แบบ RM-1

# แบบกำหนดขอบเขตความรับผิดชอบตามประเด็นยุทธศาสตร์
## ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

| ประเด็นยุทธศาสตร์มหาวิทยาลัย ที่ตอบสนอง | กลยุทธ์/ประเภทความเสี่ยง/ โครงการ/งานประจำ | วัตถุประสงค์ | ตัวชี้วัด | เป้าหมาย | ผู้รับผิดชอบ |
|---|---|---|---|---|---|
| 4. การพัฒนาสู่มหาวิทยาลัยสมรรถนะสูง | 4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาล มุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง | เพื่อบำรุงรักษาระบบเครือข่ายให้มีประสิทธิภาพในการให้บริการภายในมหาวิทยาลัยฯ | KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5)<br>KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80)<br>KPI15 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80) | (เป้าหมาย คะแนน 5) | ผศ.พรหมเมศ วีระพันธ์<br>ผศ.ศิลป์ณรงค์ ฉวีพัฒน์ |

แบบ RM-2

# แบบฟอร์มการวิเคราะห์ความเสี่ยง

## ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

| งานหลักของฝ่าย (1) | ความเสี่ยง (2) | สถานะปัจจุบัน (3) | ปัจจัยเสี่ยง (4) | | ผลกระทบ (5) | KPI (6) | โอกาสที่จะเกิด (L) (7) | ผลกระทบ (C) (8) | ระดับความเสี่ยง (9) | ระดับความเสี่ยงที่คาดหวัง (10) | แนวทางการตอบสนอง (11) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ภายนอก | ภายใน | | | | | | | |
| **งานประจำ (Routine : R)** | | | | | | | | | | | |
| 4.1 พัฒนาระบบและกลไกการบริหารจัดการด้วยหลักธรรมาภิบาลมุ่งสู่การเป็นมหาวิทยาลัยสมรรถนะสูง | O1/การโจมตีความปลอดภัยทางไซเบอร์ | 1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด<br>2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้ | 1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด<br>2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตี | 1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ<br>2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึง | 1. การหยุดชะงักของระบบสารสนเทศสำคัญของมหาวิทยาลัย (เช่น ระบบทะเบียน การเงิน ระบบการเรียนการสอนออนไลน์) ส่งผลต่อภาพลักษณ์ ความน่าเชื่อถือ และมีค่าใช้จ่ายสูงในการแก้ไขฟื้นฟูระบบ<br>2. การรั่วไหลของข้อมูลส่วนบุคคลของนักศึกษาและบุคลากร นำไปสู่การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจส่งผลให้มหาวิทยาลัยได้รับบทลงโทษทางกฎหมาย | KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมายคะแนน 5)<br>KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายร้อยละ 80)<br>KPI15 – ร้อยละของ | L2=2 | C6=5 | 10<br>สูง | ต่ำ | ควบคุมความเสี่ยง |

| งานหลักของฝ่าย (1) | ความเสี่ยง (2) | สถานะปัจจุบัน (3) | ปัจจัยเสี่ยง (4) | | ผลกระทบ (5) | KPI (6) | โอกาสที่จะเกิด (L) (7) | ผลกระทบ (C) (8) | ระดับความเสี่ยง (9) | ระดับความเสี่ยงที่คาดหวัง (10) | แนวทางการตอบสนอง (11) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ภายนอก | ภายใน | | | | | | | |
| | | | แบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้ | การสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี | | นักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมายอย่างน้อยร้อยละ 80) | | | | | |

แบบ RM 3

# แบบแสดงแนวทางตอบสนองความเสี่ยง/แผนบริหารความเสี่ยง
## ชื่อหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

| โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1) | ปัจจัยเสี่ยง (2) | KPI (3) | ระดับความเสี่ยง (4) | แผนงาน/กิจกรรม (4) | ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5) | ระยะเวลาดำเนินการ (6) |
|---|---|---|---|---|---|---|
| O3/การโจมตีความปลอดภัยทางไซเบอร์ | **ภายนอก**<br>1. นโยบายและการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยฯ ต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรฐานที่กำหนด<br>2. การเพิ่มขึ้นของอาชญากรรมไซเบอร์ เช่น มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการโจมตีแบบ DDoS ส่งผลให้มหาวิทยาลัยตกเป็นเป้าหมายของแฮกเกอร์ที่ต้องการขโมยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรโดยไม่ได้รับอนุญาต หรือทำลายระบบไอทีส่งผลให้ไม่สามารถให้บริการตามปกติได้<br>**ภายใน**<br>1. บุคลากรและนักศึกษายังขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกหลอกผ่านอีเมลฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการเข้าถึงเว็บไซต์ที่ไม่น่าเชื่อถือ | KPI13 – ระดับความสำเร็จในการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (เป้าหมาย คะแนน 5)<br>KPI14 – ร้อยละของบุคลากรที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย ร้อยละ 80)<br>KPI15 – ร้อยละของนักศึกษาชั้นปีที่ 1 ที่เข้ารับการอบรมด้านความปลอดภัยไซเบอร์ (เป้าหมาย อย่างน้อยร้อยละ 80) | ระดับสูง | 1. ดำเนินการจัดตั้งคณะทำงานและผู้รับผิดชอบ<br>2. ประชุมคณะกรรมการดำเนินงาน จัดทำนโยบายวางแผนการดำเนินงาน<br>3. จัดอบรมเกี่ยวกับ เรื่อง การป้องกันความมั่นคงปลอดภัยไซเบอร์<br>4. สรุปผลการจัดกิจกรรม<br>5. จัดทำแผนรักษาความมั่นคงปลอดภัยไซเบอร์<br>6. จัดทำแนวปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์<br>7. แบบประเมินความสอดคล้อง ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>8. จัดทำนโยบายการรักษาความมั่นคงปลอดภัย | 1. ผศ.พรหมเมศ วีระพันธ์<br>2. ผศ.ศิลป์ณรงค์ ฉวีพัฒน์ | ปีงบประมาณ 2568 |

| โครงการตามยุทธศาสตร์/ประเภทความเสี่ยง (1) | ปัจจัยเสี่ยง (2) | KPI (3) | ระดับความเสี่ยง (4) | แผนงาน/กิจกรรม (4) | ผู้รับผิดชอบ/ผู้รับผิดชอบหลัก (5) | ระยะเวลาดำเนินการ (6) |
|---|---|---|---|---|---|---|
| | 2. มาตรการรักษาความปลอดภัยด้านการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยยังไม่ครอบคลุม โดยเฉพาะการปกป้องข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด รวมไปถึงการสูญหายและความเสียหายของข้อมูลสารสนเทศที่สำคัญจากกรณีของการถูกไวรัสเรียกค่าไถ่โจมตี<br>3. บุคลากรยังขาดความรู้ความเข้าใจในการป้องกันการโจมตีรูปแบบใหม่ผ่านระบบเครือข่ายอินเตอร์เน็ต<br>4. บุคลากรขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน | | | | | |