แผนบริหารความเสี่ยง ด้านความปลอดภัยของระบบ เทคโนโลยีดิจิทัล

SECURITY RISK MANAGEMENT OF DIGITAL TECHNOLOGY SYSTEMS

ประจำปีงบประมาณ 2567

trat.peo@sueksa.go.th

trtpeo.moe.go.th

039-510742

จัดทำโดย
กลุ่มนโยบายและแผน
สำนักงานศึกษาธิการจังหวัดตราด
สำนักงานปลัดกระทรวงศึกษาธิการ

คำนำ

แผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ของสำนักงานศึกษาธิการจังหวัดตราด ประจำปีงบประมาณ พ.ศ. 2567 จัดทำขึ้น เพื่อเป็นกรอบแนวทางการปฏิบัติงานในการดำเนินงานการบริหารความเสี่ยง ให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพและมีประสิทธิผลทั่วทั้งองค์กร รวมทั้งเพื่อให้ผู้บริหารและบุคลากรของสำนักงานศึกษาธิการจังหวัดตราด มีความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล และสามารถนำไปปฏิบัติได้อย่างมีประสิทธิผลต่อเนื่อง และเกิดการพัฒนาระบบข้อมูลสารสนเทศและเครือข่ายเทคโนโลยี ผู้จัดทำหวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัลฉบับนี้ จะเป็นประโยชน์ต่อผู้บริหาร และบุคลากรในการปฏิบัติงานต่อไป

กลุ่มนโยบายและแผน
สำนักงานศึกษาธิการจังหวัดตราด
เมษายน 2567

สารบัญ

	หน้า
คำนำ	ก
สารบัญ	ข
บทที่ 1 บทนำ	**1**
หลักการและเหตุผล	1
วัตถุประสงค์	1
เป้าหมาย	1
ขอบเขตการดำเนินงาน	2
ประโยชน์ของการบริหารความเสี่ยง	2
สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ	2
ความหมายและคำจำกัดความเกี่ยวกับการบริหารความเสี่ยง	2
บทที่ 2 การบริหารจัดการความเสี่ยง	**4**
กระบวนการบริหารจัดการความเสี่ยง	4
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	8
การตอบสนองความเสี่ยง	9
ปัจจัยเสี่ยง	10
การประเมินความเสียหาย	11
การติดตามและรายงานผล	11
ระบบรักษาความปลอดภัยบนเครือข่าย	11
บทที่ 3 แผนบริการความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล	**12**
การระบุรายละเอียดของความเสี่ยง	12
วิเคราะห์วัดระดับความเสี่ยง	13
จัดทำแผนภูมิความเสี่ยง	15
รายงานผลการวิเคราะห์ความเสี่ยง	15
การจัดการความเสี่ยง	17
บทที่ 4 แผนป้องกัน/การรับมือความเสี่ยงของระบบเทคโนโลยีดิจิทัล	**19**
แผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล	19
แผนการติดตาม และประเมินผล	20
ภาคผนวก	
บันทึกข้อความแต่งตั้งคณะกรรมการบริหารความเสี่ยงฯ	22
คำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล	23
บันทึกข้อความแผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล	25

บทที่ 1
บทนำ

1. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานขององค์กร ล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์

2.1 เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักงานศึกษาธิการจังหวัดตราด

2.2 เพื่อเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3.เป้าหมาย

3.1 ผู้บริหารและบุคลากร สามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3.2 สามารถนำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศไปใช้ในการบริหารงานที่รับผิดชอบ

4. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของสำนักงานศึกษาธิการจังหวัดตราด โดยใช้หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสมตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission)

5. ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะช่วยผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจ ได้ดียิ่งขึ้น และทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1. เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี
2. สร้างฐานข้อมูลความรู้ที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร
3. ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด
4. เป็นเครื่องมือที่สำคัญในการบริหารงาน
5. ช่วยให้การพัฒนาองค์กรด้านเทคโนโลยีสารสนเทศเป็นไปในทิศทางเดียวกัน
6. ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

6. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

6.1 ระบบเทคโนโลยีสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ระบบข้อมูลสารสนเทศ, เว็บไซต์สำนักงานศึกษาธิการจังหวัดตราด และระบบสำนักงานอิเล็กทรอนิกส์ (E-Office) เป็นต้น

6.2 ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายมีสาย ภายใน (LAN) ระบบเครือข่ายไร้สายภายใน (WiFi)

6.3 อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC), เครื่องคอมพิวเตอร์ชนิดพกพา(Note Book), เครื่องสแกนเนอร์ (Scanner), เครื่องพิมพ์เลเซอร์ (Laser Printer), เครื่องพิมพ์แบบพ่นหมึก (Inkjet Printer), อุปกรณ์สำรองไฟฟ้าสำหรับ คอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB), อุปกรณ์กระจายสัญญาณ เครือข่ายชนิดไร้สาย (Wireless Access Point)

6.4 ระบบรักษาความปลอดภัย เช่น โปรแกรมตรวจสอบและป้องกันไวรัส (Antivirus Software)

7. ความหมายและคำจำกัดความเกี่ยวกับการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงานการเงิน และการบริการซึ่ง อาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไมทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

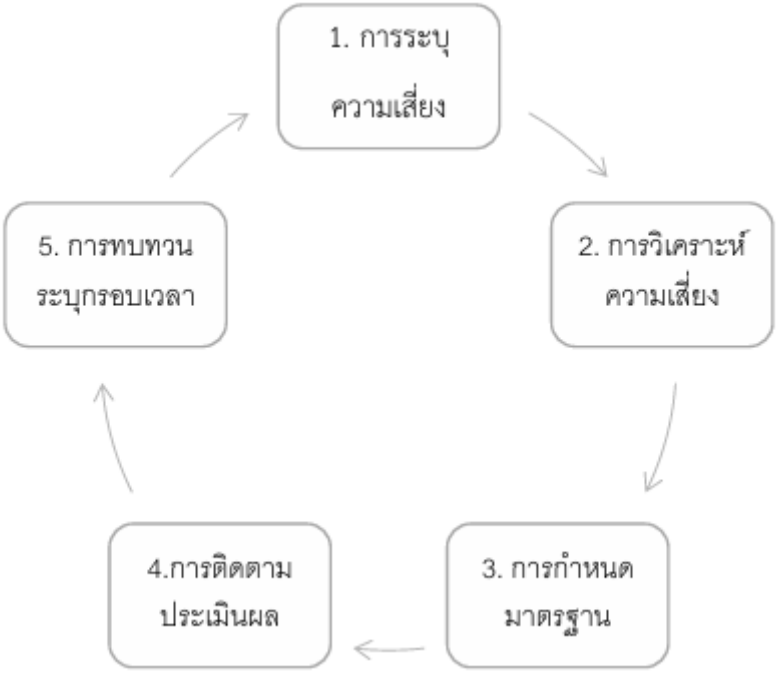
การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

บทที่ 2
การบริหารจัดการความเสี่ยง

1. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง และการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้



1.1 การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องในโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ

เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

1.2 การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

1.2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจ กำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

1.2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการ ควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

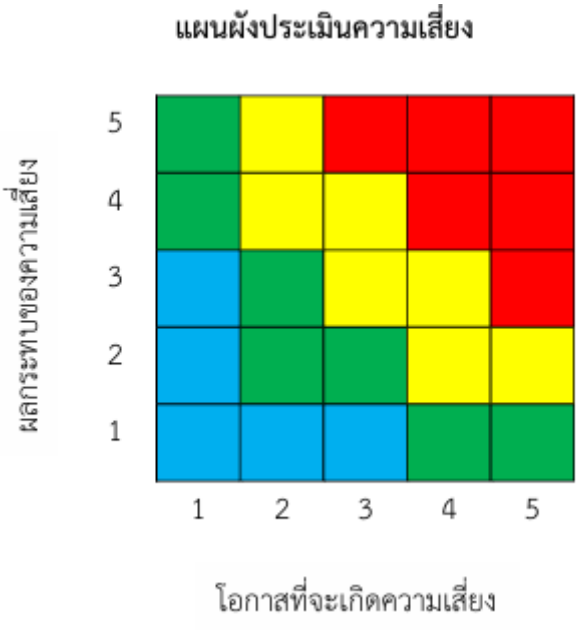
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
1	น้อยมาก
2	น้อย
3	ปานกลาง
4	สูง
5	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงปริมาณ	เชิงคุณภาพ
1	น้อยมาก	ไม่เกิน 1 ครั้งต่อปี	มีโอกาสเกิดในกรณียกเว้น
2	น้อย	2 ครั้งต่อปี	มีโอกาสเกิดแต่นานๆครั้ง
3	ปานกลาง	3 ครั้งต่อปี	มีโอกาสเกิดบางครั้ง
4	สูง	4 ครั้งต่อปี	มีโอการเกิดค่อนข้างสูงหรือบ่อยครั้ง
5	สูงมาก	มากกว่า 4 ครั้งต่อปี	มีโอกาสเกิดเกือบทุกครั้ง

