



แผนบริหารความเสี่ยง (Risk Management Plan)

สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำนำ

ปัจจุบันการบริหารความเสี่ยงเป็นเรื่องที่สำคัญ และเป็นส่วนหนึ่งของการบริหารจัดการ เพื่อนำองค์กรไปสู่ความก้าวหน้า โดยลดผลกระทบที่อาจจะเกิดขึ้นและเป็นอุปสรรคขัดขวางต่อการพัฒนาส่วนงาน ซึ่งสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ เป็นหน่วยงานที่ให้การสนับสนุนการเรียนการสอน มุ่งเน้นการบริการทางด้านเทคโนโลยีสารสนเทศเพื่อตอบสนองความต้องการของอาจารย์ เจ้าหน้าที่ และนักศึกษาในมหาวิทยาลัย พร้อมทั้งสร้างสรรค์บริการเทคโนโลยีสารสนเทศ สู่มาตรฐานสากล

ทั้งนี้ สำนักคอมพิวเตอร์ฯ ได้เล็งเห็นความสำคัญของการบริหารความเสี่ยง จึงได้จัดสัมมนาในระหว่างวันที่ 25 ถึง 26 มีนาคม 2564 เพื่อให้บุคลากรได้ร่วมกันจัดทำแผนบริหารจัดการความเสี่ยง และใช้เป็นแนวทางในการในการจัดการความเสี่ยงที่อาจจะเกิดขึ้นทั้งในปัจจุบันและอนาคตเพื่อให้การบริการทางด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพและเสถียรภาพต่อไป

(รองศาสตราจารย์ ดร.ชูพันธุ์ รัตนโกศา)

ผู้อำนวยการสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

สารบัญ

หน้า

คำนำ	
สารบัญ	
บทที่ 1 ข้อมูลเบื้องต้นของส่วนงาน	1
สถานที่ตั้ง	1
ปรัชญา ปณิธาน วิสัยทัศน์ อัตลักษณ์ พันธกิจ และวัตถุประสงค์	2
แผนยุทธศาสตร์การพัฒนสำนักคอมพิวเตอร์ฯ	3
โครงสร้างการบริหารงาน	5
อัตรากำลัง	5
บุคลากร	6
บทที่ 2 แนวทางการบริหารความเสี่ยงของมหาวิทยาลัย	7
นโยบายการบริหารความเสี่ยงของมหาวิทยาลัย	7
วัตถุประสงค์การบริหารความเสี่ยงของมหาวิทยาลัย	7
โครงสร้างการบริหารความเสี่ยง	7
บทที่ 3 การบริหารความเสี่ยงของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ	9
การศึกษาวัตถุประสงค์ และยุทธศาสตร์ของส่วนงาน	9
การระบุความเสี่ยง	9
การประเมินความเสี่ยง	10
การบริหาร/จัดการความเสี่ยง	12
การติดตาม และประเมินผล	13
การรายงาน	13
บทที่ 4 สรุปผลการสัมมนา	14

บทที่ 1

ข้อมูลเบื้องต้นของส่วนงาน

สถานที่ตั้ง

สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ กรุงเทพมหานคร

ตั้งอยู่ ณ ชั้น 3, 4 และ 5 อาคารอเนกประสงค์ และ FINN Space ชั้นใต้ดิน อาคาร 79 มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ 1518 ถนนประชากรราษฎร์ 1 แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพมหานคร 10800 โดยมีรายละเอียด ดังนี้

ชั้น 3 จัดพื้นที่สำหรับห้องบริการคอมพิวเตอร์สำหรับนักศึกษาโดยแบ่งเป็น ห้องบริการเครื่องคอมพิวเตอร์ จำนวน 1 ห้อง ห้องบริการเครือข่ายไร้สาย จำนวน 1 ห้อง ห้องแลกเปลี่ยนเรียนรู้และศึกษาค้นคว้าด้วยตนเอง จำนวน 4 ห้อง และ IT Clinic จำนวน 1 ห้อง

ชั้น 4 จัดพื้นที่สำหรับห้องปฏิบัติการคอมพิวเตอร์เพื่อการเรียนการสอนและการฝึกอบรม จำนวน 4 ห้อง ห้องทำงานของเจ้าหน้าที่ฝ่ายวิศวกรรมระบบเครือข่าย ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ (NOC) และห้องระบบเครือข่ายคอมพิวเตอร์ (Data Center)

ชั้น 5 จัดพื้นที่สำหรับห้องทำงานของฝ่ายบริหาร สำนักงานผู้อำนวยการ ฝ่ายบริการวิชาการ และส่งเสริมการวิจัย และฝ่ายพัฒนาระบบสารสนเทศ

FINN Space ชั้นใต้ดินอาคาร 79 จัดพื้นที่สำหรับรองรับการทำงานและเรียนรู้ร่วมกัน มีเครื่องคอมพิวเตอร์ให้บริการ จำนวน 8 เครื่อง Help Center และ IT Clinic

สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี

ตั้งอยู่ ณ ชั้น 5 และ 6 อาคารสิรินธร มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ วิทยาเขตปราจีนบุรี 129 หมู่ 21 ตำบลเนินหอม อำเภอเมือง จังหวัดปราจีนบุรี 25230 โดยมีรายละเอียด ดังนี้

ชั้น 5 จัดพื้นที่สำหรับห้องระบบเครือข่ายคอมพิวเตอร์ (Data Center) จำนวน 1 ห้อง

ชั้น 6 จัดพื้นที่สำหรับห้องปฏิบัติการคอมพิวเตอร์เพื่อการเรียนการสอน จำนวน 2 ห้อง ห้องบริการเครือข่ายไร้สาย จำนวน 2 ห้อง ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ จำนวน 1 ห้อง ห้องประชุมทางไกล จำนวน 1 ห้อง และห้องเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี จำนวน 1 ห้อง

สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ วิทยาเขตระยอง

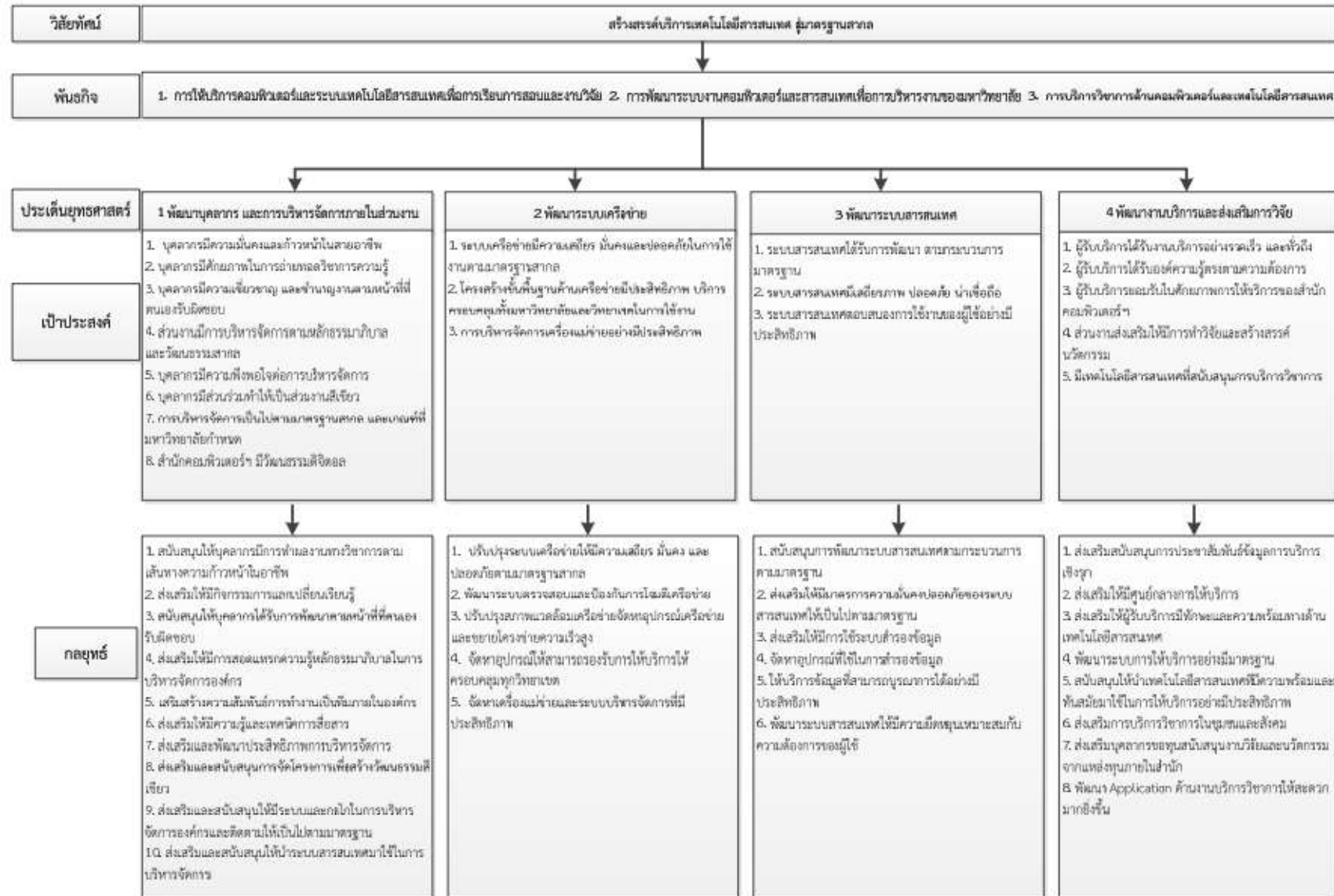
ตั้งอยู่ ณ ชั้น 7 อาคารอเนกประสงค์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ วิทยาเขตระยอง ตำบลหนองละลอก อำเภอบ้านค่าย จังหวัดระยอง 21120 โดยมีรายละเอียด ดังนี้

ชั้น 7 จัดพื้นที่สำหรับห้องระบบเครือข่ายคอมพิวเตอร์ (Data Center) จำนวน 1 ห้อง ห้องประชุมทางไกล จำนวน 1 ห้อง ห้องบริการคอมพิวเตอร์ จำนวน 1 ห้อง ห้องอบรม จำนวน 1 ห้อง และห้องเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง จำนวน 1 ห้อง

