****

**รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยง มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย**

**รอบ 12 เดือน (1 ต.ค. 66 – 30 ก.ย. 67)**

**ประจำปีงบประมาณ พ.ศ. 2567**

|  |  |  |
| --- | --- | --- |
| **สถานะความเสี่ยง** | **เกณฑ์การประเมิน** | **ระดับความเสี่ยง** |
| ระดับความเสี่ยงลดลง | ดำเนินการตามแนวทาง/มาตรการควบคุมความเสี่ยงครบถ้วนทุกข้อและประเมินระดับความเสี่ยงตามแผนบริหารความเสี่ยง ปีงบประมาณ พ.ศ. 2567 ดังนี้  ⮚โอกาสและผลกระทบลดลง  ⮚โอกาสหรือผลกระทบลดลง  ⮚ทั้งโอกาสและผลกระทบคงเดิมแต่มีมาตรการหรือกลยุทธ์ใหม่ที่ควบคุมโอกาสและผลกระทบไม่ให้สูงขึ้น นอกเหนือจากแนวทาง/มาตรการควบคุมที่ปรากฏในแผนบริหารความเสี่ยง |  |
| ระดับความเสี่ยงเท่าเดิม | ดำเนินการตามแนวทาง/มาตรการควบคุมความเสี่ยงไม่ครบถ้วนทุกข้อและประเมินระดับความเสี่ยงตามแผนบริหารความเสี่ยง ปีงบประมาณ พ.ศ. 2567 ดังนี้  ⮚โอกาสเกิดเท่าเดิม  ⮚ผลกระทบเท่าเดิม  ⮚ทั้งโอกาสและผลกระทบเท่าเดิม |
| ระดับความเสี่ยงสูงขึ้น | ดำเนินการตามแนวทาง/มาตรการควบคุมความเสี่ยงไม่ครบถ้วนทุกข้อหรือไม่ดำเนินการตามมาตรการควบคุมความเสี่ยงและประเมินระดับความเสี่ยงตามแผนบริหารความเสี่ยง ปีงบประมาณ พ.ศ. 2567 ดังนี้  ⮚โอกาสเกิดสูงขึ้น  ⮚ผลกระทบสูงขึ้น  ⮚ทั้งโอกาสและผลกระทบสูงขึ้น |

**เกณฑ์การประเมิน :**

หมายเหตุ : 1. เกณฑ์การประเมินใช้สำหรับประเมินแต่ละปัจจัยเสี่ยง

2. สถานะความเสี่ยงแต่ละระดับ ขึ้นอยู่กับโอกาสและผลกระทบ โดยประเมินจากระดับความเสี่ยง เช่น ระดับความเสี่ยงลดลง อาจเกิดจากโอกาสเท่าเดิม ผลกระทบลดลง เป็นต้น

**3. ด้านการบริหารจัดการองค์กรสมัยใหม่**

**ความเสี่ยง : 1. การบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย**

| **ปัจจัยเสี่ยง** | **แนวทาง/มาตรการควบคุมความเสี่ยง** | **เป้าหมาย**  **การบริหารความเสี่ยง** | **ตัวชี้วัดประเมินความเสี่ยงตามมาตรการ**  **KRI** | **ประเมินความเสี่ยง** | | | | | | **ผลการประเมินความเสี่ยง** | **ผลลัพธ์ หลังการจัดการความเสี่ยง** | **ผู้รับผิดชอบ/**  **กำหนดเสร็จ** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ก่อน** | | | **หลัง** | | |
| **โอกาส** | **ผลกระทบ** | **ระดับ ความเสี่ยง** | **โอกาส** | **ผลกระทบ** | **ระดับ ความเสี่ยง** |
| 1. ระบบป้องกันการบุกรุกไม่ทันสมัย | 1.1 จัดทำแผนเพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย | ข้อมูลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ไม่เกิดความเสียหาย | มีการตรวจพบหรือมีรายงานความเสียหาย มากกว่า 2 ครั้งต่อปี | 3 | 5 | 15  สูงมาก  ....... | 1 | 1 | 1  น้อยมาก | (ลดลง) | ลดลง | สำนักวิทยบริการฯ/กอง/สำนัก/คณะ/วิทยาลัย/  วิทยาเขต  30 กันยายน 2567  ผู้กำกับติดตาม  รองอธิการบดี |
| 1. ขาดการปรับปรุงระบบ ปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย | 2.1 จัดทำแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย |
| 3. ความถี่ในการตรวจสอบป้องกันการบุกรุกไม่เพียงพอ | 3.1 ดำเนินการตามแผนข้อ 1 และ 2 |
| 4. เครื่องคอมพิวเตอร์ แม่ข่ายมีประสิทธิภาพลดลง | 4.1 จัดทำระบบรายงานผลปรับปรุงระบบ ปฏิบัติการและระบบป้องกันการบุกรุก |

