดับประสิทธิภาพการดำเนินงาน (Driving Digital University and Leverage Performance Efficiency)

1.2 กระบวนการปฏิบัติงาน/โครงการ/กิจกรรม : ยกระดับมหาวิทยาลัยสีเขียว

1.3 วัตถุประสงค์ :

1.3.1 เพื่อป้องกันและรับมือต่อเหตุการณ์ที่ไม่ได้คาดการณ์ไว้ล่วงหน้าได้อย่างมีประสิทธิภาพ

1.3.2 เพื่อลดอัตราความเสี่ยงต่อความผิดพลาด ติดขัดต่อการปฏิบัติงานของบุคลากร ผู้ใช้บริการและนักศึกษา

1.3.3 เพื่อสร้างความมั่นใจในเรื่องความปลอดภัยจากเหตุความไม่ปลอดภัยแก่นักศึกษา บุคลากรและผู้มาใช้บริการ

1.3.4 เพื่อรองรับการปฏิบัติงานของบุคลากรและการเรียนการสอนของอาจารย์ได้อย่างเต็มประสิทธิภาพ

1.4 ผู้กำกับดูแล : ผู้ช่วยอธิการด้านเทคโนโลยีสารสนเทศ

1.5 หน่วยงานผู้รับผิดชอบ : สำนักงานอธิการบดี

1.6 ประเภทความเสี่ยง:

1.6.1 O: Operational Risk (ด้านปฏิบัติงาน)

1.6.2 H: Hazard Risk (ด้านความปลอดภัย จากอันตรายต่อชีวิตและทรัพย์สิน)

1.7 แหล่งที่มา: ☑ ภายใน ☑ ภายนอก

1.8 กลยุทธ์: ☑ ควบคุม

1.9 การประเมินความเสี่ยง:

1.9.1 โอกาส (Likelihood): 4

1.9.2 ผลกระทบ (Impact): 3

1.9.3 ระดับความเสี่ยง (Degree of Risk) : 4 x 3 = 12 (สูง)

1.10 เหตุผลและสถิติการเกิดเหตุการณ์ที่ผ่านมา ภายในปีงบประมาณ พ.ศ. 2568

1.10.1 ประเทศไทยเกิดเหตุการณ์แผ่นดินไหว ในวันที่ 28 มีนาคม 2568 ขนาดประมาณ 7.7-8.2 แมกนิจูด เกิดความเสียหายต่ออาคารและโครงสร้างพื้นฐาน และมีเหตุการณ์ตึกถล่มระหว่างการก่อสร้าง ส่งผลให้มีผู้เสียชีวิตและบาดเจ็บจำนวนมาก และแรงสั่นสะเทือนรับรู้ถึงจังหวัดเพชรบุรี

1.10.2 ไม่มีอุบัติเหตุและผู้ได้รับความเสียหายในการใช้อาคารของมหาวิทยาลัยราชภัฏเพชรบุรี

1.10.3 เกิดการขัดข้องจากการจ่ายกระแสไฟฟ้า จำนวน 16 ครั้ง

1.10.4 ลิฟต์เกิดการขัดข้อง จำนวน 2 ครั้ง

1.10.5 เกิดอุบัติเหตุจราจรบนท้องถนน ภายในและบริเวณใกล้เคียงมหาวิทยาลัย จำนวน 3 ครั้ง

1.11 ตัวชี้วัดความเสี่ยง (KPI) :

KPI	Risk Limit (เพดานความเสี่ยง)	
	Risk Appetite **(ระดับความเสี่ยงที่ยอมรับได้)**	Risk Tolerance **(ระดับความเบี่ยงเบนจากระดับที่ยอมรับได้)**
1	อัตราการเกิดอุบัติภัยร้ายแรงหรือสภาวะวิกฤตที่ส่งผลกระทบต่อชีวิตและทรัพย์สินส่วนรวมในพื้นที่มหาวิทยาลัยเป็น ร้อยละ 0	อัตราการเกิดอุบัติภัยร้ายแรงหรือสภาวะวิกฤตที่ส่งผลกระทบต่อชีวิตและทรัพย์สินส่วนรวมในพื้นที่มหาวิทยาลัยเป็น ร้อยละ 0 อาจมีผู้ได้รับความเสียหายในระดับต้น เช่น เป็นแผลเล็กน้อย หรือเสียหายทรัพย์สินไม่เกิน 1,000 บาท

