# บทที่ ๑

# บทนำ

## ๑.๑ หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีจะช่วยให้การบริหารงาน และการตัดสินใจ ด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามมามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูลการใช้งานอุปกรณ์คอมพิวเตอร์การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานผ่านระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร ดังนั้น สำนักส่งเสริมวิชาการและงานทะเบียน จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาศและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

## ๑.๒ วัตถุประสงค์ของการจัดทำแผนความเสี่ยง

๑.๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๑.๒.๓ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีที่เกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

## ๑.๓ เป้าหมาย

มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักส่งเสริมวิชาการและงานทะเบียน

## ๑.๔ ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของสำนักส่งเสริมวิชาการและงานทะเบียน

## ๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑.๕.๑ มีความพร้อมในการรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๕.๒ มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

## ๑.๖ ระยะเวลาดำเนินการ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ลำดับ | กิจกรรม | ปีงบประมาณ ๒๕๖๔ | | | | | หน่วยงานรับผิดชอบ |
| มี.ค. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. |  |
| ๑ | ศึกษาข้อมูลในการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักส่งเสริมวิชาการและงานทะเบียน |  |  |  |  |  | สสท. |
| ๒ | วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักส่งเสริมวิชาการและงานทะเบียน |  |  |  |  |  | สสท. |
| ๓ | สรุปผลการประเมิน |  |  |  |  |  | สสท. |

## ๑.๗ ผู้รับผิดชอบ

๑.๗.๑ นายวุฒิพงษ์ พันธุมนันท์ ผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน

๑.๗.๒ รศ.วาสนา เกษมสินธ์ รองผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน

๑.๗.๓ ผศ.ดร.นพรัตน์ สิทธิวงศ์ รองผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน

๑.๗.๔ ผศ.ดร.พรรณนภา หาญมนตรี รองผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน

๑.๗.๕ นายศักดิ์ชัย ฟองอ่อน หัวหน้าสำนักส่งเสริมวิชาการและงานทะเบียน

๑.๗.๖ นายภาณุมาศ บุตรสีผา หัวหน้างานบริการการศึกษา

๑.๗.๗ นายวงเวียน วงค์กะโซ่ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๑.๗.๘ นายนววิช ธงษาราษฎร์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

# บทที่ ๒

# การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

## ๒.๑ สภาพแว้ดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database และ Software) เช่นฐานข้อมูลด้านทะเบียนนักศึกษา การลงทะเบียนเรียน การชำระค่าธรรมเนียมการศึกษา การสมัครเรียน และฐานข้อมูลการติดต่อเพื่อข้อใช้บริการต่างๆ เป็นต้น

ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ระบบฐานข้อมูลระบบบริหารการศึกษา ทั้งส่วนของนักศึกษา อาจารย์ และเจ้าหน้าที่ ที่เข้าใช้งานระบบ(SNRU Connect) ฐานข้อมูลหลักสูตรตาม มคอ เป็นต้น

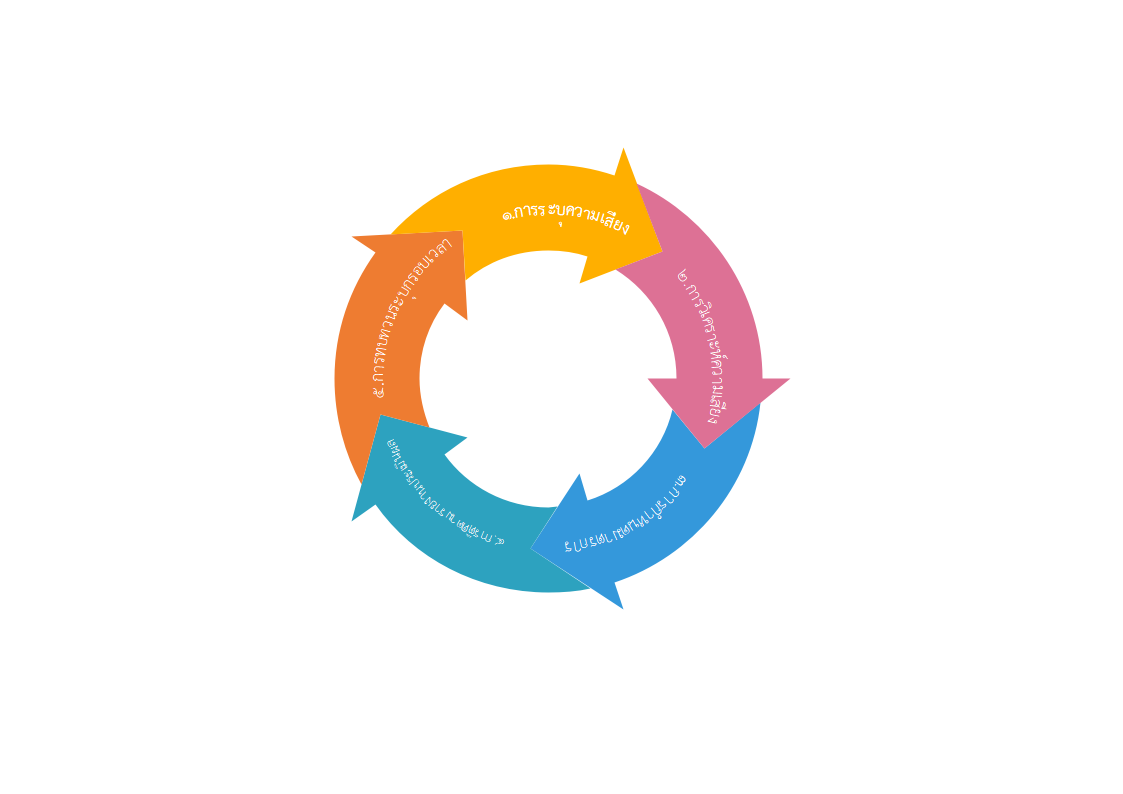
ระบบการให้บริการบนเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบที่ให้บริการในรูปแบบเว็บแอพพลิเคชั่น(Web Application Program) เช่น ระบบบริหารการศึกษา(SNRU Connect) ระบบจัดการข้อมูลหลักสูตรตาม มคอ.ออนไลน์(TQF Management System ) และระบบจัดการ Zoom License มหาวิทยาลัยราชภัฏสกลนคร เป็นต้น

ระบบที่ให้บริการในรูปแบบแอพพลิเคชั่น Windows ได้แก่ระบบบริหารจัดการตารางสอน ระบบติดต่อเพื่อข้อใช้บริการต่างๆ(ระบบคิว) ระบบพิมพ์ใบรายงานผลการศึกษา ระบบอนุมัติผู้สำเร็จการศึกษา เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่าย (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรอง ข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) เครื่องไมโครคอมพิวเตอร์ เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching) และชุดคอมพิวเตอร์สำหรับ เป็นต้น

