แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศคลังดิจิทัล
สำนักบรรณสารสนเทศ ปี พ.ศ. 2568 - 2570

คำนำ

เพื่อให้ระบบสารสนเทศคลังดิจิทัลของสำนักบรรณสารสนเทศมีความพร้อมใช้งาน มีประสิทธิภาพ และเกิดประสิทธิผลสูงสุดทั้งส่วนการปฏิบัติงานและการให้บริการสารสนเทศ มีความต่อเนื่องของให้บริการทั้งในปัจจุบันและอนาคต สนับสนุนระบบการเรียนการสอนของมหาวิทยาลัย ตลอดจนให้บริการผู้ใช้ที่เป็นนักศึกษา คณาจารย์ บุคลากร และผู้สนใจทั่วไป ที่มุ่งสู่การเป็นมหาวิทยาลัยเปิดที่ใช้ระบบการเรียนการสอนทางไกลแบบดิจิทัล สำนักบรรณสารสนเทศจึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศคลังดิจิทัล ประจำปี พ.ศ. 2568 ขึ้นเพื่อบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศคลังดิจิทัลในมิติต่างๆ ไม่ให้เกิดขึ้นกับข้อมูลดิจิทัล หรือเกิดผลกระทบน้อยที่สุด สามารถใช้เป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยระบุความเสี่ยง วิเคราะห์ความเสี่ยง และกำหนดแนวทาง หรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง เพื่อลดผลกระทบ ผลเสีย หรือความสูญเสียที่จะเกิดขึ้นทั้งทางตรงและทางอ้อมต่องานด้านเทคโนโลยีของสำนักบรรณสารสนเทศต่อไป

กัลยาณี ศุภดิษฐ์
บรรณารักษ์ชำนาญการพิเศษ
รักษาการในตำแหน่งหัวหน้าศูนย์เทคโนโลยีบรรณสารสนเทศ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศคลังดิจิทัล สำนักบรรณสารสนเทศ ปี พ.ศ. 2568 – 2570

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นกลยุทธ์สำคัญของการดูแลระบบเทคโนโลยีสารสนเทศคลังดิจิทัล สำนักบรรณสารสนเทศ ที่จะช่วยให้การบริหารระบบและการตัดสินใจและการวางแผนด้านต่างๆ อาทิ ด้านการกำหนดกลยุทธ์ ด้านการติดตามควบคุม ด้านการวัดผลการปฏิบัติงาน และด้านการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพ ช่วยลดการสูญเสียและโอกาสที่จะทำให้เกิดความเสียหายต่อระบบ และส่งผลกระทบต่องานบริการของห้องสมุดและมหาวิทยาลัย สำนักบรรณสารสนเทศจึงจำเป็นต้องการการจัดการความเสี่ยงอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อระบบ และความเสี่ยงใดบ้างที่มีโอกาสจะเกิดขึ้น การจัดลำดับความสำคัญของปัจจัยเสี่ยง และการกำหนดแนวทางในการจัดการความเสี่ยง โดยคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงนั้นๆ อย่างเหมาะสม

วัตถุประสงค์

1. เพื่อเตรียมความพร้องรองรับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีคลังดิจิทัลของสำนักบรรณสารสนเทศ
2. เพื่อเป็นแนวทางในการดูแลรักษาความปลอดภัยของระบบเทคโนโลยีคลังดิจิทัลให้มีความเสถียรและมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานด้านระบบเทคโนโลยีคลังดิจิทัลเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขปัญญาได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติขึ้น

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศคลังดิจิทัล สำนักบรรณสารสนเทศ เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยง ที่มีผลกระทบต่อระบบคลังสารสนเทศดิจิทัลของสำนักบรรณสารสนเทศ รวมทั้งการบริหารและการจัดการความเสี่ยง รวมทั้งการดำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมป้องกัน เพื่อลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการตามหลักเกณฑ์อย่างเหมาะสม ครอบคลุม 5 ขั้นตอน คือ

กระบวนการบริหารความเสี่ยงระบบเทคโนโนโลยีคลังดิจิทัล สำนักบรรณสารสนเทศ

1. การระบุความเสี่ยง

เป็นกระบวนการที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศคลังดิจิทัล และสำนักคอมพิวเตอร์ของมหาวิทยาลัย ร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้อง เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ทั้งนี้ สามารถแบ่งความเสี่ยงออกเป็น 5 ด้าน ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งเป็น