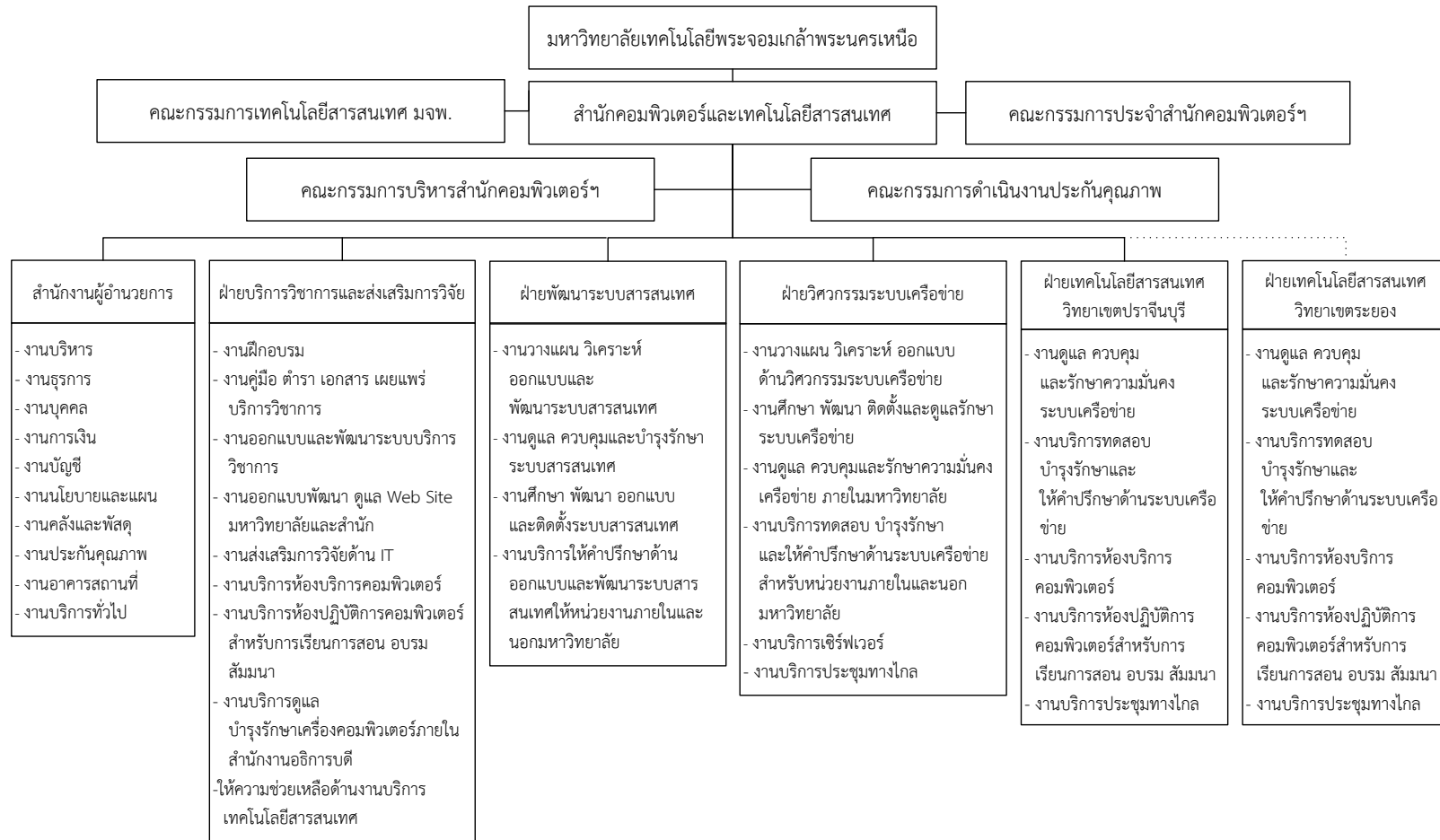
ปรัชญา ปณิธาน วิสัยทัศน์ อัตลักษณ์ พันธกิจ และวัตถุประสงค์

ปรัชญา	พัฒนาคน พัฒนาเทคโนโลยีสารสนเทศ
ปณิธาน	มุ่งเน้นการบริการทางด้านเทคโนโลยีสารสนเทศเพื่อตอบสนองความต้องการของนักศึกษาตลอดจนบุคลากรของมหาวิทยาลัยในการสนับสนุนการพัฒนาวิทยาศาสตร์และเทคโนโลยีให้อยู่ในระดับแนวหน้าของประเทศ และเป็นที่ยอมรับในระดับชาติ
วิสัยทัศน์	สร้างสรรค์บริการเทคโนโลยีสารสนเทศ สู่มาตรฐานสากล
อัตลักษณ์	ศูนย์กลางการให้บริการด้านเทคโนโลยีสารสนเทศ
พันธกิจ	1. การให้บริการคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศเพื่อการเรียนการสอนและงานวิจัย 2. การพัฒนาระบบงานคอมพิวเตอร์และสารสนเทศเพื่อการบริหารงานของมหาวิทยาลัย 3. การบริการวิชาการด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
วัตถุประสงค์	1. ให้บริการทางคอมพิวเตอร์และอุปกรณ์สนับสนุนแก่หน่วยงานภายในมหาวิทยาลัย 2. เป็นศูนย์กลางทางคอมพิวเตอร์และอุปกรณ์สนับสนุนแก่หน่วยงานภายในมหาวิทยาลัย 3. ฝึกอบรม วิจัย และให้บริการทางวิชาการด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ 4. พัฒนาและดูแลระบบงานสารสนเทศให้กับมหาวิทยาลัย

แผนผัง : แผนยุทธศาสตร์การพัฒนาสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ระยะกลางแผน พ.ศ. 2563-2564



แผนภูมิที่ 2 การแบ่งหน่วยงานภายในสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ



บุคลากร

ตารางที่ 1 จำนวนบุคลากรของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ จำแนกตามฝ่าย

รายการ	ประเภทบุคลากร		รวม
	พนักงานมหาวิทยาลัย	พนักงานพิเศษ	
ผู้บริหาร	7*	-	7*
สำนักงานผู้อำนวยการ	6	1	7
ฝ่ายบริการวิชาการและส่งเสริมการวิจัย	5	10	15
ฝ่ายพัฒนาระบบสารสนเทศ	6	-	6
ฝ่ายวิศวกรรมระบบเครือข่าย	6	-	6
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี	1	-	1
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง	-	1	1
รวม	24	11	36

* ผู้บริหารมาจากส่วนงานสายวิชาการในมหาวิทยาลัยในตารางจึงไม่นับรวม

ตารางที่ 2 จำนวนบุคลากรของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ จำแนกตามตำแหน่ง

รายการ	ประเภทบุคลากร		รวม
	พนักงานมหาวิทยาลัย	พนักงานพิเศษ	
นักวิชาการพัสดุ	1	-	1
นักวิชาการเงินและบัญชี	2	-	2
นักวิเคราะห์นโยบายและแผน	1	-	1
บุคลากร	1	-	1
เจ้าหน้าที่บริหารงานทั่วไป	1	-	1
พนักงานบริการ	-	1	1
นักวิชาการคอมพิวเตอร์	12	1	13
วิศวกร	5	1	6
ช่างเครื่องคอมพิวเตอร์	1	-	1
ช่างเทคนิค	-	9	9
รวม	24	12	36

บทที่ 2

แนวทางการบริหารความเสี่ยงของมหาวิทยาลัย

นโยบายการบริหารความเสี่ยงของมหาวิทยาลัย

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือมีระบบบริหารความเสี่ยงโดยการบริหารจัดการปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่มหาวิทยาลัยจะเกิดความเสียหายในระดับความเสี่ยงและความรุนแรงของความเสียหายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงการบรรลุเป้าหมายตามยุทธศาสตร์ที่สำคัญ จึงกำหนดนโยบายการบริหารความเสี่ยง ดังนี้

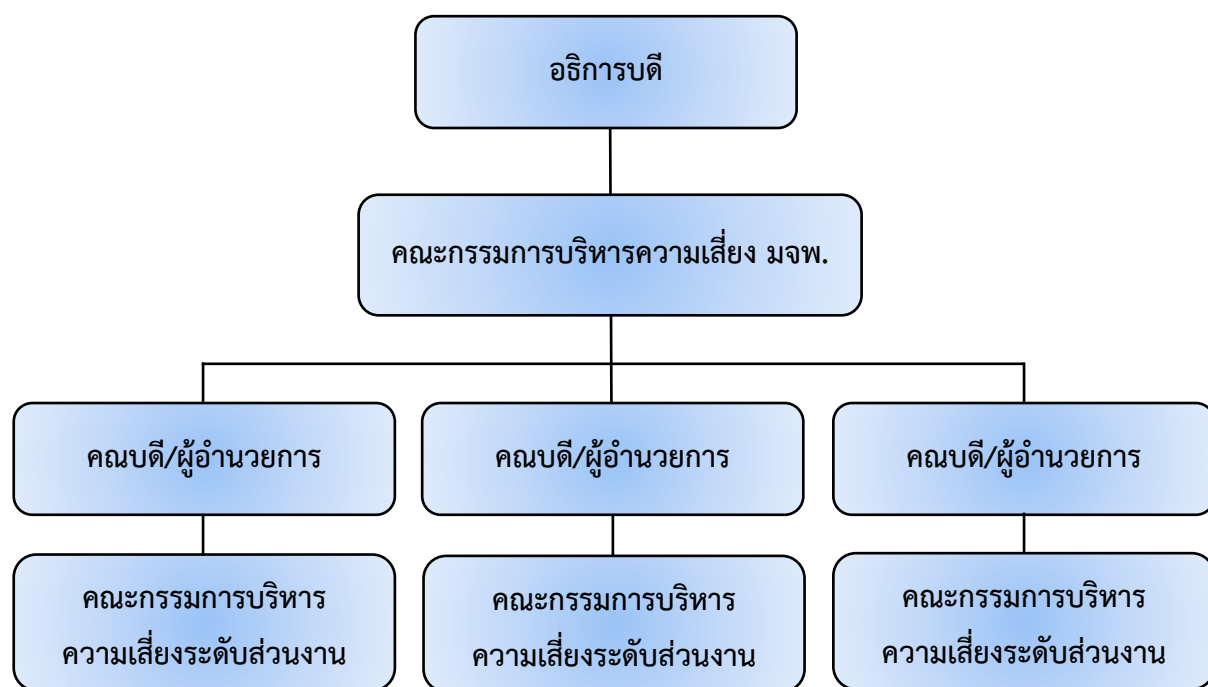
1. ให้มีการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัยแบบบูรณาการ โดยมีการจัดการอย่างเป็นระบบและต่อเนื่อง
2. ให้มีการกำหนดกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั่วทั้งมหาวิทยาลัย
3. ให้มีการติดตามประเมินผลการบริหารความเสี่ยงที่มีการทบทวน และปรับปรุงอย่างสม่ำเสมอ
4. ให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการจัดการที่ดี
5. ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานตามปกติ

วัตถุประสงค์การบริหารความเสี่ยงของมหาวิทยาลัย

1. เพื่อให้มหาวิทยาลัยสามารถลดมูลเหตุของโอกาสที่จะเกิดความเสียหาย และลดความรุนแรงของความเสียหายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ สามารถควบคุมได้ และตรวจสอบได้
2. เพื่อให้มหาวิทยาลัยมีผลการดำเนินงานบรรลุเป้าหมายตามยุทธศาสตร์

โครงสร้างการบริหารความเสี่ยง

มหาวิทยาลัย ได้กำหนดการบริหารความเสี่ยงไว้ 2 ระดับ ได้แก่ ระดับมหาวิทยาลัย และระดับส่วนงาน



ภาพที่ 1 โครงสร้างการบริหารความเสี่ยงระดับมหาวิทยาลัย

บทที่ 3

การบริหารความเสี่ยงของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

การบริหารความเสี่ยงทำให้ทราบถึงปัญหาล่วงหน้า เพื่อเตรียมการป้องกัน แก้ไข ช่วยลดโอกาสความสูญเสีย และเพิ่มโอกาสความสำเร็จ ส่งผลให้สำนักคอมพิวเตอร์ฯ มีการให้บริการอย่างต่อเนื่อง มีประสิทธิภาพ และเสถียรภาพ โดยนำกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของการดำเนินงาน รวมทั้งการบริหารจัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกัน หรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกระบวนการดังกล่าวนี้จะสำเร็จได้ต้องบุคลากรของส่วนงานจะต้องมีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงในทิศทางเดียวกัน เพื่อใช้ในการวิเคราะห์ ประเมินความเสี่ยง ทั้งนี้สำนักคอมพิวเตอร์ฯ มีกระบวนการและขั้นตอนการบริหารความเสี่ยง ประกอบด้วย 6 ขั้นตอน ดังนี้

1. การศึกษาวัตถุประสงค์ และยุทธศาสตร์ของส่วนงาน

เป็นขั้นตอนที่สำคัญ โดยบุคลากรต้องดำเนินการศึกษาและทำความเข้าใจเกี่ยวกับวัตถุประสงค์ในการจัดตั้งส่วนงาน รวมถึง ปรัชญา ปณิธาน วิสัยทัศน์ อัตลักษณ์ พันธกิจ พร้อมทั้งยุทธศาสตร์การพัฒนากส่วนงาน เพื่อให้ทราบถึงส่วนงานจัดตั้งมาเพื่ออะไร มีหน้าที่อย่างไร ต้องการผลลัพธ์ หรือเป้าหมายอย่างไร เพื่อให้มีทิศทางและจุดมุ่งหมายไปทางเดียวกัน

2. การระบุความเสี่ยง

เป็นการค้นหาความเสี่ยงที่เกิดขึ้นว่ามีอะไรบ้าง ทั้งที่มีผลดี และผลเสียต่อการทำให้บรรลุวัตถุประสงค์ของส่วนงาน โดยต้องระบุถึงสาเหตุ หรือเหตุผลที่ทำให้เกิดเหตุการณ์เสี่ยงนั้นๆ การระบุความเสี่ยงต้องทำความเข้าใจและพิจารณา 2 ประเด็น ได้แก่ ความเสี่ยง และปัจจัยเสี่ยง