## ๒.๒ กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมินและจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร และการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



**รูปที่ ๑** แสดงกระบวนการบริหารความเสี่ยง

**2.2.1 การระบุความเสี่ยงหรือปัจจัยเสี่ยง**

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้อง

โครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตาม

วัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

2.2.1.1 การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

2.2.1.2 การใช้ Checklist

2.2.1.3 การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

2.2.1.4 การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย

และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่

ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

**2.2.2 การวิเคราะห์และประเมินความเสี่ยง**

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัด

ระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

2.2.2.1 **การกำหนดเกณฑ์การประเมินมาตรฐาน** เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง

ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความ

เสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง

เกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ

(สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนด

เป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

2.2.2.2 **การประเมินโอกาสและผลกระทบของความเสี่ยง** เป็นการนำความเสี่ยงและปัจจัย

เสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรง

หรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความ

เสี่ยง ก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับ

มาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาส

ของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) เป็นดังนี้

ระดับ การประเมิน

1 น้อยมาก (แทบไม่มีผลกระทบเลย)

2 น้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)

3 ปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)

4 สูง (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)

5 สูงมาก (ผู้บริหารถูกลงโทษทางวินัย)

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

ระดับ การประเมิน

1 เกิดขึ้นน้อยมาก นานๆครั้ง (แทบไม่เกิดขึ้นเลย)

2 เกิดขึ้นน้อย ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)

3 เกิดขึ้นปานกลาง (อาจเกิดขึ้นได้ทุกปี)

4 เกิดขึ้นสูง หรือ บ่อย (อาจเกิดขึ้นได้ทุกเดือน)

5 เกิดขึ้นสูงมาก หรือ บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

2.2.2.3 **การวิเคราะห์ความเสี่ยง** เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง

และผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยง

สูงสุดที่จะต้องบริหารจัดการก่อน ดังร

**แผนผังประเมินความเสี่ยง**

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง 15-25

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  **ผลกระทบของความเสี่ยง** |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 |
| **โอกาสที่จะเกิดความเสี่ยง** | | | | | |

สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8-14

สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4-7

รูปที่ 2 แสดงแผนผังประเมินความเสี่ยง

สีฟ้า ระดับความเสี่ยงต่ำ

ค่าระหว่าง 1-3

2.2.2.4 **การจัดลำดับความเสี่ยง** เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กร

เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจาก

ระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงก่อน

**2.2.3 การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม**

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

2.2.3.1 **ควบคุมเพื่อความป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกัน

ไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุมและการเข้าถึง

เอกสาร เป็นต้น

2.2.3.2 **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้นหา

ข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับและการรายงานข้อบกพร่อง เป็นต้น

2.2.3.3 **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริมหรือ

กระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

2.2.3.4 **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไข

ข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคต

หลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อ

ลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการ

ควบคุมเป็นอันดับแรก โดยใช้ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมากหรือสูง มากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความ

เสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

**2.2.4 การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่กำหนดไว้**

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาส

ที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรม

ควบคุมความเสี่ยงหรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ซึ่งทางเลือกในการบริหารความเสี่ยง

มีหลายวิธีสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง

การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงและเมื่อองค์กรทราบความ

เสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยงและการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และ

ค่าใช้จ่ายแต่ละทางเลือกเพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจากประเด็นต่างๆ ดังนี้

2.2.4.1 พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่

ในระดับที่ยอมรับได้

2.2.4.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์

ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

2.2.4.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยง ให้กำหนดวิธีควบคุมในแผน

บริหารความเสี่ยง

2.2.4.4 ในรอบปีต่อไป ให้พิจารณาผลการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมา

บริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุ

วัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วย

การรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่

ถ้ายังมีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อ

ผู้บริหารเพื่อทราบและสั่งการ

**2.2.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน**

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้ว

เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของ

วิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นราย

ครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

## 2.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานนโยบายและแผนการขนส่งและจราจรได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

และการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น 8 ประเภท ดังนี้

**2.3.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)**

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย

อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความ

ปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มี

ประสิทธิภาพเพียงพอ

**2.3.2 ความเสี่ยงด้านบุคลากร (Human Risk)**

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ

และการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และ

คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้

งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้อง

ทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

**2.3.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร**

**(Hardware and Data Communication Risk)**

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์

การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Ransomware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

**2.3.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)**

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มี การอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

**2.3.5 ความเสี่ยงด้านระบบข้อมูล (Database Risk)**

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะ

ก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ

การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่

องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษา

ความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับ

ผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและ

คอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้อง

มีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

**2.3.6 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)**

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจาก

การเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนด

ยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

**2.3.7 ความเสี่ยงด้านการเงิน (Financial Risk)**

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่าย

งบประมาณไม่ทันตามกำหนดเวลา

**2.3.8 ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)**

หมายถึง ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

## 2.4 การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยง

ที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึง

ความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยง

มีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับ

โอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) โดยมี

หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

**2.4.1 การหลีกเลี่ยง (Terminate)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะ

ไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยง

ความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความ

เสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้

คิดทบทวนถึงผลที่จะได้รับ อาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

**2.4.2 การยอมรับ (Take)** เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่

ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่

ในวิสัย ที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความ

เสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้

User/Password ที่กำหนดให้แล้ว อาจจะบอก User/Password ของตนให้ผู้ใต้บังคับบัญชาทราบ และเมื่อ

ผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบ

ต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย และหน่วยงาน

ที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น แล้วจึงแก้ไขโดยการกำหนด User/Password

ใหม่ ให้กับหัวหน้างาน เป็นต้น

**2.4.3 การควบคุม (Treat)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อ

หาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเราไม่

สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการ

จัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีการควบคุมความสูญเสีย

มีสองวิธี คือ

2.4.3.1 การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิด

ความสูญเสีย ก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบ

ป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบ

เครือข่ายเป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงาน

ของระบบคอมพิวเตอร์ เป็นต้น

2.4.3.2 การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความ

สูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน

เครื่องตรวจจับความร้อนหรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิด

เหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อย

ที่สุด หรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

**2.4.4 การถ่ายโอน (Transfer)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น

อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะเวลาในการรับประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์

เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายให้ทันก่อนระยะเวลาใน

การรับประกันจะสิ้นสุด

## 

## 2.5 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของ สนข. มี

ดังนี้

**2.5.1 ปัจจัยภายนอก** ได้แก่

2.5.1.1 ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของ

เครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์

ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่นๆ

2.5.1.2 การขโมยอุปกรณ์เครื่องข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