1.1) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)

1.2) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง

1.3) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ

1.4) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า

1.5) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง

2) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งเป็น

2.1) ความเสี่ยงจากผู้ดูแลระบบ

2.2) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย

3) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งเป็น

3.1) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

3.2) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์

3.3) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร

3.4) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายในและ ภายนอกสถานที่ทำงาน

3.5) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

3.6) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)

3.7) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น

4.1) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

4.2) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

4.3) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)

5) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น

5.1) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน

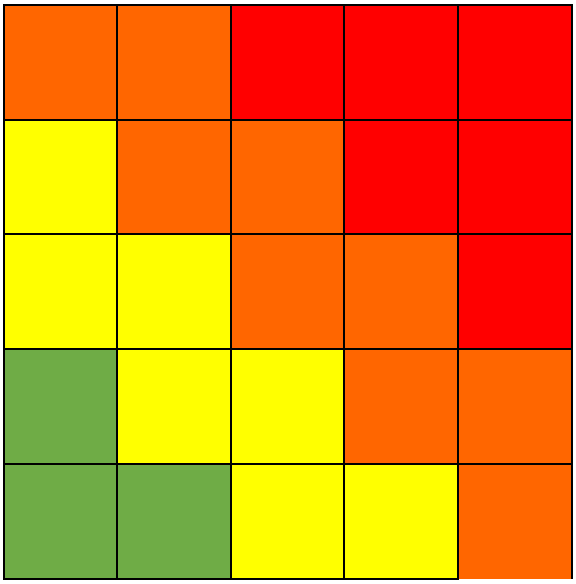
5.2) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล

5.3) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

2 การวิเคราะห์และประเมินค่าความเสี่ยง

การวิเคราะห์และประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และ ประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ระดับของผลกระทบที่เกิดขึ้น



สูงมาก
สีแดง ความเสี่ยงสูงมาก
ค่าระหว่าง 15 - 25

สูง
สีส้ม ความเสี่ยงสูง
ค่าระหว่าง 8 - 14

ปานกลาง
สีเหลือง ความเสี่ยงปานกลาง
ค่าระหว่าง 4 - 7

ต่ำ
สีเขียว ความเสี่ยงต่ำ
ค่าระหว่าง 1 - 3

แผนภูมิความเสี่ยง (Risk Map)

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
1	**ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม**				
1.1	ความเสี่ยงจากการเกิดไฟไหม้ห้อง Server	1	5	5	ปานกลาง
1.2	ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้อง Server	4	5	20	สูงมาก
1.3	ความเสี่ยงจากอุณหภูมิและความชื้นของห้อง Server ผิดปกติ	4	2	8	สูง
1.4	ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์ เครือข่ายและระบบไฟฟ้า	1	3	3	ต่ำ
1.5	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	1	3	3	ต่ำ

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
2	**ความเสี่ยงด้านบุคลากร**				
2.1	ความเสี่ยงจากผู้ดูแลระบบ	1	3	3	ต่ำ
2.2	ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และ ระบบเครือข่าย	1	3	3	ต่ำ
3	**ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย**				
3.1	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	4	5	20	สูงมาก
3.2	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	1	5	5	ปานกลาง
3.3	ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบ เครือข่ายจากภายในและภายนอกองค์กร	2	5	10	สูง
3.4	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินทราเน็ตและอินเทอร์เน็ตภายในและภายนอก สถานที่ทำงาน	1	2	2	ต่ำ
3.5	ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)	1	3	3	ต่ำ
3.6	ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	1	2	2	ต่ำ
3.7	ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)	1	1	1	ต่ำ
4	**ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์**				
4.1	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	2	5	10	สูง

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
4.2	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรม ประยุกต์ภายในองค์กร	1	1	1	ต่ำ
4.3	ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	1	4	4	ปานกลาง
5	**ความเสี่ยงด้านระบบฐานข้อมูล**				
5.1	ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็น ปัจจุบัน และไม่ครบถ้วน	2	2	4	ปานกลาง
5.2	ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถ กู้คืนระบบฐานข้อมูล	1	5	5	ปานกลาง
5.3	ความเสี่ยงจากการโจรกรรมระบบฐานข้อมูล	1	3	3	ต่ำ