2.1 ความเสี่ยง หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเสียเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจจะเกิดขึ้นในอนาคต และมีผลกระทบ หรือทำให้การดำเนินงานของส่วนงานไม่ประสบความสำเร็จ สามารถจำแนกความเสี่ยงได้ 5 ลักษณะ ดังนี้

2.1.1 ความเสี่ยงด้านยุทธศาสตร์ เป็นความเสี่ยงที่เกี่ยวข้องระดับยุทธศาสตร์หรือกลยุทธ์ เช่น การเมือง เศรษฐกิจ กฎหมาย ตลาด ภาพลักษณ์ ผู้นำ เป็นต้น

2.1.2 ความเสี่ยงด้านการปฏิบัติ เป็นความเสี่ยงที่เกี่ยวข้องในระดับปฏิบัติการ เช่น ระบบงาน ขั้นตอนการทำงาน เทคโนโลยี ทรัพยากร และบุคลากรในส่วนงาน เป็นต้น

2.1.3 ความเสี่ยงด้านการเงิน เป็นความเสี่ยงที่เกี่ยวข้องกับด้านการเงิน เช่น ขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงาน เพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง และเหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันเหตุการณ์ เป็นต้น

2.1.4 ความเสี่ยงด้านอันตราย เป็นความเสี่ยงที่เกี่ยวข้องในด้านความปลอดภัยจากอันตรายต่อชีวิต และทรัพย์สิน เช่น การสูญเสียชีวิต และทรัพย์สินจากภัยพิบัติทางธรรมชาติ และการก่อการร้าย เป็นต้น

2.1.5 ความเสี่ยงด้านชื่อเสียง เป็นความเสี่ยงที่เกี่ยวข้องกับชื่อเสียง หรือความน่าเชื่อถือ เช่น การรับรองมาตรฐานต่างๆ หรือบุคลากรประพฤติดิวินัยหรือศีลธรรม เป็นต้น

2.2 ปัจจัยเสี่ยง เป็นต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่ทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องสามารถระบุถึงเหตุผล หรือสาเหตุที่ทำให้เกิดเหตุการณ์เสี่ยงนั้นได้อย่างไร เพื่อจะได้นำมาวิเคราะห์ และกำหนดมาตรการลดความเสี่ยงในภายหลัง

3. การประเมินความเสี่ยง

เป็นการวิเคราะห์ และจัดลำดับความเสี่ยงตามความรุนแรง โดยพิจารณาจากการประเมินโอกาสที่จะเกิดขึ้น และผลกระทบจากเหตุการณ์ความเสี่ยง โดยอาศัยเกณฑ์มาตรฐานที่ได้กำหนดไว้ ทำให้การตัดสินใจจัดการกับความเสี่ยงเป็นไปได้อย่างเหมาะสม โดยนำความเสี่ยงและปัจจัยเสี่ยงมาวิเคราะห์ โดยดำเนินการ 4 ขั้นตอน

3.1 การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นการกำหนดเกณฑ์ที่ใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับของความเสี่ยง ซึ่งมีทั้งเชิงปริมาณ และเชิงคุณภาพ ขึ้นอยู่กับข้อมูล สภาพแวดล้อม และดุลยพินิจของส่วนงาน

3.1.1 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ

ตารางที่ 3 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (เชิงปริมาณ)

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (เชิงปริมาณ)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	เกิด 1 ครั้ง หรือมากกว่าในรอบ 1 เดือน
4	สูง	เกิดไม่เกิน 5 ครั้ง ในรอบ 6 เดือน
3	ปานกลาง	เกิดไม่เกิน 1 ครั้ง ในรอบ 1 ปี
2	น้อย	เกิดไม่เกิน 1 ครั้ง ในรอบ 2 ปี
1	น้อยมาก	เกิดไม่เกิน 1 ครั้ง ในรอบ 5 ปี

ตารางที่ 4 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (เชิงคุณภาพ)

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (เชิงคุณภาพ)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสดังกล่าวเกิดขึ้นบ่อยครั้ง
4	สูง	มีโอกาสดังกล่าวเกิดขึ้นค่อนข้างสูง หรือบ่อยๆ
3	ปานกลาง	มีโอกาสดังกล่าวเกิดขึ้นบ้าง
2	น้อย	อาจมีโอกาสดังกล่าวเกิดขึ้นนานๆ ครั้ง
1	น้อยมาก	มีโอกาสดังกล่าวเกิดขึ้นน้อยมาก

3.1.2 ระดับความรุนแรงของผลกระทบความเสี่ยง

ตารางที่ 5 ระดับความรุนแรงของผลกระทบของความเสี่ยง (เชิงปริมาณ)

ระดับความรุนแรงของผลกระทบของความเสี่ยง (เชิงปริมาณ)		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	มากกว่า 5,000,000 บาท
4	สูง	มากกว่า 500,000 บาท – 5,000,000 บาท
3	ปานกลาง	มากกว่า 100,000 – 500,000 บาท
2	น้อย	มากกว่า 10,000 – 100,000 บาท
1	น้อยมาก	ไม่เกิน 10,000 บาท

ตารางที่ 6 ระดับความรุนแรงของผลกระทบของความเสี่ยง (เชิงคุณภาพ)

ระดับความรุนแรงของผลกระทบของความเสี่ยง (เชิงคุณภาพ)		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	มีการสูญเสียทรัพย์สินอย่างมหันต์ มีการบาดเจ็บถึงชีวิต
4	สูง	มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นพักงาน
3	ปานกลาง	มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นหยุดงาน
2	น้อย	มีการสูญเสียทรัพย์สินพอสมควร มีการบาดเจ็บรุนแรง
1	น้อยมาก	มีการสูญเสียทรัพย์สินเล็กน้อย ไม่มีการบาดเจ็บรุนแรง

ตารางที่ 7 ระดับความรุนแรงของผลกระทบด้านชื่อเสียง

ระดับ	ผลกระทบ	ขอบเขตการรับรู้				
		มจพ.	ผู้ปกครอง	วงการ มหาวิทยาลัย	มวลชน	ต่างประเทศ
5	สูงมาก	✓	✓	✓	✓	✓
4	สูง	✓	✓	✓	✓	
3	ปานกลาง	✓	✓	✓		
2	น้อย	✓	✓			
1	น้อยมาก	✓				

3.2 การประเมินระดับโอกาส และระดับผลกระทบของความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินระดับโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงต่างๆ และประเมินระดับความรุนแรง หรือมูลค่าความเสียหายจากความเสียหาย เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม

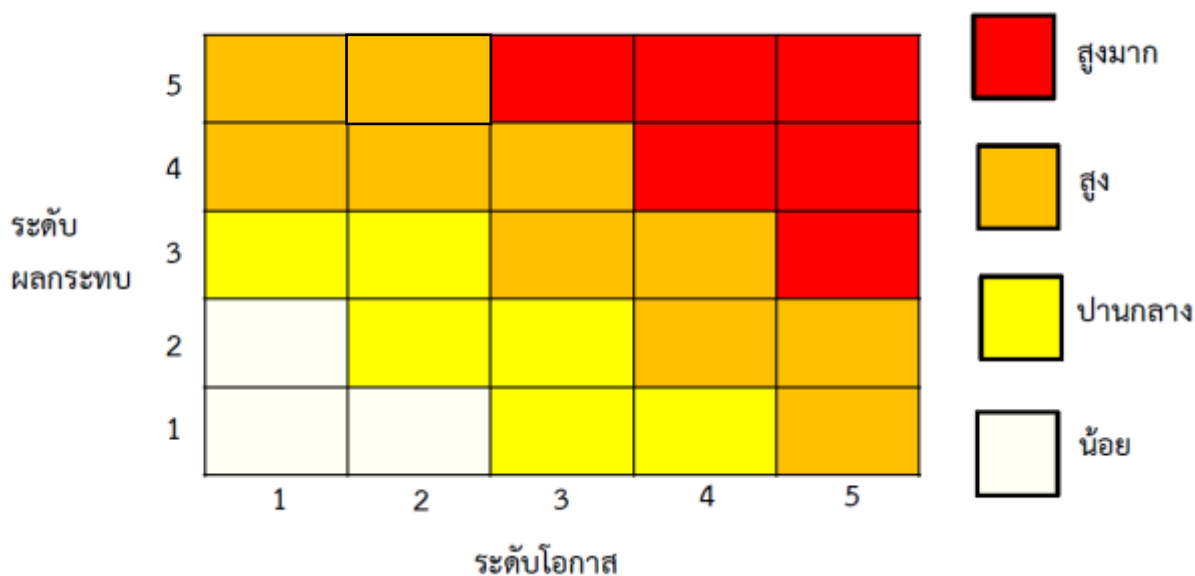
3.2.1 พิจารณาโอกาส/ความถี่ในการเกิดเหตุการณ์ต่างๆ ที่จะเกิดขึ้นนั้นมากน้อยเพียงใด

3.2.2 พิจารณาความรุนแรงของผลกระทบของความเสี่ยง ว่ามีความรุนแรงระดับใด หรือมีความเสียหายเพียงใด

3.3 การวิเคราะห์ความเสี่ยง

เมื่อพิจารณาระดับโอกาส/ความถี่ในการเกิดเหตุการณ์ และระดับความรุนแรงของผลกระทบแต่ละปัจจัยเสี่ยงแล้ว ให้นำผลที่ได้มาพิจารณาความสัมพันธ์เพื่อกำหนดระดับความเสี่ยง โดยกำหนดเกณฑ์ไว้ 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และน้อย โดยให้นำค่าคะแนนของระดับโอกาส และค่าคะแนนของผลกระทบมากำหนดลงในตารางกำหนดระดับความเสี่ยง

ตารางที่ 8 กำหนดระดับของความเสียง



3.4 การจัดลำดับความเสี่ยง

เมื่อได้ระดับความเสี่ยงแล้ว นำมาจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อส่วนงาน เพื่อพิจารณากำหนดโครงการ/กิจกรรม ควบคุมในแต่ละสาเหตุของความเสี่ยงนั้นๆ ให้เหมาะสม โดยเรียงจากระดับสูงมาก สูง ปานกลาง และน้อย และเลือกพิจารณาเฉพาะความเสี่ยงที่มีระดับสูงมาก และสูง มาจัดทำแผนบริหารจัดการความเสี่ยงเป็นลำดับต่อไป

4. การบริหาร/จัดการความเสี่ยง

เป็นการนำกลยุทธ์ มาตรการ แผนงาน โครงการ หรือกิจกรรม มาใช้ปฏิบัติเพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง โดยการจัดการความเสี่ยงมีหลายวิธี และสามารถนำมาผสมผสานให้เหมาะสมได้ ซึ่งการบริหาร/จัดการความเสี่ยงแบ่งได้ 5 วิธี ดังนี้

4.1 ยอมรับความเสี่ยง เป็นการยอมรับความเสี่ยงที่จะเกิดขึ้น เนื่องจากไม่คุ้มค่าในการจัดการ หรือป้องกันความเสี่ยงที่ต้องเสียค่าใช้จ่าย แต่อย่างไรก็ตามยังต้องเฝ้าระวังความเสี่ยงนี้อย่างสม่ำเสมอ

4.2 ลด/ควบคุมความเสี่ยง เป็นการปรับปรุงระบบการทำงาน หรือมีการออกแบบวิธีหรือขั้นตอนการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดความเสียหายให้อยู่ในระดับที่ยอมรับได้ เช่น การจัดอบรมเพื่อเพิ่มทักษะในการทำงาน การจัดทำคู่มือการปฏิบัติงาน เป็นต้น

4.3 บรรเทาความเสี่ยง เป็นการจัดการเพื่อลดผลกระทบ หรือระดับความรุนแรงของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4.4 กระจายความเสี่ยง หรือการโอนความเสี่ยง เป็นการกระจาย หรือถ่ายโอนความเสี่ยงให้กับหน่วยงานอื่นรับผิดชอบ เช่น การทำประกันภัย เป็นต้น