1.12 เกณฑ์การประเมินระดับความเสี่ยง: โอกาส (Likelihood) และผลกระทบ (Impact)

1.12.1 โอกาส (Likelihood)

ระดับ	โอกาสที่จะเกิด
5	โอกาสเกิดมากกว่าร้อยละ 90 หรือเกิดขึ้นอย่างน้อย 1 ครั้งภายในระยะเวลา 1 เดือน
4	โอกาสเกิดร้อยละ 70-90 หรือเกิดขึ้นอย่างน้อย 1 ครั้งภายในระยะเวลา 2-4 เดือน
3	โอกาสเกิดร้อยละ 40-69 หรือเกิดขึ้นอย่างน้อย 1 ครั้งภายในระยะเวลา 5-7 เดือน
2	โอกาสเกิดร้อยละ 20-39 หรือเกิดขึ้นอย่างน้อย 1 ครั้งภายในระยะเวลา 8-10 เดือน
1	โอกาสเกิดร้อยละ 10-19 หรือเกิดขึ้นอย่างน้อย 1 ครั้งภายในระยะเวลา 11-12 เดือน

1.12.2 ผลกระทบ (Impact)

ระดับ	ผลกระทบที่จะเกิด
5	มีผลกระทบต่อร่างกาย หรือทรัพย์สิน หรือชื่อเสียงขององค์กร บุคลากรและนักศึกษา ในระดับรุนแรงมาก (มีการบาดเจ็บต้องพักรักษาตัวในโรงพยาบาล ทุพพลภาพ หรือ เสียชีวิต)
4	มีผลกระทบต่อร่างกาย หรือทรัพย์สิน หรือชื่อเสียงขององค์กร บุคลากรและนักศึกษา ในระดับรุนแรง (มีการบาดเจ็บที่ต้องได้รับการรักษาทางการแพทย์)
3	มีผลกระทบต่อร่างกาย หรือทรัพย์สิน หรือชื่อเสียงขององค์กร บุคลากรและนักศึกษา ในระดับปานกลาง (มีการบาดเจ็บเล็กน้อยในระดับได้รับการปฐมพยาบาล)
2	มีผลกระทบต่อร่างกาย หรือทรัพย์สิน หรือชื่อเสียงขององค์กร บุคลากรและนักศึกษา ในระดับน้อย (มีการบาดเจ็บเล็กน้อยไม่ถึงระดับปฐมพยาบาล
1	ไม่มีผลกระทบต่อร่างกาย หรือทรัพย์สิน หรือชื่อเสียงขององค์กร บุคลากรและนักศึกษา (ไม่เกิดการบาดเจ็บ)

1.13 การวิเคราะห์ภัยภายนอกที่ควบคุมไม่ได้และความเปราะบางภายใน (Hazard and Vulnerability)

1.13.1 Hazard (ภัยภายนอกที่ควบคุมไม่ได้):

1) ภัยธรรมชาติ: ปัญหาน้ำท่วมฉับพลัน หรือน้ำไหลหลากจากแม่น้ำเพชรบุรีในช่วงฤดูมรสุม ซึ่งเป็นปัจจัยภูมิศาสตร์ที่เลี่ยงยาก

2) อุบัติภัยภายนอกและภัยคุกคามทางสังคม: เหตุเพลิงไหม้จากชุมชนรอบข้าง การก่อเหตุทะเลาะวิวาทของวัยรุ่นภายนอกที่อาจลุกลามเข้ามาในพื้นที่มหาวิทยาลัย หรืออุบัติเหตุจากถนนสายหลักรอบมหาวิทยาลัย

