แผนการกู้คืนระบบเทคโนโลยีสารสนเทศและข้อมูลภายในวิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล
IT Disaster Recovery Plan (IT DRP) for Mahidol University International College (MUIC)

1. บทนำ (Introduction)

แผนการกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan - DRP) ฉบับนี้จัดทำขึ้นเพื่อรวบรวมข้อมูลและสรุปข้อมูลด้านความพร้อมและแนวทางปฏิบัติของวิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล ในการรับมือกับเหตุการณ์ภัยพิบัติ พร้อมทั้งกำหนดขั้นตอนต่าง ๆ ที่ต้องดำเนินการเพื่อให้สามารถกู้คืนระบบและกลับสู่การดำเนินงานได้อย่างรวดเร็วและมีประสิทธิภาพ

คำนิยามของ "ภัยพิบัติ" (Definition of a Disaster)

ภัยพิบัติ หมายถึง เหตุการณ์ที่เกิดขึ้นโดยมีสาเหตุจากทางธรรมชาติหรือมนุษย์ ซึ่งส่งผลกระทบต่อโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) และระบบงานต่าง ๆ ของวิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล ทำให้ไม่สามารถดำเนินงานได้ตามปกติเป็นระยะเวลาหนึ่ง โดยวิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล กำหนดลักษณะของสถานการณ์ที่ถือว่าเป็น “ภัยพิบัติ” ไว้ดังนี้

1.1. ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญอย่างน้อยหนึ่งระบบไม่สามารถทำงานได้
1.2. อาคารสำนักงานไม่สามารถใช้งานได้ในระยะเวลานาน แต่ระบบและบริการด้านเทคโนโลยีสารสนเทศภายในอาคารยังคงใช้งานได้
1.3. อาคารสำนักงานสามารถใช้งานได้ แต่ระบบทั้งหมดไม่สามารถทำงานได้
1.4. อาคารสำนักงานและระบบทั้งหมดไม่สามารถใช้งานได้

เหตุการณ์ต่อไปนี้อาจนำไปสู่ภัยพิบัติและจำเป็นต้องมีการประกาศใช้แผนการกู้คืนระบบตามเอกสารฉบับนี้

เหตุการณ์ Incident	**นิยาม** Term Definition
เหตุการณ์อัคคีภัย หรือไฟไหม้ Fire	เหตุการณ์เพลิงไหม้ภายในหรือบริเวณโดยรอบพื้นที่ของวิทยาลัยฯ ซึ่งอาจทำให้เกิดความเสียหายต่ออาคาร สาธารณูปโภค ระบบไฟฟ้า หรือโครงสร้างพื้นฐานที่เกี่ยวข้อง รวมถึงส่งผลกระทบต่อความปลอดภัยของบุคลากรและความสามารถในการให้บริการของระบบสารสนเทศ
เหตุการณ์อุทกภัย Flash Flood	เหตุการณ์น้ำท่วม หรือเกิดพายุรุนแรง ภายในบริเวณของวิทยาลัยฯ ซึ่งอาจก่อให้เกิดความเสียหายต่ออาคาร สาธารณูปโภค และสิ่งปลูกสร้าง ส่งผลกระทบต่อการดำเนินงาน ความปลอดภัยของบุคลากร และอาจทำให้ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศไม่สามารถใช้งานได้ตามปกติ
เหตุการณ์แผ่นดินไหว Earthquake	เหตุการณ์สั่นสะเทือนของเปลือกโลกที่ส่งผลกระทบต่ออาคาร สาธารณูปโภค และสิ่งปลูกสร้างของวิทยาลัยฯ ซึ่งอาจทำให้โครงสร้างพื้นฐาน ระบบไฟฟ้า และระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย ตลอดจนส่งผลกระทบต่อความปลอดภัยของบุคลากรและการดำเนินงานของวิทยาลัยฯ
เหตุการณ์ด้านความปลอดภัยทางไซเบอร์ Cyber security incident	เหตุการณ์ที่ก่อให้ระบบเทคโนโลยีสารสนเทศของวิทยาลัยฯ เกิดการชะงักหรือหยุดทำงาน เช่น การถูกโจมตีทางไซเบอร์ (Cyber Attack) ระบบล่ม หรือการเจาะช่องโหว่ของเว็บไซต์ ซึ่งส่งผลกระทบต่อความมั่นคงและความต่อเนื่องของการให้บริการด้านสารสนเทศของวิทยาลัยฯ
เหตุการณ์การแพร่ระบาดของโรค Pandemic	การแพร่ระบาดของโรคที่ส่งผลกระทบต่อสุขภาพของบุคลากร นักศึกษา และผู้มีส่วนเกี่ยวข้อง จนไม่สามารถดำเนินกิจกรรมหรือให้บริการต่างๆ ของวิทยาลัยฯ ได้ตามปกติของวิทยาลัยได้

เหตุการณ์ Incident	นิยาม Term Definition
เหตุการณ์การขาดแคลนพลังงาน Power outage	เหตุการณ์ที่แหล่งจ่ายพลังงานหลัก เช่น ไฟฟ้า หรือระบบสำรองพลังงาน ไม่สามารถจ่ายพลังงานได้ตามปกติ ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ การสื่อสาร และการดำเนินงานของวิทยาลัยฯ
เหตุการณ์การโจรกรรม Theft	เหตุการณ์ที่ทรัพย์สิน อุปกรณ์ หรือข้อมูลสำคัญของวิทยาลัยฯ ถูกขโมยหรือสูญหาย ส่งผลกระทบต่อความมั่นคงของระบบและความต่อเนื่องในการดำเนินงาน
เหตุการณ์การก่อการร้าย Terrorist attack	เหตุการณ์ที่มีการกระทำโดยเจตนามุ่งก่อให้เกิดความเสียหายรุนแรงต่อชีวิต ทรัพย์สิน หรือโครงสร้างพื้นฐานของวิทยาลัยฯ ส่งผลต่อความมั่นคงและความต่อเนื่องในการดำเนินงานของวิทยาลัยฯ
เหตุการณ์การชุมนุมประท้วง หรือเหตุการณ์จลาจล Protest March	การชุมนุมหรือการจลาจลที่เกิดขึ้นภายในหรือบริเวณใกล้เคียงกับพื้นที่ของวิทยาลัยฯ ซึ่งอาจส่งผลกระทบต่อความปลอดภัยของบุคลากร และนักศึกษา รวมถึงหยุดชะงักการดำเนินงานตามปกติของวิทยาลัย

ตารางที่ 1. *เหตุการณ์สำคัญที่ต้องดำเนินการตามแผนกู้คืนระบบ (DRP Activation Triggers)*

การประเมินความเสี่ยงและภัยคุกคาม

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล ได้ดำเนินการประเมินความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นในพื้นที่ปฏิบัติงาน ซึ่งอาจส่งผลกระทบรุนแรงต่อการดำเนินงานของวิทยาลัยฯ โดยได้ประสานงานกับทุกหน่วยงานที่เกี่ยวข้อง พร้อมทั้งทบทวนกิจกรรมและกระบวนการทำงานที่สำคัญ เพื่อประเมินระดับผลกระทบในกรณีที่กิจกรรมดังกล่าวหยุดชะงักจากสภาวะวิกฤต จากการประเมินสามารถสรุปผลกระทบของเหตุการณ์ต่าง ๆ และทรัพยากรที่สำคัญได้ดังแสดงในตารางต่อไปนี้

เหตุการณ์	ผลกระทบ				
	อาคาร/สถานที่	วัสดุอุปกรณ์	เทคโนโลยี/ข้อมูล	บุคลากร	ผู้มีส่วนได้ส่วนเสีย
เหตุการณ์อัคคีภัย หรือไฟไหม้	✓	✓	✓	✓	✓
เหตุการณ์อุทกภัย	✓	✓	✓	✓	✓
เหตุการณ์แผ่นดินไหว	✓	✓	✓	✓	✓
เหตุการณ์การแพร่ระบาดของโรค	-	✓	-	✓	✓
เหตุการณ์ด้านความปลอดภัยทางไซเบอร์	-	✓	✓	✓	✓
เหตุการณ์การโจรกรรม	✓	✓	✓	✓	✓
เหตุการณ์การขาดแคลนพลังงาน	✓	✓	✓	✓	✓
เหตุการณ์การก่อการร้าย	✓	✓	✓	✓	✓
เหตุการณ์การชุมนุมประท้วง หรือเหตุการณ์จลาจล	✓	✓	✓	✓	✓

ตารางที่ 2. *การประเมินความเสี่ยงและภัยคุมคาม และผลกระทบต่อทรัพยากรสำคัญ*

2. บริการข้อมูลสำคัญและระบบเทคโนโลยีสารสนเทศหลัก (Key information services and IT systems)

# *	บริการข้อมูลและระบบเทคโนโลยีสารสนเทศที่มีความสำคัญต่อภารกิจหลักของวิทยาลัยฯ	ข้อกำหนดด้านความพร้อมใช้งาน			แผนการสำรองข้อมูล		
		Availability (H, M, L)	RTO (hrs)	RPO (hrs)	Frequency (hrs)	Backup location	SLA
1	ระบบทะเบียนนักศึกษา (SKY+)	H	4	1	12	3-2-1	
2	ระบบเว็บไซต์วิทยาลัย (College Website)	M	8	4	24		
3	ระบบจัดเก็บไฟล์ (File Server)	H	2	1	6		
4	ระบบโทรศัพท์ผ่านเครือข่าย (VoIP)	M	8	4	24		
5	ระบบควบคุมภายในห้อง Datacenter	H	1	1	1		
6	โครงสร้างพื้นฐานเครือข่าย (IT Network Infrastructure)	H	1	1	6		
7	ช่องสัญญาณอินเทอร์เน็ต (Link Internet)	H	0.5	0.5	H		
8	ระบบเครือข่ายไร้สาย (WiFi)	M	6	3	12		
9	ระบบทะเบียนนักศึกษาศูนย์เตรียมความพร้อมภาษาและคณิตศาสตร์ (PC-Online)	M	6	2	24		
10	เครือข่ายภายในวิทยาลัยฯ (my.muic.io)	L	24	12	48		
11	แอปพลิเคชันของวิทยาลัยนานาชาติ (IC APP)	M	6	3	12		

ตารางที่ 3. *บริการข้อมูลสำคัญและระบบเทคโนโลยีสารสนเทศหลัก (Key information services and IT systems)*

คำอธิบายเพิ่มเติม

Availability H = สูง (High), M = กลาง (Medium), L = ต่ำ (Low)

RTO (Recovery Time Objective) เวลาที่ต้องทำให้ระบบกลับมาใช้งานได้

RPO (Recovery Point Objective) เวลาที่ข้อมูลสูญหายได้สูงสุด

Frequency ความถี่ในการสำรองข้อมูล (เช่น ทุก 6 ชม., 24 ชม.)

Backup location สถานที่เก็บข้อมูลสำรอง เช่น Local, Cloud, Cloud

SLA มีข้อตกลงบริการจากผู้ให้บริการหรือไม่ (✓ = มี, ✗ = ไม่มี)

3. การประเมินความเสี่ยง (Risk Assessment)

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล ได้ดำเนินการวิเคราะห์ความเสี่ยงโดยพิจารณาจาก 2 มิติหลัก ได้แก่ โอกาสในการเกิด (Likelihood) และผลกระทบ (Impact) เพื่อใช้ในการกำหนด ระดับความเสี่ยง (Level of Risk) ต่อเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานของวิทยาลัยฯ ซึ่งการวิเคราะห์สามารถดำเนินได้ทั้งในรูปแบบ เชิงคุณภาพ (Qualitative) กึ่งปริมาณ (Semi-Quantitative) และเชิงปริมาณ (Quantitative) โดยผลลัพธ์จะใช้เป็นข้อมูลสำคัญในการวางแผน รับมือกับภัยพิบัติ และฟื้นฟูระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

3.1. โอกาสที่จะเกิด (Likelihood)

โอกาสที่จะเกิด (Likelihood) หมายถึง การประเมินความเป็นไปได้ของการที่เหตุการณ์ความเสี่ยงจะเกิดขึ้น โดยพิจารณาจากข้อมูลสถิติในอดีต สถานการณ์ปัจจุบัน หรือการคาดการณ์ล่วงหน้าในอนาคต ดังนี้

ระดับ	ความหมาย
1	โอกาสหรือผลกระทบน้อยมาก แทบไม่เคยเกิดขึ้น หรือไม่มีข้อมูลสถิติ หรือเหตุการณ์ในอดีตที่สามารถยืนยันความเป็นไปได้ของการเกิดเหตุการณ์นี้
2	โอกาสหรือผลกระทบน้อย แต่เคยเกิดขึ้นในอดีตเป็นเวลานานมาแล้ว และไม่มีแนวโน้มชัดเจนว่าจะเกิดซ้ำในปัจจุบัน
3	โอกาสหรือผลกระทบปานกลาง มีความเป็นไปได้ที่จะเกิดขึ้นในบางสถานการณ์ โดยเคยเกิดขึ้นประมาณ 1 ครั้งในช่วง 5 ปีที่ผ่านมา
4	โอกาสหรือผลกระทบสูง เคยเกิดขึ้นแล้วอย่างน้อย 1 ครั้งในช่วง 2–3 ปีที่ผ่านมา และมีแนวโน้มที่จะเกิดขึ้นอีก
5	โอกาสหรือผลกระทบสูงมาก มีแนวโน้มที่จะเกิดเหตุการณ์นี้เกือบทุกปี หรือเกิดขึ้นซ้ำบ่อยในรอบหลายปีที่ผ่านมา