2.5.1.3 การขำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการ

เคลื่อนย้าย หรืออื่นๆ

2.5.1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

2.5.1.5 ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

**2.5.2 ปัจจัยภายใน** ได้แก่

2.5.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.5.2.2 การถูกไวรัสคอมพิวเตอร์ (Virus Computer) ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ

2.5.2.3 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่าย

คอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

## 2.6 การประเมินความเสียหาย

**2.6.1** ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง

ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูก

ทำลายเสียหายจากไวรัส

**2.6.2** ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล

ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

## 2.7 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็น

ประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี

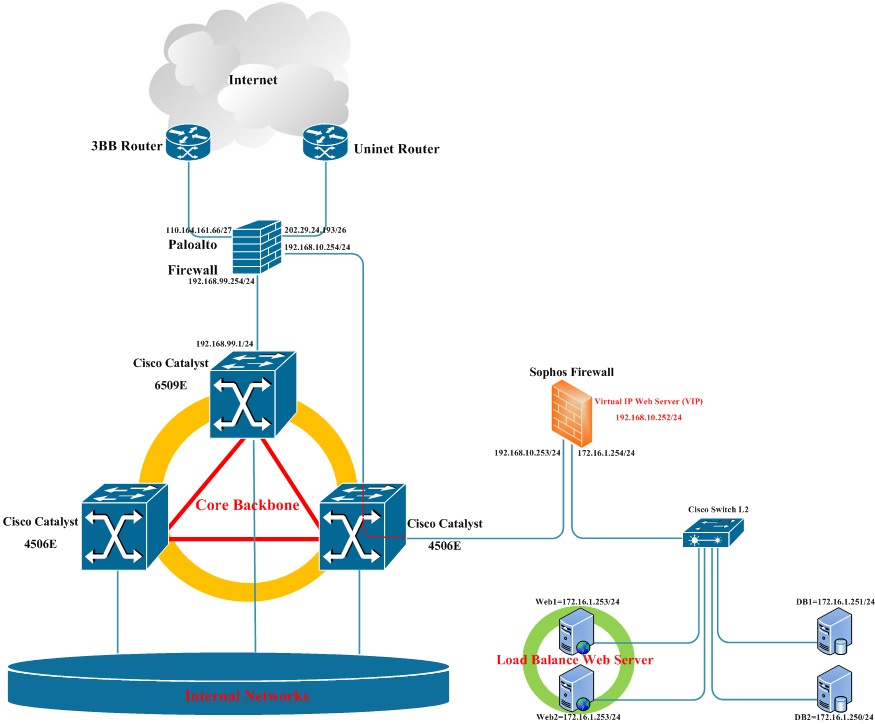
ตามที่ระบุ

## 2.8 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ของสำนักส่งเสริมวิชาการและงานเบียน ได้พัฒนาอย่างต่อเนื่อง เพื่อให้ระบบคอมพิวเตอร์สามารถทำงานผ่านระบบเครือข่ายได้อย่างมีประสิทธิภาพ โดยเครื่องคอมพิวเตอร์แม่ข่ายสำนักส่งเสริมวิชาการและงานเบียน อยู่ในการดูแลด้านอุปกรณ์ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร โดยตั้งอยู่ที่ อาคารศูนย์ข้อมูลคอมพิวเตอร์ (อาคาร SNRU DATA CENTER ) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนครเลขที่ 680 ตำบลธาตุเชิงชุม อำเภอเมืองสกลนคร จังหวัดสกลนคร รหัสไปรษณีย์ 47000

ระบบเครือข่ายคอมพิวเตอร์ของสำนักส่งเสริมวิชาการและงานเบียน มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองกลุ่ม ของข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์สำนักส่งเสริมวิชาการและงานเบียน จากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต และเครือข่าย Uninet เป็นต้น

นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์ แม่ข่าย (Server Zone หรือ Deminitalized Zone : DMZ) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของสำนักส่งเสริมวิชาการและงานเบียน ให้ บุคคลภายนอกเข้าถึงได้ เช่น Web Server และ FTP Server เป็นต้น



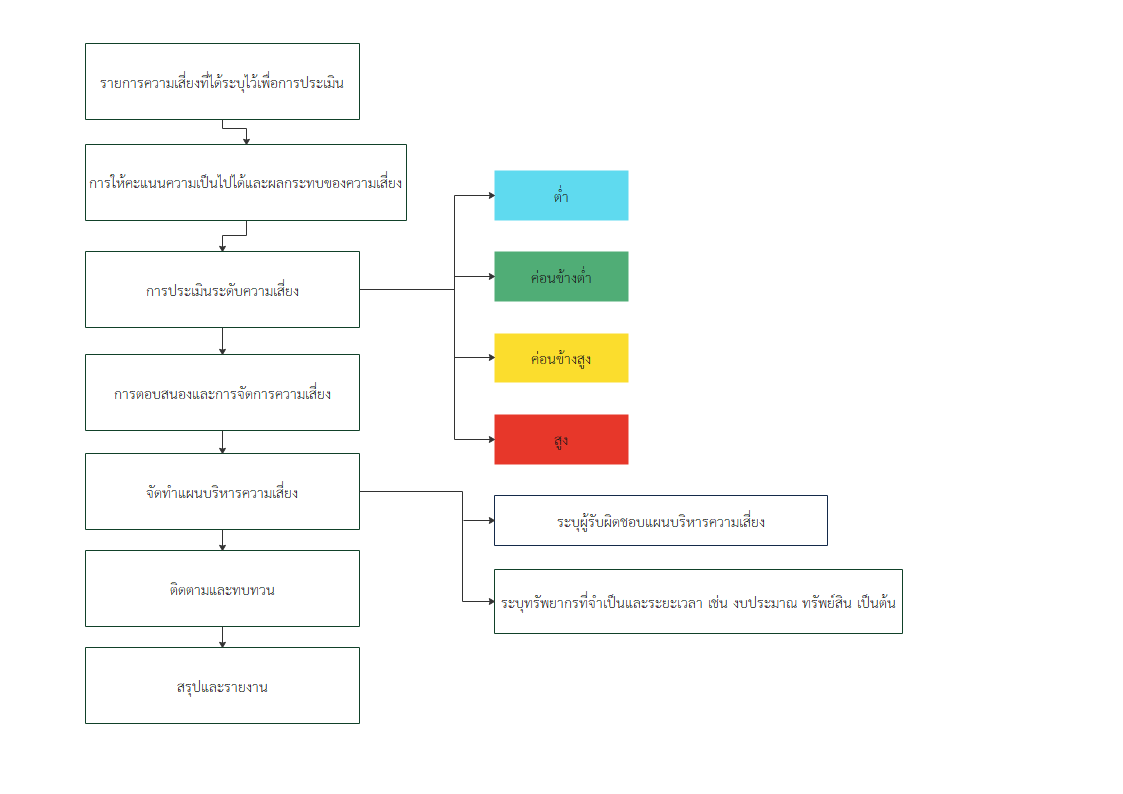
**รูปที่ 3** แสดงกระบวนการบริหารความเสี่ยง