1.13.2 Vulnerability (ความเปราะบางภายใน):

1) โครงสร้างกายภาพ (Physical Vulnerability): อาคารเรียนเก่าบางแห่งไม่มีทางหนีไฟที่ได้มาตรฐาน

2) ระบบและการสื่อสาร (Systemic Vulnerability): ไม่มีระบบแจ้งเตือนภัยฉุกเฉินแบบส่งตรงถึงมือถือ (SMS Broadcast หรือ Line Alert) ของนักศึกษาและบุคลากรทุกคนพร้อมกันอย่างทันท่วงทีเมื่อเกิดเหตุ

3) ความพร้อมของคน (Cognitive Vulnerability): บุคลากรและนักศึกษาขาดการฝึกซ้อมอพยพหนีไฟหรือเผชิญเหตุฉุกเฉินอย่างจริงจัง

1.13 แนวทางการจัดการความเสี่ยง :

ปัจจัยเสี่ยง	แนวทางการจัดการความเสี่ยง
1. ความไม่ปลอดภัย จากการวางระบบสาธารณูปโภคพื้นฐาน	1.1 จัดทำแผนตรวจสอบทางวิศวกรรม สำหรับอาคารเรียนและอาคารปฏิบัติการที่มีอายุการใช้งานสูง โดยเฉพาะระบบทางหนีไฟ ไฟส่องสว่างฉุกเฉิน และถังดับเพลิงประจำคณะ 1.2 จัดตั้งระบบบำรุงรักษาเชิงป้องกัน สำหรับระบบสายล่อฟ้า ระบบกราวด์ดิ้ง และระบบจำหน่ายกระแสไฟฟ้าแรงสูง โดยประสานความร่วมมือกับการไฟฟ้าส่วนภูมิภาคในการตรวจสอบวงรอบทุก 6 เดือน 1.3 ติดตั้งระบบพลังงานแสงอาทิตย์ (Solar Rooftop) บนหลังคาอาคารส่วนกลางและอาคารเรียนคณะ เพื่อเป็นแหล่งพลังงานสำรองและขับเคลื่อนเป้าหมายมหาวิทยาลัยสีเขียว 1.4 มีการทำป้ายประชาสัมพันธ์ในการประหยัดทรัพยากร เช่น ไฟฟ้า ประปา แอร์ 1.5 มีการทบทวนแผนการจ้างเจ้าหน้าที่รักษาความปลอดภัยให้มีความรัดกุมและเชี่ยวชาญมากยิ่งขึ้น
2. การเกิดอัคคีภัย	2.1 จัดทำแผนป้องกันและระงับอัคคีภัยระดับมหาวิทยาลัย และบังคับใช้ให้ทุกหน่วยงาน จัดการฝึกซ้อมอพยพหนีไฟอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมทั้งบุคลากรและนักศึกษา 2.2 ตรวจสอบระบบการจ่ายกระแสไฟฟ้าจากการไฟฟ้าส่วนภูมิภาค วงรอบ 6 เดือนต่อครั้ง 2.2 การใช้ระบบผลิตไฟฟ้าพลังงานแสงอาทิตย์บนหลังคา (Solar Rooftop) เพื่อลดการใช้ไฟฟ้า และเข้าสู่มหาวิทยาลัยสีเขียว
3. ด้านความปลอดภัย 3.1 การระบาดของโรคระบาดใหม่ 3.2 อุบัติเหตุจากการปฏิบัติงาน เช่น การตกจากที่สูง 3.3 อุบัติเหตุทางธรรมชาติ เช่น ฟ้าผ่า อุทกภัย วาตภัย	3.1 พัฒนาและปรับปรุงระบบระบายน้ำภายในมหาวิทยาลัยเพื่อรองรับน้ำหลากจากแม่น้ำเพชรบุรี พร้อมติดตั้งเครื่องสูบน้ำสำรองในจุดลุ่มต่ำ เช่น บริเวณลานจอดรถใต้ดินหรืออาคารเรียนรวม 3.2 พัฒนาระบบปรับอากาศและระบายอากาศในห้องเรียนรวมและห้องปฏิบัติการขนาดใหญ่ โดยติดตั้ง