ตารางที่ 4. *ตารางระดับโอกาสที่จะเกิด (Likelihood Rating Table)*

3.2. ผลกระทบ (Impact)

ผลกระทบ (Impact) หมายถึง ความเสียหายหรือผลกระทบที่อาจเกิดขึ้นต่อวิทยาลัยฯ หากเหตุการณ์ความเสี่ยงเกิดขึ้นจริง โดยพิจารณาจากระดับความรุนแรงและมูลค่าความเสียหายที่อาจได้รับ ทั้งในด้านการดำเนินงาน ทรัพยากร สารสนเทศ บุคลากร หรือชื่อเสียงของวิทยาลัยฯ

ระดับ	ความหมาย
1	หากเกิดเหตุการณ์ จะมีผลกระทบเพียงเล็กน้อยมากหรือไม่มีผลกระทบต่อการดำเนินงานเลย และไม่จำเป็นต้องใช้ทรัพยากรเพิ่มเติมในการฟื้นฟู
2	ส่งผลกระทบเพียงเล็กน้อยต่อการดำเนินงาน แก้ไขได้ด้วยทรัพยากรขั้นต่ำ และไม่กระทบต่อภารกิจหลักของวิทยาลัยฯ
3	ส่งผลกระทบต่อกระบวนการทำงานบางส่วน จำเป็นต้องใช้ทรัพยากรในการฟื้นฟู แต่ยังสามารถดำเนินงานได้บางส่วน
4	ส่งผลกระทบต่อภารกิจหลักของหน่วยงานบางส่วน ทำให้การดำเนินงานหยุดชะงักชั่วคราวหรือสูญเสียทรัพยากรสำคัญบางรายการ
5	ส่งผลกระทบในระดับรุนแรงมาก ทำให้วิทยาลัยฯ ไม่สามารถดำเนินงานหลักได้ สูญเสียข้อมูลสำคัญ หรือเกิดความเสียหายเชิงภาพลักษณ์และชื่อเสียงในวงกว้าง

ตารางที่ 5. *ตารางระดับผลกระทบ (Impact Rating Table)*

โดยการประเมินความเสี่ยงสามารถกำหนดเป็น ระดับคะแนน (Rating Scale) ทั้งในด้าน โอกาสในการเกิดเหตุการณ์ (Likelihood) และผลกระทบที่อาจเกิดขึ้น (Impact) โดยผลการประเมินทั้งสองด้านจะถูกนำมาใช้ร่วมกันในการวิเคราะห์และจัดลำดับ ระดับความเสี่ยงโดยรวม (Overall Risk Level) ของวิทยาลัยฯ เพื่อใช้ในการกำหนดแนวทางจัดการความเสี่ยงอย่างเหมาะสม

ระดับผลกระทบ (Impact)						
	5	1x5	2x5	3x5	4x5	5x5
	4	1x4	2x4	3x4	4x4	5x4
	3	1x3	2x3	3x3	4x3	5x3
	2	1x2	2x2	3x2	4x2	5x2
	1	1x1	2x1	3x1	4x1	5x1
		1	2	3	4	5
		ระดับโอกาสเกิด (Likelihood)				

ระดับความเสี่ยง	แนวทางการจัดการ
สูงมาก	ควรมีการดำเนินการแก้ไขทันที
สูง	ควรวางแผนควบคุมความเสี่ยงอย่างเป็นระบบ
ปานกลาง	ควรติดตามและทบทวนอย่างสม่ำเสมอ
ต่ำ	สามารถยอมรับความเสี่ยงได้ในระดับที่เหมาะสม

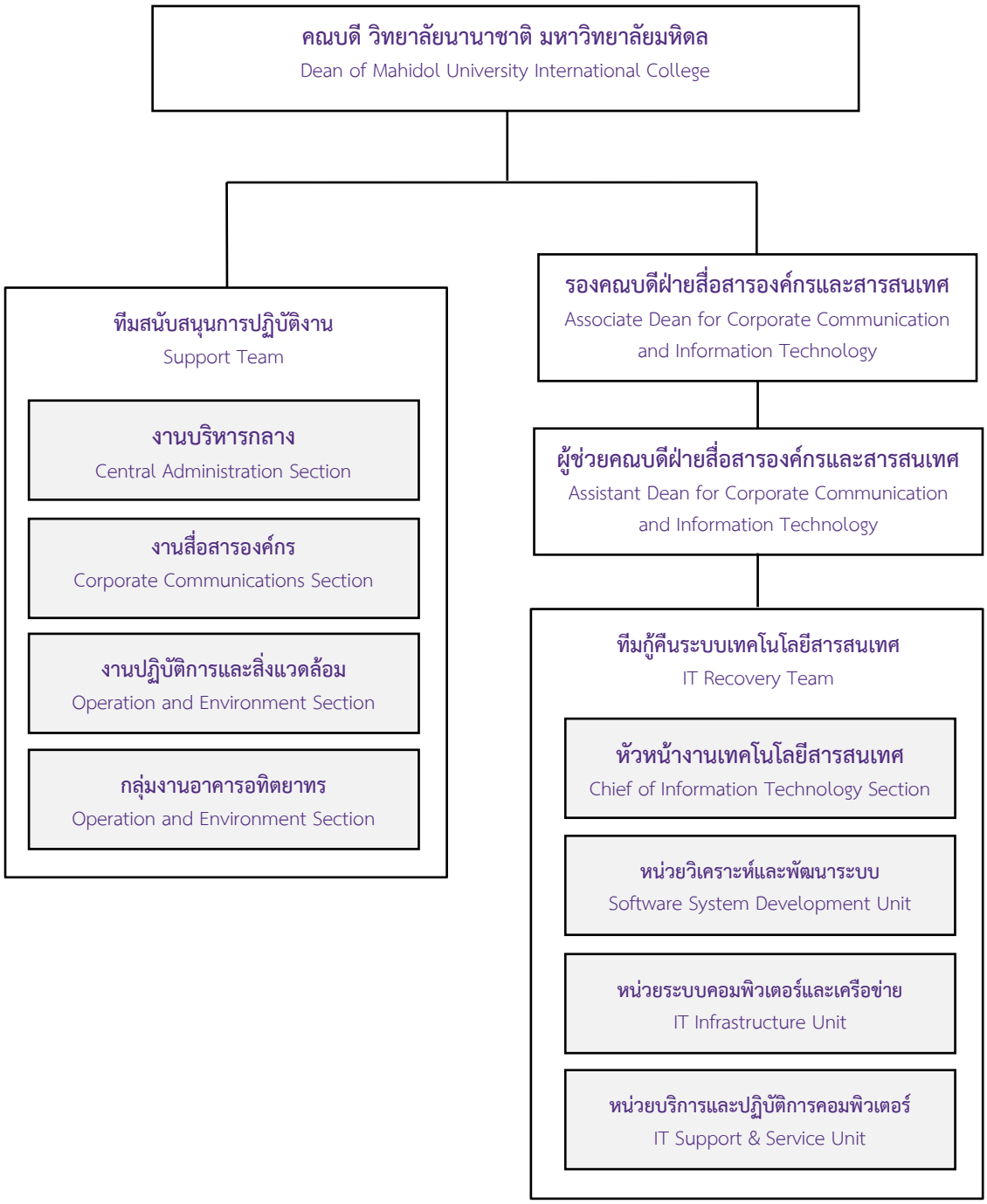
ตารางที่ 6. *ตารางเมทริกซ์ประเมินระดับความเสี่ยง (Risk Matrix Table)*

เหตุการณ์ภัยพิบัติที่อาจเกิดขึ้น Potential Disaster scenario	ระบบสารสนเทศที่ได้รับผลกระทบ IT systems impacted	ระดับความน่าจะเป็น 1-5 Probability Rating	ระดับผลกระทบ 1-5 Impact Rating	คำอธิบายผลกระทบที่อาจเกิดขึ้นและแนวทางแก้ไข Description of potential consequences and remedial actions

ตารางที่ 7. *ตารางวิเคราะห์สถานการณ์ภัยพิบัติและผลกระทบต่อระบบสารสนเทศ (Disaster Recovery Scenarios Table)*

4. บทบาทหน้าที่และความรับผิดชอบ (Disaster Recovery Roles & Responsibilities)

ในกรณีที่เกิดภัยพิบัติหรือภาวะฉุกเฉินด้านความต่อเนื่องทางการดำเนินงาน เวลาเป็นปัจจัยที่สำคัญอย่างยิ่ง วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล จึงนำรูปแบบสายการติดต่อ (Call Tree) มาประยุกต์ใช้งาน เพื่อให้สามารถแจ้งเหตุและประสานงานกับบุคลากรที่เกี่ยวข้องได้อย่างรวดเร็วและมีประสิทธิภาพ โดยผู้นำในการกู้คืนระบบ (Disaster Recovery Team Lead) จะเป็นผู้รับผิดชอบในการเริ่มต้นการแจ้งเหตุและติดต่อผู้มีส่วนเกี่ยวข้องตามลำดับความสำคัญที่กำหนดไว้ในแผน



รูปที่ 1. *ผังแสดงบทบาทและความรับผิดชอบของบุคลากรในแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Roles & Responsibilities)*

บทบาท	ความรับผิดชอบ
คณบดี วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล	ผู้บริหารสูงสุด / ผู้มีอำนาจตัดสินใจขั้นสุดท้าย ● อนุมัติการประกาศภาวะฉุกเฉิน / การใช้งานแผนกู้คืนระบบ (Disaster Declaration) ● รับทราบสถานการณ์ความเสียหายโดยรวม ● สื่อสารกับผู้บริหารระดับมหาวิทยาลัย หรือหน่วยงานภายนอก ● ประเมินผลกระทบเชิงนโยบาย และกำหนดทิศทางการฟื้นฟูระบบ
รองคณบดีฝ่ายสื่อสารองค์กรและสารสนเทศ	ผู้ควบคุมดูแลการบริหารจัดการเทคโนโลยีสารสนเทศในภาพรวม ● ตัดสินใจเชิงนโยบายเมื่อเกิดเหตุฉุกเฉิน ● สั่งการให้เริ่มต้นหรือยกเลิกการดำเนินการตามแผน DRP ● ประสานงานกับคณบดี และรายงานความคืบหน้า ● กำกับดูแลภาพรวมการสื่อสารในภาวะวิกฤต
ผู้ช่วยคณบดีฝ่ายสื่อสารองค์กรและสารสนเทศ	ผู้ประสานงานเชิงปฏิบัติการระหว่างฝ่ายเทคนิคและผู้บริหาร ● ประสานงานระหว่างทีม IT Recovery กับรองคณบดี ● ตรวจสอบสถานะของระบบและประเมินระดับความเสียหายเบื้องต้น ● จัดทำรายงานสถานการณ์ และข้อเสนอแนะแนวทางแก้ไข ● ดูแลการดำเนินการของหัวหน้าเทคโนโลยีสารสนเทศให้เป็นไปตามแผน
ทีมกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Recovery Team)	
หัวหน้างานเทคโนโลยีสารสนเทศ	ผู้นำด้านเทคนิคในการตอบสนองเหตุฉุกเฉิน ● วิเคราะห์และระบุปัญหาทางเทคนิคที่เกิดขึ้น ● สั่งการและจัดลำดับความสำคัญของระบบที่ต้องกู้คืน ● ควบคุมและติดตามการปฏิบัติงานของทีม IT Recovery ● ประสานกับผู้ช่วยคณบดีเพื่อรายงานความคืบหน้า และประสานกับทีมสนับสนุนการปฏิบัติงาน (Support Team)
หน่วยวิเคราะห์และพัฒนาระบบ	● พัฒนาและดูแลระบบสารสนเทศของวิทยาลัยฯ ● สำรองฐานข้อมูลอย่างต่อเนื่อง และเตรียมการกู้คืนระบบกรณีเกิดความเสียหาย ● ทดสอบระบบใหม่และวางแผนความต่อเนื่องทางธุรกิจด้านซอฟต์แวร์
หน่วยระบบคอมพิวเตอร์และเครือข่าย	● ดูแลโครงสร้างพื้นฐานด้านระบบเครือข่าย เซิร์ฟเวอร์ ระบบเก็บข้อมูล ● ติดตั้ง บำรุงรักษา และดำเนินการฟื้นฟูระบบในกรณีเกิดเหตุผิดปกติ ● ประสานงานการเปลี่ยนถ่ายระบบชั่วคราว (Failover) หรือย้ายไปยัง DR Site
หน่วยบริการและปฏิบัติการคอมพิวเตอร์	● ให้ความช่วยเหลือและแก้ไขปัญหาการใช้งานด้านไอทีแก่บุคลากร ● จัดเตรียมเครื่องมือและบริการไอทีในช่วงการกู้คืนระบบ ● ตรวจสอบความเสียหายของอุปกรณ์ผู้ใช้งานและดำเนินการแก้ไข
ทีมสนับสนุนการปฏิบัติงาน (Support Team)	
งานบริหารกลาง	● ตรวจสอบความถูกต้องของเอกสาร/ประกาศ/สัญญาในภาวะฉุกเฉินให้เป็นไปตามกฎหมาย ● ให้คำปรึกษาทางกฎหมายเกี่ยวกับสิทธิ์การยกเลิกสัญญา/การจัดซื้อจัดจ้างฉุกเฉิน ● ประสานกับหน่วยงานกำกับหรือที่ปรึกษากฎหมายภายนอกหากจำเป็น
งานสื่อสารองค์กร	● วางแผนและรับผิดชอบการสื่อสารภายใน และกับผู้มีส่วนได้ส่วนเสียภายนอกในช่วงภาวะวิกฤต ● ประสานงานกับสื่อมวลชนและหน่วยงานภายนอกที่เกี่ยวข้องกับการสื่อสาร เพื่อสร้างความเข้าใจอันถูกต้องเกี่ยวกับเหตุการณ์ ● ติดตามและประเมินผลการสื่อสาร พร้อมจัดการประเด็นที่อาจเกิดความเข้าใจคลาดเคลื่อนหรือส่งผลกระทบต่อภาพลักษณ์ของวิทยาลัย
งานปฏิบัติการและสิ่งแวดล้อม และ กลุ่มงานอาคารอทิตยาทร	● ตรวจสอบความเสียหายของอาคาร สถานที่ และระบบสาธารณูปโภคภายหลังเกิดเหตุภัยพิบัติ ● ประสานงานการซ่อมแซมหรือฟื้นฟูสถานที่ พร้อมจัดเตรียมพื้นที่ทำงานชั่วคราวหากสถานที่หลักไม่สามารถใช้งานได้ ● ดูแลการเข้าถึงสถานที่ของทีมงานที่เกี่ยวข้องกับการกู้คืนระบบ และควบคุมความปลอดภัยของพื้นที่ ● ประสานงานกับผู้รับเหมา หน่วยงานภายนอก หรือเจ้าหน้าที่รักษาความปลอดภัยในกรณีที่มีการเคลื่อนย้ายอุปกรณ์หรือบุคลากร

