Risk Management Plan

Academic Year 2017

Office of Information Technology Services

Document No. 1

Risk Evaluation
Academic Year 2016

Specific Risk	Risk Category						Risk Analysis Before Mitigation			Mitigation	Residual Risk After Mitigation		
	1. Strategy	2. Operations	3. Student Graduation	4. Finance	5. People	6. Reputation	Likelihood (1-5)	Impact (1-5)	Risk Factor Matrix Result *(Likelihood xImpact)*	Project (OYPB)	Likelihood (1-5)	Impact (1-5)	Remaining Risk Factors
1. *การไม่มีสารสนเทศสำหรับผู้บริหารระดับสูงในการตัดสินใจ*	X	X	X	X	X	X	5	5	25	- *การพัฒนาระบบสารสนเทศของงมหาวิทยาลัย* (AU-IS) - *การพัฒนาบุคลากรในการพัฒนา ดูแลรักษา และใช้สารสนเทศ*	5	5	25
2. *การหยุดการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย*		X		X		X	3	5	15	- *การติดตั้งและบำรุงรักษาระบบสำรองข้อมูล* - *การสำรองข้อมูลที่จำเป็นทุกวัน การทดสอบกู้คืนข้อมูลเป็นระยะ* - *การบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย* (Server) - *การพัฒนาระบบเครื่องคอมพิวเตอร์แม่ข่าย*	2	5	10

										(Server Consolidation Expansion)			
3. *การหยุดการให้บริการการเชื่อมต่อเครือข่ายในมหาวิทยาลัย*		X		X			2	3	6	- *การติดตั้งระบบสำรองไฟของจุดเชื่อมต่อย่อย* - *การติดตั้งวงจรเชื่อมต่อสำรองระหว่างวิทยาเขต*	1	3	3
4. *การหยุดการให้บริการของระบบ* Internet		X				X	2	4	8	- *โครงการติดตั้งช่องทางสำรองในการเชื่อมต่อเครือข่าย* Internet	1	4	4
5. *ความไม่สมบูรณ์ของความปลอดภัยของระบบเทคโนโลยีสารสนเทศ*	X	X		X		X	4	3	12	- *การบำรุงรักษาระบบ* Firewaoo *ในการป้องกันและแก้ไขการละเมิดการใช้งานระบบและสารสนเทศ* - *การติดตามและดูแลรักษาระบบสำรองการประมวลผลและการสำรองข้อมูล*	3	3	9
6. *การละเมิดลิขสิทธิ์ทางปัญญา*			X		X	X	3	4	12	- *การติดตั้ง* Software *ป้องกันที่ถูกต้องในการป้องกันการติดตั้งและใช้งาน* Software *ที่ไม่มีลิขสิทธิ์*	2	3	6

Document No. 2

Risk Assessment
Academic Year 2017

Specific Risk	Risk Category						Risk Analysis			Risk Response Options			
	1. Strategy	2. Operations	3. Student Graduation	4. Finance	5. People	6. Repulation	Likelihood (1-5)	Impact (1-5)	Risk Factor Matrix (*Likelihood x Impact*)	Take/Accept	Mitigate	Transfer	Terminate
1. *การไม่มีสารสนเทศที่มีประสิทธิภาพในการบริหารและปฏิบัติงาน*	X	X	X	X	X	X	**5**	**5**	**25**	X			
2. *เครื่องคอมพิวเตอร์แม่ข่ายเสียและไม่สามารถให้บริการได้*	X	X	X	X	X	X	**4**	**5**	**20**	X			
3. *อุปกรณ์เครือข่ายเสียและไม่สามารถให้บริการการเชื่อมเครือข่ายทั้งในและนอกมหาวิทยาลัย*	X	X	X	X	X	X	**3**	**5**	**15**		X		
4. *การเชื่อมต่อข้อมูลระหว่างวิทยาเขตหยุดการให้บริการ*		X			X		**2**	**3**	**6**		X		

5. *ความไม่สมบูรณ์ของความปลอดภัยของระบบเทคโนโลยีสารสนเทศ*	X	X		X	X	X	**4**	**3**	**12**		X		

Risk Likelihood Scale

Risk Likelihood Scale (Quantitative Measure)		
Level	**Likelihood**	**Description**
5	Very high	Mostly every month
4	High	Once or less than 5 occurs in 1-6 months
3	Moderate	Once in 1 year
2	Little	Once in 2-3 years
1	Very little	Once in 5 years