ปัจจัยเสี่ยง	แนวทางการจัดการความเสี่ยง
3.4 อุบัติเหตุจราจรบนท้องถนนภายในและบริเวณใกล้เคียงมหาวิทยาลัย	แผ่นกรองอากาศประสิทธิภาพสูง หรือระบบฆ่าเชื้อเพื่อรองรับสถานการณ์โรคระบาดใหม่ 3.3 จัดทำข้อตกลงความร่วมมือ (MOU) กับโรงพยาบาลในพื้นที่ในการส่งต่อผู้ป่วยและบริหารจัดการงบประมาณสำรองฉุกเฉินทางการแพทย์ 3.4 สนับสนุนให้ใช้รถสวัสดิการของมหาวิทยาลัยแทนรถส่วนตัวเพื่อลดความหนาแน่นของการจราจร 3.5 วิเคราะห์งานทุกขั้นตอนก่อนเริ่ม เช่น การซ่อมหลังคาต้องประเมินความแข็งแรงของโครงสร้างก่อน 3.6 ติดตั้งระบบกระจายเสียงและส่งข้อความแจ้งเตือนภัย เข้ามือถือทุกคนในพื้นที่เมื่อเรดาร์ตรวจพบกลุ่มฝนหรือความเสี่ยงฟ้าผ่า 3.7 แยกเลนรถจักรยานและทางเดินเท้าออกจากเลนรถยนต์อย่างชัดเจน 3.8 ใช้กล้อง CCTV พร้อมระบบ AI ตรวจจับผู้ที่ไม่สวมหมวกนิรภัยหรือขับรถย้อนศร เพื่อส่งหนังสือเตือนหรือตัดคะแนนวินัย 3.8 มหาวิทยาลัยจัดทำประกันอุบัติเหตุกลุ่มให้นิสิตทุกคนเพื่อรองรับค่ารักษาพยาบาล ผ่านกลไกการลงทะเบียน
4. ด้านนักศึกษาและบุคลากร 4.1 สุขภาพจิต 4.2 การหลอกลวงจากมิจฉาชีพ	4.1 บูรณาการเนื้อหาการรู้เท่าทันสื่อและภัยไซเบอร์เข้าไปในรายวิชาศึกษาทั่วไป หรือกิจกรรมปฐมนิเทศนักศึกษาใหม่ เพื่อป้องกันการตกเป็นเหยื่อมิจฉาชีพและการพนันออนไลน์ 4.2 สร้างตระหนัก และความเข้าใจให้เกี่ยวกับปัญหาที่จะเกิดขึ้นและความตระหนักในความรับผิดชอบส่วนบุคคล 4.3 มีช่องทางการให้บริการคำปรึกษา และศูนย์ให้คำปรึกษา (PBRU Wellness Mind Clinic)

<u>ประเด็นความเสี่ยงที่ 2 : การหยุดชะงักและการรั่วไหลของข้อมูลในระบบสารสนเทศ</u>

2.1 ยุทธศาสตร์ 6 การขับเคลื่อนมหาวิทยาลัยสู่ความเป็นดิจิทัล และยกระดับประสิทธิภาพการดำเนินงาน (Driving Digital University and Leverage Performance Efficiency)

2.2 กระบวนการปฏิบัติงาน/โครงการ/กิจกรรม :

2.2.1 ยกระดับโครงสร้างพื้นฐานดิจิทัลที่มั่งคง ปลอดภัยและยั่งยืน

2.2.2 Digitalizing and Streaming in Government

2.3 วัตถุประสงค์ :