ตารางที่ 8. *ตารางบทบาทและความรับผิดชอบของบุคลากรในแผนกู้คืนระบบเทคโนโลยีสารสนเทศ*

หน้าที่หลักของทีมกู้คืนระบบเทคโนโลยีสารสนเทศ (Key Responsibilities of the IT Recovery Team)

บทบาท Role	**ความรับผิดชอบ** Responsibility
1. วางแผนการกู้คืนระบบ (Disaster Recovery Planning)	1.1. จัดทำและปรับปรุงแผนกู้คืนระบบ IT ให้ทันสมัยและเหมาะสมกับสถานการณ์ 1.2. ระบุระบบที่มีความสำคัญและลำดับความสำคัญในการกู้คืน
2. ประเมินความเสี่ยงและผลกระทบ	2.1. วิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อระบบ IT 2.2. จัดระดับความสำคัญของแต่ละระบบตามผลกระทบต่อภารกิจของวิทยาลัยฯ
3. ดำเนินการกู้คืนระบบ	3.1. เมื่อเกิดเหตุฉุกเฉิน ทีมจะดำเนินการตามแผนที่วางไว้ เช่น การกู้คืนจากข้อมูลสำรอง การย้ายระบบไปยังศูนย์สำรอง (DR Site)
4. ประสานงานกับหน่วยงานที่เกี่ยวข้อง	4.1. ทำงานร่วมกับผู้บริหาร หน่วยงานเทคโนโลยีสารสนเทศ และผู้ให้บริการภายนอก 4.2. สื่อสารสถานการณ์กับผู้มีส่วนได้ส่วนเสีย (Stakeholders)
5. ทดสอบแผนและฝึกซ้อม	5.1. จัดให้มีการทดสอบแผนเป็นระยะ เพื่อให้มั่นใจว่าแผนสามารถนำไปปฏิบัติได้จริง 5.2. วิเคราะห์ผลการทดสอบเพื่อปรับปรุงแผนให้ดีขึ้น
6. จัดทำรายงานเหตุการณ์และบทเรียนที่ได้รับ	6.1. รวบรวมข้อมูลหลังการกู้คืนเพื่อวิเคราะห์จุดบกพร่อง 6.2. เสนอแนะแนวทางปรับปรุงกระบวนการในอนาคต

ตารางที่ 9. *หน้าที่หลักของทีมกู้คืนระบบเทคโนโลยีสารสนเทศ (Key Responsibilities of the IT Recovery Team)*

5. แผนการแจ้งเหตุและติดต่อประสานงานในภาวะฉุกเฉิน (Disaster Recovery Call Tree)

ผู้ติดต่อ Contact	**โทรศัพท์สำนักงาน** Work	**โทรศัพท์มือถือ** Mobile	

ตารางที่ 10. *Disaster recovery call tree*

6. แนวทางการสื่อสารระหว่างเกิดภัยพิบัติ (Communicating During a Disaster)

ในกรณีที่เกิดภาวะวิกฤตหรือภาวะฉุกเฉิน วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล จำเป็นต้องดำเนินการสื่อสารอย่างเร่งด่วนกับผู้มีส่วนเกี่ยวข้องในทุกระดับ เพื่อแจ้งให้ทราบถึงผลกระทบที่เกิดขึ้นต่อระบบสารสนเทศ การเรียนการสอน และการดำเนินงานของวิทยาลัยฯ รวมถึงระยะเวลาที่คาดว่าจะสามารถกลับเข้าสู่ภาวะปกติได้

คณะทำงานด้านการสื่อสารในภาวะฉุกเฉิน จะรับผิดชอบในการประสานงานการติดต่อกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก อาทิ คณาจารย์ บุคลากร นักศึกษา ผู้ปกครอง หน่วยงานกำกับดูแล และพันธมิตรทางวิชาการ โดยมีการกำหนดเนื้อหาที่ต้องสื่อสาร ช่องทางการสื่อสารที่เหมาะสม และรายชื่อผู้ติดต่อไว้ล่วงหน้า เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและมีประสิทธิภาพเมื่อเกิดสถานการณ์จริง

ผู้มีส่วนได้ส่วนเสีย Stakeholders	**เนื้อหาการสื่อสาร** Communication content	**ช่องทางและกระบวนการสื่อสาร** Contact details
ผู้มีส่วนได้ส่วนเสียภายใน (Internal Stakeholders) เช่น คณาจารย์ พนักงาน ผู้บริหาร นักศึกษา	• ผลกระทบของเหตุการณ์ต่อระบบเทคโนโลยีสารสนเทศและการให้บริการ • รายการระบบที่ได้รับผลกระทบ • แนวทางการดำเนินการแก้ไขชั่วคราว	• ประกาศทางกลุ่มอีเมลภายใน (Internal Email Distribution List) • ระบบสารสนเทศของวิทยาลัยฯ • กลุ่ม Line Official Account

		• เว็บไซต์วิทยาลัยฯ
ผู้มีส่วนได้ส่วนเสียภายนอก (External Stakeholders) เช่น หน่วยงานภาครัฐ มหาวิทยาลัยมหิดล ผู้ปกครอง พันธมิตรทางวิชาการ	• ผลกระทบที่อาจเกิดขึ้นต่อการให้บริการหรือข้อมูลของนักศึกษา • มาตรการรักษาความปลอดภัยของข้อมูล • ระยะเวลาประเมินการฟื้นฟูระบบโดยประมาณ	• เว็บไซต์วิทยาลัยฯ • อีเมลแจ้งเตือน (External Email List) • โทรศัพท์ฉุกเฉิน • แถลงข่าวสาธารณะ • ประชาสัมพันธ์ผ่านสื่อสังคมออนไลน์ของวิทยาลัยฯ • กลุ่ม Line Official Account

ตารางที่ 11. Stakeholder Communications

7. การรับมือกับเหตุการณ์ภัยพิบัติ (Dealing with a Disaster)

เมื่อเกิดเหตุการณ์ภัยพิบัติขึ้นที่วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล สิ่งสำคัญอันดับแรก คือ ความปลอดภัยของบุคลากรทุกคน และต้องยืนยันว่าทุกฝ่ายปลอดภัย และได้รับการดูแลอย่างเหมาะสม จากนั้นจึงดำเนินมาตรการลดผลกระทบต่อสถานที่ ระบบ และข้อมูล พร้อมบรรเทาผลกระทบต่อการดำเนินงานของวิทยาลัยฯ โดยไม่ว่าจะเป็นภัยพิบัติประเภทใด การรับมือสามารถแบ่งออกเป็นขั้นตอนหลัก ดังนี้

1) การระบุและประกาศเหตุการณ์ภัยพิบัติ (Disaster Identification and Declaration)
2) การเปิดใช้งานแผนกู้คืนระบบและการสื่อสาร (Disaster Recovery Plan activation and communication)
3) การฟื้นฟูระบบเทคโนโลยีสารสนเทศให้กลับมาใช้งานได้ (Restoring IT system functionality)

7.1. การระบุและประกาศเหตุการณ์ภัยพิบัติ (Disaster Identification and Declaration)

เนื่องจากไม่สามารถคาดการณ์ล่วงหน้าได้ว่าเหตุการณ์ภัยพิบัติจะเกิดขึ้นเมื่อใดและในลักษณะใด วิทยาลัยฯ จึงต้องเตรียมความพร้อมในการรับทราบสถานการณ์จากแหล่งข้อมูลที่หลากหลาย ซึ่งอาจรวมถึง

7.1.1. การสังเกตโดยตรงจากเจ้าหน้าที่หรือผู้พบเห็น
7.1.2. สัญญาณเตือนจากระบบเครือข่ายหรืออุปกรณ์ตรวจจับ
7.1.3. ระบบแจ้งเตือนด้านสิ่งแวดล้อมหรือความปลอดภัย
7.1.4. การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
7.1.5. การแจ้งจากผู้ใช้งาน (End Users)
7.1.6. ผู้ให้บริการภายนอก (Third-party vendors)
7.1.7. รายงานข่าวจากสื่อมวลชน

เมื่อผู้นำการกู้คืนระบบ (Disaster Recovery Lead) ได้ตรวจสอบและยืนยันว่าเหตุการณ์ที่เกิดขึ้นเข้าข่ายภัยพิบัติ จะต้องประกาศอย่างเป็นทางการ ว่าวิทยาลัยฯ เข้าสู่สถานะภัยพิบัติ และเตรียมเปิดใช้งานแผนกู้คืนระบบ (DRP)

7.2. การเปิดใช้งานแผนกู้คืนระบบและการสื่อสาร (Disaster Recovery Plan activation and communication)

เมื่อมีการประกาศว่าเหตุการณ์ภัยพิบัติได้เกิดขึ้นอย่างเป็นทางการ ผู้นำการกู้คืนระบบจะต้องดำเนินการ เปิดใช้งานแผนกู้คืนระบบ (DRP) โดยเริ่มต้นจากการแจ้งเหตุผ่าน สายการติดต่อ (Disaster Recovery Call Tree) ในการสื่อสารควรระบุข้อมูลสำคัญ ได้แก่

7.2.1. ลักษณะของภัยพิบัติที่เกิดขึ้น
7.2.2. ผลกระทบที่มีต่อระบบหรือการดำเนินงาน
7.2.3. ระยะเวลาที่คาดว่าจะฟื้นฟูได้
7.2.4. มาตรการที่กำลังดำเนินการอยู่

หากผู้นำการกู้คืนระบบไม่สามารถปฏิบัติหน้าที่ได้ ตัวแทนจากทีมผู้บริหารระดับสูง จะเป็นผู้รับช่วงความรับผิดชอบในการดำเนินการกู้คืนระบบทันที

หมายเหตุ ทีมผู้บริหารระดับสูงควรเป็นกลุ่มแรกที่ได้รับแจ้งเมื่อมีการประกาศสถานการณ์ภัยพิบัติ สำหรับแนวทางการสื่อสารอื่น ๆ ให้ดูรายละเอียดในหัวข้อที่ 6 การสื่อสารในระหว่างเกิดเหตุการณ์ภัยพิบัติ (Communicating During a Disaster)

7.3. การฟื้นฟูการทำงานของระบบเทคโนโลยีสารสนเทศ (Restoring IT system functionality)

หากสถานการณ์ภัยพิบัติเกิดขึ้นจริงและวิทยาลัยต้องดำเนินการตามแผนกู้คืนระบบ (DRP) ส่วนนี้จะเป็น แนวทางอ้างอิงหลัก โดยแสดงรายละเอียดขั้นตอนการฟื้นฟูระบบและบริการด้านเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ ข้อมูลที่ควรรวบรวมในส่วนนี้ ได้แก่