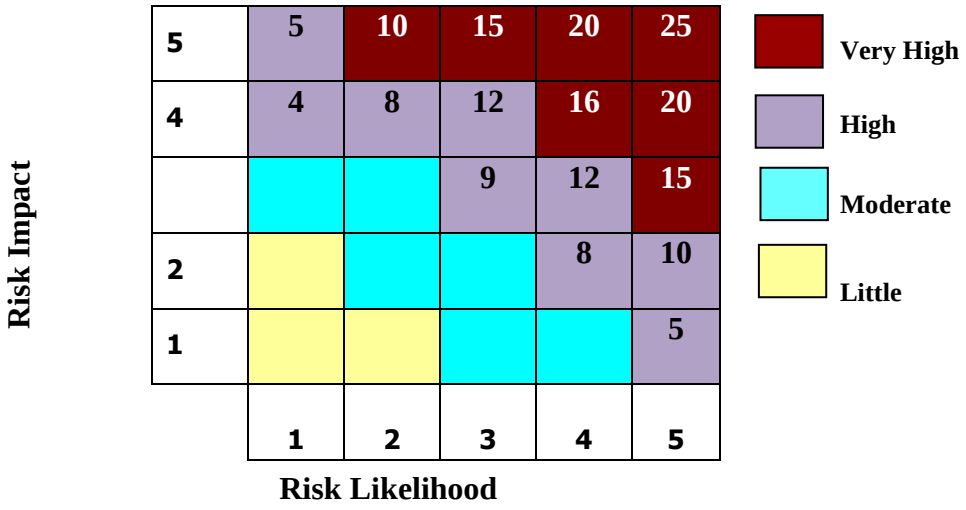
Risk Likelihood Scale (Qualitative Measure)		
Level	**Likelihood**	**Description**
5	Very high	Imminent - is expected to occur in most circumstances
4	High	Probably occur in most circumstances
3	Moderate	Might occur at some time
2	Little	Could occur at some time
1	Very little	May occur only in exceptional circumstances

Risk Impact Scale

Risk Impact Scale (Quantitative Measure)		
Level	**Likelihood**	**Description**
5	Very high	> 10 million baht
4	High	> 250,000 baht - 10 million baht
3	Moderate	> 50,000 baht - 250,000 baht
2	Little	> 10,000 baht - 50,000 baht
1	Very little	Less than 10,000 baht

Risk Impact Scale (Qualitative Measure)		
Level	**Severity**	**Description**
5	Severe	Severe injury causing death or disability
4	Major	Severe injury causing hospitalization resulting in temporary work stoppage
3	Moderate	Medical assistance required with possible hospitalization resulting in work absence
2	Minor	First aid treatment required
1	Negligible	No medical assistance or basic first aid attention required

Risk Matrix



Risk Acceptance Criteria

Risk Level	Color Coded	Definition
Very High		Unacceptable Level, it is required to be urgently managed and controlled to reach an Acceptable Level.
High		Unacceptable Level, it is required to be managed to reach an Acceptable Level.
Moderate		Acceptable Level, it must be controlled to prevent risk moving to an Unacceptable Level.
Little		Acceptable Level that does not require any control or additional management.

Document No. 6

Plan and Project of Risk Management for AU
Academice Year 2017

1. การไม่มีสารสนเทศที่มีประสิทธิภาพในการบริหารและปฏิบัติงาน

Risk Factors	Cause and Source of Risk Factors	Initiative	Project/Plan or Activity	Responsible Unit Unit(s)/person(s)	Completion Time frame
1.1 ผู้ใช้สารสนเทศไม่มีสารสนเทศที่มีประสิทธิในการบริหารและดำเนินงานด้านการเรียนการสอน	1.1.1 ระบบสารสนเทศของแต่ละหน่วยงานถูกพัฒนาขึ้นด้วยเครื่องมือ (ภาษา) ที่ต่างกัน และไม่เชื่อมโยงเพื่อแบ่งปันข้อมูลกัน 1.1.2 ระบบสารสนเทศมีระบบจัดการฐานข้อมูลที่แตกต่างกัน	- สร้างโครงสร้างสารสนเทศของมหาวิทยาลัยให้มีโครงสร้างหลักหนึ่งเดียวที่เชื่อมโยงข้อมูลต่างๆ ที่แต่ละหน่วยงานจะต้องรับผิดชอบตามสิทธิ์และหน้าที่	- การพัฒนาระบบสารสนเทศของมหาวิทยาลัย (AU-IS) - การพัฒนาบุคลากรในการพัฒนา ดูแลรักษา และใช้สารสนเทศ	- ทุกคณะ - ทุกหน่วยงานสนับสนุน	มีนาคม 2562

2. เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการประมวลผลได้

Risk Factors	Cause and Source of Risk Factors	Initiative	Project/Plan or Activity	Responsible Unit Unit(s)/person(s)	Completion Time frame
2.1 เครื่องคอมพิวเตอร์และ อุปกรณ์ไม่สามารถประมวลผลได้	2.2.1 อุปกรณ์มีอายุการใช้งานมากกว่า 9 ปี 2.2.2 อุปกรณ์มีประสิทธิภาพในการประมวลผลที่ช้าและจำกัด	- ปรับปรุงเครื่อง Physical Servers ที่มีอายุการใช้งานนานมาเป็นระบบ Virtualization ที่	- การบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) - การปรับปรุง Single Data	- ITS – Engineering Division	กรกฎาคม 2561