2.3.1 เพื่อป้องกันการเกิดความผิดพลาดของการปฏิบัติงาน

2.3.2 เพื่อส่งเสริมความรู้และความเข้าใจของบุคลากรให้เท่าทันต่อการเปลี่ยนแปลงของ กฎระเบียบข้อบังคับต่าง ๆ

2.4 ผู้กำกับดูแล : ผู้ช่วยอธิการบดีด้านเทคโนโลยีดิจิทัล

2.5 หน่วยงานผู้รับผิดชอบ : สำนักงานอธิการบดี

2.6 ประเภทความเสี่ยง:

2.6.1 O: Operational Risk (ด้านปฏิบัติงาน)

2.6.2 T: Technological Factors (ความเสี่ยงด้านการเปลี่ยนแปลงเทคโนโลยี)

2.7 แหล่งที่มา: ☑ ภายใน ☑ ภายนอก

2.8 กลยุทธ์: ☑ ควบคุม

2.9 การประเมินความเสี่ยง:

2.9.1 โอกาส (Likelihood): 3

2.9.2 ผลกระทบ (Impact): 3

2.9.3 ระดับความเสี่ยง (Degree of Risk) : 3 x 3 = 9 (สูง)

2.10 เหตุผลและสถิติการเกิดเหตุการณ์ที่ผ่านมา ภายในปีงบประมาณ พ.ศ. 2568

2.10.1 เกิดการโจมตีในระบบสารสนเทศสำเร็จหรือติดมัลแวร์ จำนวน 16 ครั้ง

2.10.2 เกิดการขัดข้องของระบบสารสนเทศที่มีผลกระทบต่อการปฏิบัติงาน (นานเกินระยะเวลา 30 นาที) จำนวน 3 ครั้ง

2.11 ตัวชี้วัดความเสี่ยง (KPI) :

KPI	Risk Limit (เพดานความเสี่ยง)	
	Risk Appetite (ระดับความเสี่ยงที่ยอมรับได้)	Risk Tolerance (ระดับความเบี่ยงเบนจากระดับที่ยอมรับได้)
1	ความพร้อมใช้งานของระบบสารสนเทศหลัก ไม่น้อยกว่า ร้อยละ 100 และไม่มีเหตุการณ์ข้อมูลนักศึกษารั่วไหลสู่สาธารณะ	ความพร้อมใช้งานของระบบสารสนเทศหลัก ไม่น้อยกว่า ร้อยละ 99 และไม่มีเหตุการณ์ข้อมูลนักศึกษารั่วไหลสู่สาธารณะ

2.12 เกณฑ์การประเมินระดับความเสี่ยง: โอกาส (Likelihood) และผลกระทบ (Impact)

2.12.1 โอกาส (Likelihood)

ระดับ	โอกาสที่จะเกิด
5	ถูกโจมตีทางระบบสารสนเทศ จำนวน มากกว่า 21 ครั้ง/ปี และไม่สามารถป้องกันได้
4	ถูกโจมตีทางระบบสารสนเทศ จำนวน 20 ครั้ง/ปี และไม่สามารถป้องกันได้
3	ถูกโจมตีทางระบบสารสนเทศ จำนวน 15 ครั้ง/ปี และไม่สามารถป้องกันได้
2	ถูกโจมตีทางระบบสารสนเทศ จำนวน 10 ครั้ง/ปี ไม่สามารถป้องกันได้
1	ถูกโจมตีทางระบบสารสนเทศ จำนวน 5 ครั้ง/ปี สามารถป้องกันได้

2.12.2 ผลกระทบ (Impact)