**แนวทางประเมินผล**

1. **ดำเนินการตามมาตรการควบคุมความเสี่ยง**

ชี้แจง : กรุณาทำเครื่องหมาย ✓ หน้าข้อที่หน่วยงานดำเนินการ

**🞎** ดำเนินการครบถ้วนทุกข้อ

🗹 ดำเนินการบางข้อ

**🞎** ไม่ดำเนินการ

1. **รายงานผลการดำเนินงานตามแนวทาง/มาตรการควบคุมความเสี่ยง**

ชี้แจง : กรุณารายงานผลการดำเนินงานให้สอดคล้องกับการประเมินในข้อที่ 1

**ความเสี่ยงด้านระบบเครือข่าย** หมายถึง ความเสี่ยงหรือภัยต่าง ๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กร ทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP โดยความเสี่ยงที่เป็นเป็นภัยคุกคามอาจจะเกิดได้จากหลายสาเหตุ เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบเครื่องคอมพิวเตอร์แม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย หรือความเสี่ยงจากภัยคุกคามอื่น ๆ ส่งผลกระทบระบบเครือข่ายด้วย **การบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย**

การบริหารจัดการความเสี่ยงด้านระบบเครือข่ายเป็นกระบวนการที่สำคัญในการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นกับระบบเครือข่ายขององค์กร กระบวนการนี้รวมถึงการระบุการประเมิน การจัดการ และการติดตามความเสี่ยงที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ เพื่อให้แน่ใจว่าข้อมูลและบริการต่างๆ ภายในองค์กรสามารถดำเนินการได้อย่างต่อเนื่องและปลอดภัย ในการบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีขั้นตอนดังนี้

การระบุความเสี่ยง คือ การระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบเครือข่าย ซึ่งรวมถึงภัยคุกคามจากภายนอก เช่น การโจมตีแบบไซเบอร์ และภัยคุกคามจากภายใน เช่น การกระทำผิดพลาดโดยผู้ปฏิบัติงานดูแลความมั่นคงปลอดภัยเครือข่าย

การประเมินความเสี่ยง คือ การประเมินความเสี่ยง และวิเคราะห์ความน่าจะเป็นของการเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

การกำหนดกลยุทธ์ในการจัดการความเสี่ยง คือ การเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสม รวมถึงการหลีกเลี่ยง การรับความเสี่ยง การลดความเสี่ยง หรือการโอนย้ายความเสี่ยง

การปรับปรุงและการบังคับใช้มาตรการความปลอดภัย คือ การดำเนินการเพื่อป้องกันและลดความเสี่ยง รวมถึงการปรับปรุงนโยบายความปลอดภัย การติดตั้งซอฟต์แวร์ป้องกันไวรัสและไฟร์วอลล์ การทำการฝึกอบรมเรื่องความปลอดภัยให้กับพนักงาน

การติดตามและการทบทวน คือ การจัดการความเสี่ยงเป็นกระบวนการที่ต่อเนื่อง จำเป็นต้องมีการติดตามและการทบทวนอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ามาตรการความปลอดภัยที่ได้วางไว้นั้นยังคงมีประสิทธิภาพและสามารถรับมือกับภัยคุกคามใหม่ๆ ได้

การบริหารจัดการความเสี่ยงด้านระบบเครือข่ายจึงป็นส่วนสำคัญที่ช่วยให้องค์กรสามารถประกันความต่อเนื่องของการดำเนินงานและป้องกันข้อมูลสำคัญจากการถูกโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต การดำเนินการตามขั้นตอนเหล่านี้อย่างเป็นระบบและต่อเนื่องจะช่วยลดความเสี่ยงต่อระบบเครือข่ายได้อย่างมีประสิทธิภาพ

**แนวทางการบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีการดำเนินการดังนี้**

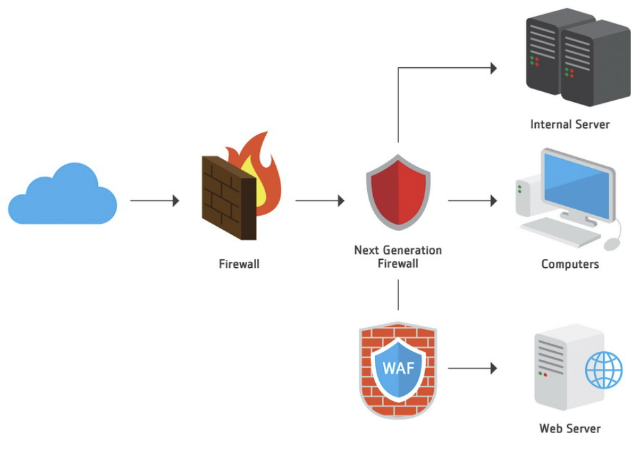
1. ลดความเสียหายที่เกิดจากระบบเครือข่าย ด้วยการเฝ้าระวังและตรวจสอบระบบเครือข่าย และการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่ายได้ การดำเนินการควรจัดให้มีระบบการติดตามและเฝ้าดูการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน **รวมทั้งการสร้าง Firewall เพื่อป้องกันการบุกรุกจากภายนอกให้มีความทันสมัย**

2. พัฒนาระบบงานด้านเครือข่าย ด้วยการพัฒนาบริหารควบคุม กำกับดูแล และบำรุงรักษา **ปรับปรุงระบบปฏิบัติการของคอมพิวเตอร์แม่ข่าย**และเครือข่ายสารสนเทศพื้นฐาน พัฒนาระบบการให้บริการเครือข่ายเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูลผ่านระบบเครือข่าย

3. เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณฐานข้อมูล และการเคลื่อนไหวของฐานข้อมูล

4. มีมาตราการสำหรับกระบวนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้ไม่สามารถเข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูล หรือ การทำงานของระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์แม่ข่ายในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่าย มีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส ไม่ให้เข้าถึงหรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์แม่ข่าย โดยมีเนื้อหารายละเอียดเกี่ยวกับแนว ทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย **โดยจัดทำแผนเพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย จัดทำแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์แม่ข่ายด้านความปลอดภัย** เป็นอย่างน้อย

**ปัจจัยเสี่ยงที่ 1 ระบบป้องกันการบุกรุกไม่ทันสมัย**



Firewall

**ปัจจุบัน** ความเสี่ยงด้านระบบเครือข่ายมีความเสี่ยงที่สูงขึ้น เนื่องจากผู้ไม่หวังดีมีจำนวนมาก มีพฤติกรรมในการโจมตีระบบเครือข่ายที่ไม่เจาะจงเป้าหมายทำให้ส่งผลกระทบต่อระบบเครือข่ายในวงกว้างหรือทั้งหมดที่เชื่อมต่อเข้าสู่โลกอินเทอร์เน็ต ทุกเครือข่ายจำเป็นต้องมีสร้างระบบป้องกันให้แข็งแกร่งมีความทันสมัย ทันต่อเทคโนโลยีในการโจมตี การมีอุปกรณ์ป้องกันการบุกรุก Firewall จึงเป็นสิ่งสำคัญซึ่งเป็นหน้าด่านแรกของระบบเครือข่ายขององค์กร ปัจจุบันอุปกรณ์มีอายุการใช้งานมากกว่า 5 ปี สำนักวิทยบริการและเทคโนโลยีได้ตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นจึงได้พยายามอัปเดตซอฟแวร์ที่เกี่ยวข้องให้มีความทันสมัยรองรับภัยที่จะตามมา และได้จัดทำแผนในการจัดซื้ออุปกรณ์ใหม่ พร้อมทั้งหมั่นตรวจสอบการบุกรุกโจมตีระบบเครือข่ายและดูแลเครื่องคอมพิวเตอร์แม่ข่ายให้มีความปลอดภัย รายละเอียดดังนี้

**มาตรการที่ 1** : จัดทำแผนเพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีการวางแผนการตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย โดยการเพิ่มความถี่ในการตรวจสอบจากเดิมวันละ 1 ครั้งเป็นวันละ 2 ครั้ง ทั้งช่วงเช้าและช่วงบ่าย มีการตรวจสอบการโจมตีเครือข่ายบนอุปกรณ์ป้องกัน Firewall และติดตามข่าวสารการรายงานผลการโจมตีระบบเครือข่าย ในช่วงเช้า เวลา 8.30-9.00 น. และช่วงบ่าย เวลา 16.00-16.30 น. นอกจากนั้นมีการติดตามตรวจสอบการแจ้งเตือนจากอีเมล์ รายละเอียดดังภาพที่ 1