1) Run-book และแผนผังระบบเครือข่าย
2) รายละเอียดเกี่ยวกับรูปแบบซอฟต์แวร์และการกำหนดค่าระบบ
3) แผนผังโครงสร้างระบบในปัจจุบัน (Current System Architecture)
4) สถานที่สำหรับฟื้นฟูระบบ (Physical Recovery Facilities)
5) ระบบเทคโนโลยีสารสนเทศ (IT Systems)

Current System Architecture

Physical Recovery Facilities

IT Systems

ลำดับความสำคัญ Rank	**ชื่อระบบ** IT System	**องค์ประกอบของระบบ** System components (in order of importance)
1	ระบบทะเบียนนักศึกษา (Student Registration System)	• ฐานข้อมูลนักศึกษา • ระบบลงทะเบียนเรียน • ระบบประมวลผลผลการเรียน • ระบบออกเอกสารทางการศึกษา (ใบรับรอง, Transcript)
2	ระบบเว็บไซต์วิทยาลัย (College Website)	• Web Server • Content Management System (CMS) • DNS & Hosting • Analytics Integration
3	ระบบจัดเก็บไฟล์ (File Server)	• Network Attached Storage (NAS) • File sharing & permission control • Backup & archive services
4	ระบบโทรศัพท์ผ่านเครือข่าย (VoIP)	• IP-PBX System • VoIP Gateway • Internal extension network • Call recording & logs

ตารางที่ 12. การฟื้นฟูระบบเทคโนโลยีสารสนเทศ (IT System Restoration)

8. การทดสอบและการบำรุงรักษาแผน (Plan Testing & Maintenance)

แม้ว่า วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล จะได้ดำเนินการจัดทำแผนกู้คืนระบบจากภัยพิบัติอย่างรอบคอบและครบถ้วนที่สุดเท่าที่จะสามารถดำเนินการได้ แต่อย่างไรก็ตาม การจัดทำแผนให้สามารถรองรับสถานการณ์ที่อาจเกิดขึ้นได้ในทุกกรณียังคงเป็นสิ่งที่มีความท้าทาย เนื่องจากความต้องการและบริบทในการดำเนินงานของสถานศึกษาย่อมมีการเปลี่ยนแปลงอย่างต่อเนื่องตามช่วงเวลา

ด้วยเหตุนี้ แผนกู้คืนระบบจากภัยพิบัติ จึงจำเป็นต้องได้รับการ ทดสอบอย่างสม่ำเสมอ เพื่อประเมินความพร้อม ตรวจสอบข้อบกพร่อง และระบุช่องว่างที่อาจเกิดขึ้นในการปฏิบัติจริง อีกทั้งยังควรได้รับการ บำรุงรักษาและปรับปรุงอย่างต่อเนื่อง เพื่อให้แผนดังกล่าวมีความทันสมัย และสามารถรองรับการเปลี่ยนแปลงของระบบงานและโครงสร้างพื้นฐานของสถานศึกษาได้อย่างเหมาะสม ทั้งนี้เพื่อให้สามารถนำแผนไปใช้ได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดเมื่อเกิดเหตุการณ์ไม่คาดคิดขึ้นจริง

8.1. Maintenance

แผนกู้คืนระบบจากภัยพิบัติ นี้จะต้องได้รับการปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับเปลี่ยนหรืออัปเกรดระบบ หรือบริการเทคโนโลยีสารสนเทศที่สำคัญ ไม่ว่าจะกรณีใดเกิดก่อน โดยให้งานเทคโนโลยีสารสนเทศ

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล เป็นผู้รับผิดชอบหลักในการดูแล บำรุงรักษา และดำเนินการปรับปรุงแผนฉบับนี้ให้มีความถูกต้อง ครบถ้วน และสอดคล้องกับสภาพแวดล้อมขององค์กร โดยมีอำนาจในการประสานงาน ขอรับข้อมูล หรือขอความร่วมมือจากหน่วยงานหรือบุคลากรที่เกี่ยวข้องภายในองค์กร เพื่อให้การปรับปรุงแผนเป็นไปอย่างมีประสิทธิภาพและทันต่อสถานการณ์

การบำรุงรักษาแผนจะครอบคลุมถึงกิจกรรมต่าง ๆ ดังต่อไปนี้

8.1.1. การปรับปรุงข้อมูลในสายการติดต่อกรณีฉุกเฉิน (Disaster Recovery Call Tree) ให้เป็นปัจจุบัน

8.1.2. การทบทวนบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้องในการกู้คืนระบบ

8.1.3. การตรวจสอบและปรับปรุงเนื้อหาในแผนให้สอดคล้องกับบริบทปัจจุบันของสถานศึกษา

8.1.4. การปรับปรุงแผนให้สะท้อนถึงการเปลี่ยนแปลงด้านโครงสร้างองค์กร ระบบเทคโนโลยีสารสนเทศ และเป้าหมายขององค์กร

8.1.5. การตรวจสอบให้แน่ใจว่าแผนยังคงสอดคล้องกับกฎหมาย ระเบียบ หรือข้อบังคับที่มีผลบังคับใช้ในปัจจุบัน

8.1.6. การดำเนินการบำรุงรักษาอื่น ๆ ตามบริบทเฉพาะและความจำเป็นของวิทยาลัย

8.2. การทดสอบแผน (Testing) จำลองเหตุการณ์ไฟไหม้ จำลอง

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล มีความมุ่งมั่นในการดำเนินการให้แผนการกู้คืนระบบจากภัยพิบัตินี้สามารถนำไปปฏิบัติได้จริงอย่างมีประสิทธิภาพในกรณีเกิดเหตุฉุกเฉิน เพื่อให้แผนดังกล่าวมีความพร้อมใช้งานและสามารถตอบสนองต่อสถานการณ์ได้อย่างเหมาะสม จึงกำหนดให้มีการ ทดสอบแผนอย่างน้อยปีละ 1 ครั้ง หรือบ่อยครั้งตามความเหมาะสมหรือเมื่อมีการปรับเปลี่ยนระบบสารสนเทศที่สำคัญ

8.2.1. การทดสอบจะดำเนินการโดยใช้วิธีการที่เหมาะสมกับบริบทของวิทยาลัย เช่น

(1) การจำลองสถานการณ์ (Simulation Exercise)

(2) การฝึกอบรมเชิงปฏิบัติการ (Tabletop Exercise)

(3) การทดสอบระบบจริงบางส่วนหรือทั้งหมด (Live Test or Partial Failover)

8.2.2. วัตถุประสงค์ของการทดสอบ

(1) การประเมินความพร้อมของระบบ บุคลากร และกระบวนการตามที่กำหนดไว้ในแผน

(2) การตรวจสอบความเข้าใจของบุคลากรที่มีหน้าที่รับผิดชอบ

(3) การระบุจุดอ่อน ข้อบกพร่อง หรือช่องว่างที่อาจเกิดขึ้นในการดำเนินการตามแผน

(4) การนำผลการทดสอบมาใช้เป็นข้อมูลประกอบการปรับปรุงแผนให้มีประสิทธิภาพยิ่งขึ้น

ผลการทดสอบจะถูกจัดทำเป็นรายงานอย่างเป็นทางการ พร้อมข้อเสนอแนะในการปรับปรุงแก้ไข และจัดเก็บเป็นหลักฐานสำหรับการตรวจสอบหรืออ้างอิงในอนาคต

9. ข้อมูลเวอร์ชันและการเปลี่ยนแปลง (Version Information and Changes)

เวอร์ชัน Version	**คำอธิบายการเปลี่ยนแปลง** Change Description	**ตรวจสอบโดย** Reviewed By	**อนุมัติโดย** Approved By	**วันที่** Date

เอกสารแนบที่ 2

แบบฟอร์มบันทึกการทดสอบการกู้คืนระบบ (System Recovery Test Record Form)

ทดสอบการกู้คืนระบบ (Disaster Recovery Test)

Date of Inspection	Name of Inspector	Department	System Name	Description	System Category	Type	Date of Latest Backup	Type of Backup	Backup Storage Location	Recovery Testing Procedures	Status	Test Result Summary	Suggestions
4/18/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	KS Database	Production Keystone Database	ระบบฐานข้อมูล (Database)	Virtual Machine	4/18/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	KS Database Replication	Production Keystone Replication Da	ระบบฐานข้อมูล (Database)	Virtual Machine	m/d/yyyy xx:xx	เพิ่มเติม (Incremental)	Cloud Storage	ตรวจสอบความถูกต้องของข้อมูลหลังการกู้คืน	Fail	Fail	Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	Swarm NFS	Swarm NFS Storage VM	ระบบไฟล์เซิร์ฟเวอร์ (File Server)	Virtual Machine	m/d/yyyy xx:xx	เพิ่มเติม (Incremental)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Post-ev...	Post-event	Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	Zabbix	Network Monitoring & Notification	ระบบเครือข่าย (Network System)	Virtual Machine	m/d/yyyy xx:xx	Completed	Completed				Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	Active Directory (muic.io)	Active Directory for MUIC	LDAP	Virtual Machine	m/d/yyyy xx:xx						Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	Keycloak	IdP for Inhouse Application Authent	Identity Provider (IdP)	Virtual Machine	m/d/yyyy xx:xx						Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	SKY-Database	Legacy Database for the older SKY a	ระบบฐานข้อมูล (Database)	Bare metal	m/d/yyyy xx:xx						Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	Swarm-Node-01	Swarm Cluster Node 1	ระบบแอปพลิเคชัน (Application)	Virtual Machine	m/d/yyyy xx:xx						Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	ZealData	Legacy Ticket Application	ระบบแอปพลิเคชัน (Application)	File	m/d/yyyy xx:xx						Suggestions
m/d/yyyy xx:xx	Artit Taweedeit	IT Infrastructure Unit	QNAP-06-Configuration	Configuration file for QNAP-06	ระบบไฟล์เซิร์ฟเวอร์ (File Server)	Configuration	m/d/yyyy xx:xx		0.2"				Suggestions
4/21/2025 8:10:00	Warunya Bavornkijsutee	IT Infrastructure Unit	ad.muic.io-Win2022	Recovery Test	ระบบฐานข้อมูล (Database)	Virtual Machine	4/21/2025 8:10:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	มี path update windows
4/21/2025 8:55:00	Warunya Bavornkijsutee	IT Infrastructure Unit	IC-Data-230	Recovery Test	ระบบฐานข้อมูล (Database)	Virtual Machine	4/21/2025 8:55:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
4/21/2025 10:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	IC-DB-200	Recovery Test	ระบบฐานข้อมูล (Database)	Virtual Machine	4/21/2025 10:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
4/21/2025 14:30:00	Warunya Bavornkijsutee	IT Infrastructure Unit	MU-Haproxy-243	Recovery Test	ระบบเครือข่าย (Network System)	Virtual Machine	4/21/2025 14:30:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
4/21/2025 14:30:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Web-Dspace-126	Recovery Test	ระบบแอปพลิเคชัน (Application)	Virtual Machine	4/21/2025 14:30:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
4/23/2025 8:40:00	Warunya Bavornkijsutee	IT Infrastructure Unit	EDX App - 251	Recovery Test	ระบบแอปพลิเคชัน (Application)	Virtual Machine	m/d/yyyy xx:xx						Suggestions
4/25/2025 14:30:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Web-Netbox-240-Local10k	Recovery Test	ระบบแอปพลิเคชัน (Application)	Virtual Machine	m/d/yyyy xx:xx						Suggestions
5/26/2025 0:00:00	Artit Taweedeit	IT Infrastructure Unit	DB - Keystone - Prod - 234	DB - Production Keystone Database	ระบบฐานข้อมูล (Database)	Database	5/26/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	ทดสอบ reconfigure repliaction เพราะ ทาง ม. ลบไป เพื่อแก้ปัญหาดิสก์บวม
5/26/2025 0:00:00	Artit Taweedeit	IT Infrastructure Unit	DB - Keystone - Replicate - 243	DB - Production Keystone Database	ระบบฐานข้อมูล (Database)	Database	5/26/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	ทดสอบ reconfigure repliaction เพราะ ทาง ม. ลบไป เพื่อแก้ปัญหาดิสก์บวม
6/25/2025 9:05:00	Warunya Bavornkijsutee	IT Infrastructure Unit	DB-Keystone-Prod-234	DB - Production Keystone Database	ระบบฐานข้อมูล (Database)	Database	5/26/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass		Suggestions
7/7/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	PC - Online - 29	Recovery systems update security	ระบบแอปพลิเคชัน (Application)	Configuration	7/7/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass		Suggestions
7/7/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Web-Wiki-240	Recovery systems update security	ระบบแอปพลิเคชัน (Application)	Configuration	7/7/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass		Suggestions
7/7/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Web - ICPayment - 220	Recovery systems update security	ระบบแอปพลิเคชัน (Application)	Configuration	7/7/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	Correction of technical issues in systems	Pass		Suggestions
8/8/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	PC - Online - 29	Recovery systems update security	ระบบแอปพลิเคชัน (Application)	Virtual Machine	8/8/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	A config encryption file backup
8/8/2025 16:30:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Toshiba-Printer-138	Printer Solutions	ระบบแอปพลิเคชัน (Application)	Virtual Machine	8/8/2025 16:40:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	A config encryption file backup
9/24/2025 9:30:00	Warunya Bavornkijsutee	IT Infrastructure Unit	EDX App - 251	https://muiclms.mahidol.ac.th/	ระบบแอปพลิเคชัน (Application)	Virtual Machine	9/24/2025 10:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Testing after encrypting data in the backup process (https://muiclms.mahidol.ac.th/)
10/6/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	Web-Netbox-240-Local10k	Infra	ระบบแอปพลิเคชัน (Application)	Virtual Machine	9/24/2025 10:30:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Testing after encrypting data in the backup process
10/6/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	APISIX - 199		ระบบแอปพลิเคชัน (Application)	Virtual Machine	10/6/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ตรวจสอบข้อมูลสำรองล่าสุด	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	Suggestions
10/8/2025 0:00:00	Warunya Bavornkijsutee	IT Infrastructure Unit	EntraSync-AD	Infra	ระบบแอปพลิเคชัน (Application)	Virtual Machine	10/8/2025 0:00:00	เต็มรูปแบบ (Full)	NAS / SAN	ดำเนินการกู้คืนระบบจากข้อมูลสำรอง	Pass	ระบบสามารถกู้คืนได้อย่างสมบูรณ์	โอกย่าย Pyical Hardware

เอกสารแนบที่ 3

เอกสารการประชุมขอคำปรึกษาและข้อเสนอแนะเกี่ยวข้องกับมาตรฐานด้านเทคโนโลยีสารสนเทศ

ขอคำปรึกษาและข้อเสนอแนะเกี่ยวข้องกับมาตรฐาน ด้านเทคโนโลยีสารสนเทศ

วันอังคารที่ 5 สิงหาคม 2568 เวลา 10.00 - 12.00 น.