ระดับ	ผลกระทบที่จะเกิด
5	ระบบงานสำคัญเสียหาย หรือหยุดชะงัก ไม่สามารถให้บริการเป็นระยะเวลามากกว่า 1 ชั่วโมง ส่งผลต่อผู้ใช้งานทุกคน/ไม่สามารถกู้คืนข้อมูลได้
4	ระบบงานสำคัญบางระบบหยุดชะงัก หรือบางฟังก์ชันไม่สามารถใช้งานได้เป็นระยะเวลา 1 ชั่วโมง ไม่สามารถแก้ปัญหาได้เองต้องให้ผู้เชี่ยวชาญจากภายนอกแก้ไข
3	ระบบงานสนับสนุนหยุดชะงัก มีผลต่อการดำเนินการ มากกว่า 30 นาที ส่งผลต่อผู้ใช้งานบางส่วน
2	ระบบงานสนับสนุนหยุดชะงัก น้อยกว่า 30 นาที มีผลต่อการดำเนินการ สามารถแก้ปัญหาได้เอง
1	ระบบงานทุกระบบใช้งานได้ตามปกติ

2.13 ภัยภายนอกที่ควบคุมไม่ได้และความเปราะบางภายใน (Hazard and Vulnerability)

2.13.1 Hazard (ภัยภายนอกที่ควบคุมไม่ได้):

1) Cybersecurity Attacks: การโจมตีของ Hacker ข้ามชาติด้วยมัลแวร์เรียกค่าไถ่ (Ransomware), การส่งลิงก์หลอกลวง (Phishing) นามมหาวิทยาลัย, หรือการเข้ามาแอบดึงข้อมูลเกรด/ฐานข้อมูลส่วนตัวของนักศึกษาเพื่อไปขายให้คอลเซ็นเตอร์

2) Infrastructure Failure: ภัยธรรมชาติน้ำท่วมห้องเครื่องเซิร์ฟเวอร์ หรือภัยจากการจ่ายกระแสไฟฟ้าที่ดับกะทันหัน ส่งผลให้ฮาร์ดดิสก์หลักชำรุด

2.13.2 Vulnerability (ความเปราะบางภายใน):

1) ด้านเทคโนโลยีระบบ (Technical Vulnerability):

- การใช้ระบบปฏิบัติการและซอฟต์แวร์หลังบ้านที่หมดอายุการสนับสนุน (Legacy Systems/Out-of-date Software)
- ไม่มีระบบสำรองข้อมูลภายนอกแบบออฟไลน์ (Offsite Cold Backup) ทำให้หากโดนไวรัสเรียกค่าไถ่ จะไม่สามารถย้อนคืนระบบได้

2) ด้านพฤติกรรมมนุษย์ (Behavioral Vulnerability):

- บุคลากรและอาจารย์ใช้รหัสผ่านที่คาดเดาง่าย และนำอีเมลมหาวิทยาลัยไปสมัครบริการบันเทิงภายนอก
- การส่งต่อข้อมูลคะแนน นิสิตนักศึกษา หรือข้อมูลพัสดุผ่านแอปลิงก์ทั่วไป (เช่น Google Drive ส่วนตัว) โดยไม่จำกัดการเข้าถึง (ละเมิดกฎหมาย PDPA โดยไม่ตั้งใจ)

2.14 แนวทางการจัดการความเสี่ยง :

ปัจจัยเสี่ยง	แนวทางการจัดการความเสี่ยง
1. ภัยคุกคามจากระบบเทคโนโลยีสารสนเทศ	1.1 ปรับปรุงระบบเครือข่ายความปลอดภัยขั้นสูง ติดตั้งและอัปเดตระบบ Firewall, Antivirus และระบบตรวจจับการบุกรุก ในระดับแม่ข่ายของมหาวิทยาลัย 1.2 กำหนดนโยบายมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน บังคับใช้ระบบการยืนยันตัวตนแบบหลายปัจจัย สำหรับอาจารย์และบุคลากรในการเข้าถึงระบบฐานข้อมูลภายในและระบบนักศึกษา 1.3 อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดเพื่อลดช่องโหว่ของระบบ 1.4 จัดให้มี การสำรองข้อมูลและทดสอบการกู้คืนระบบ 1.5 จัดทำหลักสูตรฝึกอบรมและทดสอบความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ภาคบังคับสำหรับบุคลากรสายวิชาการและสายสนับสนุนทุกคน

