**แผนป้องกันภัยคุกคามทางระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2562**

**คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนสุนันทา**

**หลักการและเหตุผล**

ระบบเครือข่ายคอมพิวเตอร์ รวมถึงระบบข้อมูลสารสนเทศ ถือเป็นทรัพยากรที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาให้มีความถูกต้องและปลอดภัย เพื่อให้มั่นใจว่าระบบเครือข่ายคอมพิวเตอร์ และ ระบบข้อมูลสารสนเทศสามารถใช้ได้งานได้ตามปกติ ส่งเสริมสนับสนุนการปฏิบัติตามภารกิจของกรมควบคุมโรคได้ ศูนย์คอมพิวเตอร์ คณะวิทยาการจัดการได้ตระหนักถึงภัยคุกคามระบบสารสนเทศ ทั้งในรูปแบบไวรัสคอมพิวเตอร์ การโจมตีระบบ ศูนย์คอมพิวเตอร์ฯ จึงได้จัดทำแผนป้องกันภัยคุกคามทางระบบเทคโนโลยีสารสนเทศของคณะวิทยาการจัดการ เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาเมื่อเกิดภัยคุกคามทางระบบสารสนเทศ เพื่อให้ระบบสารสนเทศสามารถใช้งานได้ตามปกติหรือจำกัดความเสียหายให้น้อยที่สุด ตลอดจนการดูแลรักษาระบบสารสนเทศให้มีเสถียรภาพ พร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

**วัตถุประสงค์**

1. เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ
2. เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้การปฏิบัติราชการ ดำเนินไปได้อย่างมีเสถียรภาพ
4. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยด้านเทคโนโลยีสารสนเทศของคณะวิทยาการจัดการ

**ขั้นตอนวิธีและแนวทางปฏิบัติ**

1. การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางระบบสารสนเทศ

1.1 การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน รองคณบดีผู้ดูแลรับผิดชอบงานด้านระบบสาสนเทศของหน่วยงาน จะทำการแจ้งให้คณบดี หรือ ผู้มีอำนาจสูงสุดของหน่วยงานทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

1.2 กระบวนการดำเนินงาน (Procedure)

ศูนย์คอมพิวเตอร์จัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมข้อมูล หลักฐานเพื่อหาช่องโหว่ วิธีการที่

ถูกโจมตีหรือระบุตัวผู้โจมตี เพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างถูกต้อง ทันเวลา และสามารถป้องกันการโจมตีในลักษณะเดิม ระบบงานต่างๆ ที่มีความสำคัญต้องมีการสำรองข้อมูล เพื่อความ พร้อมในการกู้คือข้อมูลหากข้อมูลความเสียหายจากการถูกโจมตี

1.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อหรือให้คำปรึกษาทางด้านความมั่นคงทางระบบสารสนเทศกรณีที่มีความจำเป็นฉุกเฉิน เช่น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา, สำนักบริหารเทคโนโลยีสารสนเทศภาครัฐ, ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) เป็นต้น

1.4 การจัดเตรียมอุปกรณ์โครงสร้างพื้นฐานด้านระบบเครือข่ายคอมพิวเตอร์ (Computer Network Infrastructure Device)

การเตรียมพร้อมรับภัยคุกคามที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ คณะวิทยาการจัดการ ซึ่งเป็นฝ่ายงานที่มีหน้าที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีระบบคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- ชุดติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย
- เทปสำรองข้อมูลหรือฮาร์ดดิสก์แบบพกพา
- ชุดโปรแกรม antivirus
- อุปกรณ์สำรองไฟฟ้า
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์
- อุปกรณ์ระบบเครือข่าย
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์
- ชุดเครื่องมือแก้ไขปัญหาคอมพิวเตอร์และระบบเครือข่าย

1.5 การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับข้อมูลหรือระบบงาน จากภัยคุกคามระบบสารสนเทศ ให้สามารถกู้คืนข้อมูลที่เสียหายหรือถูกทำลายกลับมาได้ให้มากที่สุด ให้การดำเนินงานขององค์กรมีความต่อเนื่อง โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

1.6 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

1) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากกรณีจำเป็นให้มีเจ้าหน้าที่ของศูนย์คอมพิวเตอร์ เป็นผู้รับผิดชอบนำพาเข้าไป เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย

2) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลาและมีการ Monitor เป็นประจำ

3) มีการติดตั้งระบบบัญชีรายชื่อเพื่อควบคุมและอนุญาตเข้าใช้งานระบบเครือข่าย เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์

4) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

5) มีการทำระบบ Authentication โดยมีการ Login ชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย

6) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของ องค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

7) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

2. การเตรียมความพร้อมรบสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่ส่วนงานต่างๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

1) ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

2) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

3) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

3. กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

3.1 เจ้าหน้าที่ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้ความเสียหายแพร่กระจายในวงกว้าง โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบ ประกอบด้วย

นายสิริธนธราธร จิรทีปต์ธนชาติ เบอร์โทรศัพท์ติดต่อ 02-160-1510

นายวชิรศักดิ์ ถิ่นทวี เบอร์โทรศัพท์ติดต่อ 02-160-1510

3.2 แจ้งรองคณบดีฝ่ายบริหาร อาจารย์ ดร.สมศักดิ์ คล้ายสังข์ เพื่อทราบ และดำเนินการสั่งการให้ทีมที่ได้รับมอบหมายเข้าควบคุมสถานการณ์ ให้ระบบเครือข่ายคอมพิวเตอร์ ได้รับความเสียหายน้อยที่สุด และสามารถกลับมาใช้งานได้ตามปกติโดยเร็วที่สุด

4. ขั้นตอนการปฏิบัติการและกู้คืนระบบ กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

4.1 ตรวจสอบภัยคุกคาม

1) ตรวจสอบภัยคุกคามระบุสาเหตุ เพื่อแก้ไขปัญหาเบื้องต้นในทันที

2) รายงานผู้บังคับบัญชา และเรียกประชุมทีมงานที่เกี่ยวข้องเพื่อติดตามสถานการณ์

3) วิเคราะห์ข้อมูลถึงความร้ายแรงของผลกระทบที่เกิดขึ้น

4.2 ควบคุมภัยคุกคาม

1) ควบคุมภัยคุกคามเพื่อบรรเทาความเสียหายที่เกิดขึ้นให้ส่งผลกระทบน้อยที่สุด

2) ระบุช่องว่างหรือแหล่งที่มาของภัยคุกคามในระบบเพื่อปิดช่องทางโจมตีเบื้องต้น

4.3 แก้ไขปัญหา

1) วิเคราะห์และหาสาเหตุของภัยคุกคามฯที่เกิดขึ้น และพร้อมดำเนินการแก้ไขเพื่อกำจัดเหตุ

2) หากไม่สามารถแก้ไขได้ให้ติดต่อสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา เพื่อขอคำแนะนำหรือความช่วยเหลือ

3) กำจัดข้อมูล โปรแกรม หรือสิ่งแปลกปลอมทั้งหลายออกจากระบบ

4) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่นๆ

5) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

4.4 กู้คืนระบบคอมพิวเตอร์

1) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

2) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

3) อุดช่องโหว่ในระบบเครือข่าย

4) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

4.5 สรุปรายงานผลการดำเนินงาน

1) สรุปผลการดำเนินการในการรับมือภัยคุมคามฯ รายงานต่อผู้บังคับบัญชา

2) แจ้งผลการดำเนินงานให้ผู้เกี่ยวข้องทราบ

**กำหนดหน้าที่ความรับผิดชอบบุคลากรในองค์กร ข้อมูลขององค์กร**

| **รายละเอียด** | |
|---|---|
| ชื่อองค์กร | ศูนย์คอมพิวเตอร์ คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนสุนันทา |
| ที่อยู่ | 1 ถนนอู่ทองนอก แขวงดุสิต เขตดุสิต กรุงเทพมหานคร 10300 |
| สถานที่ตั้ง | คณะวิทยาการจัดการ อาคาร 57 ชั้น 1 |
| เบอร์โทรศัพท์ | 02-160-1510 |
| อีเมล์ | sirithanatarathorn.j@ssru.ac.th, wachirasak.th@ssru.ac.th |

**คณะทำงานหลัก – การติดต่อและบทบาทหน้าที่**

| **ชื่อ สกุล** | **โทรศัพท์ที่ทำงาน** | **โทรศัพท์มือถือ** | **บทบาทหน้าที่ต่อการเตรียมความพร้อมสำหรับภัยคุกคามระบบสารสนเทศ** |
|---|---|---|---|
| อาจารย์ ดร.สมศักดิ์ คล้ายสังข์ | 0-2160-1491 | - | - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ<br>- ให้คำปรึกษา ตัดสินใจ สั่งการและควบคุมการดำเนินงาน<br>- รับรายงานให้สรุปผลการดำเนินงานให้ข้อเสนอแนะหลังการดำเนินงาน |
| นายสิริธนธราธร จิรทีปต์ธนชาติ | 0-2160-1510 | 061-414-1535 | - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ<br>- ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน<br>- ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุด อื่นๆ<br>- การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น<br>- ป้องกนไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก |
| นายวชิรศักดิ์ ถิ่นทวี | 0-2160-1510 | 085-186-2520 | - Backup ระบบเว็บไซต์<br>- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ<br>- ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ |

| | | | |
|---|---|---|---|
| | | | ประเมินผลกระทบ และระบุถึงหน่วยงาน<br>- ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ<br>- การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น<br>- ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก |

**รายชื่อผู้สานงานนอกหน่วยงานในการให้คำปรึกษาและช่วยเหลือ**

| องค์กร | ชื่อ สกุล | โทรศัพท์ที่ทำงาน | Email |
|---|---|---|---|
| สำนักวิทยบริการและเทคโนโลยีสารสนเทศ | คุณอโณทัย อรุณเรือง | 0-2160-1231 | anothai@ssru.ac.th |
| สำนักบริหารเทคโนโลยีสารสนเทศภาครัฐ | - | 0-2612-6060 | - |
| ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert) | - | 0-2590-3033 | - |

**ขั้นตอนการปฏิบัติของทีมงาน**

| ทีม : กลุ่มบริหารจัดการเทคโนโลยีสารสนเทศ | | รองคณบดีฝ่ายบริหาร : อาจารย์ ดร. สมศักดิ์ คล้ายสังข์ | | |
|---|---|---|---|---|
| | | หัวหน้าสำนักงาน : นางสาว นิภาวรรณ ธาราศักดิ์ | | |
| **ขั้นตอนการปฏิบัติ** | **กิจกรรม** | | | |
| | **ก่อนการถูกโจมตี**<br>- | **ผู้รับผิดชอบ**<br>- | | **เอกสาร/ทรัพยากร**<br>- |
| | **ระหว่างการถูกโจมตี**<br>1. รับเรื่องภัยคุกคามและแจงไปผู้รับผิดชอบ | **ผู้รับผิดชอบ**<br>กลุ่มบริหารจัดการเทคโนโลยีสารสนเทศ | **เวลาที่ใช้ (นาที)**<br>1-5 | **เอกสาร/ทรัพยากร**<br>- โทรศัพท์,คอมพิวเตอร์ |
| | **หลังการถูกโจมตี**<br>- | **ผู้รับผิดชอบ** | **เวลาที่ใช้ (นาที)** | **เอกสาร/ทรัพยากร** |
| ทีม : กลุ่มสนับสนุนระบบบริการ | | หัวหน้าฝ่ายบริหารงานทั่วไป : นายสิริธนธราธร จิรทีปต์ธน | | |
| | | ผู้ปฏิบัติงาน: นายวชิรศักดิ์ ถิ่นทวี | | |
| **ขั้นตอนการปฏิบัติ** | **กิจกรรม** | | | |
| 1. ประชุมกลุ่มสนับสนุนระบบบริการเพื่อพิจารณาแนวทาง วิธีการดำเนินงานรวมทั้งการมอบหมายงานภายในกลุ่ม<br>2. พิจารณามอบหมายงานเจ้าหน้าที่ภายในกลุ่ม และหรือเจ้าหน้าที่ในทีมอื่น ให้ปฏิบัติงานแทนกรณีเหตุ | **ก่อนการถูกโจมตี**<br>1. เฝ้าระวังตรวจสอบความผิดปกติของระบบ<br>2. ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ<br>3. มีกระบวนการ Backup ข้อมูลตามแผน<br>4. จัดทำคู่มือการกู้คืนระบบและแก้ไขปัญหาเบื้องต้น | **ผู้รับผิดชอบ**<br>นายสิริธนธราธร จิรทีปต์ธนชาติ<br>นายวชิรศักดิ์ ถิ่นทวี | | **เอกสาร/ทรัพยากร**<br>- ระบบ Monitor, คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- คู่มือการกู้คืนระบบ,แก้ไข |