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีดิจิทัล สำนักบรรณสารสนเทศสามารถสรุป ความเสี่ยงออกเป็น 4 ระดับ เรียงตามลำดับค่าความเสี่ยง ดังนี้

1) ความเสี่ยงระดับสูงมาก แบ่งออกเป็น

1.1) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้อง Server

1.2) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย

2) ความเสี่ยงระดับสูง แบ่งออกเป็น

2.1) ความเสี่ยงจากอุณหภูมิและความชื้นของห้อง Server ผิดปกติ

2.2) ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบ เครือข่ายจากภายในและภายนอกองค์กร

2.3) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

3) ความเสี่ยงระดับปานกลาง แบ่งออกเป็น

3.1) ความเสี่ยงจากการเกิดไฟไหม้ห้อง Server

3.2) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ มัลแวร์

3.3) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็น ปัจจุบัน และไม่ครบถ้วน

3.4) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถ กู้คืนระบบฐานข้อมูล

3.5) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ มัลแวร์

3.6) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแล ระบบโดยผู้รับจ้างภายนอก (Outsource)

4) ความเสี่ยงระดับต่ำ แบ่งออกเป็น

4.1) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า

4.2) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน

4.3) ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย (Black List)

4.4) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่าน เครือข่าย (VDO Conference)

4.5) ความเสี่ยงจากการใช้งานระบบโทรศัพท์ (IP Phone)

4.6) ความเสี่ยงจากการโจรกรรมระบบฐานข้อมูล

4.7) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง

4.8) ความเสี่ยงจากผู้ดูแลระบบ

4.9) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และ ระบบเครือข่าย

3 การบริหารความเสี่ยง

เป็นการวางแผนเพื่อกำหนดแนวทางและมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน มีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้น เพื่อลดและตรวจหาความเสี่ยงที่ได้มีการประเมินเอาไว้ การบริหารความเสี่ยงแบ่งออกได้เป็น 5 ประเภท คือ

3.1 การตรวจสอบเพื่อการป้องกัน เป็นวิธีการควบคุมโดยการตรวจสอบระบบด้านต่างๆ เป็นประจำ เพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การตรวจสอบช่องโหว่ (Vulnerability Scanning) การประเมินความเสี่ยงในกระบวนการทำงานและระบบ เพื่อค้นหาและแก้ไขปัญหาก่อนที่จะเกิดการบุกรุกหรือความล้มเหลวของระบบ

3.2 การติดตั้งระบบ การติดตั้งเครื่องมือและระบบเพื่อสร้างชั้นความปลอดภัยสำหรับข้อมูลและเครือข่าย เป็นการสร้างอุปสรรคเพิ่มเติมที่ช่วยลดโอกาสในการโจมตีและการบุกรุกจากภายในและภายนอกองค์กร

3.3 การกำหนดนโยบาย นโยบายเป็นกรอบกำกับการดำเนินงานที่กำหนดวิธีการจัดการกับความเสี่ยง เช่น การกำหนดมาตรการความปลอดภัยไซเบอร์ การเข้าถึงข้อมูล หรือการใช้งานซอฟต์แวร์ โดยนโยบายเหล่านี้ต้องมีความชัดเจนและสอดคล้องกับกฎหมายหรือมาตรฐานที่เกี่ยวข้อง

3.4 การควบคุมการใช้งาน เน้นการควบคุมการเข้าถึงระบบและการใช้งานเทคโนโลยีต่าง ๆ อย่างเหมาะสม เพื่อป้องกันการใช้ทรัพยากรอย่างผิดวัตถุประสงค์หรือการใช้งานที่อาจนำมาซึ่งความเสี่ยง การควบคุมนี้ช่วยลดโอกาสในการเข้าถึงข้อมูลที่ไม่เหมาะสมหรือการโจมตีจากภายในองค์กร

3.5 การปรับปรุงระบบ การปรับปรุงและบำรุงรักษาระบบเป็นการเพิ่มประสิทธิภาพในการป้องกันความเสี่ยงและลดโอกาสเกิดปัญหาจากความเสื่อมสภาพของระบบ การอัพเดทซอฟต์แวร์และการพัฒนาโครงสร้างพื้นฐานให้ทันสมัยทำให้ระบบสามารถป้องกันภัยคุกคามที่เกิดขึ้นใหม่ได้ดียิ่งขึ้

ความเสี่ยง	การประเมินความเสี่ยง	วิธีการบริหารความเสี่ยง	
	ผลกระทบ	แนวทางการควบคุม	ผู้รับผิดชอบ
1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)			
1.ความเสี่ยงจากการเกิดไฟไหม้ห้อง Server	1.ระบบคอมพิวเตอร์และระบบเครือข่ายถูกทำลาย 2.ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย	1.ตรวจสอบระบบดับเพลิงแบบอัตโนมัติตามมาตรฐานเดือนละ 1 ครั้ง 2.ตรวจสอบการทำงานของการสำรองข้อมูลทุกๆ 3 เดือน	สำนักคอมพิวเตอร์
2.ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้อง Server	1.ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ 2.ไม่สามารถใช้ระบบสารสนเทศและระบบฐานข้อมูลได้	1.ตรวจสอบระบบสำรองไฟฟ้า UPS สัปดาห์ละ 1 ครั้ง 2.ตรวจสอบเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน Electrical Generator) สัปดาห์ละ 1 ครั้ง	สำนักคอมพิวเตอร์
3.ความเสี่ยงจากอุณหภูมิและความชื้นของห้อง Server ผิดปกติ	1.ความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย	ตรวจสอบเครื่องปรับอากาศและอุณหภูมิและควบคุมความชื้น วันละ 1 ครั้ง	สำนักคอมพิวเตอร์
4.ความเสี่ยงจากแมลง สัตว์กัดแทะอุปกรณ์ เครือข่ายและระบบไฟฟ้า	1.ไม่สามารถใช้งานระบบเครือข่ายได้ 2.ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	ตรวจสอบอุปกรณ์เครือข่ายและระบบไฟฟ้าเดือนละ 1 ครั้ง	
5.ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์ เครื่องแม่ข่าย เครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	1.อุปกรณ์และข้อมูลที่มีความสำคัญสูญหาย 2.เสียภาพลักษณ์ของหน่วยงาน	1.ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2.ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ ติดตั้ง 3.ตรวจสอบการทำงานของศูนย์สำรอง Disaster Recovery Site (DR Site) ทุกๆ 3 เดือน	

ความเสี่ยง	การประเมินความเสี่ยง	วิธีการบริหารความเสี่ยง	
	ผลกระทบ	แนวทางการควบคุม	ผู้รับผิดชอบ
2. ความเสี่ยงด้านบุคลากร (Human Risk)			
6.ความเสี่ยงจากผู้ดูแลระบบ	1.ข้อมูลที่อยู่ในชั้นความลับรั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	1.การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) 2.การจัดระดับการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล	
7.ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และ ระบบเครือข่าย	1.สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ 2.เครื่องคอมพิวเตอร์เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ	1. กำหนด Policy ของ Firewall ให้เหมาะสมต่อ การใช้งาน 2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่าง ๆ ไป ใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งาน และรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา 3. ตรวจสอบและแนะนำผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	

ความเสี่ยง	การประเมินความเสี่ยง	วิธีการบริหารความเสี่ยง	
	ผลกระทบ	แนวทางการควบคุม	ผู้รับผิดชอบ
3. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)			
8.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล 2. ไม่สามารถใช้งานระบบสารสนเทศ ที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	1. ตรวจสอบการทำงานของ เครื่องคอมพิวเตอร์แม่ข่ายหลักทุกวัน 2. สำรองระบบและข้อมูล (Backup) ทุกวัน 3. ทดสอบการกู้คืนระบบแม่ข่ายหลัก เดือนละ 1 ครั้ง	
9.ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือ ระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูลที่สำคัญ	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและให้มีผลบังคับใช้อย่างเคร่งคัด	
10.ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบ เครือข่ายจากภายในและภายนอกองค์กร	1.ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ 2. ทำให้ระบบเครื่องแม่ข่ายหรือลูก ข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่น ๆ ทั้งหมดในเครือข่าย 3. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของหน่วยงาน 4. ถูกโจรกรรมข้อมูลที่เป็นความลับ 5. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ตรวจสอบ Policy และ การทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่ายทุกวัน 3. มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ตของมหาวิทยาลัยสุโขทัยธรรมาธิราช	