4.5 หลีกเลี่ยงความเสี่ยง เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงมาก และส่วนงานไม่อาจยอมรับความเสี่ยงได้ จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมที่จะก่อให้เกิดความเสี่ยงนั้น

5. การติดตาม และประเมินผล

เพื่อให้ระบบบริหารความเสี่ยงมีความสมบูรณ์ จำเป็นต้องติดตามผลการดำเนินการตามแผนบริหารความเสี่ยง ที่มีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลง รวมถึงเป็นการทบทวนประสิทธิภาพของแนวทางการบริหารความเสี่ยงในทุกขั้นตอน เพื่อพัฒนาส่วนงานให้ดียิ่งขึ้น

6. การรายงาน

เป็นการรายงานผลการบริหารจัดการความเสี่ยงที่ได้ดำเนินการทั้งหมดตามลำดับให้ผู้บริหารทราบและให้ความเห็นชอบผลการดำเนินการตาม รวมถึงรายงานให้มหาวิทยาลัยทราบด้วย



ภาพที่ 2 แผนผังภาพรวมของแนวทางการบริหารความเสี่ยง

บทที่ 4

สรุปผลการสัมมนา

สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศได้จัดสัมมนาจัดทำแผนบริหารความเสี่ยง ระหว่างวันที่ 25 ถึง 26 มีนาคม 2564 โดยได้แบ่งกลุ่มตามฝ่ายที่บุคลากรสังกัด ซึ่งประกอบด้วย 5 กลุ่ม ได้แก่

1. ผู้บริหาร
2. สำนักงานผู้อำนวยการ
3. ฝ่ายพัฒนาระบบสารสนเทศ
4. ฝ่ายบริการวิชาการและส่งเสริมการวิจัย
5. ฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง

ให้ทุกกลุ่มวิเคราะห์ประเด็นปัญหา หรือปัจจัยเสี่ยงที่อาจเกิดขึ้นในอนาคต ผลของความเสี่ยงที่อาจเกิดขึ้น รวมถึงประเมินความเสี่ยงทั้งด้านโอกาสที่จะเกิดและผลกระทบที่จะได้รับหากเกิดความเสี่ยงนั้น เพื่อนำมากำหนดระดับความเสี่ยง โดยให้วิเคราะห์ในด้านต่างๆ จำนวน 5 ด้าน ได้แก่ ด้านยุทธศาสตร์ ด้านปฏิบัติงาน ด้านการเงิน ด้านชื่อเสียง และด้านนโยบายและกฎหมาย

ตารางที่ 9 กลุ่มผู้บริหาร ด้านยุทธศาสตร์

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	บุคลากรยังกลัวกับการทำงานวิจัยและเห็นว่าการวิจัยมีประโยชน์เฉพาะในการขอตำแหน่ง	บุคลากรขาดประสบการณ์ และความรู้เกี่ยวกับการนำเทคโนโลยีใหม่ๆ มาประยุกต์ใช้งานในสำนัก	4	1	ปานกลาง
2	บุคลากรขาดความตระหนักถึงความสำคัญของการทำมาตรฐานสากล	บริการไม่บรรลุตามอัตลักษณ์และวิสัยทัศน์ ในการเข้าสู่มาตรฐานสากล	3	2	ปานกลาง
3	บุคลากรยังไม่เชี่ยวชาญ ขาดทักษะในการถ่ายทอดความรู้	ไม่สามารถเป็นวิทยากรฝึกอบรมบุคลากร และนักศึกษา ได้	3	1	ปานกลาง
4	ผู้บริหารขาดจิตวิทยาการบริหารและความสามารถทำให้บุคลากรบางคนที่ไม่ค่อยปฏิบัติงานและเข้าร่วมกิจกรรมภายในสำนัก	บุคลากรที่ไม่เข้าร่วมขาดการรับรู้ข้อมูล ที่เท่าเทียมกันทั้งสำนัก, งานกระจุกอยู่ที่บุคลากรกลุ่มใดกลุ่มหนึ่ง, บุคลากรมีพฤติกรรมเลียนแบบส่งผลกระทบต่อการทำงานเป็นทีมภายในสำนัก	3	3	สูง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
5	บุคลากรไม่ทันต่อเทคโนโลยีใหม่ เนื่องด้วยเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว	บริการไม่ทันสมัย ทำให้ผู้ใช้งานมีความพึงพอใจในบริการของสำนักน้อยลง	4	3	สูง
6	ขาดการเฝ้าระวังและติดตามปัญหาที่เกิดขึ้นในระบบเครือข่ายอย่างเป็นระบบ	สำนักขาดความน่าเชื่อถือในการให้บริการ	3	3	สูง
7	ขาดนโยบายส่งเสริมให้บุคลากรใช้งาน open source ในการปฏิบัติงาน	งบประมาณในการบำรุงรักษาอุปกรณ์และ software ที่มีราคาสูง อาจจะไม่เพียงพอในอนาคต	5	2	สูง
8	ขาดทีมงานพัฒนาระบบสารสนเทศเพื่อใช้ในการบริหารงานภายในสำนัก	ทำให้ภาพลักษณ์ของสำนักดูไม่ทันสมัยและไม่เป็นองค์กรดิจิทัล	4	3	สูง
9	ขาดแบบฟอร์มการประเมินผลงานและการวัด KPI รายบุคคลที่ตรงต่อภาระงานจริงที่ปฏิบัติอยู่	รายงานผลการปฏิบัติงานไม่สะท้อนผลงานและการปฏิบัติงานจริงที่ทำอยู่	5	5	สูงมาก

ตารางที่ 10 กลุ่มผู้บริหาร ด้านปฏิบัติงาน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	สถานที่การปฏิบัติงานยังเป็นแบบดั้งเดิม ไม่ทันสมัย	บุคลากรขาดบรรยากาศ ให้การมีความคิดสร้างสรรค์ในการปฏิบัติงาน	3	2	ปานกลาง
2	ขาดทักษะและประสบการณ์ในการบริหารงานระดับองค์กร (People management skill, soft skill, technology, communication)	แนวทางการบริหารยังไม่ชัดเจนอย่างเป็นรูปธรรม และเป็นที่ยอมรับของบุคลากร	4	3	สูง
3	ขาดแผนปฏิบัติงานของผู้บริหาร	การทำงานของผู้บริหารไม่มีประสิทธิภาพ	5	3	สูงมาก

ตารางที่ 11 กลุ่มผู้บริหาร ด้านนโยบายและกฎหมาย

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่สามารถปรับปรุงระบบรับ จ่ายเงินแบบออนไลน์ได้	บริการไม่ทันสมัย	4	2	สูง
2	ไม่สามารถปฏิบัติงานนอกสถานที่ผ่านระบบสารสนเทศได้อย่างเต็มรูปแบบ เพราะยังมีข้อบกพร่องบางเอกสารต้องเป็นกระดาษ	ถ้ามีภัยพิบัติที่ร้ายแรง จะทำให้การทำงานของสำนักคอมไปสามารถปฏิบัติงานได้อย่างต่อเนื่อง	3	3	สูง

ตารางที่ 12 กลุ่มสำนักงานผู้อำนวยการ ด้านยุทธศาสตร์

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ขาดนโยบาย/แนวทางการหารายได้เพิ่ม	รายได้ลดลงอย่างต่อเนื่อง	2	2	ปานกลาง
2	ผู้ปฏิบัติงานในสำนักไม่เข้าใจว่ายุทธศาสตร์ของสำนักคืออะไร	ทำให้แผนยุทธศาสตร์ไม่บรรลุตามตัวชี้วัดระดับยุทธศาสตร์	3	2	ปานกลาง
3	ศักยภาพหลักขององค์กรขาดความชัดเจน เช่น ขอบเขตความสามารถในการให้บริการของเราอยู่แค่ไหน	ผู้ใช้บริการเกิดความสับสนขอบเขตการให้บริการของสำนัก และความพึงพอใจของผู้รับบริการ	4	2	สูง
4	ความชัดเจนของผลงานที่ต้องการให้เกิดจากแผนงาน/กิจกรรม/ตัวชี้วัดก่อนกำหนดเป็นแผนปฏิบัติการใหม่ไม่เพียงพอ	ไม่มีข้อมูลประกอบการพิจารณาอนุมัติทำโครงการในแต่ละปี ทำให้โครงการเกิดการซ้ำซ้อน การใช้งบประมาณไม่มีความคุ้มค่า โครงการที่จัดทำอาจไม่มีประโยชน์หรือแก้ปัญหาที่แท้จริงของสำนัก ได้	3	4	สูง

ตารางที่ 13 กลุ่มสำนักงานผู้อำนวยการ ด้านปฏิบัติงาน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่ได้รับความร่วมมือจากบุคลากรในการทำงาน	งานไม่สำเร็จ หรือสำเร็จแต่ล่าช้า	1	2	น้อย
2	บุคลากรไม่มีความรู้จริงแต่ให้คำแนะนำ	งานไม่สำเร็จ	1	2	น้อย
3	การตรวจสอบเอกสารโดยกองคลังไม่เป็นมาตรฐานทำให้เกิดปัญหาในการเบิกจ่าย	ทำให้ต้องแก้ไขเอกสาร หรือต้องทำเอกสารใหม่ เกิดความล่าช้าในการเบิกจ่าย	3	2	ปานกลาง
4	มีความไม่แน่นอนที่อาจจะเกิดขึ้นจากโครงการ	ทำให้เกิดการล่าช้าในการดำเนินงานตามโครงการ	2	3	ปานกลาง
5	เมื่อบุคลากรลาออกจากสำนักแล้ว ผู้เกี่ยวข้องไม่ลบข้อมูลออกจากระบบสารสนเทศ	ข้อมูลรั่วไหล ข้อมูลไม่เป็นปัจจุบัน	2	3	ปานกลาง
6	บุคลากรบางส่วนไม่สามารถสื่อสารต่างประเทศกับผู้รับบริการได้	ไม่สามารถให้บริการต่อผู้ใช้บริการต่างชาติได้	3	2	ปานกลาง
7	ผู้มาขอใช้ห้องอบรมไม่มาชำระค่าห้องตามประกาศสำนักคอมพิวเตอร์ฯ	ทำให้ไม่สามารถปฏิบัติงานเป็นไปตามประกาศสำนักฯ	1	3	ปานกลาง
8	มีข้อจำกัดในการดำเนินโครงการด้านทรัพยากร เช่น งบประมาณ	ประสิทธิผลของโครงการไม่เป็นไปตามที่คาดหวังไว้	2	3	ปานกลาง
9	ตัวชี้วัดของโครงการมีมาก เนื่องจากแผนมีหลายแผน และหลายตัวชี้วัดในโครงการเดียว	ทำให้ผู้ปฏิบัติงานภายใต้โครงการนั้น สับสนในการปฏิบัติงานในแต่ละแผน	2	4	สูง
10	ปฏิบัติงานไม่ครบทุกขั้นตอนตามพรบ.จัดซื้อจัดจ้าง	ไม่ปฏิบัติตาม พรบ. ถือว่าเป็นความผิด	1	5	สูง

ตารางที่ 14 กลุ่มสำนักงานผู้อำนวยการ ด้านการเงิน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	การปฏิบัติการด้านการรับเงิน การนำฝากเงิน วิทยาเขตปราจีนและระยอง	ผู้รับเงินไม่ใช้นักวิชาการเงินและบัญชี/ฝากเงินล่าช้า	1	3	ปานกลาง
2	ไม่ได้รับการสนับสนุนเงินงบประมาณแผ่นดินในโครงการต่างๆ ที่ขอไป	ต้องนำเงินเหลืจ่ายมาใช้ทำให้เงินเหลืจ่ายลดลง/ขาดการพัฒนาหรือปรับปรุงโครงการที่ขออย่างต่อเนื่อง	2	3	ปานกลาง
3	การบำรุงรักษาระบบต่างๆ มากเกินไป	เงินเหลืจ่ายลดลงอย่างมาก	3	3	สูง