ณ ห้อง A254 อาคารอทิตยาทร

วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล

Agenda

กำหนดการ

หัวข้อที่ 1

Overview of the Information Technology Team

แนะนำโครงสร้างทีม IT แบ่งเป็น 5 ทีมหลัก พร้อมภารกิจ เช่น ดูแลระบบเครือข่าย พัฒนาระบบ สนับสนุนผู้ใช้ และบริหารจัดการข้อมูล

หัวข้อที่ 2

What We Are Doing Now

การดำเนินงานด้านโครงการเชิงยุทธศาสตร์ที่งานเทคโนโลยีสารสนเทศ

1. Seamless Data Integration
2. Modernize IT Infrastructure
3. MUIC AI Solutions

หัวข้อที่ 3

What We Are Focusing On Right Now

มุ่งเน้นด้านการกำหนดมาตรฐานเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

1. แนวปฏิบัติและนโยบายการใช้งานระบบสารสนเทศสำหรับผู้ใช้งานทั่วไป
2. การเทียบเคียงมาตรการความมั่นคงปลอดภัยไซเบอร์ CIS
3. แผนความต่อเนื่องทางธุรกิจ BCP

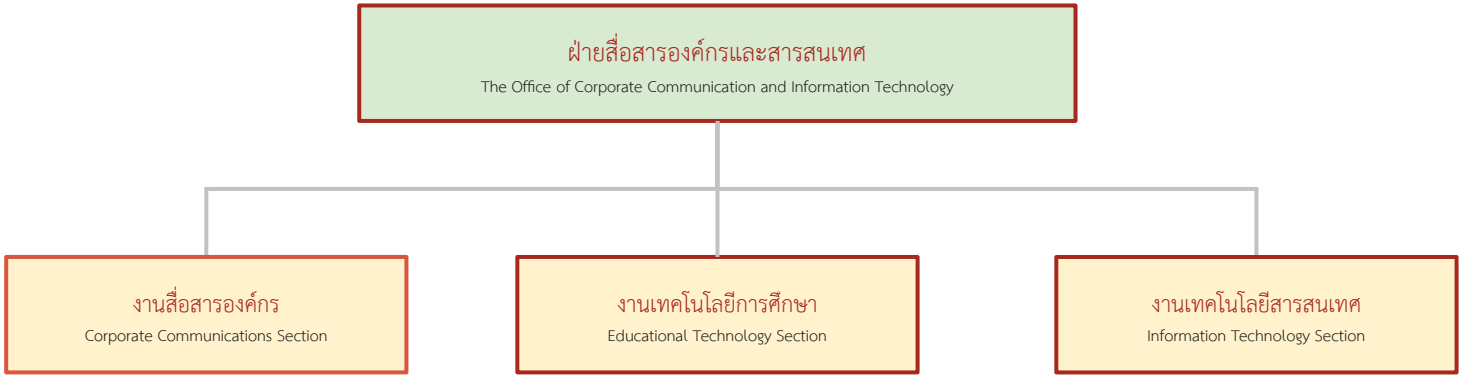
หัวข้อที่ 4

Request for Support

ขอคำแนะนำเกี่ยวกับกำหนดกรอบนโยบายและแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

Organization Chart

The Office of Corporate Communication and Information Technology



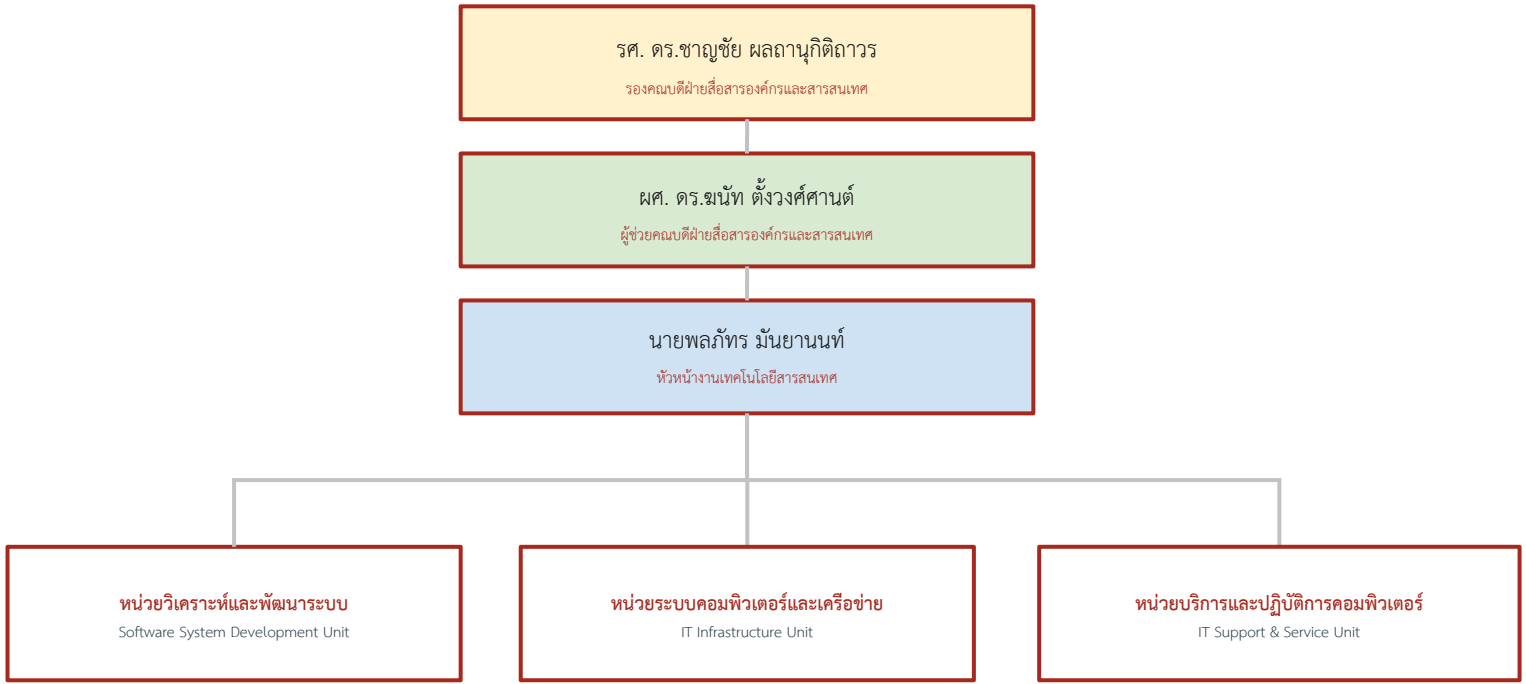
1. ดูแลและปรับปรุงเว็บไซต์ของวิทยาลัย (MUIC Website)
2. เผยแพร่ข่าวสารและข้อมูลผ่านช่องทางสื่อสารต่าง ๆ
3. ออกแบบและผลิตสื่อประชาสัมพันธ์สำหรับกิจกรรมและงานทั่วไป
4. บันทึกภาพนิ่งและวิดีโอสำหรับกิจกรรมของวิทยาลัย

1. บริการด้านอุปกรณ์และระบบโสตทัศนูปกรณ์
เช่น โปรเจกเตอร์ เครื่องเสียง ไมโครโฟน ฯลฯ
2. บริการด้านสื่อการเรียนการสอน
เช่น บริการผลิตสื่อ e-Learning และสื่อวิดีโอเพื่อการศึกษา
3. บริการออกแบบและผลิตสื่อ เช่น ออกแบบโปสเตอร์ แผ่นพับ และสื่อประชาสัมพันธ์ทางวิชาการ ตัดต่อวิดีโอ สร้างภาพประกอบ และ Presentation เพื่อการเรียนการสอน

1. ให้บริการและสนับสนุนผู้ใช้งานด้าน IT
2. ดูแลระบบเครือข่ายคอมพิวเตอร์ (LAN/Wi-Fi)
3. บริหารจัดการเครื่องแม่ข่าย (Server) และระบบจัดเก็บข้อมูล (Storage)
4. พัฒนาและบำรุงรักษาระบบสารสนเทศด้านการศึกษา
5. พัฒนาเครื่องมือและระบบงานเพื่อสนับสนุนการทำงานภายในหน่วยงาน
6. ดูแลและพัฒนาระบบบริหารจัดการการศึกษาของ MUIC
7. ดูแลและบริหารจัดการข้อมูลสารสนเทศของวิทยาลัย
8. กำกับดูแลและดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Policy)