		ทำให้การใช้ทรัพยากรของ Servers ในการใช้งานการประมวลผลต่างๆ ร่วมกันอย่างมีประสิทธิภาพ	Center และการให้บริการ Cloud		

3. *อุปกรณ์เครือข่ายเสียและไม่สามารถให้บริการการเชื่อมเครือข่ายทั้งในและนอกมหาวิทยาลัย*

Risk Factors	Cause and Source of Risk Factors	Initiative	Project/Plan or Activity	Responsible Unit Unit(s)/person(s)	Completion Time frame
4.1 ระบบเครือข่ายไม่สามารถเชื่อมต่อเครือข่ายทั้งภายในและภายนอกในการให้บริการได้	3.1.1 อุปกรณ์มีอายุการใช้งานมากกว่า 12 ปี 3.1.2 อุปกรณ์มีประสิทธิภาพในการสื่อสารที่ต่ำ	- จัดให้มีอุปกรณ์และการบำรุงรักษาเครือข่ายสำหรับการใช้งานที่มีคุณภาพเหมาะสม	- การพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย	- ITS – Engineering Division	กรกฎาคม 2561

4. *การเชื่อมต่อข้อมูลระหว่างวิทยาเขตหยุดการให้บริการ*

Risk Factors	Cause and Source of Risk Factors	Initiative	Project/Plan or Activity	Responsible Unit Unit(s)/person(s)	Completion Time frame
2.1 การเชื่อมโยงสัญญาณเครือข่ายระหว่างวิทยาเขตล่มหรือเสีย	4.3.1 วงจรเชื่อมโยงเครือข่ายระหว่างวิทยาเขตชำรุดจากอุบัติเหตุ หรือตัวอุปกรณ์	- จัดให้มีวงจรเชื่อมโยงในการเชื่อมโยงข้อมูล 2 เส้นทางระหว่างวิทยาเขตหัวหมากกับสุวรรณภูมิ	- การเชื่อมโยงเครือข่ายสำรอง Dark Fiber (Backup Link)	- ITS – Engineering Division	กันยายน 2560

5. *การไม่มีความสมบูรณ์ของความปลอดภัยของระบบเทคโนโลยีสารสนเทศ*

Risk Factors	Cause and Source of Risk Factors	Initiative	Project/Plan or Activity	Responsible Unit Unit(s)/person(s)	Completion Time frame
5.1 *ความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูล*	5.1.1 *การถูกโจมตีด้วย* Software *ที่ทำให้ระบบการประมวลผลและข้อมูลเสียหาย*	- *จัดให้มีนโยบายในการใช้อุปกรณ์คอมพิวเตอร์และเครือข่ายภายในมหาวิทยาลัย* - *จัดให้มีวิธีการและเครื่องมือในการป้องกันและแก้ไขการโจมตีที่ทำลายระบบประมวลผลและข้อมูล*	- *การติดตั้งและบำรุงรักษาระบบสำรองการประมวลผลและข้อมูล* - *การพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย*	- ITS – Engineering Division	*กรกฎาคม* 2561

Document No. 7

Risk Management Report
Academic Year 2017

Risk Factors	Risk Mitigation by: Project/Plan or Activity	Responsible Person(s)	Completion Timeframe	Operation Result: Progress	Operation Result: Completed By
1.1 *ผู้ใช้สารสนเทศไม่มีสารสนเทศที่มีประสิทธิในการบริหารและดำเนินงานด้านการเรียนการสอน*	- *การพัฒนาระบบสารสนเทศของมหาวิทยาลัย* (AU-IS) - *การพัฒนาบุคลากรในการพัฒนา ดูแลรักษา และใช้สารสนเทศ*	- *ทุกคณะ* - *ทุกหน่วยงานสนับสนุน*	*มีนาคม* 2562	X	
2.1 *เครื่องคอมพิวเตอร์ และ อุปกรณ์ไม่*	- *การบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย* (Server)	- ITS – Engineering Division	*กรกฎาคม* 2561	X	

สามารถประมวลผลได้	- *การปรับปรุง* Single Data Center *และการให้บริการ* Cloud				
3.1 *ระบบเครือข่ายไม่สามารถเชื่อมต่อเครือข่ายทั้งภายในและภายนอกในการให้บริการได้*	- *การพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย*	- ITS – Engineering Division	*กรกฎาคม* 2561	**X**	
4.1 *การเชื่อมโยงสัญญาณเครือข่ายระหว่างวิทยาเขตล่มหรือเสีย*	- *การเชื่อมโยงเครือข่ายสำรอง* Dark Fiber (Backup Link)	- ITS – Engineering Division	*กันยายน* 2560	**X**	
5.1 *ความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูล*	- *การติดตั้งและบำรุงรักษาระบบสำรองการประมวลผลและข้อมูล* - *การพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย*	- ITS – Engineering Division	*กรกฎาคม* 2561	**X**	