# บทที่ 3

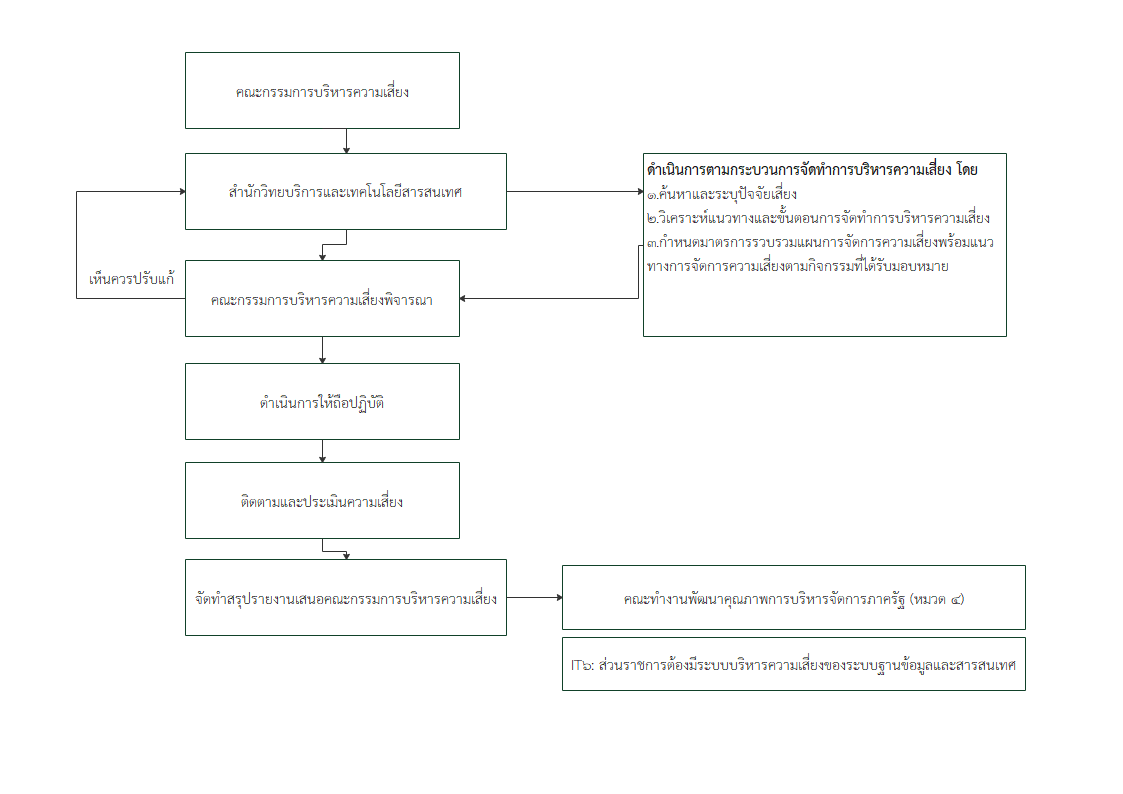
# การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักส่งเสริมวิชาการและงานเบียน

สำนักส่งเสริมวิชาการและงานเบียน ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้งานบริการการศึกษา ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พ.ศ. 25๖๔ ให้สอดคล้องกับแผนยุทธศาสตร์สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ระยะ 4 ปี (พ.ศ. 25๖๔-25๖๗ ) โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้อง กับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

## 3.1 แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



3.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



## 3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้

**แผนผังประเมินความเสี่ยง**

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง 15-25

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  **ผลกระทบของความเสี่ยง** |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 |
| **โอกาสที่จะเกิดความเสี่ยง** | | | | | |

สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8-14

สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4-7

สีฟ้า ระดับความเสี่ยงต่ำ

ค่าระหว่าง 1-3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ลำดับที่** | **ประเภทความเสี่ยง** | **ความน่าจะเป็นที่จะเกิด** | **ผลกระทบ** | **คะแนน** |
| 1. | ความเสี่ยงจากอัคคีภัย | 5 | 5 | 25 |
| 2. | ระบบกระแสไฟฟ้าขัดข้อง | 5 | 3 | 15 |
| 3. | ระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย | 5 | 3 | 15 |
| 4. | การไม่สำรองข้อมูล/ การสำรองข้อมูลขาดการอัพเดท | 5 | 5 | 25 |
| 5. | การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง | 3 | 5 | 15 |
| 6. | การบุกรุกโจมตีจากภายนอก | 3 | 4 | 12 |
| 7. | ลิขสิทธิ์ซอฟต์แวร์ | 2 | 5 | 10 |
| 8. | ไวรัสคอมพิวเตอร์/ Malware | 2 | 4 | 8 |
| 9. | ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร | 3 | 3 | 9 |
| **ลำดับที่** | **ประเภทความเสี่ยง** | **ความน่าจะเป็นที่จะเกิด** | **ผลกระทบ** | **คะแนน** |
| 10. | ความเสี่ยงจากการถูก Black List จาก search engine/spamhaus | 2 | 2 | 4 |
| 11. | การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผน  บริหารความต่อเนื่อง | 2 | 3 | 6 |
| 12. | ความเสี่ยงจากอุทกภัย | 2 | 3 | 6 |
| 13. | ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้ | 2 | 3 | 6 |
| 14. | ความเสี่ยงจากแมลง/สัตว์กัดแทะ | 1 | 5 | 5 |
| 15. | การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย /อุปกรณ์ | 1 | 5 | 5 |
| 16. | การโจมตีเซิร์ฟเวอร์ของหน่วยงานไม่ให้สามารถให้บริการ  ได้ (Denial of Service-DoS) | 1 | 5 | 5 |
| 17. | ความเสี่ยงจากการใช้ Wireless เข้าเครือข่าย  อินทราเน็ต | 1 | 5 | 5 |
| 18. | เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์ | 2 | 2 | 4 |
| 19. | ความเสี่ยงจากไฟกระชากจากปลั๊กพ่วง | 2 | 2 | 4 |
| 20. | วินาศภัย/ การก่อการร้าย | 1 | 3 | 3 |
| 21. | ความเสี่ยงจากความชื้น อุณหภูมิ | 2 | 1 | 2 |
| 22. | ความเสี่ยงจากแผ่นดินไหว | 1 | 1 | 1 |
| 23. | การโจรกรรมฐานข้อมูล | 1 | 1 | 1 |