ตารางที่ 15 กลุ่มสำนักงานผู้อำนวยการ ด้านชื่อเสียง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่มีระบบสารสนเทศที่ใช้ภายในสำนัก	ภาพลักษณ์องค์กรด้อยกว่าบางส่วนงาน และไม่สะท้อนที่เป็นสำนัก	1	3	ปานกลาง
2	โครงการที่ได้รับเงินงบประมาณจัดทำ TOR ช้า	ภาพลักษณ์องค์กรเสียเมื่อถูกถามในที่ประชุมคณะกรรมการเร่งรัดของมหาวิทยาลัย / กองแผนงานอาจตัดงบของโครงการในปีถัดไป	1	3	ปานกลาง

ตารางที่ 16 กลุ่มสำนักงานผู้อำนวยการ ด้านนโยบายและกฎหมาย

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	งานบุคคล การเงิน บัญชี พัสดุ มีพรบ. กฎ ระเบียบ ประกาศ จดหมายเวียน คำสั่ง และอื่นๆ ที่เกี่ยวข้องมารวมถึงการยกเลิกเอกสารฉบับเก่าและออกฉบับใหม่ทดแทน	ปฏิบัติงานไม่ครบ ปฏิบัติงานไม่ถูกต้อง ปฏิบัติงานไม่ครอบคลุม ปฏิบัติงานผิด	3	2	ปานกลาง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
2	บุคลากรขาดความรู้และขาดการตระหนัก และขาดการใส่ใจในการปฏิบัติตามจรรยาบรรณวิชาชีพ	ทำให้เกิดการกระทำผิดหรือละเลยต่อการปฏิบัติงานตามจรรยาบรรณในวิชาชีพ	1	5	สูง

ตารางที่ 17 กลุ่มฝ่ายพัฒนาระบบสารสนเทศ ด้านยุทธศาสตร์

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ระบบสารสนเทศที่มีไม่สามารถตอบสนองความต้องการของผู้ใช้ได้ครบถ้วน	ผู้ใช้ไม่ได้รับความพึงพอใจในการใช้บริการ	3	3	สูง
2	ระบบสารสนเทศถูกโจมตี (ประเด็นยุทธศาสตร์:ระบบสารสนเทศมีความปลอดภัยน่าเชื่อถือ)	ไม่สามารถให้บริการระบบสารสนเทศได้	1	5	สูง

ตารางที่ 18 กลุ่มฝ่ายพัฒนาระบบสารสนเทศ ด้านปฏิบัติงาน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	บุคลากรพัฒนาระบบสารสนเทศอย่างล่าช้า เพราะความต้องการเปลี่ยนแปลงบ่อย หรือผู้พัฒนาไม่มีความชำนาญในการเก็บความต้องการ	ผู้ใช้ไม่มีระบบสารสนเทศที่ช่วยอำนวยความสะดวกให้ใช้งาน	1	2	น้อย
3	ภาษาที่ใช้ในการพัฒนาระบบสารสนเทศมีข้อจำกัดในการใช้งานประสิทธิภาพของเครื่องแม่ข่าย	ผู้ใช้งานไม่พึงพอใจต่อการใช้งานระบบสารสนเทศ	2	3	ปานกลาง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
4	ระบบสารสนเทศใช้เทคโนโลยีเก่าในการพัฒนา และถูกออกแบบและพัฒนา รวมถึงใช้งานมาเป็นระยะเวลานานแล้ว	- หากเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นมีปัญหาอาจไม่สามารถหาอุปกรณ์ทดแทนได้ส่งผลให้ไม่สามารถใช้ระบบสารสนเทศนั้นได้	2	3	ปานกลาง
		- เมื่อโปรแกรมมีปัญหาไม่สามารถทำงานบน Hardware ใหม่ได้ - ต้องใช้งานกับอุปกรณ์รุ่นเก่าบางครั้งเมื่อมีการอัปเดตระบบปฏิบัติการทำให้ Driver ไม่รองรับ	2	3	ปานกลาง
		- ต้องใช้งานกับอุปกรณ์รุ่นเก่าบาง ครั้งเมื่อมีการอัปเดตระบบปฏิบัติการทำให้ Driver ไม่รองรับ	2	4	สูง
5	บุคลากรไม่สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ เนื่องจากมีความชำนาญในภาษาที่ใช้พัฒนาระบบคนละภาษา	- ระบบสารสนเทศที่พัฒนาไม่เสร็จทันตามความต้องการใช้งาน	1	3	ปานกลาง
6	ระบบสารสนเทศที่มีข้อจำกัดในการพัฒนาหรือปรับปรุงการทำงานของระบบ เช่น Source code ที่มีอยู่ในปัจจุบัน อาจจะไม่ใช้เวอร์ชันล่าสุดเป็นต้น	หากระบบสารสนเทศทำงานผิดพลาด จะไม่สามารถแก้ไขได้	2	4	สูง
7	บุคลากรไม่สามารถทำงานทดแทนกันได้	หากระบบมีปัญหา แต่ผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ ปัญหานั้นจะไม่ได้รับการแก้ไขในทันที	5	5	สูงมาก
8	มีการตัดกระแสไฟฟ้าบ่อยครั้งและไม่มีแผนการซ่อมบำรุงรายปีพร้อมทั้งไม่มีเครื่องปั่นกระแสไฟฟ้า เพื่อให้ระบบสารสนเทศให้บริการได้เป็นปกติ	ไม่สามารถให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง	2	5	สูง

ตารางที่ 19 กลุ่มฝ่ายพัฒนาระบบสารสนเทศ ด้านชื่อเสียง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่มีการประชาสัมพันธ์อย่างต่อเนื่องเกี่ยวกับระบบสารสนเทศที่ให้บริการ	ผู้ใช้ไม่ได้รับข้อมูลที่ถูกต้องของระบบสารสนเทศที่สำนักคอมพิวเตอร์ให้บริการ	4	1	ปานกลาง
2	ไม่มีแผนการตรวจสอบความพร้อมใช้งานของระบบสารสนเทศเป็นรายวัน	ไม่มีการตรวจสอบความพร้อมใช้งานไม่ได้ นำเป็นความเสี่ยงด้านความพึงพอใจโดยตรงควรเป็น ความเสี่ยงระบบสารสนเทศให้บริการไม่ต่อ เนื่องอย่างเดียว	2	3	ปานกลาง

ตารางที่ 20 กลุ่มฝ่ายพัฒนาระบบสารสนเทศ ด้านนโยบายและกฎหมาย

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่มีการกำหนดขึ้นหรือการปรับปรุงระเบียบหรือนโยบายให้ทันสมัยตามความต้องการของผู้ใช้งาน	การให้บริการที่ทันสมัย อาจผิดระเบียบของมหาวิทยาลัยได้ เช่น การรับเงินออนไลน์ เป็นต้น	3	3	สูง
2	ไม่มีทีมงานที่มีความเชี่ยวชาญด้านกฎหมาย	การดำเนินงานต่างๆ ที่ขาดความรู้ความเข้าใจด้านกฎหมายที่ชัดเจน อาจขัดต่อกฎหมายได้	3	5	สูงมาก

ตารางที่ 21 กลุ่มฝ่ายบริการวิชาการและส่งเสริมการวิจัย ด้านปฏิบัติงาน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่สามารถเปิดอบรมหลักสูตรนั้นๆ ได้(บริการวิชาการภายนอก)	จำนวนผู้เข้าร่วมอบรมน้อย ความพึงพอใจของผู้รับบริการน้อยลง	1	2	น้อย

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
2	การจัดสัมมนามีการเปลี่ยนแปลงวันเวลา หรือยกเลิกตามกำหนดเดิม	ความพึงพอใจของผู้รับบริการน้อยลง	1	2	น้อย
		การบริหารงบประมาณไม่เป็นไปตามที่กำหนดไว้			
3	ห้องบริการเปิดให้บริการไม่ได้เนื่องจากเกิดเหตุฉุกเฉิน	ความพึงพอใจของผู้รับบริการน้อยลง	2	3	ปานกลาง
4	อุปกรณ์เครือข่ายในห้องบริการขัดข้อง	ความพึงพอใจของผู้รับบริการน้อยลง	2	3	ปานกลาง
5	ขาดประชาสัมพันธ์เชิงรุก มีความล่าช้าและไม่สม่ำเสมอ	ผู้ใช้บริการได้รับข่าวสารไม่ทั่วถึงและทำให้งานบริการไม่เป็นไปตามเป้าหมาย	3	2	ปานกลาง
6	คุณสมบัติเจ้าหน้าที่ช่างเทคนิคไม่เป็นไปตามต้องการหรือไม่มีผู้สมัคร	การให้บริการงานต่างๆ มีความล่าช้าลง	2	2	ปานกลาง
		ความพึงพอใจของผู้รับบริการน้อยลง			
7	การเข้า-ออกของช่างเทคนิค	การให้บริการขาดความต่อเนื่อง	3	2	ปานกลาง
8	การปิดจ่ายกระแสไฟฟ้าภายในมหาวิทยาลัย	ผู้ใช้ไม่สามารถเข้าถึงข้อมูลงานบริการในช่วงขณะนั้นได้	2	2	ปานกลาง
9	ผู้เข้าร่วมอบรมขาดความรับผิดชอบในการเข้าอบรมหลังจากได้รับการยืนยันการอบรมแล้วหรือเข้าอบรมไม่ครบตามกำหนด	งบประมาณในส่วนของการใช้จ่ายบางส่วนไม่สามารถเบิกจ่ายได้	4	2	ปานกลาง
10	การจัดการหลักสูตรในการอบรมไม่ตอบสนองต่อความต้องการของผู้รับบริการ	ผู้เข้าร่วมอบรมหรือบรรยายมีจำนวนน้อยลง	3	2	ปานกลาง
11	มีผู้ตอบแบบประเมินความพึงพอใจในการใช้บริการน้อย	ผลสรุปไม่สะท้อนความต้องการของผู้รับบริการส่วนใหญ่ ทำให้พัฒนางานบริการได้ไม่ตรงตาม เป้าหมาย	4	3	สูง
12	ความรู้ความสามารถของวิทยากรที่มาบรรยาย/ฝึกอบรมยังขาดประสบการณ์และไม่ตรงกับความต้องการของผู้รับบริการ	ความพึงพอใจของผู้รับบริการน้อยลง	3	2	ปานกลาง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
13	ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อในห้องปฏิบัติการคอมพิวเตอร์	เกิดช่องโหว่หรือความไม่ปลอดภัยในระบบเครือข่าย	2	4	สูง
14	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ผู้ใช้บริการขาดความพึงพอใจ ขาดการยอมรับในการให้บริการ	2	3	ปานกลาง
15	ไม่มีขั้นตอนที่สามารถระบุตัวตนที่แท้จริงในการใช้งานเครื่องคอมพิวเตอร์ของบุคคลภายนอก	ไม่สามารถระบุตัวตนเมื่อมีปัญหาจากการใช้งานคอมพิวเตอร์ เช่น การใช้โปรแกรมละเมิดลิขสิทธิ์ การเข้าเว็บไซต์ที่ไม่ปลอดภัย	2	4	สูง
16	อุปกรณ์ที่ให้บริการถูกโจรกรรม	เครื่องคอมพิวเตอร์หรืออุปกรณ์ไม่สามารถทำงานได้	2	4	สูง
17	นโยบายการให้บริการไม่ชัดเจน	ผู้ปฏิบัติงานขาดความชัดเจนในการให้บริการ ส่งผลให้ผู้รับบริการได้รับบริการช้าลง	4	3	สูง

ตารางที่ 22 กลุ่มฝ่ายบริการวิชาการและส่งเสริมการวิจัย ด้านชื่อเสียง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ระบบสารสนเทศไม่สามารถให้บริการ ได้อย่างต่อเนื่อง	ทำให้สำนักขาดความเชื่อมั่นในการให้บริการ	2	5	สูง
2	โปรแกรมระบบบริหารงานพิมพ์หยุดการทำงาน	ไม่สามารถให้บริการได้ทำให้เสียชื่อเสียง	2	3	ปานกลาง
3	ความผิดพลาดในการซ่อมคอมพิวเตอร์ของบริการ IT Clinic	เสียชื่อเสียงและขาดความน่าเชื่อถือในการให้บริการ	2	4	สูง