รูปภาพประกอบด้วย ข้อความ, ไลน์, พล็อต, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

**ภาพที่ 1** แผนเพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย

**ปัจจัยเสี่ยงที่ 2 ขาดการปรับปรุงระบบ ปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย**

การปรับปรุงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย เป็นการบริหารจัดการความเสี่ยงด้านการ พัฒนาระบบงานด้านเครือข่าย อีกวิธีหนึ่งที่จะลดช่องโหว่ที่อาจจะเกิดขึ้น เพิ่มความมั่นคงปลอดภัยจากภัยคุกคามที่เล็ดลอดเข้ามาในระบบเครือข่ายสู่เครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นขุมทรัพย์แหล่งที่อยู่ของข้อมูลขององค์กรแต่ละองค์กร โดยมีการจัดทำแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย

**มาตรการที่ 1** : จัดทำแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้วางแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย โดยได้เพิ่มความถี่ในการตรวจสอบจากเดิมวันละ 1 ครั้งเป็นวัน 2 ครั้ง คือ ช่วงเช้า เวลา 8.30-9.00 น. และช่วงบ่าย เวลา 16.00.16.30 น. รายละเอียดดังภาพ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีการวางแผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย โดยการเพิ่มความถี่ในการตรวจสอบจากเดิมวันละ 1 ครั้งเป็นวันละ 2 ครั้ง ทั้งช่วงเช้าและช่วงบ่าย มีการตรวจสอบการใช้งานคอมพิวเตอร์แม่ข่ายด้านความปลอดภัย ในช่วงเช้า เวลา 8.30-9.00 น. และช่วงบ่าย เวลา 16.00-16.30 น. และตรวจสอบการปรับปรุงอัปเดทซอฟแวร์ทุกสัปดาห์ รายละเอียดดังภาพที่ 2

รูปภาพประกอบด้วย ข้อความ, ไลน์, พล็อต, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

**ภาพที่ 2** แผนตรวจสอบและบำรุงรักษาคอมพิวเตอร์แม่ข่ายด้านความปลอดภัย

**ปัจจัยเสี่ยงที่ 3. ความถี่ในการตรวจสอบป้องกันการบุกรุกไม่เพียงพอ**

**มาตรการที่ 1** : ดำเนินการตามแผนข้อ 1 และ 2

**ผลการดำเนินการตามแผนข้อ 1 (เพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย)**

รูปภาพประกอบด้วย ภาพหน้าจอ, ข้อความ, มีสีสรร, ออกแบบ

คำอธิบายที่สร้างโดยอัตโนมัติสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้มอบหมายให้เจ้าหน้าที่ที่มีความรู้ความสามารถทางด้านการรักษาความมั่นคงปลอดภัยทางเครือข่าย ในการตรวจสอบและเฝ้าระวังการบุกรุกโจมตีทางเครือข่าย โดยมีการตรวจสอบทุกวัน วันละ 2 ช่วงเวลาเป็นอย่างน้อย คือ ช่วงเช้า เวลา 8.30 – 9.00 น. ช่วงบ่ายเวลา 16.00 – 16.30 และช่วงที่มีการแจ้งเตือนผ่านสื่อสารสนเทศตามแผนเพิ่มความถี่การตรวจสอบการบุกรุกคอมพิวเตอร์แม่ขาย **จากระยะเวลาเดือนตุลาคม 2566 – มิถุนายน 2567 มีการโจมตี 2 ครั้ง** ช่วงเดือน มกราคม 2567 สามารถตรวจจับป้องกันได้ไม่พบความเสียหาย และในช่วงเดือน มิถุนายน 2567 สามารถตรวจจับป้องกันได้ไม่พบความเสียหาย แสดงผลการตรวจสอบได้ดังภาพที่ 3 รวมถึงการรายงานผลเพื่อให้ผู้บริหารและผู้ปฏิบัติงานเครือข่ายทราบ ดังภาพที่ 4 ตามลำดับ

**ภาพที่ 3** การรายงานผลการตรวจสอบการบุกรุกคอมพิวเตอร์แม่ข่าย

|  |  |
| --- | --- |
|  |  |
| (ก) ผลการดำเนินการ | (ข) ช่องทางการติดตามข่าวสารเรื่องความปลอดภัยทางเครือข่ายของผู้ปฏิบัติงาน |