Organization Chart
Information Technology Section
งานเทคโนโลยีสารสนเทศ

ลักษณะตามโครงสร้าง

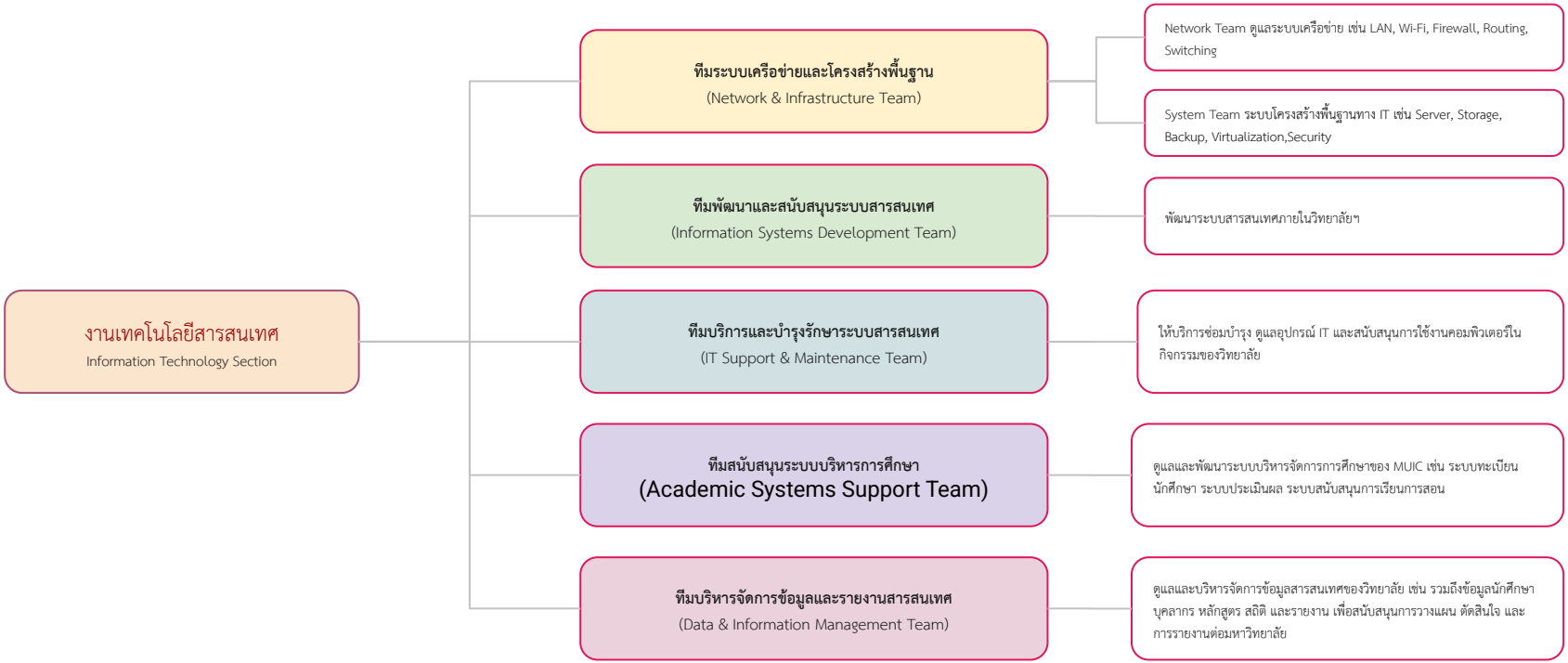


Organization Chart

Information Technology Section

งานเทคโนโลยีสารสนเทศ

ลักษณะตามการดำเนินงาน



Organization Chart

IT Infrastructure Unit

หน่วยระบบคอมพิวเตอร์และเครือข่าย

นายพลภัทร มันยานนท์

หัวหน้างานเทคโนโลยีสารสนเทศ

Network Infrastructure

นายกรกฎ อินทราเวช

หัวหน้าหน่วยระบบคอมพิวเตอร์และเครือข่าย

นายจิรา ฉัตรนราธิป

นักวิชาการคอมพิวเตอร์

System Infrastructure

นายอาทิตย์ ทวีเดช

นักวิชาการคอมพิวเตอร์

นางสาววรัญญา บวรกิจสุธี

นักวิชาการคอมพิวเตอร์

Organization Chart

Software System Development Unit

หน่วยวิเคราะห์และพัฒนาระบบ

นายพลภัทร มันยานนท์

หัวหน้างานเทคโนโลยีสารสนเทศ

- SKY+ Team
  - 
    นายเจตพัสดิ์ เสาทอง
    นักวิชาการคอมพิวเตอร์
  - 
    น.ส.ทิพวรรณ งามนิธิชวนันท์
    นักวิชาการคอมพิวเตอร์
- Data Team
  - 
    น.ส.จันทิมา นุชโยธิน
    นักวิชาการคอมพิวเตอร์
- In-house development
  - 
    นายนิวัฒน์ ศรีสมโภช
    นักวิชาการคอมพิวเตอร์
  - 
    นายกฤษณะ ชื่นชม
    นักวิชาการคอมพิวเตอร์
  - 
    นายปฏิภาณ วัจนาภรณ์
    นักวิชาการคอมพิวเตอร์

Organization Chart

IT Infrastructure Unit

หน่วยระบบคอมพิวเตอร์และเครือข่าย

นายพลภัทร มันยานนท์

หัวหน้างานเทคโนโลยีสารสนเทศ

IT Support & Service Unit

น.ส.อรอัจจิมา ประวัติเจริญฉัตร

หัวหน้าหน่วยบริการและปฏิบัติการคอมพิวเตอร์

นายเกศวิทย์ ภูพวก

เจ้าหน้าที่ระบบงานคอมพิวเตอร์

นายนภวิชญ์ เลิศเจริญพงศา

นักวิชาการคอมพิวเตอร์

นายเมษา นุตาลัย

นักวิชาการคอมพิวเตอร์

Key Strategic Projects Under the Leadership of the IT Unit

โครงการเชิงยุทธศาสตร์ที่งานเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบหลัก

PJ11	**โครงการจัดทำนโยบายและพัฒนาการบริหารจัดการข้อมูลวิทยาลัยนานาชาติ** (Seamless Data Integration) ระยะเวลาดำเนินการ 2567 - 2570 จำนวน 4 ปี	• ผลักดันให้วิทยาลัยมีการบริหารจัดการข้อมูลอย่างมีคุณภาพและนำไปใช้ประโยชน์ได้จริง • กำหนดกรอบการบริหารจัดการข้อมูลที่ชัดเจน มีสิทธิการเข้าถึง และกระบวนการทำงานที่เป็นระบบ • เชื่อมโยงและบูรณาการข้อมูลระหว่างหน่วยงานอย่างมีประสิทธิภาพ
PJ12	**โครงการยกระดับความมั่นคงปลอดภัยทางด้าเทคโนโลยีสารสนเทศ** (Modernize IT Infrastructure) ระยะเวลาดำเนินการ 2567 - 2569 จำนวน 3 ปี	• วางมาตรการ นโยบาย และกลไกในการป้องกันและรับมือเหตุอุกเฉินทางไซเบอร์ • ตรวจสอบและควบคุมเครือข่าย เพื่อป้องกันการโจมตีและรักษาความปลอดภัยระบบ • เพิ่มช่องทางรับส่งข้อมูล (Bandwidth) และช่องทางสื่อสารสำรองกรณีระบบหลักขัดข้อง
PJ14	**โครงการ MUIC AI Solutions** ระยะเวลาดำเนินการ 2568 - 2569 จำนวน 2 ปี	• พัฒนา ระบบ Copter เพื่อให้ข้อมูลและคำปรึกษาแก่นักศึกษาแบบอัตโนมัติ ตลอด 24 ชั่วโมง • พัฒนา ระบบ Helix เพื่อให้บุคลากรและอาจารย์เข้าถึงเครื่องมือ Generative AI อย่างปลอดภัยและมีประสิทธิภาพ พัฒนา AI-Powered Productivity Suite เพื่อเพิ่มประสิทธิภาพการทำงาน และสนับสนุนแนวคิด Smart Office • วางรากฐานสู่ Smart Campus ที่ขับเคลื่อนด้วยข้อมูลและเทคโนโลยีอัจฉริยะ

โครงการยกระดับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (Modernize IT Infrastructure)

ผลผลิต – OUTPUT (ผลผลิตที่ได้รับการดำเนินกิจกรรม)

1. มีกรอบนโยบายและแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สามารถเทียบเคียงกับมาตรฐานสากลอย่างใดอย่างหนึ่ง
2. มีกรอบนโยบายมาตรฐานและแนวทางการปฏิบัติ เพื่อรับมือกับสถานการณ์ฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ (Business Continuity Planning : BCP)
3. มีพิมพ์เขียวด้านเทคโนโลยีสารสนเทศ (Enterprise Blueprint) เพื่อเป็นกรอบแนวทางและขั้นตอนวิธีการสำหรับการวิเคราะห์ ออกแบบ วางแผน ด้านเทคโนโลยีสารสนเทศ
4. มีระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ (Firewall)
5. มีช่องทางการรับส่งข้อมูล (Bandwidth) ที่เพิ่มขึ้น เพื่อรองรับความต้องการของผู้ใช้งานด้านเครือข่ายไร้ข่าย (Wi-Fi) และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้ของวิทยาลัยฯ
6. มีระบบบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) ซึ่งสามารถนำมาคาดการงบประมาณ การบำรุงรักษา (End of life) การบริหารความเสี่ยงด้านการสิ้นสุดการผลิตอะไหล่หรือยุติการให้บริการจากผู้ผลิต (End of support) เพื่อนำมาตัดสินใจในเชิงปฏิบัติและเชิงกลยุทธ์ต่อไป

แผนการดำเนินโครงการ และตัวชี้วัดความสำเร็จ

เชิงปริมาณ	หน่วยนับ	ปีงบ 2567		ปีงบ 2568		ปีงบ 2569	
		แผน	ผล	แผน	ผล	แผน	ผล
1. มีกรอบนโยบายและแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สามารถเทียบเคียงกับมาตรฐานสากลอย่างใดอย่างหนึ่ง	1 ฉบับ	35%		70%		100%	1 ฉบับ
2. มีกรอบนโยบายมาตรฐานและแนวทางการปฏิบัติ เพื่อรับมือกับสถานการณ์ฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ (Business Continuity Planning : BCP)	1 ฉบับ	100%	1 ฉบับ				
3. มีพิมพ์เขียวด้านเทคโนโลยีสารสนเทศ (Enterprise Blueprint) เพื่อเป็นกรอบแนวทางและขั้นตอนวิธีการสำหรับการวิเคราะห์ ออกแบบ วางแผน ด้านเทคโนโลยีสารสนเทศ	1 ฉบับ	100%	1 ฉบับ				
4. มีระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ	1 ระบบ	35%		70%		100%	1 ระบบ
5. มีระบบบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)	1 ระบบ	35%		70%		100%	1 ระบบ

ตารางเปรียบเทียบผลการดำเนินงานกับแผนปฏิบัติงาน Internet Bandwidth

ในปีงบประมาณ พ.ศ. 2568 องค์กรมีการเชื่อมต่ออินเทอร์เน็ตผ่านผู้ให้บริการอินเทอร์เน็ต (ISP) จำนวน 3 ราย โดยแต่ละรายมีแบนด์วิธไม่น้อยกว่า 2 กิกะบิตต่อวินาที (Gbps)

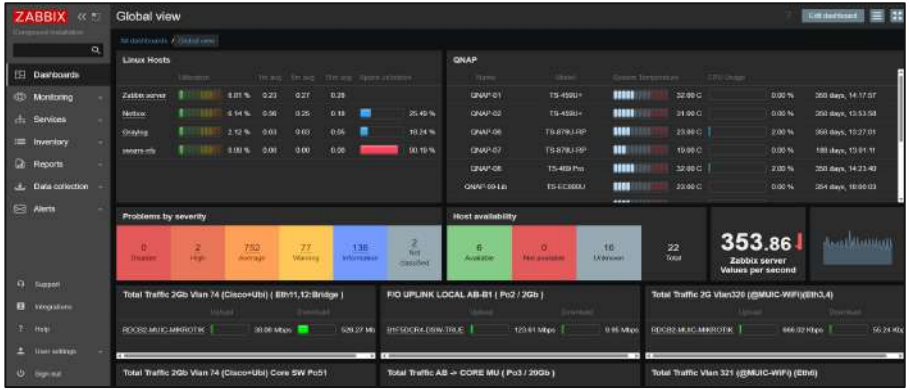
ISP	Internet Bandwidth (Domestic/International)		
	2568	2569	2570
UIH	950/950 Mbps	950/950 Mbps	เป้าหมายของเราสำหรับปีงบประมาณ 2570 จะดำเนินการปรับเพิ่ม Bandwidth ให้ไม่น้อยกว่า 2,000 Mbps
True	300/300 Mbps	350/350 Mbps	
3BB	300/300 Mbps	350/350 Mbps	
Target	**1,550/1,550 Mbps**	**≥ 1,650/1,650 Mbps**	**≥ 2,000/2,000 Mbps**

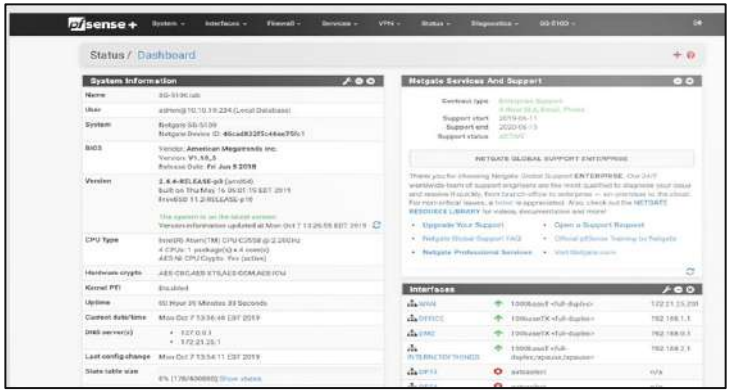
หมายเหตุ: เป้าหมาย Bandwidth ที่กำหนดไว้สอดคล้องกับการเติบโตของวิทยาลัยฯ และความต้องการใช้งานที่เพิ่มขึ้นอย่างต่อเนื่อง

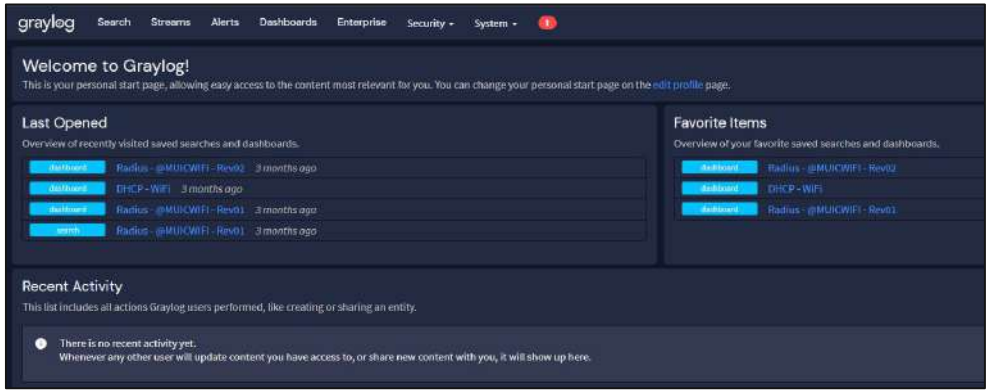
การดำเนินงานด้านเทคโนโลยีสารสนเทศ ปี 2568 ที่ผ่านมา

หัวข้อการดำเนินงาน	รายละเอียด / แผนงาน	สถานะการดำเนินงาน
กรอบนโยบายและแนวทางการปฏิบัติงาน	แผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ	มีการนำเสนอกับการประชุมผู้บริหาร ครั้งที่ 8/2568 (MUIC Executive Meeting No.08/2025)
	แนวปฏิบัติและนโยบายการใช้งานระบบสารสนเทศสำหรับผู้ใช้งานทั่วไป	อยู่ระหว่างรอนำเสนอเพื่อพิจารณาโดยคณะกรรมการวิชาการ (Faculty Committee)
	แผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning – BCP)	อยู่ระหว่างการปรับปรุง/จัดทำข้อมูลประกอบ
	การเทียบเคียงมาตรการความมั่นคงปลอดภัยไซเบอร์ Center for Internet Security (CIS)	อยู่ระหว่างการจัดทำข้อมูล
พิมพ์เขียวด้านเทคโนโลยีสารสนเทศ (Enterprise Blueprint)	ระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ	- อยู่ระหว่างการ Update ข้อมูล Physical Diagram และระบบ Netbox ในการช่วยทำ automate - อยู่ในระหว่างการประเมินทรัพยากร ติดตั้ง คอนฟิก และทดสอบ ระบบ SIEM
Cyber Surveillance	พัฒนาและติดตั้งระบบ Cyber Surveillance และตอบสนองต่อภัยคุกคาม	ติดตั้งและกำหนดค่าเพื่อใช้งาน Security Onion และ Wazuh ในการตรวจจับและวิเคราะห์เหตุการณ์ความปลอดภัยแบบเรียลไทม์
ระบบบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)	นำเครื่องมือ Netbox มาใช้ในการจัดเก็บข้อมูลสินทรัพย์ เช่น เครื่องแม่ข่าย, อุปกรณ์เครือข่าย, IP Address, Rack และสายเชื่อมต่อ	มีการใช้งานระบบ และอยู่ระหว่างการ Update ข้อมูลให้มีความสมบูรณ์

ภาพตัวอย่างระบบต่างๆ







แผนดำเนินงานด้านเทคโนโลยีสารสนเทศ ปี 2569

1. **เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ (MUIC cyber security framwork) 100%**
    - นำแนวทางจากมาตรฐาน CIS (Center for Internet Security) มาประยุกต์ใช้เป็นกรอบการดำเนินงานด้านความปลอดภัยของ MUIC

2. **จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning – BCP) 100%**
    - พัฒนาแนวทางการรับมือเหตุฉุกเฉิน และวางระบบสำรองเพื่อให้บริการทาง IT ดำเนินต่อได้อย่างต่อเนื่อง

3. **ออกแบบโครงสร้างระบบ IT เชิงสถาปัตยกรรม (Enterprise Blueprint) 100%**
    - จัดทำ Template Flow, Logical Diagram, และ Physical Diagram เพื่อกำหนดภาพรวมระบบและแนวทางการพัฒนาโครงสร้างพื้นฐาน

4. **ระบบติดตามและเฝ้าระวัง IT (IT Monitoring System) 100%**
    - ใช้เครื่องมือ Zabbix และ Graylog ในการติดตามสถานะระบบเครือข่าย, Server, บริการสำคัญ และตรวจสอบ Log อย่างต่อเนื่อง และนำ SIEM มาใช้งานเพื่อเฝ้าระวังระบบที่เกี่ยวข้อง

5. **บริหารจัดการสินทรัพย์ด้าน IT อย่างเป็นระบบ (IT Asset Management) 100%**
    - นำเครื่องมือ Netbox มาใช้ในการจัดเก็บข้อมูลสินทรัพย์ เช่น เครื่องแม่ข่าย, อุปกรณ์เครือข่าย, IP Address, Rack และสายเชื่อมต่อ

6. **เพิ่มขีดความสามารถด้านเครือข่าย (Strengthen Network Capability) 100%**
    - ขยายความเร็วอินเทอร์เน็ตสำหรับการเชื่อมต่อ (Domestic/International) ≥ 1,550/1,550 Mbps

ขอความอนุเคราะห์ในการให้คำแนะนำเพื่อประกอบการดำเนินการในประเด็นดังกล่าว

1. แผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ - แผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ.pdf
2. แนวปฏิบัติและนโยบายการใช้งานระบบสารสนเทศสำหรับผู้ใช้งานทั่วไป - แนวปฏิบัติและนโยบายการใช้งานระบบสารสนเทศสำหรับผู้ใช้งานทั่วไป.pdf
3. แผนความต่อเนื่องทางธุรกิจ (Business Continuity Planning – BCP) - BCP.pdf
4. การเทียบเคียงมาตรการความมั่นคงปลอดภัยไซเบอร์ Center for Internet Security (CIS) - CIS_Controls_Version_8.1_6_24_2024.xlsx

ช่วงถาม-ตอบข้อสงสัย (Q & A)

1. เรื่องที่ควรทำก่อน - ลำดับงานที่ควรทำ (ก่อนหลัง)
2. เรื่องที่น่าทำ (เร่งด่วน เพราะจะสามารถยกระดับความปลอดภัยได้อย่างรวดเร็ว)

<u>สรุปหลังประชุมที่ต้องดำเนินการ</u>

การบ้านที่ต้องส่งในวันอังคารที่ 2 กันยายน 2568

1. Topology Network Diagram
2. Firewall Rule
3. Network Segmentation
4. Overview Inventory

เอกสารแนบที่ 4

โครงการยกระดับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (ICIT Modernize IT Infrastructure)

Mahidol University
International College

รหัสโครงการ **PJ12/2567**

แบบเสนอโครงการงบประมาณเงินรายได้ ประจำปีงบประมาณ 2567

ส่วนที่ 1 : ข้อมูลพื้นฐาน

1.1 ชื่อโครงการ:

โครงการยกระดับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (Modernize IT Infrastructure)

1.2 ผู้รับผิดชอบโครงการ: น.ส.วรัญญา บวรกิจสุธี

หน่วยงาน: งานเทคโนโลยีสารสนเทศ

1.3 แผนงาน: แผนงานยุทธศาสตร์ / Strategic Plan

1.4 ผลผลิต / โครงการ: ผู้สำเร็จการศึกษาด้านสังคมศาสตร์

1.5 ลักษณะโครงการ: โครงการของหน่วยงาน

1.6 ประเภทของโครงการ: โครงการใหม่ / New projects

1.7 ปีงบประมาณปัจจุบัน: 2567 **ปี**

งบประมาณเริ่มต้นโครงการ: ตุลาคม 2566 ปี

งบประมาณสิ้นสุดโครงการ: กันยายน 2569 ปี

ระยะเวลาดำเนินโครงการทั้งหมด: 3 ปี

1.8 ที่ตั้งโครงการ/พื้นที่ให้บริการ: วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล

ความสอดคล้องกับนโยบาย:

1.8.1 สอดคล้องกับนโยบายรัฐบาล:

การพัฒนาและส่งเสริมการใช้ประโยชน์จากวิทยาศาสตร์เทคโนโลยี การวิจัยพัฒนา และนวัตกรรม

1.8.2 สอดคล้องกับยุทธศาสตร์มหาวิทยาลัยมหิดล:

Management for Self-Sufficiency and Sustainable Organization

1.8.3 สอดคล้องกับยุทธศาสตร์วิทยาลัยนานาชาติ:

Optimize sustainability of the organization

1.8.4 SDG :

Goal 9: Industry, Innovation and Infrastructure: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation

1.8.5 เป้าหมายการให้บริการหน่วยงาน:

เพื่อบริการวิชาการแก่หน่วยงาน/ประชาชนในชุมชนและสังคมให้มีความรู้ความสามารถในการพัฒนาตนเองเพื่อเพิ่มศักยภาพในการแข่งขันของประเทศ

ส่วนที่ 2 : ข้อมูลทั่วไปของโครงการ

2.1 หลักการและเหตุผลของโครงการ

ในปัจจุบันเทคโนโลยีต่างๆ ได้เข้ามามีบทบาทสำคัญและมีความจำเป็นต่อการดำเนินงานภายในองค์กรอย่างมีนัยสำคัญ รวมทั้งยังมีการพัฒนาอย่างรวดเร็วแบบก้าวกระโดด ทำให้องค์กรทั้งภาครัฐและเอกชนต้องตระหนักถึงการปรับปรุงเปลี่ยนแปลงกลไกด้านเทคโนโลยีให้ทันสมัยและสอดคล้องกับกระแสโลก และยังคงต้องคำนึงถึงภัยคุกคามต่อความปลอดภัยของระบบเครือข่าย โดยระบบสารสนเทศภายในของวิทยาลัยฯ มีโครงสร้างพื้นฐานการเชื่อมโยงเครือข่ายผ่านช่องทางการสื่อสารของมหาวิทยาลัยเป็นหลัก ซึ่งพบว่านโยบายการเชื่อมโยงข้อมูลผ่านเครือข่ายของมหาวิทยาลัยมีข้อจำกัดในการบริหารจัดการด้านสารสนเทศ ส่งผลกระทบให้ระบบสารสนเทศภายในของวิทยาลัยฯ ที่จำเป็นต้องใช้บริการผ่านช่องทางภายนอกเกิดข้อจำกัดเช่นกัน จึงไม่สามารถตอบสนองความต้องการของกลุ่มผู้ใช้งานได้อย่างทันท่วงที งานเทคโนโลยีสารสนเทศ ได้เล็งเห็นถึงปัญหาข้างต้น จึงมีแนวความคิดริเริ่มในการวางแผนเพื่อเพิ่มขีดความสามารถในการบริหารจัดการเครือข่าย และการยกระดับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศของวิทยาลัยฯ โดยมีการกำหนดกรอบนโยบายและแนวทางการปฏิบัติที่สามารถเทียบเคียงกับมาตรฐานสากล พร้อมทั้งเพิ่มปริมาณช่องทางการรับส่งข้อมูล และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้ รวมถึงจัดหาระบบสารสนเทศเพื่อสนับสนุนการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน สำหรับการรับมือกับสถานการณ์ฉุกเฉิน หรือภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้น

2.2 วัตถุประสงค์ เป้าหมาย และผลประโยชน์ที่จะได้รับ

2.2.1 วัตถุประสงค์ (จัดทำโครงการเพื่ออะไร)

1. เพื่อกำหนดมาตรการ นโยบายและกลไกในการป้องกันความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พร้อมรับมือและตอบโต้กับสถานการณ์ฉุกเฉิน หรือภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้นของวิทยาลัยฯ

2. เพื่อใช้ในการตรวจสอบเครือข่ายและควบคุมการใช้อินเทอร์เน็ต เพื่อป้องกันการโจมตีและการรักษาความปลอดภัยเครือข่ายของวิทยาลัยฯ

3. เพื่อเพิ่มปริมาณช่องทางการรับส่งข้อมูล (Bandwidth) และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้ของวิทยาลัยฯ

2.2.2 ผลผลิต - OUTPUT (ผลผลิตที่ได้จากการดำเนินกิจกรรม)

1. มีกรอบนโยบายและแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สามารถเทียบเคียงกับมาตรฐานสากลอย่างใดอย่างหนึ่ง

2. มีกรอบนโยบายมาตรฐานและแนวทางการปฏิบัติ เพื่อรับมือกับสถานการณ์ฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ (Business Continuity Planning: BCP)

3. มีพิมพ์เขียวด้านเทคโนโลยีสารสนเทศ (Enterprise Blueprint) เพื่อเป็นกรอบแนวทางและขั้นตอนวิธีการสำหรับการวิเคราะห์ ออกแบบ วางแผน ด้านเทคโนโลยีสารสนเทศ

4. มีระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ (Firewall)

5. มีช่องทางการรับส่งข้อมูล (Bandwidth) ที่เพิ่มขึ้น เพื่อรองรับความต้องการของผู้ใช้งานด้านเครือข่ายไร้ข่าย (Wi-Fi) และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้ของวิทยาลัยฯ

6. มีระบบบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) ซึ่งสามารถนำมาคาดการงบประมาณ การบำรุงรักษา (End of life) การบริหารความเสี่ยงด้านการสิ้นสุดการผลิตอะไหล่หรือยุติการให้บริการจากผู้ผลิต (End of support) เพื่อนำมาตัดสินใจในเชิงปฏิบัติและเชิงกลยุทธ์ต่อไป

2.2.3 ผลลัพธ์ - OUTCOME (ผลประโยชน์ที่จะได้รับ)

1. มีมาตรการนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Policy and Procedure) เพื่อพัฒนากลไกในการป้องกันความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พร้อมรับมือและตอบโต้กับสถานการณ์ฉุกเฉิน หรือภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้นของวิทยาลัยฯ

2. มีแนวทางและขั้นตอนในการตรวจสอบเครือข่ายและการควบคุมข้อมูลจากอินเทอร์เน็ตหรือภายในเครือข่าย สามารถกำหนดสิทธิ์การเข้าถึงข้อมูล เพื่อป้องกันการโจมตีและการรักษาความปลอดภัยเครือข่ายของวิทยาลัยฯ

3. มีช่องทางการรับส่งข้อมูล (Bandwidth) ที่เพิ่มขึ้น เพื่อรองรับความต้องการของผู้ใช้งานด้านเครือข่ายไร้ข่าย (Wi-Fi) และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้ของวิทยาลัยฯ

2.2.4 ผลกระทบ - IMPACT (ทั้งเชิงบวก และเชิงลบ)

1. ทำให้เกิดนโยบายและแนวทางการปฏิบัติที่สามารถเทียบเคียงกับมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ สำหรับการป้องกันความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พร้อมรับมือผลกระทบและตอบโต้กับสถานการณ์ฉุกเฉิน หรือภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้น

2. เป็นการดำเนินงานเชิงรุกที่ช่วยลดความเสี่ยง และความรุนแรงของการถูกโจมตีผ่านระบบเครือข่าย

2.2.5 กลุ่มเป้าหมาย/ผู้ที่ได้รับผลประโยชน์

อาจารย์ พนักงาน นักศึกษา ของวิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล

ผลกระทบที่อาจเกิดขึ้นต่อโครงการอื่น

☑ ไม่ส่งผลกระทบต่อโครงการอื่น

2.3 ความพร้อมในการดำเนินโครงการ

2.3.1 ประสบการณ์และความเชี่ยวชาญในการดำเนินการ

โครงการริเริ่มใหม่ไม่เคยมีมาก่อน

2.3.2 ความเหมาะสมของโครงการ

- ความพร้อมของพื้นที่ดำเนินโครงการ

อยู่ในระหว่างเตรียมการ

- ความพร้อมของบุคลากร/ทีมงาน

ปานกลาง

- ความพร้อมของการบริหารจัดการ

ปานกลาง

- ความเสี่ยงที่อาจจะเกิดขึ้น

ด้านการดำเนินการ

2.3.3 มีการตรวจสอบและดำเนินการตามกฎหมายหรือระเบียบที่เกี่ยวข้อง ฯ

พรบ.คอม /พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA

ส่วนที่ 3 : ข้อมูลการดำเนินงานโครงการและตัวชี้วัดของโครงการ

3.1 แผนการปฏิบัติงาน/กิจกรรมที่ดำเนินการ

วิธีดำเนินการ	ปีงบประมาณ 2566	ปีงบประมาณ 2567	ปีงบประมาณ 2568	ปีงบประมาณ 2569	ปีงบประมาณ 2570	ปีงบประมาณ 2571
1. ดำเนินการจัดทำเอกสารขออนุมัติโครงการยกระดับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ (Modernize IT Infrastructure)	ก.ค.-ก.ย.	ต.ค.-ธ.ค.				
2. Requirement Definition: รวบรวมปัญหาและวิเคราะห์ความต้องการ และขอบเขตการแก้ไขปัญหาต่างๆ ด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของวิทยาลัยฯ	ก.ค.-ก.ย.	ต.ค.-มี.ค.	ต.ค.-มี.ค.	ต.ค.-มี.ค.		
3. System Analysis : วางแผนการดำเนินการเพื่อกำหนดมาตรฐาน นโยบายและกลไกในการป้องกันความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และทดสอบระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ	ก.ค.-ก.ย.	ต.ค.-มี.ค.	ต.ค.-มี.ค.	ต.ค.-มี.ค.		

วิธีดำเนินการ	ปีงบประมาณ 2566	ปีงบประมาณ 2567	ปีงบประมาณ 2568	ปีงบประมาณ 2569	ปีงบประมาณ 2570	ปีงบประมาณ 2571
4. กำหนดมาตรฐาน นโยบายและกลไกในการป้องกันความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พร้อมรับมือและตอบโต้กับสถานการณ์ฉุกเฉินหรือภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้นของวิทยาลัยฯ		ต.ค.-ก.ย.	ต.ค.-ก.ย.	ต.ค.-ก.ย.		
5. จัดหาเครื่องแม่ข่าย (Server) สำหรับทำหน้าที่เพื่อให้สามารถตรวจสอบ ดูแล รักษา การทำงานของระบบต่างๆ และสามารถคาดการณ์แนวโน้มของการเกิดปัญหา หรือเพื่อป้องกันการโจมตีและการรักษาความปลอดภัยเครือข่ายของวิทยาลัยฯ		ต.ค.-มิ.ย.	ต.ค.-มิ.ย.	ต.ค.-มิ.ย.		
6. เช่าใช้บริการเชื่อมต่ออินเทอร์เน็ต (Link Internet Fiber Optics) 500 Mbps เพื่อเพิ่มปริมาณช่องทางการรับส่งข้อมูล (Bandwidth) และช่องทางการสื่อสารสำรองกรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้		ม.ค.-มิ.ย.	ม.ค.-ก.ย.	ม.ค.-ก.ย.		
7. System Design & Development : ออกแบบและพัฒนาระบบสารสนเทศ เพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน การทำงานของระบบต่างๆ ด้านเทคโนโลยีสารสนเทศ		ต.ค.-ก.ย.	ต.ค.-ก.ย.	ต.ค.-ก.ย.		

วิธีดำเนินการ	ปีงบประมาณ 2566	ปีงบประมาณ 2567	ปีงบประมาณ 2568	ปีงบประมาณ 2569	ปีงบประมาณ 2570	ปีงบประมาณ 2571
8. System Testing : การทดสอบระบบสารสนเทศฯ เพื่อประเมินความพร้อมของระบบฯ ในการบริหารจัดการความปลอดภัยของเครือข่าย (Firewall) และจัดการความเสี่ยงที่อาจจะเกิดขึ้น		ม.ค.-ก.ย.	ม.ค.-ก.ย.	ม.ค.-ก.ย.		
9. สรุปผลการดำเนินการสร้างและพัฒนาระบบสารสนเทศ		ก.ค.-ก.ย.	ก.ค.-ก.ย.	ก.ค.-ก.ย.		
10. System Maintenance (MA) การบำรุงรักษาระบบ		ก.ค.-ก.ย.	ก.ค.-ก.ย.	ก.ค.-ก.ย.		
11. ติดตามและรายงานผลการดำเนินงานโครงการ		เม.ย.-ก.ย.	เม.ย.-ก.ย.	เม.ย.-ก.ย.		

3.2 เป้าหมายโครงการ ตัวชี้วัดความสำเร็จของโครงการ

ตัวชี้วัด	หน่วยนับ	ปีงบประมาณ 2567		ปีงบประมาณ 2568		ปีงบประมาณ 2569		ปีงบประมาณ 2570		ปีงบประมาณ 2571	
		แผน	ผล	แผน	ผล	แผน	ผล	แผน	ผล	แผน	ผล
เชิงปริมาณ											
1. มีกรอบนโยบายและแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่สามารถเทียบเคียงกับมาตรฐานสากลอย่างใดอย่างหนึ่ง	1 ฉบับ	35%		70%		100%	1 ฉบับ				
2. มีกรอบนโยบายมาตรฐานและแนวทางการปฏิบัติ เพื่อรับมือกับสถานการณ์ฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ (Business Continuity Planning : BCP)	1 ฉบับ	100%	1 ฉบับ								
3. มีพิมพ์เขียวด้านเทคโนโลยีสารสนเทศ (Enterprise Blueprint) เพื่อเป็นกรอบแนวทางและขั้นตอนวิธีการสำหรับการวิเคราะห์ ออกแบบ วางแผน ด้านเทคโนโลยีสารสนเทศ	1 ฉบับ	100%	1 ฉบับ								
4. มีระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ	1 ระบบ	35%		70%		100%	1 ระบบ				
5. มีระบบบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)	1 ระบบ	35%		70%		100%	1 ระบบ				
เชิงคุณภาพ											
เชิงเวลา											

ส่วนที่ 4 : งบประมาณของโครงการ

4.1 งบประมาณปี 2567 ทั้งหมด 1,000,000 บาท โดยขอใช้จาก

- เงินรายได้ (วิทยาลัยฯ) 1,000,000 บาท
- เงินงบประมาณ 0 บาท

โครงการ / กิจกรรม	รายละเอียดค่าใช้จ่าย	รวม	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
ระบบสารสนเทศเพื่อการสนับสนุนในการตรวจสอบการเฝ้าระวัง และการแจ้งเตือน ด้านเทคโนโลยีสารสนเทศ	1. เครื่องแม่ข่าย (Server) สำหรับทำหน้าที่ดูแลความปลอดภัยในระดับเครือข่ายแบบรวมศูนย์ (Firewall) เพื่อป้องกันการโจมตีและการรักษาความปลอดภัยเครือข่ายของวิทยาลัยฯ	300,000										300,000		
	2. ค่าเช่าใช้บริการเชื่อมต่ออินเทอร์เน็ต (Link Internet Fiber Optic) 500 Mbps เพื่อเพิ่มปริมาณช่องทางการรับส่งข้อมูล (Bandwidth) และช่องทางการสื่อสารสำรอง กรณีที่ระบบสื่อสารหลักประสบปัญหาหรือไม่สามารถให้บริการได้	300,000										300,000		
	3. เครื่องแม่ข่าย (Server) สำหรับติดตั้งระบบตรวจสอบ การเฝ้าระวัง และการแจ้งเตือน (Monitoring and Control System)	400,000										400,000		

4.2 งบประมาณทั้งโครงการ 3,300,000 บาท

หมวดรายจ่าย	ปีงบประมาณ 2566	ปีงบประมาณ 2567	ปีงบประมาณ 2568	ปีงบประมาณ 2569	ปีงบประมาณ 2570	ปีงบประมาณ 2571
1. งบบุคลากร						
2. งบดำเนินงาน		300,000	700,000	800,000		
3. งบลงทุน		700,000	450,000	350,000		
4. งบเงินอุดหนุน						

5.1 ประสิทธิภาพและความคุ้มค่าของโครงการ

1. ความครบถ้วนของผลผลิตตามเป้าหมายโครงการ

2. การบริหารจัดการโครงการอย่างเป็นระบบ ประกอบด้วย การวางแผนโครงการ /การกำหนดหน้าที่ ผู้รับผิดชอบ /การติดตามการดำเนินงาน /อุปสรรคในการดำเนินโครงการ และระยะเวลาดำเนินโครงการเป็นไปตามแผน

3. การบริหารจัดการโครงการโดยใช้ทรัพยากรอย่างคุ้มค่าและสมเหตุสมผล โดยมีการแจกแจงค่าใช้จ่ายในแต่ละกิจกรรมหรือทรัพยากรที่ใช้ในโครงการ เช่น เครื่องแม่ข่าย การจัดหาเครือข่ายสำรอง เป็นต้น

5.2 ปัญหาอุปสรรคและแนวทางแก้ไข

หากไม่ได้รับการอนุมัติทรัพยากรเครื่องแม่ข่ายสำหรับติดตั้งซอฟต์แวร์ (Firewall) ซึ่งเป็นอุปกรณ์หลักที่จะมาทำหน้าที่ตรวจสอบคัดกรองข้อมูลการสื่อสารที่ผ่านเข้า-ออกระบบเครือข่ายของวิทยาลัยฯ งานเทคโนโลยีสารสนเทศอาจจำเป็นต้องนำทรัพยากรเครื่องแม่ข่ายที่มีการปลดระวาง (End of life) และอยู่ในระหว่างการส่งคืนงานพัสดุ มาใช้ทดแทน แต่จะเพิ่มความเสี่ยงหากอุปกรณ์เกิดการชำรุดจะส่งผลให้ไม่สามารถแก้ไขได้อย่างทันท่วงที และเพิ่มในเรื่องค่าใช้จ่ายของการซ่อมบำรุงฮาร์ดแวร์ภายในตัวเครื่อง ที่อาจจะมีการสิ้นสุดการผลิตอะไหล่หรือยุติการให้บริการจากผู้ผลิต (End of support) หรือต้องใช้เวลาในการสั่งอุปกรณ์ รวมไปถึงไม่รองรับซอฟต์แวร์รุ่นใหม่ที่ต้องการนำมาใช้งาน

5.3 ข้อเสนอแนะ

ความเห็นของผู้บริหารประจำสังกัดของผู้รับผิดชอบโครงการ

.....

.....

.....

ลงชื่อ .....

(รศ.ดร.ชาญชัย ผลถานุกิติถาวร)

รองคณบดีฝ่ายสื่อสารองค์กรและสารสนเทศ

ความเห็นของรองคณบดีฝ่ายวางแผนกลยุทธ์และพัฒนาคุณภาพ

.....

.....

.....

ลงชื่อ .....

(ผศ.ดร.ภัสริณ รอดโพธิ์ทอง วงศ์กำแหง)

รองคณบดีฝ่ายการวางแผนกลยุทธ์และพัฒนาคุณภาพ

ความเห็นของคณบดี

.....

.....

.....

☑ อนุมัติ ☐ ไม่อนุมัติ

ลงชื่อ .....

(ศาสตราจารย์ พญ.จุฬธิดา โฉมฉาย)

คณบดีวิทยาลัยนานาชาติ