ปัจจัยเสี่ยง	แนวทางการจัดการความเสี่ยง
2. ความมั่นคงของระบบสารสนเทศ	2.1 จัดทำแผนบริหารความต่อเนื่องทางธุรกิจด้านไอที และกำหนดมาตรการสำรองข้อมูลตามหลัก 3-2-1 โดยให้มีการจัดทำข้อมูลสำรองภายนอกสถาบัน หรือระบบคลาวด์ที่ปลอดภัย 2.2 พัฒนาระบบโครงสร้างพื้นฐานด้าน IT ให้มีความเสถียรและเพียงพอ เช่น Server, Network และ Cloud Infrastructure 2.3 กำหนดมาตรฐานการบริหารจัดการระบบ เช่น การตรวจสอบประสิทธิภาพของระบบ และการบำรุงรักษาเชิงป้องกัน 2.4 กำหนด สิทธิ์การเข้าถึงระบบ ตามระดับหน้าที่ความรับผิดชอบ 2.5 ประเมินความเสี่ยงของระบบสารสนเทศเป็นระยะ และปรับปรุงระบบให้รองรับปริมาณผู้ใช้งานที่เพิ่มขึ้น และรับการประเมินจากหน่วยงานภายนอกที่มีความเชี่ยวชาญ
3. ความปลอดภัยของข้อมูลส่วนบุคคล (PDPA)	3.1 ประกาศใช้แผนแม่บทและนโยบาย PDPA ของมหาวิทยาลัย จัดทำระบบ Data Classification แยกแยะระดับสิทธิ์ความลับของข้อมูลนักศึกษาและบุคลากร 3.2 จัดทำแนวปฏิบัติการส่งและเผยแพร่คะแนน หรือผลการเรียนของนักศึกษา โดยห้ามไม่ให้อาจารย์ผู้สอนใช้แอปพลิเคชันหรือลิงก์สาธารณะที่ไม่ได้จำกัดสิทธิ์การเข้าถึง 3.3 กำหนด กระบวนการขอความยินยอมและการใช้ข้อมูลตามวัตถุประสงค์ที่กำหนด 3.4 ใช้มาตรการรักษาความปลอดภัยของข้อมูล เช่น การเข้ารหัสข้อมูลและการควบคุมสิทธิ์การเข้าถึงข้อมูล 3.5 จัดทำขั้นตอนการแจ้งเหตุข้อมูลรั่วไหล เพื่อให้สามารถรายงานและแก้ไขเหตุการณ์ได้อย่างรวดเร็ว

ข้อเสนอแนะของคณะกรรมการบริหารความเสี่ยง

1. ประเด็นการไม่ปฏิบัติตามระเบียบ อันอาจก่อให้เกิดข้อบกพร่องทางกฎหมาย ซึ่งมีการประเมินความเสี่ยงอยู่ในระดับต่ำ เพื่อป้องกันไม่ให้เกิดความประมาทหรือละเลย แนะนำให้การออกกฎหมายหรือการกระทำที่เกี่ยวข้องใด ๆ ควรผ่านฝ่ายกฎหมายตรวจสอบก่อนเสมอ ซึ่งเป็นความเสี่ยงที่ต้องเฝ้าระวังอย่างสม่ำเสมอ และควบคุมให้องค์กรเข้าใจไปในทิศทางเดียวกัน

2. เห็นควรให้หน่วยงานที่เกี่ยวข้องกำกับดูแลและเร่งรัดการดำเนินงานให้เป็นไปตามแผนกลยุทธ์ทางการเงิน แผนการเบิกจ่าย และแผนการจัดหารายได้อย่างเคร่งครัด พร้อมทั้งจัดให้มีระบบติดตามและรายงานผลการบริหารจัดการการเงินการคลังอย่างสม่ำเสมอ เพื่อเฝ้าระวังและลดความเสี่ยงจากการไม่บรรลุผลสำเร็จตามเป้าหมายของแผนฯ ที่กำหนดไว้