## 

## 3.4 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 25๖๔

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| **ความเสี่ยงสูงมาก** |  |  |  |  |  |  |
| 1. ความเสี่ยงจากการ  เกิดอัคคีภัย | 1. คอมพิวเตอร์และ  เครือข่ายถูกทำลาย  2. ข้อมูลถูกทำลาย  3. การบาดเจ็บหรือ  เสียชีวิตของเจ้าหน้าที่  หรือลูกจ้างภายใน  อาคาร | 1. เสียงบประมาณในการ  จัดหาระบบทดแทน  2. การไม่สามารถใช้งาน  ระบบระหว่างที่มีการ  จัดหาระบบทดแทน | สูงมาก  ๕x๕=25 | 1. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์  ดับเพลิง  2. ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้  ระบบดับเพลิง  3. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับ  ความสำคัญ | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 3. ความเสี่ยงจากการ  ระบบคอมพิวเตอร์แม่  ข่ายหลักเสียหาย | 1. ไม่สามารถใช้  ระบบงานได้เต็ม  ประสิทธิภาพ  2. เสี่ยงต่อความ  เสียหายของข้อมูลและ  การกู้คืนข้อมูล | **1.** การใช้งานระบบงานไม่  สามารถใช้ได้ตามปกติ | สูงมาก  ๕x๕=25 | 1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและ  สำรองฐานข้อมูล  2. จัดตั้งศูนย์สำรองข้อมูล (Backup Site) | 5 | สำนักส่งเสริมวิชาการและงานทะเบียน |
| 4. ความเสี่ยงจากการ  ไม่ทำการสำรองข้อมูล  หรือทำการสำรอง  ข้อมูลแต่ขาดการ  อัพเดท | 1. เสี่ยงต่อการสูญหาย  ของข้อมูล ในขั้น  เล็กน้อยหรือมากจนไม่  สามารถดำเนินงานได้  ตามปกติ  2. เสี่ยงต่อการมีข้อมูล  ที่ไม่ถูกต้องกับความ  เป็นจริง | 1. เสียค่าใช้จ่ายในการกู้  คืนข้อมูล หรือ การจัดทำ  ขึ้นมาใหม่  2. ไม่สามารถนำข้อมูลที่มี  อยู่ไปใช้งานได้เนื่องจาก  ขาดความมั่นใจในข้อมูล | สูงมาก  3x๕=15 | 1. มีการบริหารจัดการในการทำการสำรองข้อมูล  (Backup) เป็นประจำอย่างสม่ำเสมอ  2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ  (Restore) | 5 | สำนักส่งเสริมวิชาการและงานทะเบียน |
| 5. ความเสี่ยงจากการ  เชื่อมต่อระบบครือข่าย  อินเทอร์เน็ต และ  อินทราเน็ตขัดข้อง | 1. ไม่สามารถใช้งาน  ระบบงานของ  สำนักงานฯ ผ่าน  เครือข่ายอินทราเน็ตได้  2. ไม่สามารถเชื่อมต่อ  ภายนอกสำนักงานฯ  ผ่านเครือข่าย  อินเทอร์เน็ตได้ | 1. ขัดขวางการทำงานของ  เจ้าหน้าที่และผู้บริหารงาน  สำนักงานฯ  2. บุคคลภายนอกไม่  สามารถเข้าใช้ Web  Server หรือค้นหาข้อมูลที่  ต้องการได้ | สูงมาก  5x3=15 | ตรวจสอบระบบเครือข่ายสื่อสารหลัก | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| **ความเสี่ยงสูง** |  |  |  |  |  |  |
| 1. ความเสี่ยงจากการบุก  รุกโจมตีจากภายนอก | เสี่ยงต่อการถูกโจมตี  จากภายนอกผ่าน  เครือข่ายอินเทอร์เน็ต | 1. ทำให้ระบบเครื่องแม่  ข่าย หรือลูกข่ายติดไวรัส  และแพร่กระจายสู่เครื่อง  อื่นๆ ทั้งหมดในเครือข่าย  2. ถูกแก้ไขหรือเปลี่ยน  แปลงข้อมูล หรือ รูปภาพ  บน Web Site ของหน่วยงาน  3. ถูกโจรกรรมข้อมูลที่  เป็นความลับ | สูง  3x4=12 | 1. ติดตั้งระบบเครือข่ายเพื่อป้องกัน และเตือน  ภัย  2. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็น  ตามลำดับ  3. ตรวจสอบ Policy และ Log ของระบบ  ป้องกันการบุกรุกระบบเครือข่าย | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| 2. ความเสี่ยงจากการใช้  ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ | 1. การสูญหายของ  ข้อมูล  2. การถูกฟ้องร้อง  และเสื่อมเสียชื่อเสียง  และความน่าเชื่อถือ  ของสำนักงานฯ | 1. การใช้งานอาจไม่ได้  ประสิทธิภาพตาม  ความสามารถของ  ซอฟต์แวร์นั้นๆ  2. มหาวิทยาลัย อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ  3. ความไม่สะดวกหากไป  ใช้งานด้วยซอฟต์แวร์ ที่ไม่  จำเป็นต้องมีลิขสิทธิ์  (Open Source) | สูง  2x๕=10 | 1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งาน  ตามความจำเป็น  2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ใน  การใช้งานซอฟต์แวร์ที่ถูกกฎหมาย | 4 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 3. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware | 1. โปรแกรมหรือ  ข้อมูลถูกทำลาย  2. ไม่สามารถเรียกใช้  โปรแกรมหรือ  ระบบงานได้ตามปกติ  3. การถูกขโมยข้อมูล | 1. ใช้คอมพิวเตอร์ไม่ได้  2. ใช้ระบบงานไม่ได้  3. ข้อมูลที่สำคัญสูญหาย | สูงมาก  2x4=8 | 1. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย  2. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| **ความเสี่ยงปานกลาง** |  |  |  |  |  |  |
| 1. ความเสี่ยงจากช่องโหว่  จากการพัฒนาโปรแกรม  ประยุกต์ภายในองค์กร | 1. การถูกขโมยข้อมูล  2. โปรแกรมเสียหาย  3. การใช้ช่องโหว่ของ  โปรแกรมหรือซ่อน  Script ไว้เพื่อ  วัตถุประสงค์แอบแฝง | 1. ลดความน่าเชื่อถือต่อ  สนข. หากข้อมูลถูกขโมย  ไปและนำไปเผยแพร่  2. กรณีที่เป็นข้อมูลลับ  อาจสร้างความเสียหายต่อ  สนข. เป็นอย่างยิ่ง | ปานกลาง  2x3=6 | 1. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตาม  คำแนะนำของ OWASP- Top 10 Web  Application Security Risks เพื่อลดความเสี่ย  2. มีมาตรการกำหนดชั้นความลับของข้อมูล  และการเข้าถึงข้อมูลที่เป็นความลับ | 4 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 2. ความเสี่ยงจากการถูก  Black List โดย Search  Engine หรือ Spamhaus  (http://www.spamhaus.  org) | 1. ผู้ใช้งานที่ต้องการ  ข้อมูลของ สนข. หรือ  ประชาชนทั่วไปไม่  สามารถเข้าใช้งาน  Web Server ได้ | 1. ลดความน่าเชื่อถือหรือ ข้อมูลของมหาวิทยาลัย  2. มหาวิทยาลัยอาจถูกฟ้องร้อง  โดยผู้มีส่วนได้ส่วนเสีย | ปานกลาง  3x2=6 | 1. ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่า  ไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง  Spam ออกไปยังเครือข่ายอินเทอร์เน็ต  2. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อน  การอัพโหลดข้อมูลขึ้น Web Server หรือ  FTP Server  3. มีการอัพเดทตัวโปรแกรมและ Signature  อย่างสม่ำเสมอ และการทำการบำรุงรักษา  (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์  พร้อมทั้ง Update Licenses | 2 และ 3 | สำนักส่งเสริมวิชาการและงานทะเบียน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 3. ความเสี่ยงจากการใช้  โปรแกรมที่พัฒนาโดยผู้  รับจ้างภายนอก  (Outsource) และการขาด  แผนบริหารความต่อเนื่อง | 1. เสี่ยงต่อการถูก  ขโมยข้อมูล  2. เสี่ยงต่อการทำ  ความเสียหายแก่  โปรแกรม  3. ไม่สามารถแก้ไข  ข้อบกพร่องได้เอง  4. ขาดการดูแล  บำรุงรักษาโปรแกรม  และข้อมูล ทำให้ไม่  สามารถใช้งานได้ใน  ระยะยาว  5. เสียค่าใช้จ่ายสูง | 1. ลดความน่าเชื่อถือต่อ  สนข. หากข้อมูลถูกขโมย  ไปและนำไปเผยแพร่  2. กรณีที่เป็นข้อมูลลับ  อาจสร้างความเสียหายต่อ  สำนักงานฯ เป็นอย่างยิ่ง  3. จัดหางบประมาณ  เพื่อทำการบำรุงรักษา  โปรแกรมและข้อมูล  พร้อมกับการทำการ  บำรุงรักษาเครื่องแม่ข่าย  และอุปกรณ์ที่เกี่ยวข้องที่  ต้องมีการอัพเดทอยู่เสมอ | ปานกลาง  2x3=6 | 1. การออกแบบระบบให้อิงมาตรฐาน Data  Flow Diagram (DFD) Level 2  2. การออกแบบอ้างอิงแผนผังความสัมพันธ์  ระหว่างกลุ่มข้อมูล – ER Diagram  3. ให้มีการส่งมอบ Source Code ในรูปแบบ  DVD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถ  ปรับปรุงแก้ไขได้  4. หากมีการพัฒนา Library ด้วยตนเอง ต้อง  ส่ง Source Code Library ที่สามารถแก้ไขได้  5. มีการถ่ายทอดความรู้ เทคโนโลยีในการ  พัฒนาระบบให้กับเจ้าหน้าที่  6. มีมาตรการในการกำหนดให้นำข้อมูลใด  ออกไปนอกสถานที่ได้ให้ชัดเจนและมีการ  ควบคุมอย่างรัดกุม  7. มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึง  การแก้ไขข้อผิดพลาดในการเขียนโปรแกรม  (Bug) การอัพเดท เมื่อมี Version หรือ  Release ใหม่ การแก้ไขเมื่อเกิดการ Crash  ของโปรแกรมหรือฐานข้อมูล (Database) เกิด  ความเสียหาย เป็นต้น | 4 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียนสำนัก/หรือหน่วยงานอื่น ที่พัฒนา  ระบบงาน  ขึ้นใช้เอง |
| 4. ความเสี่ยงจากการเกิด  อุทกภัย | ความเสียหายของ  เครื่องคอมพิวเตอร์  และอุปกรณ์ | เสียงบประมาณในการ  ซ่อมแซมหรือจัดหาใหม่  ทดแทน | ปานกลาง  2x3=6 | 1. ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มี  ความไวต่อน้ำ  2. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับ  ความสำคัญ | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 5. ความเสี่ยงจากข้อมูล  รั่วไหลจากการเปลี่ยนมือ  ผู้ใช้ | ข้อมูลที่สำคัญมีการ  รั่วไหลจากการ  ซ่อมแซมเครื่องที่เสีย  เช่น Hard Disk Flash Drive หรือ Cloud Storage | 1. ข้อมูลที่อยู่ในชั้น  ความลับ รั่วไหลทำให้  เสียหายต่อความเชื่อถือ  ของสำนักส่งเสริมวิชาการและงานทะเบียน  **2.** ข้อมูลที่รั่วไหลอาจทำ  ให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้  ประโยชน์ได้ | ปานกลาง  2x3=6 | มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น  Hard Disk หรือ Flash Drive  ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หาก  ทำได้ มีนโยบายห้ามเก็บข้อมูลสำคัญไว้ใน Public Cloud | 5 | สำนักส่งเสริมวิชาการและงานทะเบียน |
| 6. ความเสี่ยงจากแมลง  หรือสัตว์กัดแทะ  คอมพิวเตอร์ อุปกรณ์ หรือ  สายไฟฟ้า/ สายสัญญาณ | เสี่ยงต่อการไม่สามารถ  ใช้งานได้ปกติ | เสียงบประมาณในการ  ซ่อมแซมหรือจัดหา  ทดแทน | ปานกลาง  1x5=5 | 1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่  มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack  2. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้  ในบริเวณที่มีความเสี่ยง | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| 7. ความเสี่ยงจากการ  โจรกรรมอุปกรณ์  คอมพิวเตอร์แม่ข่าย หรือ  เครื่องลูกข่ายและอุปกรณ์  ต่อพ่วง |  |  |  |  |  |  |
| 7.1 เครื่องแม่ข่าย | เสี่ยงต่อการสูญหาย  ของอุปกรณ์ และ  ข้อมูลที่มีความสำคัญ | 1. เสียงบประมาณในการ  จัดหาเครื่องแม่ข่าย  ทดแทนที่มีมูลค่าสูง  2. เสียเวลาในการกู้ระบบ  3. เสียภาพลักษณ์ของ  นักงานฯ | ปานกลาง  1x5=5 | 1. ติดตั้งระบบรักษาความปลอดภัยในการ  ควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย  2. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย  (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array)  และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจ  ตลอดเวลา  3. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถ  เคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่  มิดชิดเมื่อไม่ได้ใช้งาน | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| 7.2 เครื่องลูกข่ายและ  อุปกรณ์ต่อพ่วง | เสี่ยงต่อการสูญหาย  ของอุปกรณ์ และ  ข้อมูลที่มีความสำคัญ | 1. เสียงบประมาณในการ  จัดหาอุปกรณ์ทดแทน  2. เสียภาพลักษณ์ของหน่วยงาน | ปานกลาง  1x5=5 | 1. ควบคุมการเข้าออกอาคาร  2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-  ออกอาคารตลอดเวลา  3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มี  เครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่ | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 8. ความเสี่ยงจากการโจมตี  เครื่องแม่ข่ายของ สนข.  ไม่ให้สามารถให้บริการได้  (Denial of Service-DoS) |  |  |  |  |  |  |