ตารางที่ 23 กลุ่มฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และ
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง ด้านยุทธศาสตร์

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	Software และ Tool ต่างไม่ได้ถูกนำมาใช้ตามวัตถุประสงค์เพื่อประโยชน์ในการบริหารหรือการทำงานอย่างจริงจัง ส่วนใหญ่ทำไปเพื่อตอบเอกสารตามคำสั่งเท่านั้น เช่น KM	ประสิทธิภาพของหน่วยงาน ไม่เป็นไปตามที่ควรจะเป็น	2	1	น้อย

ตารางที่ 24 กลุ่มฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และ
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง ด้านปฏิบัติงาน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ขาดระบบแจ้งเตือน Air ห้องเซิร์ฟเวอร์แบบออนไลน์, มอนิเตอร์และดูย้อนหลังไม่ได้	อาจทำให้อุปกรณ์ในห้องเซิร์ฟเวอร์เสียหายได้ กรณี Air เสีย	2	3	ปานกลาง
2	ขาดระบบมอนิเตอร์และแจ้งเตือน UPS แบบออนไลน์, มอนิเตอร์และดูย้อนหลังไม่ได้	อาจทำให้ไฟฟ้าห้องเซิร์ฟเวอร์ดับได้ โดยที่เราไม่ทราบล่วงหน้า และอุปกรณ์อาจเสียหายได้	2	3	ปานกลาง
3	บุคลากรไม่ตระหนักถึงความสำคัญของมาตรการการบริหารจัดการช่วงโรคระบาด	หากมีบุคลากรเสี่ยง จะทำให้ทุกคนเสี่ยงไปด้วย แล้วจะไม่มีใครสามารถเข้าทำงานได้	1	3	ปานกลาง
4	การควบคุมการเข้าออกห้องเซิร์ฟเวอร์	การควบคุมมีความหละหลวม บุคคลภายนอกเข้าห้อง server โดยไม่มีการลง ชื่อใน Log book ทำให้ละเมิดการดำเนินการ ISO27001	2	5	สูง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
5	ขาดเส้นทางสำรอง (Fiber) สำหรับเครือข่ายตามคณะ (Core Switch พร้อมแล้ว)	ทำให้คณะ/ส่วนงานใช้งานอินเทอร์เน็ตไม่ต่อเนื่อง	2	3	ปานกลาง
6	SSID หลักของมหาวิทยาลัยไม่ครอบคลุมทุกตึก และแต่ละตึกมีไม่ครบทุกชั้น (วิทยาเขตระยอง)	บริการของสำนักคอมพิวเตอร์ฯ ไม่ครอบคลุม	2	3	ปานกลาง
7	การล็อกอินไวไฟไม่เป็นระบบเดียวกัน (วิทยาเขตระยอง)	ทำให้ผู้ใช้งานสับสน	2	1	น้อย
8	ระบบปรับอากาศในห้อง Server มีแหล่งจ่ายไฟฟ้าเพียงแหล่งเดียว	เมื่อแหล่งจ่ายไฟฟ้าเกิดปัญหา ขัดข้อง ทำให้ ความร้อนในห้อง Datacenter สูงขึ้น เกินกว่า ที่เครื่องแม่ข่ายสามารถดำเนินงานได้และเสี่ยงต่อความเสียหายที่จะเกิดขึ้นกับ Server	1	4	สูง
9	ไม่มีระบบปรับอากาศสำรอง (วิทยาเขตระยอง)	ทำให้ความร้อนในห้อง Datacenter สูงขึ้น (เครื่องแม่ข่ายอาจทำงานผิดปกติทำระบบสารสนเทศไม่สามารถออนไลน์ได้อย่างต่อเนื่อง)	2	3	ปานกลาง
10	อุปกรณ์หลักในระบบอินเทอร์เน็ตไม่สามารถทำงานได้ตามหน้าที่ เนื่องจาก 1.การถูกโจมตี 2.ชำรุดเสียหาย	ทำให้ไม่สามารถใช้งานอินเทอร์เน็ตได้ทั้งมหาวิทยาลัย	1	5	สูง
11	ไม่มีระบบรักษาความปลอดภัยเครือข่ายสำรอง (HA Firewall)	ทำให้ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่องกรณีอุปกรณ์เสียหาย	2	5	สูง
12	ระบบไฟฟ้าภายในมหาวิทยาลัยขัดข้อง	ทำให้ระบบหรืออุปกรณ์ อาจเกิดการเสียหายได้ เช่น เครื่องสำรองไฟฟ้า เครื่องปรับอากาศในห้องเซิร์ฟเวอร์ หรือ อุปกรณ์เครือข่ายต่างๆ	2	4	สูง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
13	ขาดระบบแจ้งเตือน Fire Alarm แบบออนไลน์ และระบบดับเพลิง ห้องเซิร์ฟเวอร์, มอนิเตอร์และดูย้อนหลังไม่ได้	อาจทำให้เกิดไฟไหม้ห้องเซิร์ฟเวอร์ โดยที่ไม่ทราบล่วงหน้า	1	4	สูง
14	ขาดการติดต่อประสานงานจากหน่วยงานภายนอกตั้งแต่เริ่มต้น เมื่อมีงานที่ต้องปฏิบัติงานร่วมกัน	ทำให้ใช้เวลาในการดำเนินงานมากกว่าปกติ เกิดขอบเขตงานที่ไม่แน่ชัดว่าเนื้องานจริง ๆ ต้องทำแค่ไหน อาจต้องทำงานอื่นเพิ่มเติมจากงานจริง เช่น มีการสร้างตึกใหม่ไม่มีการพูดคุยถึงการเดินเครือข่ายเมื่อต้องการทำเครือข่ายทีหลังต้องทำการขุดเจาะพื้นที่ใหม่อีกครั้ง	3	3	สูง
15	Admin ไม่พร้อมปฏิบัติงาน เช่น ลาป่วย ไม่อยู่หน้างาน (ไม่มีคนทดแทนกัน)	ไม่มีคนทดแทนกันหรือคนอื่นไม่สามารถทำงานต่อได้ (งานไม่ต่อเนื่อง)	3	3	สูง
16	ขาดการสำรองข้อมูล เช่น ความเสี่ยงที่เกิดจากฮาร์ดดิสก์เสียหาย, ระบบ CCTV เป็นต้น	ข้อมูลเสียหายไม่สามารถกู้คืนได้	3	3	สูง
17	ระบบอินเทอร์เน็ตสำรองไม่ทำงานทันที ที่อินเทอร์เน็ตหลักดาวน์ (วิทยาเขตระยอง)	ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่อง	3	4	สูง
18	ไม่มี Private link สำรองระหว่างวิทยาเขต (วิทยาเขตระยอง)	เมื่อ Private link Down ระบบที่วิทยาเขตจะใช้งานไม่ได้บางส่วน	3	4	สูง
19	การรับเงินค่าบริการงานพิมพ์ (วิทยาเขตระยองและปราจีน)	เสี่ยงต่อการผิดระเบียบทางการเงิน เสี่ยงต่อการฝากเงินไม่ทัน (กรณีมีงานด่วนหรืออยู่คนเดียว)	2	4	สูง
20	ไม่มีระบบยืนยันตัวตนและเก็บ Log ยูสเซอร์ที่เป็นศูนย์กลางทั้งมหาวิทยาลัย	ยืนยันตัวตนตาม พรบ. คอมพิวเตอร์ฯ 2560 ไม่ได้	5	3	สูงมาก

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
21	ไม่สามารถควบคุมสิทธิการใช้งานเครือข่ายรายบุคคลได้	ผู้ใช้อาจจะใช้งานเครือข่ายในทางที่ไม่ดี โดยที่ไม่สามารถควบคุมได้	5	2	สูง
22	โครงสร้างเครือข่ายหลัก (Router, Core Switch, Firewall) ไม่สามารถทำงานในลักษณะ Redundancy ได้	ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่อง	2	5	สูง
23	การทำ MOU ไม่ผ่านสำนัก เช่น WiFi เป็นต้น	ไม่สามารถบริหารจัดการได้อย่างเต็มที่ เมื่อมีปัญหาก็ต้องเป็นด่านแรกในการรับทราบและแก้ไขปัญหา	2	3	ปานกลาง

ตารางที่ 25 กลุ่มฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และ
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง ด้านการเงิน

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ตามเทคโนโลยีใหม่ไม่ทันและมีค่อนข้างราคาสูง	อุปกรณ์ที่มีราคาสูงและราคา MA แพง	3	2	ปานกลาง

ตารางที่ 26 กลุ่มฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และ
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง ด้านชื่อเสียง

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1	ไม่มีระบบการตรวจสอบความสมบูรณ์ของไฟล์ในระบบ เช่น เว็บไซต์ถูกแก้ไข, ไฟล์ Log ถูกแก้ไข เป็นต้น	อาจมีการแก้ไขเนื้อหาเว็บไซต์โดยผู้ไม่ประสงค์ดีไปในทางที่ไม่ดี ทำให้เสียชื่อเสียงได้ เป็นต้น	2	4	สูง

ตารางที่ 27 กลุ่มฝ่ายวิศวกรรมระบบเครือข่าย ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตปราจีนบุรี และ
ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง ด้านนโยบายและกฎหมาย

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับ ความเสี่ยง
1	ไม่มีนโยบายการใช้งานที่ชัดเจน	คนใช้งาน หรือ คนทำงาน สับสน ให้บริการไม่ถูก อธิบายไม่ได้	2	3	ปานกลาง
2	ขาดนโยบายการใช้ระบบเครือข่ายที่ ใช้งานได้ เช่น การติดตั้งแอนตี้ไวรัส การอัปเดต Windows สม่ำเสมอ เป็นต้น	เครื่องผู้ติดเชื้อไวรัส	2	3	ปานกลาง
3	ขาดการสร้างความตระหนักให้กับผู้ใช้ พฤติกรรมการใช้งานระบบเครือข่าย	อาจจะไปดาวน์โหลดไฟล์ไวรัส, เครื่อง ผู้ใช้งานกลายเป็นซอมบี้	2	3	ปานกลาง
4	ไม่ให้ความสำคัญ และเสริมสร้าง ความตระหนักทางด้านกฎหมายที่ เกี่ยวข้อง เช่น PDPA กับบุคลากร	ไม่รู้ว่า อะไรทำได้ ทำไม่ได้ หรือ กระทบงานอย่างไร	2	3	ปานกลาง

เมื่อได้ระดับความเสี่ยงของประเด็นปัญหา/ปัจจัยเสี่ยงต่างๆ แล้ว สำนักคอมพิวเตอร์ฯ จะนำระดับ
ความเสี่ยงที่สูง และสูงมาก มาพิจารณาถึงการจัดการความเสี่ยง และจัดโครงการ/กิจกรรมรองรับเพื่อให้
ความเสี่ยงนั้นน้อยลง หรือหมดไป