1.2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปต่อไปนี้



สีแดง หมายถึง ระดับความเสี่ยงสูง ค่าระหว่าง 15 - 25

สีเหลือง หมายถึง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8 - 14

สีเขียว หมายถึง ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4 - 7

สีฟ้า หมายถึง ระดับความเสี่ยงต่ำ ค่าระหว่าง 1 – 3

1.2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยง ที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทาแผนการบริหารความเสี่ยงเป็นลำดับแรก

1.3 การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

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

1.3.1 ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยง และข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

1.3.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

1.3.3 การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิด ความสำเร็จตามวัตถุประสงค์

1.3.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

1.4 การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยง มีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยง ที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสม โดยพิจารณาจาก

1.4.1 พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

1.4.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

1.4.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

1.4.4 ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร โดยเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

1.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดาเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

2. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) แบ่งออกเป็น 8 ประเภท ดังนี้

2.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2.2 ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

2.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

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

2.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

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

2.5 ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษา ความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็น ปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูล และคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบเทคโนโลยีสารสนเทศ

2.6 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

2.7 ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

2.8 ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

3. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยง ที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ

จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยง มีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธี รวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

3.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรม ความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรม ความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

3.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

3.3 การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทางานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสียเป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียโดยการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

3.4 การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

4. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงานศึกษาธิการจังหวัดตราด ได้แก่

4.1 ปัจจัยภายนอก ได้แก่

4.1.1 ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของสำนักงาน ได้แก่ ไฟไหม้ ภัยพิบัติ

4.1.2 การขโมยอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

4.1.3 การชำรุดเสียหายของอุปกรณ์คอมพิวเตอร์

4.1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

4.1.5 ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

4.1.6 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดย ไม่ได้รับอนุญาต

4.2 ปัจจัยภายใน ได้แก่

4.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

4.2.2 การถูกไวรัสโจมตี (Virus) ทำลายข้อมูลสำคัญ และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

4.2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

5. การประเมินความเสียหาย

5.1 ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลเสียหาย และระบบฐานข้อมูลหลักถูกทำให้เสียหายจากไวรัส

5.2 ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

6. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

7. ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานศึกษาธิการจังหวัดตราด ได้รับการปรังปรุง และบำรุงรักษาเป็นประจำ เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่ายขององค์กร เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยมีการติดตั้งระบบอยู่ภายในอาคารสำนักงานศึกษาธิการจังหวัดตราด ซึ่งมีการปิดล็อคและกำหนดสิทธิ การเข้าถึงระบบ

บทที่ 3
แผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล

สำนักงานศึกษาธิการจังหวัดตราด ได้สรุปประเด็นวิเคราะห์และระบุความเสี่ยงเพื่อกำหนดแผนการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ประจำปีงบประมาณ พ.ศ. 2567 ดังนี้

1. การระบุรายละเอียดของความเสี่ยง (Description of risk) ซึ่งประกอบด้วย ลักษณะความเสี่ยง ปัจจัยเสี่ยง สิ่งคุกคาม ผู้ได้รับผลกระทบ และผลกระทบที่อาจจะเกิดขึ้นกับองค์กรจากปัจจัยความเสี่ยงต่างๆ โดยแสดงรายละเอียดของความเสี่ยงตามตาราง ดังนี้