**ภาพที่ 4** การรายงานผลเพื่อให้ผู้บริหารและผู้ปฏิบัติงานเครือข่ายทราบ

**ผลการดำเนินการตามแผนข้อ 2 (การตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย)**

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มอบหมายให้ผู้ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางเครือข่ายและระบบปฏิบัติการ ตรวจสอบความพร้อมในการใช้งานทุกวัน วันละ 2 ช่วงเวลาเป็นอย่างน้อย คือ ช่วงเช้า เวลา 8.30 – 9.00 น. ช่วงบ่ายเวลา 16.00 – 16.30 และช่วงที่มีการแจ้งเตือนผ่านสื่อสารสนเทศ พร้อมทั้งตรวจสอบการอัปเดตซอฟแวร์ที่เกี่ยวข้องทุกสัปดาห์ ช่วงระยะเวลาเดือนตุลาคม 2566 – มิถุนายน 2567 การปรับปรุงอัปเดตซอฟแวร์ จำนวน 4 ครั้ง และรายงานผลเพื่อให้ผู้บริหารและผู้ที่เกี่ยวข้อง ดังภาพที่ 5-6 ตามลำดับ

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ขนาน, ไลน์

คำอธิบายที่สร้างโดยอัตโนมัติ

**ภาพที่ 5** การตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย

|  |  |
| --- | --- |
|  | รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, หน้าเว็บ  คำอธิบายที่สร้างโดยอัตโนมัติ รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, จำนวน, ซอฟต์แวร์  คำอธิบายที่สร้างโดยอัตโนมัติ |
| (ก) ผลการดำเนินการ | (ข) ช่องทางการติดตามข่าวสารการอัปเดตซอฟแวร์ที่เกี่ยวข้อง |

**ภาพที่ 6** การตรวจสอบและบำรุงรักษาคอมพิวเตอร์ แม่ข่ายด้านความปลอดภัย

**ปัจจัยเสี่ยงที่ 4.** **เครื่องคอมพิวเตอร์แม่ข่ายมีประสิทธิภาพลดลง**

**มาตรการที่ 4** : จัดทำระบบรายงานผลปรับปรุงระบบปฏิบัติการและระบบป้องกันการบุกรุก (อยู่ระหว่างการดำเนินการ)

ดำเนินการจัดทำระบบรายงานผลการป้องกันโจมตี โดยสามารถเข้าระบบเพื่อตรวจสอบการรายงานผล ดังภาพที่ 7 ซึ่งระบบดังกล่าวมีวัตถุประสงค์ ในการรายงานผลการปรับปรุงระบบปฏิบัติการที่มีการอัปเดตหรือเปลี่ยนแปลง และรายงานสถานะการปรับปรุงและประสิทธิภาพของระบบป้องกันการบุกรุก ที่สามารถพิจารณาการปรับปรุงที่ทำ เช่น การอัปเดตซอฟต์แวร์ การติดตั้งแพทช์ และระบุผลกระทบที่อาจเกิดขึ้นจากการปรับปรุง เช่น การปรับปรุงที่อาจทำให้ระบบหยุดทำงานชั่วคราว และผลการทดสอบประสิทธิภาพของระบบป้องกันการบุกรุกหลังการปรับปรุง เช่น การตรวจพบการบุกรุก การป้องกันการโจมตี เพื่อจัดทำและรายงานข้อเสนอแนะสำหรับการปรับปรุงในครั้งถัดไป

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, ไอคอนคอมพิวเตอร์, หน้าเว็บ

คำอธิบายที่สร้างโดยอัตโนมัติ รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

**ภาพที่ 7** ระบบรายงานผลปรับปรุงระบบปฏิบัติการและระบบป้องกันการบุกรุก

1. **เป้าหมายการบริหารความเสี่ยง**

3.1 ข้อมูลระบบเครื่องคอมพิวเตอร์แม่ข่ายไม่เกิดความเสียหาย

ขณะนี้ข้อมูลของระบบสารสนเทศทั้งหมด ยังไม่เกิดความเสียหาย

1. **ประเมินระดับความเสี่ยงตามแผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ. 2567**

ชี้แจง : กรุณาทำเครื่องหมาย ✓ หน้าข้อที่ตรงกับหน่วยงานประเมิน

✓ โอกาสเกิดลดลง เนื่องจาก (โปรดระบุ) มีการอัปเดตและป้องกันการบุกรุกโจมตี พร้อมสำรองข้อมูล