ตารางที่ 28 ประเด็นปัญหา/ปัจจัยเสี่ยงที่มีการประเมินระดับความเสี่ยงในเกณฑ์มาก

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
1	ผู้บริหารขาดจิตวิทยาการบริหารและความสามารถทำให้บุคลากรบางคนที่ไม่ค่อยปฏิบัติงาน และเข้าร่วมกิจกรรมภายในสำนัก	บุคลากรที่ไม่เข้าร่วมขาดการรับรู้ข้อมูลที่เท่าเทียมกันทั้งสำนัก, งานกระจุกอยู่ที่บุคลากรกลุ่มใดกลุ่มหนึ่ง, บุคลากร มีพฤติกรรมเลียนแบบ ส่งผลกระทบกับการทำงานเป็นทีม	3	3	สูง	ควบคุม	โครงการอบรมหลักสูตรการบริหารของผู้บริหาร	2565 (ผู้บริหาร)
2	บุคลากรไม่ทันต่อเทคโนโลยีใหม่ เนื่องด้วยเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว	บริการไม่ทันสมัย ทำให้ผู้ใช้งานมีความพึงพอใจในบริการของสำนักน้อยลง	4	3	สูง	ควบคุม	โครงการอบรมพัฒนาความรู้และทักษะของบุคลากร	ทุกปี (ผู้บริหาร)
3	ขาดการเฝ้าระวัง และติดตามปัญหาที่เกิดขึ้นในระบบเครือข่ายอย่างเป็นระบบ	สำนักขาดความน่าเชื่อถือในการให้บริการ	3	3	สูง	ควบคุม	กิจกรรมปรับปรุงกระบวนการทำงานให้เป็นมาตรฐาน	2566 (ผู้บริหาร)
4	ขาดนโยบายส่งเสริมให้บุคลากรใช้งาน open source ในการปฏิบัติงาน	งบประมาณในการบำรุงรักษาอุปกรณ์และ software ที่มีราคาสูง อาจจะไม่เพียงพอในอนาคต	5	2	สูง	ควบคุม	กิจกรรมกำหนดนโยบายการใช้งาน Open source	2566 (ผู้บริหาร)
5	ขาดทีมงานพัฒนาระบบสารสนเทศเพื่อใช้ในการบริหารงานภายในสำนัก	ทำให้ภาพลักษณ์ของสำนักคอม ดูไม่ทันสมัยและไม่เป็นองค์กรดิจิทัล	4	3	สูง	ยอมรับ	กิจกรรมเพิ่มทักษะการควบคุมงานและตรวจสอบงาน Out source	2566 (ผู้บริหาร)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
6	ขาดทักษะและประสบการณ์ในการบริหารงานระดับองค์กร (People management skill, soft skill, technology, communication)	แนวทางการบริหารยังไม่ชัดเจนอย่างเป็นรูปธรรม และเป็นที่ยอมรับของบุคลากร	4	3	สูง	ควบคุม	โครงการอบรมหลักสูตรการบริหารของผู้บริหาร	2565 (ผู้บริหาร)
7	ไม่สามารถปรับปรุงระบบรับ จ่ายเงินแบบออนไลน์ได้	บริการไม่ทันสมัย	4	2	สูง	กระจาย	ให้คณะกรรมการ IT เป็นผู้ผลักดันนโยบายแก่มหาวิทยาลัย	ทุกปี (ผู้บริหาร)
8	ไม่สามารถปฏิบัติงานนอกสถานที่ผ่านระบบสารสนเทศได้อย่างเต็มรูปแบบ เพราะยังมีข้อบ่งคับบางเอกสารต้องเป็นกระดาษ	ถ้ามีภัยพิบัติที่ร้ายแรง จะทำให้การทำงานของสำนักคอมไปสามารถปฏิบัติงานได้อย่างต่อเนื่อง	3	3	สูง	กระจาย	ให้คณะกรรมการ IT เป็นผู้ผลักดันนโยบายแก่มหาวิทยาลัย	ทุกปี (ผู้บริหาร)
9	ศักยภาพหลักขององค์กรขาดความชัดเจน เช่น ขอบเขตความสามารถในการให้บริการของเราอยู่แคไหน	ผู้ใช้บริการเกิดความสับสนขอบเขตการให้บริการของสำนัก และความพึงพอใจของผู้รับบริการ	4	2	สูง	ควบคุม	พัฒนาขีดความสามารถในการให้บริการให้ชัดเจน และ จัด โครงการ ประชาสัมพันธ์ ส่งเสริม	ทุกปี (สำนักงานผู้อำนวยการ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							การรับรู้ ความเข้าใจต่อ งานบริการ	
10	ความชัดเจนของผลงานที่ต้องการให้ เกิดจากแผนงาน/กิจกรรม/ตัวชี้วัด ก่อนกำหนดเป็นแผนปฏิบัติการใหม่ ไม่เพียงพอ	ไม่มีข้อมูลประกอบการพิจารณาอนุมัติทำ โครงการในแต่ละปี ทำให้โครงการเกิดการ ซับซ้อน การใช้งบประมาณไม่มีความคุ้มค่า โครงการที่จัดทำอาจไม่มีประโยชน์หรือ แก้ปัญหาที่แท้จริงของสำนัก ได้	3	4	สูง	ควบคุม	จัดทำแนวทางการเขียน โครงการ แจ้งให้ ผู้รับผิดชอบโครงการ วิเคราะห์ผลการ ดำเนินงานของโครงการทั้ง เชิงปริมาณ และเชิง คุณภาพ เพื่อเสนอต่อ ผู้บริหารประกอบการ ตัดสินใจ	ทุกปี (สำนักงาน ผู้อำนวยการ)
11	ตัวชี้วัดของโครงการมีมาก เนื่องจาก แผนมีหลายแผน และหลายตัวชี้วัด ในโครงการเดียว	ทำให้ผู้ปฏิบัติงานภายใต้โครงการนั้น สับสนใน การปฏิบัติงานในแต่ละแผน	2	4	สูง	ควบคุม	จัดทำแนวทางการเขียน โครงการที่มีความเชื่อมโยง แผนทุกแผนในรูปแบบ ที่เข้าใจง่าย	ทุกปี (สำนักงาน ผู้อำนวยการ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							ประชาสัมพันธ์ให้บุคลากรทราบ ตอนแจ้งกำหนดการจัดทำแผนแต่ละปี	
12	ปฏิบัติงานไม่ครบทุกขั้นตอนตามพรบ.จัดซื้อจัดจ้าง	ไม่ปฏิบัติตาม พรบ. ถือว่าเป็นความผิด	1	5	สูง	ควบคุม	จัดทำ Check List ขั้นตอนการทำงาน	ทุกปี (สำนักงาน ผู้อำนวยการ)
13	ค่าบำรุงรักษาระบบต่างๆ มากเกินไป	เงินเหลือจ่ายลดลงอย่างมาก	3	3	สูง	ควบคุม	รายงานยอดเงินคงเหลือให้ผู้บริหารทราบอย่างสม่ำเสมอ ใช้ประกอบ การพิจารณาค่าใช้จ่ายบำรุงรักษาระบบ เพื่อหาแนวทางการบริหารจัดการด้านการเงินต่อไป	ทุกปี (สำนักงาน ผู้อำนวยการ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
14	บุคลากรขาดความรู้และขาดการตระหนัก และขาดการใส่ใจในการปฏิบัติตามจรรยาบรรณวิชาชีพ	ทำให้เกิดการกระทำผิดหรือละเลยต่อการปฏิบัติงานตามจรรยาบรรณในวิชาชีพ	1	5	สูง	ควบคุม	จัดฝึกอบรมให้ความรู้ในเรื่องของจรรยาบรรณในวิชาชีพ และเพิ่มมาตรการตรวจสอบ สอบทานที่มีประสิทธิภาพ	ทุกปี (ในโครงการผู้บริหารพบผู้ปฏิบัติงาน) (สำนักงานผู้อำนวยการ)
15	ระบบสารสนเทศที่มีไม่สามารถตอบสนองความต้องการของผู้ใช้ได้ครบถ้วน	ผู้ใช้ไม่ได้รับความพึงพอใจในการใช้บริการ	3	3	สูง	ควบคุม	กิจกรรมพัฒนาหรือปรับปรุงระบบสารสนเทศ	ทุกปี (ฝ่ายพัฒนาระบบสารสนเทศ)
16	ระบบสารสนเทศถูกโจมตี	ไม่สามารถให้บริการระบบสารสนเทศได้	1	5	สูง	ควบคุม	กิจกรรมเพิ่มความปลอดภัยให้กับระบบสารสนเทศ - ขอใช้บริการ Web App Firewall สำหรับระบบสารสนเทศที่เป็น Web	ทุกปี (ฝ่ายพัฒนาระบบสารสนเทศ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							Application - ขอการใช้งาน SSL สำหรับระบบสารสนเทศที่เป็น Web Application กิจกรรมติดตามการแก้ไข ช่องโหว่และภัยคุกคามของระบบ - เขียนโปรแกรมแบบ Secure Coding - อัปเดตซอฟต์แวร์ที่เป็น ส่วนประกอบของระบบ สารสนเทศให้ทันสมัยและ เข้ากันได้กับระบบ สารสนเทศ	