ความเสี่ยง	ประเภท	รายละเอียด
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านระบบข้อมูล	ลักษณะความเสี่ยง ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศเช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน ปัจจัยเสี่ยง/สิ่งคุกคาม การอำพรางหรือสวมรอยผู้ใช้ การเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ลักษณะความเสี่ยง การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ ปัจจัยเสี่ยง/สิ่งคุกคาม แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่ ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ
3. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์/ความเสี่ยงด้านระบบข้อมูล	ลักษณะความเสี่ยง การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม ปัจจัยเสี่ยง/สิ่งคุกคาม แฮ็คเกอร์ แคร็กเกอร์ การโจมตีการให้บริการ (denial of services/ DOS) การดักจับข้อมูล คำสั่งเจตนาร้าย ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ไวรัส/เวิร์ม ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
4. ความเสี่ยงจากการขาดแคลนบุคลากผู้ปฏิบัติงาน	ความเสี่ยงในด้านการบริหารจัดการ	ลักษณะความเสี่ยง การขาดแคลนบุคลากรด้านคอมพิวเตอร์และสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ ปัจจัยเสี่ยง/สิ่งคุกคาม นโยบายจากรัฐบาล/กระทรวง/กรม ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

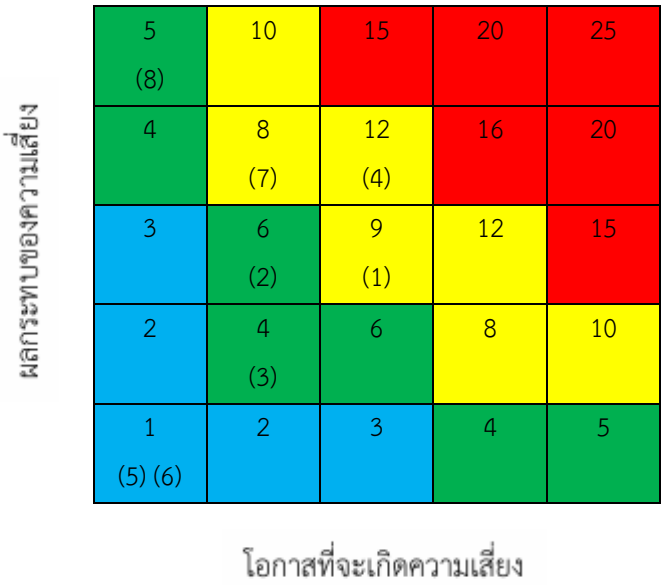
ความเสี่ยง	ประเภท	รายละเอียด
5. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านกลยุทธ์/ความเสี่ยงในด้านการบริหารจัดการ	ลักษณะความเสี่ยง การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหาจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ ปัจจัยเสี่ยง/สิ่งคุกคาม - ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
6. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง โรคระบาด	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	ลักษณะความเสี่ยง การเกิดสถานการณ์ความรุนแรง ความไม่สงบเรียบร้อย หรือโรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ ปัจจัยเสี่ยง/สิ่งคุกคาม การชุมนุมประท้วง การจลาจล การก่อการร้าย การระบาดของโรค ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ
7. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	ลักษณะความเสี่ยง เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนู หรือแมลง เป็นต้น ปัจจัยเสี่ยง/สิ่งคุกคาม ความล้มเหลวทางเทคนิค สัตว์กัดแทะประเภทหนู แมลง ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
8. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	ลักษณะความเสี่ยง การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้ ปัจจัยเสี่ยง/สิ่งคุกคาม การลักทรัพย์ ผู้ได้รับผลกระทบ/ผลกระทบ ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

2. วิเคราะห์วัดระดับความเสี่ยง จากโอกาสที่เกิดความเสี่ยงและผลกระทบจากความเสี่ยง เพื่อประเมินระดับความเสี่ยงจากการดำเนินงาน แสดงดังตารางต่อไปนี้

ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
1. **ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น**	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านระบบข้อมูล	**ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศเช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน**	3	3	9 (ค่อนข้างสูง)
2. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	2	3	6 (ค่อนข้างต่ำ)

ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	การประเมินความเสี่ยง		
			โอกาส	ผลกระทบ	ระดับความเสี่ยง
3. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์/ความเสี่ยงด้านระบบข้อมูล	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	1	4	4 (ค่อนข้างต่ำ)
4. ความเสี่ยงจากการขาดแคลนบุคลากร ผู้ปฏิบัติงาน	ความเสี่ยงในด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านคอมพิวเตอร์และสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	3	4	12 (ค่อนข้างสูง)
5. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านกลยุทธ์/ความเสี่ยงในด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหาจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	1	1	1 (ต่ำ)
6. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง โรคระบาด	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดสถานการณ์ความรุนแรง ความไม่สงบเรียบร้อย หรือโรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	1	1	1 (ต่ำ)
7. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนู หรือแมลง เป็นต้น	2	4	8 (ค่อนข้างสูง)
8. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	1	5	5 (ค่อนข้างต่ำ)

3. จัดทำแผนภูมิความเสี่ยง Risk Map โดยนำรหัสแต่ละประเด็นความเสี่ยงใส่ลงใน Risk Matrix เพื่อใช้วิเคราะห์ผลความเสี่ยง ดังนี้



สีแดง หมายถึง ระดับความเสี่ยงสูง ค่าระหว่าง 15 - 25

สีเหลือง หมายถึง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8 - 14

สีเขียว หมายถึง ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4 - 7

สีฟ้า หมายถึง ระดับความเสี่ยงต่ำ ค่าระหว่าง 1 – 3

ระดับความเสี่ยงที่ยอมรับได้ของสำนักงานศึกษาธิการจังหวัดตราดคือ ≤ 9

4. รายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) โดยนำผลการประเมินความเสี่ยงมาจัดลำดับความสำคัญของความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ ดังนี้

ลำดับ	ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	ระดับความเสี่ยง
1	4. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงในด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านคอมพิวเตอร์และสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	12 (ค่อนข้างสูง)
2	1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านระบบข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	9 (ค่อนข้างสูง)

ลำดับ	ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	ระดับความเสี่ยง
3	7. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนู หรือแมลง เป็นต้น	8 (ค่อนข้างสูง)
4	2. ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับแรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	6 (ค่อนข้างต่ำ)
5	8. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	5 (ค่อนข้างต่ำ)
6	3. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์/ความเสี่ยงด้านระบบข้อมูล	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	4 (ค่อนข้างต่ำ)
7	5. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านกลยุทธ์/ความเสี่ยงในด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหาจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	1 (ต่ำ)
8	6. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง โรคระบาด	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดสถานการณ์ความรุนแรง ความไม่สงบเรียบร้อย หรือโรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	1 (ต่ำ)

5. การจัดการความเสี่ยง โดยยึดตามหลัก 4T ทั้งนี้ ระดับความเสี่ยงที่ยอมรับได้ของสำนักงานศึกษาธิการจังหวัดตราดคือ ≤ 9 การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	ระดับความเสี่ยง	การจัดการความเสี่ยง
1	4. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงในด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านคอมพิวเตอร์และสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนา และควบคุมดูแลระบบ	12 (ค่อนข้างสูง)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
2	1. **ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น**	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านระบบข้อมูล	**ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน**	9 (ค่อนข้างสูง)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
3	7. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนู หรือแมลง เป็นต้น	8 (ค่อนข้างสูง)	ยอมรับความเสี่ยง
4	2. ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับแรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	6 (ค่อนข้างต่ำ)	ยอมรับความเสี่ยง
5	8. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านอุปกรณ์เทคโนโลยีฯ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	5 (ค่อนข้างต่ำ)	ยอมรับความเสี่ยง
6	3. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านบุคลากร/ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์/ความเสี่ยงด้านระบบข้อมูล	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	4 (ค่อนข้างต่ำ)	ยอมรับความเสี่ยง
7	5. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านกลยุทธ์/ความเสี่ยงในด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหาจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	1 (ต่ำ)	ยอมรับความเสี่ยง