✓ ผลกระทบลดลง เนื่องจาก (โปรดระบุ) มีความพยายามในการบุกรุก แต่สามารถตรวจจับป้องกันได้ไม่เกิดความเสียหายต่อข้อมูล

🞎 ทั้งโอกาสและผลกระทบคงเดิมแต่มีมาตรการหรือกลยุทธ์ใหม่ที่ควบคุมโอกาสและผลกระทบไม่ให้สูงขึ้น นอกเหนือจากมาตรการควบคุมที่ปรากฏในแผนบริหารความเสี่ยง

เนื่องจาก (โปรดระบุ)……………………………………………………………………………………………………………………………………………………………………………………………………………………….

🞎 โอกาสเกิดเท่าเดิม เนื่องจาก (โปรดระบุ)……………………………………………………………………………………………………………………………………………………………………………………………

🞎 ผลกระทบเท่าเดิม เนื่องจาก (โปรดระบุ)……………………………………………………………………………………………………………………………………………………………………………………………

🞎 ทั้งโอกาสและผลกระทบเท่าเดิม เนื่องจาก (โปรดระบุ)………………………………………………………………………………………………………………………………………………………………………..

🞎 โอกาสเกิดสูงขึ้น เนื่องจาก (โปรดระบุ)………………………………………………………………………………………………………………………………………………………………………………………………

🞎 ผลกระทบสูงขึ้น เนื่องจาก (โปรดระบุ)………………………………………………………………………………………………………………………………………………………………………………………………

🞎 ทั้งโอกาสและผลกระทบสูงขึ้น เนื่องจาก (โปรดระบุ)………………………………………………………………………………………………………………………………………………………………………….

1. **สรุปผลการประเมิน**

ชี้แจง : กรุณาสรุปผลการประเมินความเสี่ยง โดยทำเครื่องหมาย ✓ หน้าข้อที่ตรงกับการประเมิน และให้ระบุตัวเลขในช่องผลทั้ง โอกาส ผลกระทบ และประเมินระดับความเสี่ยง

✓ ระดับความเสี่ยงลดลง

🞎 ระดับความเสี่ยงเท่าเดิม

🞎 ระดับความเสี่ยงสูงขึ้น

**ประเด็นความเสี่ยง : 1. การบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย**

| **ความเสี่ยง** | **แผน/ผล** | **ประเมินความเสี่ยง** | | **ระดับความเสี่ยง** | |
| --- | --- | --- | --- | --- | --- |
| **โอกาส** | **ผลกระทบ** |
| 1. การบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย | แผน | 3 | 5 | 15  สูงมาก | **(ไม่เปลี่ยนแปลง/**  **ลดลง/เพิ่มขึ้น)** |
| ผล | 1 | 1 | น้อยมาก |

**โอกาส**

|  |  |  |
| --- | --- | --- |
| **ระดับ** | **โอกาสเกิด** | **ความหมาย** |
| 5 | สูงมาก | มีการตรวจพบหรือมีรายงานความเสียหาย มากกว่า 4 ครั้งต่อปี |
| 4 | สูง | มีการตรวจพบหรือมีรายงานความเสียหาย มากกว่า 3 ครั้งต่อปี |
| 3 | ปานกลาง | มีการตรวจพบหรือมีรายงานความเสียหาย มากกว่า 2 ครั้งต่อปี |
| 2 | น้อย | มีการตรวจพบหรือมีรายงานความเสียหาย มากกว่า 1 ครั้งต่อปี |
| 1 | น้อยมาก | ไม่มีรายงานแจ้งการบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย |

**ผลกระทบ**

|  |  |  |
| --- | --- | --- |
| **ระดับ** | **ผลกระทบ** | **ความหมาย** |
| 5 | สูงมาก | เกิดความเสียหายไม่สามารถกู้คืนระบบได้ |
| 4 | สูง | เกิดความเสียหายสามารถกู้คืนระบบได้แต่ไม่เป็นปัจจุบัน |
| 3 | ปานกลาง | เกิดความเสียหายสามารถกู้คืนระบบให้เป็นปัจจุบัน |
| 2 | น้อย | เกิดการบุกรุก ไม่สามารถตรวจจับได้แล้วระบบไม่เกิดความเสียหาย |
| 1 | น้อยมาก | เกิดความพยายามในการบุกรุก สามารถตรวจจับป้องกันได้ |

1. **ปัญหาและอุปสรรคในการดำเนินงาน**

ไม่มี