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							- ตรวจสอบช่องโหว่และภัยคุกคามของระบบ - กิจกรรมตรวจสอบสถานะความพร้อมใช้งานของระบบสารสนเทศ	
17	ระบบสารสนเทศใช้เทคโนโลยีเก่าในการพัฒนา และถูกออกแบบและพัฒนา รวมถึงใช้งานมาเป็นระยะเวลายาวนานแล้ว	ต้องใช้งานกับอุปกรณ์รุ่นเก่า บางครั้งเมื่อมีการอัปเดตระบบปฏิบัติการทำให้ Driver ไม่รองรับ	2	4	สูง	ควบคุม	กิจกรรมพัฒนาหรือปรับปรุงระบบสารสนเทศ	ทุกปี (ฝ่ายพัฒนาระบบสารสนเทศ)
18	ระบบสารสนเทศที่มีข้อจำกัดในการพัฒนาหรือปรับปรุงการทำงานของระบบ เช่น Source code ที่มีอยู่ในปัจจุบัน อาจจะไม่ใช้เวอร์ชันล่าสุด เป็นต้น	หากระบบสารสนเทศทำงานผิดพลาด จะไม่สามารถแก้ไขได้	2	4	สูง	ยอมรับ	กิจกรรมการตรวจสอบความพร้อมใช้งานของระบบสารสนเทศและอุปกรณ์	ทุกปี (ฝ่ายพัฒนาระบบสารสนเทศ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
19	มีการตัดกระแสไฟฟ้าบ่อยครั้ง และไม่มีแผนการซ่อมบำรุงรายปี พร้อมทั้งไม่มีเครื่องปั่นกระแสไฟฟ้า เพื่อให้ระบบสารสนเทศให้บริการได้เป็นปกติ	- ไม่สามารถให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง	2	5	สูง	ควบคุม	โครงการจัดหาเครื่องมือและระบบสำหรับให้บริการบน Public Cloud	2569 (ฝ่ายพัฒนาระบบสารสนเทศ)
20	ไม่มีการกำหนดขึ้นหรือการปรับปรุงระเบียบหรือนโยบายให้ทันสมัยตามความต้องการของผู้ใช้งาน	การให้บริการที่ทันสมัย อาจผิดระเบียบของมหาวิทยาลัยได้ เช่น การรับเงินออนไลน์ เป็นต้น	3	3	สูง	กระจาย	กิจกรรมทำข้อมูล และร่างแนวนโยบายที่จำเป็นสำหรับเสนอผู้บริหารระดับสูงของมหาวิทยาลัย	2565 (ฝ่ายพัฒนาระบบสารสนเทศ)
21	มีผู้ตอบแบบประเมินความพึงพอใจในการใช้บริการน้อย	ผลสรุปไม่สะท้อนความต้องการของผู้รับบริการส่วนใหญ่ ทำให้พัฒนางานบริการได้ไม่ตรงตามเป้าหมาย	4	3	สูง	ควบคุม	ดำเนินการปรับปรุงกระบวนการเก็บรวบรวมความพึงพอใจ (ทำแบบทดสอบ และประเมินความพึงพอใจแบบ	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							ออนไลน์ก่อนจึงจะจัดส่งวุฒิปัตร์ให้อัตโนมัต)	
22	ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อในห้องปฏิบัติการคอมพิวเตอร์	เกิดช่องโหว่หรือความไม่ปลอดภัยในระบบเครือข่าย	2	4	สูง	ควบคุม	กำหนดมาตรการในการใช้งานเครือข่าย	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)
23	ไม่มีขั้นตอนที่สามารถระบุตัวตนที่แท้จริงในการใช้งานเครื่องคอมพิวเตอร์ของบุคคลภายนอก	ไม่สามารถระบุตัวตนเมื่อมีปัญหาจากการใช้งานคอมพิวเตอร์ เช่น การใช้โปรแกรมละเมิดลิขสิทธิ์ การเข้าเว็บไซต์ที่ไม่ปลอดภัย	2	4	สูง	ควบคุม	กำหนดให้ผู้ใช้ต้องมี igit account ในการเข้าใช้เครื่องคอมพิวเตอร์	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)
24	อุปกรณ์ที่ให้บริการถูกโจรกรรม	เครื่องคอมพิวเตอร์หรืออุปกรณ์ไม่สามารถทำงานได้	2	4	สูง	ควบคุม	ดำเนินการปรับปรุงกระบวนการขั้นตอนการตรวจสอบอุปกรณ์ที่ให้บริการก่อนให้บริการ	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
25	นโยบายการให้บริการไม่ชัดเจน	ผู้ปฏิบัติงานขาดความชัดเจนในการให้บริการ ส่งผลให้ผู้รับบริการได้รับบริการช้าลง	4	3	สูง	บรรเทา	สร้างช่องทางการสื่อสารระหว่างผู้บริหารถึงผู้ปฏิบัติงาน	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)
26	ระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง	ทำให้สำนัก ขาดความเชื่อมั่นในการให้บริการ	2	5	สูง	กระจาย	ย้ายระบบสารสนเทศที่มีความสำคัญสูงขึ้นสู่ ระบบ Cloud (Website)	2566 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)
27	ความผิดพลาดในการซ่อมคอมพิวเตอร์ของบริการ It clinic	เสียชื่อเสียงและขาดความน่าเชื่อถือในการให้บริการ	2	4	สูง	บรรเทาความเสี่ยง	กำหนดกรอบความรับผิดชอบและเพิ่มทักษะให้กับผู้ปฏิบัติงาน	2565 (ฝ่ายบริการวิชาการและส่งเสริมการวิจัย)
28	การควบคุมการเข้าออกห้องเซิร์ฟเวอร์	การควบคุมมีความหละหลวม บุคคลภายนอกเข้าห้อง server โดยไม่มีการ ลง ชื่อใน Log book ทำให้ละเมิดการดำเนินการ ISO27001	2	5	สูง	ควบคุม	ดำเนินการควบคุมตาม ISO27001 อย่างเคร่งครัด	ทุกปี (ฝ่ายวิศวกรรมระบบเครือข่าย)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
29	ระบบปรับอากาศในห้อง Server มีแหล่งจ่ายไฟฟ้าเพียงแหล่งเดียว	เมื่อแหล่งจ่ายไฟฟ้าเกิดปัญหาขัดข้อง ทำให้ความร้อนในห้อง Datacenter สูงขึ้น เกินกว่าที่เครื่องแม่ข่ายสามารถ ดำเนินงานได้และเสี่ยงต่อความเสียหายที่จะเกิดขึ้นกับ Server	1	4	สูง	ควบคุม	จัด ทำ าระ บวน การตรวจสอบและขั้นตอนการดำเนินการในแผนสำรองฉุกเฉิน	2567 (ฝ่ายวิศวกรรมระบบเครือข่าย)
30	อุปกรณ์หลักในระบบอินเทอร์เน็ตไม่สามารถทำงานได้ตามหน้าที่เนื่องจาก 1.การถูกโจมตี 2.ชำรุดเสียหาย	ทำให้ไม่สามารถใช้งานอินเทอร์เน็ตได้ทั้งมหาวิทยาลัย	1	5	สูง	ยอมรับ	1.ตรวจสอบการโจมตีอย่างสม่ำเสมอ 2.ทำสัญญาบำรุงรักษาอุปกรณ์ที่สามารถนำอุปกรณ์มาทดแทนอุปกรณ์ที่ชำรุดเสียหายภายในเวลาที่เหมาะสม	ทุกปี (ฝ่ายวิศวกรรมระบบเครือข่าย)
31	ไม่มีระบบรักษาความปลอดภัยเครือข่ายสำรอง (HA Firewall)	ทำให้ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่อง กรณีอุปกรณ์เสียหาย	2	5	สูง	ยอมรับ	กิจกรรมจัดหาแนวทางตรวจสอบและมอนิเตอร์ Firewall แบบ 24 ชม.	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
32	ระบบไฟฟ้าภายในมหาวิทยาลัยขัดข้อง	ทำให้ระบบหรืออุปกรณ์ อาจเกิดการเสียหายได้ เช่น เครื่องสำรองไฟฟ้า เครื่องปรับอากาศในห้องเซิร์ฟเวอร์ หรือ อุปกรณ์เครือข่ายต่างๆ	2	4	สูง	ยอมรับ	มีตรวจสอบการทำงานของระบบไฟฟ้าอย่างสม่ำเสมอ	ทุกปี (ฝ่ายวิศวกรรมระบบเครือข่าย)
33	ขาดระบบแจ้งเตือน Fire Alarm แบบออนไลน์ และระบบดับเพลิงห้องเซิร์ฟเวอร์, มอนิเตอร์และดูย้อนหลังไม่ได้	อาจทำให้เกิดไฟไหม้ห้องเซิร์ฟเวอร์ โดยที่ไม่ทราบล่วงหน้า	1	4	สูง	ควบคุม	โครงการจัดหาระบบมอนิเตอร์ห้อง Data Center	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)
34	ขาดการติดต่อประสานงานจากหน่วยงานภายนอกตั้งแต่เริ่มต้น เมื่อมีงานที่ต้องปฏิบัติงานร่วมกัน	ทำให้ใช้เวลาในการดำเนินงานมากกว่าปกติ เกิดขอบเขตงานที่ไม่แน่ชัดว่าเนื้องานจริง ๆ ต้องทำแค่ไหน อาจต้องทำงานอื่นเพิ่มเติมจากงานจริง เช่น มีการสร้างตึกใหม่ไม่มีการพูดคุยถึงการเดินเครือข่ายเมื่อต้องการทำเครือข่ายที่หลังต้องทำการขุดเจาะพื้นที่ใหม่อีกครั้ง	3	3	สูง	ยอมรับ	กิจกรรมหาช่องทางในการสื่อสารที่มีประสิทธิภาพ	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
35	Admin ไม่พร้อมปฏิบัติงาน เช่น ลาป่วย ไม่อยู่หน้างาน (ไม่มีคนทดแทนกัน)	ไม่มีคนทดแทนกันหรือคนอื่นไม่สามารถทำงานต่อได้ (งานไม่ต่อเนื่อง)	3	3	สูง	บรรเทา	กิจกรรมหาบุคคลากรจัดทำคู่มือ	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)
36	ขาดการสำรองข้อมูล เช่น ความเสี่ยงที่เกิดจากฮาร์ดดิสก์เสียหาย, ระบบ CCTV เป็นต้น	ข้อมูลเสียหายไม่สามารถกู้คืนได้	3	3	สูง	ยอมรับ	กิจกรรมให้ผู้ดูแลระบบคอยสำรองข้อมูลเอง	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)
37	ระบบอินเทอร์เน็ตสำรองไม่ทำงานทันที ที่อินเทอร์เน็ตหลักดาวน์ (วิทยาเขตระยอง)	ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่อง	3	4	สูง	ควบคุม	กิจกรรมจัดหาแนวทางการใช้งาน Internet Load Balance	2566 (ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขตระยอง)
38	ไม่มี Private link สำรองระหว่างวิทยาเขต (วิทยาเขตระยอง)	เมื่อ Private link Down ระบบที่วิทยาเขตจะใช้งานไม่ได้บางส่วน	3	4	สูง	ควบคุม	หาแนวทางการเพิ่ม private link Uninet 3 วิทยาเขต	2566 (ฝ่ายเทคโนโลยีสารสนเทศ)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
								วิทยาเขต ระยอง)
39	การรับเงินค่าบริการงานพิมพ์ (วิทยาเขตระยอง,ปราจีน)	เสี่ยงต่อการผิดระเบียบทางการเงิน เสี่ยงต่อการฝากเงินไม่ทัน (กรณีมีงานด่วนหรืออยู่คนเดียว)	2	4	สูง	ยอมรับ	คู่มือการปฏิบัติงาน รับเงินค่าบริการงานพิมพ์, ทวนสอบการปฏิบัติงาน	2565 (ฝ่ายเทคโนโลยีสารสนเทศ วิทยาเขต ปราจีนบุรีและ ระยอง)
40	ไม่สามารถควบคุมสิทธิการใช้งาน เครือข่ายรายบุคคลได้	ผู้ใช้อาจจะใช้งานเครือข่ายในทางที่ไม่ดี โดยที่ ไม่สามารถควบคุมได้	5	2	สูง	กระจาย	โครงการจัดหาระบบ ยืนยันตัวตนสำหรับการใช้ งานอินเทอร์เน็ต	2565 (ฝ่ายวิศวกรรม ระบบ เครือข่าย)
41	โครงสร้างเครือข่ายหลัก (Router, Core Switch, Firewall) ไม่สามารถทำงานในลักษณะ Redundancy ได้	ใช้งานอินเทอร์เน็ตได้ไม่ต่อเนื่อง	2	5	สูง	ควบคุม	กิจกรรมจัดหาอุปกรณ์ สำรองโดยเน้นเรื่องการ	2565

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
							ประหยังบประมาณ เช่น การใช้ OpenSource	(ฝ่ายวิศวกรรมระบบเครือข่าย)
42	ไม่มีระบบการตรวจสอบ ความสมบูรณ์ของไฟล์ในระบบ เช่น เว็บไซต์ถูกแก้ไข, ไฟล์ Log ถูกแก้ไข เป็นต้น	อาจมีการแก้ไขเนื้อหาเว็บไซต์โดยผู้ไม่ประสงค์ดีไปในทางที่ไม่ดี ทำให้เสียชื่อเสียงได้ เป็นต้น	2	4	สูง	กระจาย	ผู้ผลิตอุปกรณ์จะต้องมีมาตรฐานการป้องกัน	ทุกปี (ฝ่ายวิศวกรรมระบบเครือข่าย)

ตารางที่ 28 ประเด็นปัญหา/ปัจจัยเสี่ยงที่มีการประเมินระดับความเสี่ยงในเกณฑ์มากที่สุด

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
1	ขาดแบบฟอร์มการประเมินผลงาน และการวัด KPI รายบุคคลที่ตรงต่อภาระงานจริงที่ปฏิบัติอยู่	รายงานผลการปฏิบัติงานไม่สะท้อนผลงาน และการปฏิบัติงานจริงที่ทำอยู่	5	5	สูงมาก	ควบคุม	จัดโครงการสัมมนาจัดทำ KPI ส่วนบุคคล	2565 (ผู้บริหาร)

ลำดับ	ประเด็นปัญหา/ปัจจัยเสี่ยง	ความเสี่ยงที่อาจจะเกิดขึ้น	การประเมินความเสี่ยง			การบริหารความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง	วิธีการจัดการความเสี่ยง	โครงการ/กิจกรรมเพื่อบริหารความเสี่ยง	ปีที่จะดำเนินการ
2	ขาดแผนปฏิบัติงานของผู้บริหาร	การทำงานของผู้บริหารไม่มีประสิทธิภาพ	5	3	สูงมาก	ควบคุม	กิจกรรมจัดทำแผนปฏิบัติงานผู้บริหาร	2566 (ผู้บริหาร)
3	บุคลากรไม่สามารถทำงานทดแทนกันได้	หากระบบมีปัญหา แต่ผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ ปัญหานั้นจะไม่ได้รับการแก้ไขในทันที	5	5	สูงมาก	ควบคุม	กิจกรรมการจัดทำวิธีการแก้ไขปัญหาที่เกิดขึ้นของระบบสารสนเทศ	ทุกปี (ฝ่ายพัฒนาระบบสารสนเทศ)
4	ไม่มีทีมงานที่มีความเชี่ยวชาญด้านกฎหมาย	การดำเนินงานต่างๆ ที่ขาดความรู้ความเข้าใจด้านกฎหมายที่ชัดเจน อาจขัดต่อกฎหมายได้	3	5	สูงมาก	ควบคุม	โครงการจัดทำแนวปฏิบัติด้านข้อมูลส่วนบุคคลสำหรับผู้ดูแลระบบสารสนเทศ	2566 (ฝ่ายพัฒนาระบบสารสนเทศ)
5	ไม่มีระบบยืนยันตัวตนและเก็บ Log Userที่เป็นศูนย์กลางทั้งมหาวิทยาลัย	ยืนยันตัวตนตาม พรบ. คอมพิวเตอร์ฯ 2560 ไม่ได้	5	3	สูงมาก	กระจาย	โครงการพัฒนาระบบเก็บ Log ทั้งมหาวิทยาลัยที่เป็นศูนย์กลาง	2565 (ฝ่ายวิศวกรรมระบบเครือข่าย)