ลำดับ	ความเสี่ยง	ประเภท	ลักษณะความเสี่ยง	ระดับความเสี่ยง	การจัดการความเสี่ยง
8	6. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง โรคระบาด	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดสถานการณ์ความรุนแรง ความไม่สงบเรียบร้อย หรือโรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	1 (ต่ำ)	ยอมรับความเสี่ยง

บทที่ 4

แผนป้องกัน/การรับมือความเสี่ยงของระบบเทคโนโลยีดิจิทัล

1. แผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ของสำนักงานศึกษาธิการจังหวัดตราด ประจำปีงบประมาณ พ.ศ. 2567

ลำดับ	ความเสี่ยง	**แผนบริหารจัดการความเสี่ยง**ด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล		
		แนวทางการป้องกัน/แก้ไข/ลดผลกระทบความเสี่ยง	กลุ่ม/หน่วย ที่รับผิดชอบ	ระยะเวลา ดำเนินการ
1	4. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	1) เร่งสรรหาบุคลากรผู้มาปฏิบัติงานด้านเทคโนโลยีเพื่อรองรับงานอย่างเหมาะสม	กลุ่มบริหารงานบุคคล	ต.ค.66 - ก.ย.67
2	1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	1) สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล	กลุ่มนโยบายและแผน	ต.ค.66 - ก.ย.67
		2) เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ		
3	7. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	1) หาทางป้องกันสัตว์กัดแทะอุปกรณ์	กลุ่มอำนวยการ	ต.ค.66 - ก.ย.67
		2) จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้		
		3) จัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ในสำนักงานอย่างสม่ำเสมอ		
4	2. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับแรงดันไฟฟ้าไม่คงที่	1) จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่	กลุ่มอำนวยการ	ต.ค.66 - ก.ย.67
5	8. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	1) ตรวจสอบการเข้าออกของบุคคลภายนอก	**กลุ่มลูกเสือ ยุวกาชาด และกิจการนักเรียน**	ต.ค.66 - ก.ย.67
		2) ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ		
		3) ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง		

ลำดับ	ความเสี่ยง	แผนบริหารจัดการความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล		
		แนวทางการป้องกัน/แก้ไข/ลดผลกระทบความเสี่ยง	กลุ่ม/หน่วย ที่รับผิดชอบ	ระยะเวลา ดำเนินการ
6	3. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	1) ตรวจสอบการตั้งค่าของ firewall ของ Server อย่างสม่ำเสมอ	กลุ่มนโยบายและแผน	ต.ค.66 - ก.ย.67
		2) ติดตั้งโปรแกรมป้องกันไวรัส และ patch ของระบบปฏิบัติการอย่างสม่ำเสมอ		
		3) เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ		
		4) สำรองข้อมูลไว้ในระบบคลาวน์ เช่น google drive		

2. แผนการติดตาม และประเมินผล การบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัลของสำนักงานศึกษาธิการจังหวัดตราด ซึ่งได้กำหนดปฏิทินการดำเนินการ ดังนี้

ลำดับที่	กิจกรรมการดำเนินการ	แผนการดำเนินงานในรอบปีงบประมาณ											
		ปี 2566			ปี 2567								
		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	กำหนดนโยบาย แนวทางการดำเนินงาน และเป้าหมายการบริหารความเสี่ยง	■											
2	ระบุและวิเคราะห์ความเสี่ยง และจัดลำดับความสำคัญของปัจจัยเสี่ยง		■										
3	ประเมินระดับความเสี่ยงและจัดลำดับความสำคัญของความเสี่ยง			■									
4	จัดทำแผนการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล			■									
5	ติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยง เพื่อระบุปัญหา อุปสรรค และกำหนดแนวทางแก้ไข				■	■	■	■	■	■	■	■	■

ภาคผนวก

บันทึกข้อความ

ส่วนราชการ สำนักงานศึกษาธิการจังหวัดตราด กลุ่มนโยบายและแผน : โทร ๐ ๓๙๕๑ ๐๗๔๒
ที่ ศธ ๐๒๗๑/ **วันที่** ๒ พฤษภาคม ๒๕๖๗

เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล

เรียน ศึกษาธิการจังหวัดตราด

ต้นเรื่อง

ตามที่ กลุ่มนโยบายและแผนได้รับมอบหมายให้จัดทำคำรับรองการปฏิบัติราชการ ตามข้อ ๔.๔ ความสำเร็จในการวิเคราะห์ความเสี่ยง การป้องกันการโจมตีทางไซเบอร์และการเตรียมความพร้อมต่อภัยพิบัติและภาวะฉุกเฉิน ที่มีประสิทธิผล ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ แล้ว นั้น

ข้อเท็จจริง

กลุ่มนโยบายและแผน ได้พิจารณารายละเอียดเกี่ยวกับประเด็นตัวชี้วัดความสำเร็จในการวิเคราะห์ความเสี่ยง การป้องกันการโจมตีทางไซเบอร์และการเตรียมความพร้อมต่อภัยพิบัติและภาวะฉุกเฉิน ที่มีประสิทธิผล ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ แล้ว สิ่งที่ต้องดำเนินการเพื่อให้ตัวชี้วัดบรรลุเป้าหมาย คือ จะต้องมีแผนบริหารความเสี่ยงของระบบเทคโนโลยีดิจิทัล และแผนป้องกัน/การรับมือระบบฐานข้อมูลของหน่วยงาน

ข้อเสนอ / ข้อพิจารณา

เพื่อให้การดำเนินการดังกล่าวเป็นไปด้วยความเรียบร้อย เห็นควรจัดทำคำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล รายละเอียดดังแนบ

จึงเรียนมาเพื่อโปรดพิจารณา

(นายสิรวิชญ์ ธนสุวรรณธาร)
พนักงานจ้างปฏิบัติงานวิชาการคอมพิวเตอร์

(นางสาวพัชราภรณ์ ภานุเพ็ญ)
นักวิชาการตรวจสอบภายในชำนาญการ ปฏิบัติหน้าที่
ผู้อำนวยการกลุ่มนโยบายและแผน

- จัดทำคำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยง ฯ
- ดำเนินการแล้ว.

(นางสาวณันทิชาภา ทองหนุ่ม)
รองศึกษาธิการจังหวัด รักษาการในตำแหน่ง
ศึกษาธิการจังหวัดตราด

คำสั่งสำนักงานศึกษาธิการจังหวัดตราด
ที่ ๔๐ / ๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล

เพื่อให้การดำเนินการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล เป็นไปด้วยความเรียบร้อย บรรลุวัตถุประสงค์ของการบริหารความเสี่ยง และสอดคล้องกับคำรับรองปฏิบัติราชการของสำนักงานปลัดกระทรวงศึกษาธิการ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ สำนักงานศึกษาธิการจังหวัดตราด จึงขอแต่งตั้งคณะกรรมการดำเนินการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ดังนี้

คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ประกอบด้วย

๑. นางสาวณันทิชาภา ทองหนุ่ม	รองศึกษาธิการจังหวัดตราด	ประธานกรรมการ
๒. นางสาววันทนา อิ่มอุไร	นักวิชาการศึกษาชำนาญการ ปฏิบัติหน้าที่ผู้อำนวยการกลุ่มอำนวยการ	กรรมการ
๓. นางสาวประเสริฐพร นวพันธุ์	นักทรัพยากรบุคคลชำนาญการ ปฏิบัติหน้าที่ผู้อำนวยการกลุ่มบริหารงานบุคคล	กรรมการ
๔. นางสาววรัทยา กลมมน	ผู้อำนวยการกลุ่มพัฒนาการศึกษา	กรรมการ
๕. นางอัชญา ศรีนาราง	ผู้อำนวยการกลุ่มนิเทศ ติดตาม และประเมินผล	กรรมการ
๖. นางพัชรี คงชาตรี	ผู้อำนวยการกลุ่มส่งเสริม การศึกษาเอกชน	กรรมการ
๗. นายสุรชัย วิรัติสกุล	ผู้อำนวยการกลุ่มลูกเสือ ยุวกาชาด และกิจการนักเรียน	กรรมการ
๘. นางสาวพัชราภรณ์ ภานุเพ็ญ	นักวิชาการตรวจสอบภายในชำนาญการ ปฏิบัติหน้าที่ ผู้อำนวยการหน่วยตรวจสอบภายใน และปฏิบัติหน้าที่ผู้อำนวยการกลุ่มนโยบายและแผน	กรรมการและเลขานุการ
๙. นายสิรวิชญ์ ธนสุวรรณธาร	พนักงานจ้างปฏิบัติงาน วิชาการคอมพิวเตอร์	ผู้ช่วยเลขานุการ