| 8.1 จากภายนอก | เสี่ยงต่อการถูกโจมตีได้  จากภายนอก โดย  โจมตีทั้งเครื่องแม่ข่าย  และ/หรือ เครือข่ายใน  ทุกรูปแบบ ซึ่งจะมีการ  พัฒนาวิธีการอยู่  ตลอดเวลา | ไม่สามารถใช้งานครือข่าย  ได้ หรือใช้ได้แต่ช้ามาก | ปานกลาง  1x5=5 | 1. ติดตั้งระบบป้องกัน และเตือนภัย Spam,  Virus, Malware, Trojan และมีเจ้าหน้าที่คอย  ดูแลตรวจสอบและอัพเดทฐานข้อมูลของ  อุปกรณ์นั้นๆ อยู่เป็นประจำเพื่อลดหรือสามารถ  แก้ไขได้ทันเมื่อถูกโจมตี  2. หมั่นตรวจสอบ Policy และ Log ของ  Firewall และ IPS/ IDS อย่างสม่ำเสมอ  3. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็น  ตามลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่  จะรับกับสถานการณ์ได้โดยไม่สับสน | 3 | สำนักส่งเสริมวิชาการและงานทะเบียน |
| 8.2 จากภายใน | เสี่ยงต่อการถูกโจมตี  จากโปรแกรมต่างๆ  โดยเฉพาะประเภท  Trojan ที่มีการติดตั้งที่  เครื่องลูกข่ายโดย  ผู้ใช้งานภายใน ทั้งที่  ไม่ได้ตั้งใจและตั้งใจ | ไม่สามารถใช้งานครือข่าย  ได้ หรือใช้ได้แต่ช้ามาก | ปานกลาง  1x5=5 | 1. มีมาตรการ และกฎระเบียบในการควบคุมมิ  ให้มีการติดตั้งโปรแกรมต่างๆ ลงบนเครื่องลูก  ข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ต  2. การควบคุมด้วยระบบ Desktop  Management | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศและสำนักส่งเสริมวิชาการและงานทะเบียน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| 9. ความเสี่ยงจากการใช้  Wireless เข้าเครือข่าย  อินทราเน็ต | เสี่ยงต่อผู้ที่ไม่มีสิทธิ์  เข้าถึงข้อมูลเข้าใช้  เครือข่าย อินทราเน็ต  ผ่านทาง WiFi | ข้อมูลที่เป็นความลับถูก  เผยแพร่หรือนำไปใช้ป อัน  จะนำมาซึ่งการขาดความ  เชื่อถือของหน่วยงาน | ปานกลาง  1x5=5 | 1. ควบคุมการเข้าใช้เครือข่าย  2. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดย  ติดตั้งระบบยืนยันตน (Authentication) | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ |
| 10. ความเสี่ยงจากการที่  เจ้าหน้าที่ใช้คอมพิวเตอร์/  เครือข่ายผิดวัตถุประสงค์ | 1. เสี่ยงต่อการใช้งาน  ในทางที่ผิด หรือเปล่า  ประโยชน์ เช่น การฟัง  วิทยุหรือดูโทรทัศน์  ออนไลน์ เป็นต้น  2. การใช้ Resource  ทำผิดกฎหมาย เช่น  การดาวน์โหลด  โปรแกรม ภาพยนตร์  หรือเพล | 1. สูญเสีย Bandwidth  ในเครือข่ายทำให้ ต้องจัด  เพิ่ม Bandwidth ให้มาก  ขึ้นทุกๆ ปี  2. อาจถูกร้องเรียนหรือ  ฟ้องร้องจาก  บุคคลภายนอก | ปานกลาง  2x2=4 | 1. บริหารจัดการด้วยข้อแนะนำ Ten Ways to  Protect Your Network From Insider  Threats เพื่อลดความเสี่ยง  2. กำหนด Policy ของFirewall ให้เหมาะสม  อย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น  3. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบ  ในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ  Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการ  บันทึกการใช้งานและรายงานการใช้งานของผู้ใช้  ที่ฝ่าฝืนต่อผู้บังคับบัญชา | 2 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศและสำนักส่งเสริมวิชาการและงานทะเบียน |
| ๑๑. ความเสี่ยงจากไฟ  กระชากจากสายพ่วง  (Extension Cord) | เสี่ยงต่อไฟไหม้ ไฟดูด  ไฟย้อนกลับ ทำให้  อุปกรณ์เครื่อง  คอมพิวเตอร์เสียหาย  ทั้งหมดได้ | 1. ไม่สามารถใช้งาน  เครื่องคอมพิวเตอร์ได้  ตามปกติ  2. ไฟอาจลัดวงจรทำให้  เครื่องเสียหาย | ปานกลาง  2x2=4 | 1. งดใช้สายพ่วง หรืองดใช้สายพ่วงที่ไม่ได้  มาตรฐาน ม.อ.ก. และไม่มีสายดิน  2. ไม่ใช้อุปกรณ์ที่ไม่มีสายดิน (ปลั๊ก ๒ ขา หรือ  ๓ ขาแต่หักสายดินออก) ต่อเข้ากับสายพ่วงหรือ  เต้าไฟฟ้า (Receptacle)  3. ต่อสายพ่วงเข้ากับอุปกรณ์ที่มีระบบ  Stabilizer | 2 | ทุกหน่วยงาน |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ความเสี่ยง** | **ปัจจัยเสี่ยง** | **ผลกระทบ** | **ระดับความเสี่ยง** | **แนวทางการควบคุม** | **ประเภทความเสี่ยง** | **ผู้รับผิดชอบ** |
| **ความเสี่ยงต่ำ** |  |  |  |  |  |  |
| 1. ความเสี่ยงจากวินาศ  ภัย/การก่อการร้าย | การสูญหายและถูก  ทำลายของอุปกรณ์  และข้อมูลที่เป็นส่วน  สำคัญขององค์กร | ไม่สามารถใช้ระบบงาน  หรือข้อมูลได้เป็นปกติ | ต่ำ  1x3=3 | 1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน  2. จัดทำแผนสำรองฉุกเฉิน  3. จัดทำศูนย์สำรอง (Backup Site) | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ |
| 2. ความเสี่ยงจากความชื้น  อุณหภูมิ | เครื่องมีประสิทธิภาพ  และความเชื่อถือได้  ลดลง และเครื่องอาจ  หยุดทำงานได้ | อายุของเครื่องและ  อุปกรณ์สั้นลง | ต่ำ  2x1=2 | จัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุม  ได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่  เหมาะสมและสามารถทำงานสลับกันได้ | 3 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ |
| 3. ความเสี่ยงจาก  แผ่นดินไหว | ความเสียหายด้าน  โครงสร้างอาจทำลาย  ระบบเครื่องและข้อมูล | ไม่สามารถใช้ระบบงาน  หรือข้อมูลได้เป็น  ปกติ | ต่ำ  1x1=1 | 1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน  2. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามี  ขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทน  จากที่ใด เพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง  3. จัดทำศูนย์สำรอง (Backup Site) | 1 | สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และ สำนักส่งเสริมวิชาการและงานทะเบียน |
| 4. ความเสี่ยงจากการ  โจรกรรมฐานข้อมูล | ข้อมูลที่สำคัญรั่วไหลสู่  ภายนอกหรือ  สาธารณะ | 1. เสียชื่อเสียงและความ  น่าเชื่อถือที่มีต่อ สนข.  2. การสูญหายหรือถูก  ทำลายของข้อมูล | ต่ำ  1x1=1 | 1. มีการบริหารจัดการด้านการป้องกันข้อมูล  2. มีการบริหารจัดการด้านการเข้าถึงข้อมูล  (Access)  3. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard Disk ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่าง ถาวรหรือได้ทำลายอุปกรณ์ หรือสื่อเก็บข้อมูล นั้นๆ ทิ้งแล้ว หากทำได้ |  |  |