11.ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินทราเน็ต และอินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	1. ระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตไม่สามารถใช้งานได้ 2. ไม่สามารถเข้าใช้งานระบบสารสนเทศ ผ่านเครือข่ายอินทราเน็ต และอินเทอร์เน็ตได้	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน 2. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ต และ อินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	
12.ความเสี่ยงจากการถูกบล็อกจากผู้ให้บริการเครือข่าย)Black List)	1. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Serverได้ 2. ลดความน่าเชื่อถือของหน่วยงาน	1. อัพเดตโปรแกรมป้องกัน ไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ปรับปรุง Firewall และ การ Monitoring ระบบเครือข่ายเป็นประจำทุกปี	
13.ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่าน เครือข่าย)VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ ผู้บริหารและหน่วยงานที่เกี่ยวข้องไม่สามารถเข้าร่วมประชุมได้	ตรวจสอบการเชื่อมต่ออุปกรณ์การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน	
14.ความเสี่ยงจากการใช้งานระบบโทรศัพท์)IP Phone)	1. ระบบโทรศัพท์ (IP Phone) ขัดข้องทำให้เจ้าหน้าที่ในหน่วยงานไม่สามรถใช้งานระบบโทรศัพท์ติดต่อประสานงานทั้ง ภายใน/ภายนอก ได้อย่างต่อเนื่อง	ตรวจสอบการทำงานของระบบโทรศัพท์ (IP Phone) อย่างสม่ำเสมอ	

ความเสี่ยง	การประเมินความเสี่ยง	วิธีการบริหารความเสี่ยง	
	ผลกระทบ	แนวทางการควบคุม	ผู้รับผิดชอบ
4. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)			
15.ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1. การถูกฟ้องร้องและเสื่อมเสียชื่อเสียง และ ความน่าเชื่อถือของหน่วยงาน 2. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้น ๆ 3. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจาก ผู้เป็นเจ้าของลิขสิทธิ์นั้น ๆ	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความ จำเป็น 2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้ งาน Open Source	
16.ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรม ประยุกต์ภายในองค์กร	1. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและระบบฐานข้อมูล 2. ลดความน่าเชื่อถือต่อหน่วยงาน	1. อัพเดทเครื่องมือและโปรแกรมที่ใช้พัฒนาอย่างสม่ำเสมอ 2. ตรวจสอบช่องโหว่และ ดำเนินการแก้ไข ทุก 3 เดือน	
17.ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแล ระบบโดยผู้รับจ้างภายนอก (Outsource)	1. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ ผิดพลาดได้อย่างทันท่วงที 2. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมด ลิขสิทธิ์และขาดการปรับปรุง (Update) โปรแกรม	1. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการออกแบบ การพัฒนาระบบและ ชุดคำสั่ง (Source Code) ฉบับสมสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้นและเมื่อมีการปรับปรุงแก้ไข 2. มีกระบวนการทบทวนชุดคำสั่ง (Code Review) เพิ่มเติมในกระบวนการส่ง มอบงาน 3. มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ 4. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลให้มี ความทันสมัยและใช้งานได้อย่างต่อเนื่อง	

ความเสี่ยง	การประเมินความเสี่ยง	วิธีการบริหารความเสี่ยง	
	ผลกระทบ	แนวทางการควบคุม	ผู้รับผิดชอบ
5. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)			
18.ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็น ปัจจุบัน และไม่ครบถ้วน	1. ระบบฐานข้อมูลไม่สามารถนำไปใช้ สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ 2. ลดความน่าเชื่อถือของหน่วยงาน	1. จัดทำรายการข้อมูลและความถี่ในการปรับปรุง 2. กำหนดมาตราการแนวทางการปรับปรุงและช่องทางการเข้าถึงข้อมูล เพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	
19.ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถ กู้คืนระบบฐานข้อมูล	1.เกิดการสูญหายของข้อมูลและ กระทบต่อการทำงานตามปกติ 2.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	1. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน 2. มีการทดสอบการนำ ข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	
20.ความเสี่ยงจากการโจรกรรมระบบฐานข้อมูล	1. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ 2. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	1. ตรวจสอบระบบป้องกันการบุกรุกและระบบตรวจสอบและเฝ้าระวังเครือข่ายเป็นประจำ ทุกวัน 2. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกและระบบเฝ้าระวังเครือข่ายเป็นประจำทุกวัน	