มีหน้าที่ กำหนดนโยบายและแผนการบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ส่งเสริมและสนับสนุนให้หน่วยงานภายในดำเนินการการบริหารความเสี่ยงตามนโยบายที่กำหนด พิจารณาและประเมินผลการบริหารความเสี่ยง ค้นหาวิธีการควบคุมความเสี่ยงที่เหมาะสม ติดตามและประเมินผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล

/ให้คณะกรรมการ...

ให้คณะกรรมการที่ได้รับการแต่งตั้งปฏิบัติหน้าที่ตามที่ได้รับมอบหมายด้วยความรับผิดชอบ ให้สำเร็จลุล่วงตามวัตถุประสงค์ และเกิดประโยชน์สูงสุดแก่ทางราชการ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒ พฤษภาคม พ.ศ. ๒๕๖๗

(นางสาวณันทิชาภา ทองหนุ่ม)
รองศึกษาธิการจังหวัด รักษาการในตำแหน่ง
ศึกษาธิการจังหวัดตราด

บันทึกข้อความ

ส่วนราชการ สำนักงานศึกษาธิการจังหวัดตราด กลุ่มนโยบายและแผน : โทร ๐ ๓๙๕๑ ๐๗๔๒
ที่ ศธ ๐๒๗๑/ **วันที่** ๗ พฤษภาคม ๒๕๖๗

เรื่อง แผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

เรียน ศึกษาธิการจังหวัดตราด

ต้นเรื่อง

ตามที่ กลุ่มนโยบายและแผนได้แต่งตั้งคณะกรรมการเพื่อดำเนินการขับเคลื่อน รวมทั้งพิจารณารายละเอียดเกี่ยวกับประเด็นตัวชี้วัดความสำเร็จ ประเด็นที่ ๔.๔ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ สิ่งที่ต้องดำเนินการเพื่อให้ตัวชี้วัดบรรลุเป้าหมาย คือ จัดทำแผนบริหารความเสี่ยงของระบบเทคโนโลยีดิจิทัลและแผนป้องกัน/การรับมือระบบฐานข้อมูลของหน่วยงานแล้ว นั้น

ข้อเท็จจริง

กลุ่มนโยบายและแผน ได้ดำเนินการจัดประชุมคณะกรรมการเพื่อวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีดิจิทัล และดำเนินการจัดทำรูปเล่มแผนบริหารความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีดิจิทัล สำเร็จลุล่วงแล้ว พร้อมนำไปเผยแพร่ และดำเนินการตามแผนบริหารความเสี่ยงฯ แล้ว

ข้อเสนอ / ข้อพิจารณา

๑. เผยแพร่ขึ้นบนเว็บไซต์ของสำนักงานศึกษาธิการจังหวัดตราด
๒. แจ้งผู้รับผิดชอบดำเนินการตามแผนบริหารความเสี่ยงฯ

จึงเรียนมาเพื่อโปรดพิจารณา

(นายสิรวิชญ์ ธนสุวรรณธาร)
พนักงานจ้างปฏิบัติงานวิชาการคอมพิวเตอร์

(นางสาวพัชราภรณ์ ภานุเพ็ญ)
นักวิชาการตรวจสอบภายในชำนาญการ ปฏิบัติหน้าที่
ผู้อำนวยการกลุ่มนโยบายและแผน

- เผยแพร่บนเว็บไซต์ของสำนักงาน
- แจ้งผู้รับผิดชอบดำเนินการตามแผน บริหารความเสี่ยงฯ

(นางสาวณันทิชาภา ทองหนุ่ม)
รองศึกษาธิการจังหวัด รักษาการในตำแหน่ง

ที่ตั้ง : อาคาร Smart School โรงเรียนตราษตระการคุณ
ตำบลวังกระแจะ อำเภอเมืองตราด จังหวัดตราด 23000