**3.5 แผนปฏิบัติการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สำนักส่งเสริมวิชาการและงานทะเบียน พ.ศ. 2564**

**ผู้รับผิดชอบหลัก:** สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

**วัตถุประสงค์ :** เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สำนักส่งเสริมวิชาการและงานทะเบียน

บรรลุเป้าประสงค์ของการบริหารจัดการความเสี่ยง

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ประเภทความเสี่ยง/กิจกรรม** | **แผนปฏิบัติการ** | เริ่มต้น/สิ้นสุด | **ปี พ.ศ. 2563** | | | **ปี พ.ศ. 2564** | | | | | | | | | ผลลัพธ์/  ความก้าวหน้า |
| ต.ค. | พ.ย. | ธ.ค. | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. |
| 1. ความเสี่ยงจากการเกิดอัคคีภัย | - ตรวจสอบความพร้อม  ของการใช้งานอุปกรณ์  ดับเพลิง | ทุกวันที่ 30  ก.ย. ของทุกปี  30 ก.ย. 64 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2. ความเสี่ยงจากการเกิดระบบ  กระแสไฟฟ้าขัดข้อง | - ตรวจสอบระบบสำรอง  ไฟฟ้า (UPS) | - ทุกวันที่ 30  ก.ย. ของทุกปี  30 ก.ย. 64 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3. ความเสี่ยงจากการระบบ  คอมพิวเตอร์แม่ข่ายหลักเสียหาย | - ตรวจสอบระบบ  คอมพิวเตอร์แม่ข่าย | - ทุก 3 เดือน |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4. ความเสี่ยงจากการไม่ทำการสำรอง  ข้อมูล หรือทำการสำรองข้อมูลแต่  ขาดการอัพเดท | - จัดทำการสำรองข้อมูล  แบบอัตโนมัติ  - จัดทำการสำรองข้อมูล  แบบไม่อัตโนมัติทดสอบ  การกู้คืน | - ทุกวัน/ทุก  สัปดาห์ (Full)  - ทุก 3 เดือน |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ประเภทความเสี่ยง/กิจกรรม** | **แผนปฏิบัติการ** | เริ่มต้น/สิ้นสุด | **ปี พ.ศ. 2563** | | | **ปี พ.ศ. 2564** | | | | | | | | | ผลลัพธ์/  ความก้าวหน้า |
| ต.ค. | พ.ย. | ธ.ค. | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. |
| 5. ความเสี่ยงจากการเชื่อมต่อระบบ  ครือข่ายอินเทอร์เน็ต และ  อินทราเน็ตขัดข้อง | - ตรวจสอบระบบ  เครือข่ายสื่อสารหลัก | - ทุก 3 เดือน |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6. ความเสี่ยงจากการบุกรุกโจมตีจาก  ภายนอก | - ตรวจสอบ Policy และ  Log ของระบบป้องกันการ  บุกรุกระบบเครือข่าย | - ทุกวันที่ 1  และ 16 ของ  ทุกเดือน |  |  |  |  |  |  |  |  |  |  |  |  |  |

# บทที่ 4

# สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล

ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดคาม

เสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญให้ช่วยเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยี

สารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กรทุก

กิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูล

มหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่กับการปฏิบัติงานของทุก

หน่วยงานภายในมหาวิทยาลัยราชภัฏสกลนคร

ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วง

ละเมิด ถูกทำให้เสียหายหรือเสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดย

เจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ไขปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองคืกรให้

ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการวามเสี่ยงในองค์กรนั่นเอง

## 4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จาก

การกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด 6 อันดับแรก ได้ข้อสรุป ดังนี้

**4.1.1 ความเสี่ยงจากการเกิดอัคคีภัย** มีแนวทางปฏิบัติดังนี้

- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง

- ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง

- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

**4.1.2 ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง** มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบสำรองไฟฟ้า (UPS)

- วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับ สนข.

**4.1.3 ความเสี่ยงจากการระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย** มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักและสำรองฐานข้อมูล

- การจัดตั้งศูนย์สำรองข้อมูล (Backup Site)

**4.1.4 ความเสี่ยงไม่ทำการสำรองข้อมูล หรือสำรองข้อมูลแต่ขาดการอัพเดท** มีแนวทางปฏิบัติดังนี้

- มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ

- มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

**4.1.5 ความเสี่ยงการเชื่อมต่อระบบครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง** มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบเครือข่ายสื่อสารหลัก

- การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า 1 ทาง

- การจัดหา Bandwidth Management เพื่อควบคุมการใช้งานเครือข่ายให้มีประสิทธิภาพ

เพื่อให้การใช้งานระบบงานของสำนักงานฯ ได้รับ Bandwidth สูงกว่าการใช้งานด้านอื่นๆ

**4.1.6 ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก** มีแนวทางปฏิบัติดังนี้

- ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย

- จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ

- ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย

## 4.2 สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

**4.2.1** เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

**4.2.2** เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มี

เสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

**4.2.3** ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

**4.3 ข้อเสนอแนะ**

**4.3.1** การควบคุมคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการ

ความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคน

ที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

4.3.1.1 พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

4.3.1.2 พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

4.3.1.3 กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

**4.3.2** การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความ

เหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอ

เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตาม

การดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่าง

มีประสิทธิภาพ