4. การติดตาม รายงานผล และประเมินผล

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง การนำกลยุทธ์ มาตรการหรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง เพื่อนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยง เพื่อให้เหมาะสมกับสถานการณ์ ที่อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง โดยเมื่อทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยงแล้ว จึงมาพิจารณาต่อถึงความเป็นไปได้เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

- การยอมรับความเสี่ยง หรือจะกำหนดการควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

- การกำหนดกิจกรรมกรณีเลือกกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

- การพิจารณาผลการติดต่อการบริหารความเสียงที่ดำเนินการมา เพื่อวางแผนบริหารจัดการความเสี่ยงในรอบปีต่อไป

ทั้งนี้ การติดตามและรายงานผล มีการดำเนินงาน ดังต่อไปนี้

4.1 ติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยศูนย์เทคโนโลยีบรรณสารสนเทศ เพื่อให้เป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที โดยทำการติดตามและประเมินผลรายไตรมาส

4.2 รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้อำนวยการสำนักบรรณสารสนเทศ ทุก 6 เดือน และ 12 เดือน เพื่อให้มั่นใจว่าการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศมีคุณภาพและมีความเหมาะสม

4.3 รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารระดับสูงของทางมหาวิทยาลัย ทุก 6 เดือน และ 12 เดือน เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และวิเคราะห์ถึงปัญหาที่เกิดขึ้นเพื่อเสนอแนวทางแก้ไขอย่างถูกต้อง มีประสิทธิภาพ

5. การระบุกรอบเวลา

วัตถุประสงค์ของการระบุกรอบเวลาเพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของคลังปัญญา มสธ. บรรลุเป้าประสงค์ของการบริหารความเสี่ยง ดังนี้

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีคลังสารสนเทศ ประจำปี พ.ศ. 2568

ผู้รับผิดชอบหลัก ศูนย์เทคโนโลยีบรรณสารสนเทศสารสนเทศ

ระยะเวลาการดำเนินการ 1 ตุลาคม 2568 – 30 กันยายน 2569

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	ปีงบประมาณ 2568											
			ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย	พ.ค.	มิ.ย.	ก.ค.	ส.ค	ก.ย.
1.ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้อง Server	มีการทดสอบการทำงานของระบบสำรองไฟฉุกเฉิน (UPS)	1 เดือน	/											
2.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	กำหนดแผนฟื้นฟูระบบ (Disaster Recovery Plan) เพื่อให้ระบบสามารถกลับมาใช้งานได้อย่างรวดเร็วหลังเกิดเหตุเสียหาย	6 เดือน	/											
3.ความเสี่ยงจากอุณหภูมิและความชื้นของห้อง Server ผิดปกติ	ใช้เซ็นเซอร์ตรวจสอบอุณหภูมิและความชื้นในห้อง Server อย่างต่อเนื่อง	1 เดือน	/											
4.ความเสี่ยงจากการถูกบุกรุกและถูกโจมตีระบบเครือข่ายจากภายในและ	- ตรวจสอบสิทธิ์การเข้าถึงข้อมูล (Access control) - ติดตามและบันทึกการเข้าใช้งานระบบ	6 เดือน	/											

ประเภทความเสี่ยง	แผนปฏิบัติ	ระยะเวลา	ปีงบประมาณ 2568											
			ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย	พ.ค.	มิ.ย.	ก.ค.	ส.ค	ก.ย.
ภายนอกองค์กร	(Logging) - ตั้งค่า VPN สำหรับการเข้าถึงจากระยะไกล - อัพเดท Firewall อย่างต่อเนื่อง													
5.ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ตรวจสอบใบอนุญาตซอฟต์แวร์ที่ใช้เป็นประจำ และเน้นการใช้ Opensource	3 เดือน	/											