| | | | | |
|---|---|---|---|---|
| | 5. จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งการซ้อมปฏิบัติ | | | ปัญหาเบื้องต้น,เอกสารข่าวสาร<br>- คอมพิวเตอร์ |
| | **ระหว่างการถูกโจมตี** | **ผู้รับผิดชอบ** | **เวลาที่ใช้ (นาที)** | **เอกสาร/ทรัพยากร** |
| | 1. รับแจ้งเหตุภัยคุกคาม | นายสิริธนธราธร จิรทีปต์ธนชาติ | 5 | - โทรศัพท์,คอมพิวเตอร์ |
| | 2. ตรวจพบภัยคุกคามจากระบบ Monitor | นายวชิรศักดิ์ ถิ่นทวี | 5 | - คอมพิวเตอร์ |
| | 3. ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน | | 15 | - คอมพิวเตอร์ |
| | 4. ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ | | 5-10 | - คอมพิวเตอร์ |
| | 5. การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น | | 5-60 | - คอมพิวเตอร์ |
| | 6. ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก | | 30 | - คอมพิวเตอร์ |
| | 7. ประสานงานผู้ติดต่อภายนอก | | 5-10 | - โทรศัพท์,คอมพิวเตอร์ |
| | **หลังการถูกโจมตี** | **ผู้รับผิดชอบ** | **เวลาที่ใช้ (นาที)** | **เอกสาร/ทรัพยากร** |
| | 1. ตรวจสอบการทำงานของระบบและข้อมูลว่าถูกกระทบจากการโจมตีแค่ไหน | นายสิริธนธราธร จิรทีปต์ธนชาติ<br>นายวชิรศักดิ์ ถิ่นทวี | 30 | - คอมพิวเตอร์ |

| | | | | |
|---|---|---|---|---|
| | 2. การกู้คืนระบบหรือข้อมูล ให้อยู่ในสภาพพร้อมบริการ<br>3. ประเมินผลในการดำเนินการรับมือ<br>4. บันทึกรายงานการดำเนินงาน เพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง | | 60<br><br>30<br>60-120 | - คอมพิวเตอร์<br><br>- คอมพิวเตอร์<br>- คอมพิวเตอร์ |
| ทีม : กลุ่มพัฒนาระบบบริการ | | หัวหน้าฝ่ายบริหารงานทั่วไป : นายสิริธนธราธร จิรทีปต์ธน<br>ผู้ปฏิบัติงาน: นายวชิรศักดิ์ ถิ่นทวี | | |
| **ขั้นตอนการปฏิบัติ** | **กิจกรรม** | | | |
| 1. ประชุมกลุ่มพัฒนาระบบบริการ เพื่อพิจารณาแนวทาง วิธีการดำเนินงาน รวมทั้งการมอบหมายงานภายในกลุ่ม<br>2. พิจารณามอบหมายงานเจ้าหน้าที่ภายในกลุ่ม และหรือเจ้าหน้าที่ในทีมอื่น ให้ปฏิบัติงานแทนกรณีเหตุ | **ก่อนการถูกโจมตี**<br>1. ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ<br>2. มีกระบวนการ Backup ข้อมูลตามแผน<br>3. จัดทำคู่มือการกู้คืนระบบและแก้ไขปัญหาเบื้องต้น<br>4. จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งการซ้อมปฏิบัติ | **ผู้รับผิดชอบ**<br>นายสิริธนธราธร จิรทีปต์ธนชาติ<br>นายวชิรศักดิ์ ถิ่นทวี | | **เอกสาร/ทรัพยากร**<br>- คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- คู่มือการกู้คืนระบบ,แก้ไขปัญหาเบื้องต้น,เอกสารข่าวสาร<br>- คอมพิวเตอร์ |
| | **ระหว่างการถูกโจมตี**<br>1. รับแจ้งเหตุภัยคุกคาม<br>2. ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ<br>3. ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่ | **ผู้รับผิดชอบ**<br>นายสิริธนธราธร จิรทีปต์ธนชาติ<br>นายวชิรศักดิ์ ถิ่นทวี | **เวลาที่ใช้ (นาที)**<br>5<br>15<br><br>5-10 | **เอกสาร/ทรัพยากร**<br>- โทรศัพท์,คอมพิวเตอร์<br>- คอมพิวเตอร์<br><br>- คอมพิวเตอร์ |

| | | | | |
|---|---|---|---|---|
| | เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ<br>4. การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น<br>5. ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก<br>6. ประสานงานผู้ติดต่อภายนอก | | <br>5-60<br>30<br>5-10 | <br>- คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- โทรศัพท์,คอมพิวเตอร์ |
| | **หลังการถูกโจมตี**<br>1. ตรวจสอบการทำงานของระบบและข้อมูลว่าถูกกระทบจากการโจมตีแค่ไหน<br>2. การกู้คืนระบบหรือข้อมูล ให้อยู่ในสภาพพร้อมบริการ<br>3. ประเมินผลในการดำเนินการรับมือ<br>4. บันทึกรายงานการดำเนินงาน เพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง | **ผู้รับผิดชอบ**<br>นายสิริธนธราธร จิรทีปต์ธนชาติ<br>นายวชิรศักดิ์ ถิ่นทวี | **เวลาที่ใช้ (นาที)**<br>30<br>60<br>30<br>60-120 | **เอกสาร/ทรัพยากร**<br>- คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- คอมพิวเตอร์<br>- คอมพิวเตอร์ |