**Action Planning for Improvement Priorities**

EdPEx TSU 5

**ชื่อหน่วยงาน : สำนักคอมพิวเตอร์**

**โครงการ : การรักษาความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟท์แวร์ และภาวะฉุกเฉิน**

|  |  |
| --- | --- |
| 1. ผู้รับผิดชอบหลัก
 | สำนักคอมพิวเตอร์ |
| 1. ประเด็นจากการวิเคราะห์องค์กร (SA/OA)
 | มหาวิทยาลัยมีความเสี่ยงด้านความปลอดภัยข้อมูลทั้งที่เกิดจากผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ ซอฟท์แวร์ และภัยธรรมชาติทำให้ส่งผลกระทบต่อความพร้อมใช้งานทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์อย่างต่อเนื่อง |
| 1. เป้าหมาย/ผลที่คาดว่าจะได้รับ
 | มหาวิทยาลัยมีความมั่นคงปลอดภัยข้อมูลสารสนเทศที่เกิดจากผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ และภัยธรรมชาติ (ภาวะฉุกเฉิน) โดยมีระบบตรวจสอบและป้องกันผู้บุกรุก มีการสำรองข้อมูลอย่างสม่ำเสมอ และมีการดำเนินการทดสอบกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง เพื่อทำให้เกิดความน่าเชื่อถือและความพร้อมใช้งานทั้งด้านฮาร์ดแวร์และซอฟท์แวร์อย่างต่อเนื่อง |
| 1. ตัวชี้วัดความสำเร็จ
 | 1.มีแผนการดำเนินงานรักษาความมั่นคงปลอดภัย**ของ**ฮาร์ดแวร์ ซอฟท์แวร์และภาวะฉุกเฉิน2.มีแผนการกู้คืนระบบ (Backup and Recovery) โดยกำหนดผู้รับผิดชอบที่ชัดเจน3.มีการซักซ้อมทดสอบการกู้คืนระบบในสภาวะเกิดจากผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ และซอฟท์แวร์ หรือภัยธรรมชาติ ตามแผนการดำเนินการอย่างน้อยปีละ 1 ครั้ง |
| 1. ความสำคัญและความเชื่อมโยงกับเกณฑ์ EdPEx
 | **หมวด 4 การวัด วิเคราะห์ และการจัดการความรู้**หัวข้อ 4.2 การจัดการความรู้ สารสนเทศ และเทคโนโลยีสารสนเทศ ประเด็น 2.1 การทวนสอบและทำให้มั่นใจว่าข้อมูลและสารสนเทศที่ใช้ในสถาบันมีคุณภาพ 2.2 การทำให้มั่นใจถึงความปลอดภัยของข้อมูลและสารสนเทศที่อ่อนไหวและเป็นสิทธิพิเศษ 2.3 ความพร้อมของข้อมูลและสารสนเทศ **ประเด็น 4.การทำให้มั่นใจว่าระบบฮาร์ดแวร์และซอฟแวร์ รวมทั้งข้อมูลและสารสนเทศมีความมั่นคงปลอดภัย และพร้อมใช้งานอย่างต่อเนื่องในภาวะฉุกเฉิน****หมวด 6 ระบบปฏิบัติการ** หัวข้อ 6.2 ประสิทธิผลของการปฏิบัติการ ประเด็น 3.**การเตรียมความพร้อมต่อภัยพิบัติหรือภาวะฉุกเฉิน (กำหนดวัตถุประสงค์**/**นโยบาย วิเคราะห์ผลกระทบ ระบุภัยพิบัติและประเมินความเสี่ยง พิจารณาจัดลำดับความสำคัญ กำหนดกลยุทธ์และแผนงาน ฝึกซ้อม)** |
| 1. ระยะเวลาดำเนินการ
 | พ.ค. – ธ.ค. 61 |
| 1. งบประมาณและแหล่ง
 | - |
| 1. การรายงานผล
 | ที่ประชุมคณบดี ผู้อำนวยการและผู้บริหารระดับสูงกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร |

**แผนการดำเนินงาน**

|  |  |  |  |
| --- | --- | --- | --- |
| **กิจกรรม/ขั้นตอนการดำเนินการ** | **พ.ศ. 2561** | **ผลที่ได้รับ** | **ผู้รับผิดชอบ** |
| **เม.ย.** | **พ.ค.** | **มิ.ย.** | **ก.ค.** | **ส.ค.** | **ก.ย.** | **ต.ค.** | **พ.ย.** | **ธ.ค.** |
| 1. วิเคราะห์ผลกระทบ ระบุภัยพิบัติและประเมินความเสี่ยง ที่ผ่านมาเพื่อ พิจารณาจัดลำดับความสำคัญ ในการกำหนดกลยุทธ์และแผนงานฝึกซ้อม
 |  |  |  |  |  |  |  |  |  | ผลการวิเคราะห์ความเสี่ยงที่เกิดขึ้น ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ | สำนักคอมพิวเตอร์ |
| 1. มีการจัดทำแผนในการดำเนินงานรักษาความมั่นคงปลอดภัย ทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ แผนการกู้คืนระบบ (Backup and Recovery) และกำหนดผู้รับผิดชอบที่ชัดเจน
 |  |  |  |  |  |  |  |  |  | แผนรักษาความปลอดภัยระบบและแผนการกู้คืนระบบสารสนเทศ(Backup and Recovery) และผู้รับผิดชอบที่ชัดเจน | สำนักคอมพิวเตอร์ |
| 1. ดำเนินการกิจกรรมตามแผนฯ
 |  |  |  |  |  |  |  |  |  | 1.มีระบบตรวจสอบและป้องกัน ผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ และซอฟท์แวร์ 2 มีระบบสำรองข้อมูล ที่มีการกำหนดระยะเวลาในการสำรองข้อมูลที่ชัดเจน3.มีการซักซ้อมการกู้คืนระบบเมื่อเกิดภาวะฉุกเฉิน | สำนักคอมพิวเตอร์ |
| 1. มีการรายงานและติดตามผลการดำเนินงานประจำเดือนตาม แผนฯ
 |  |  |  |  |  |  |  |  |  | 1.รายงานผลการดำเนินการตรวจสอบและป้องกัน ผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ และภัยธรรมชาติ 2.รายงานผลการดำเนินการสำรองข้อมูลสารสนเทศมหาวิทยาลัย และกำหนดระยะเวลา  | สำนักคอมพิวเตอร์ |
| 1. มีการซักซ้อมทดสอบการกู้คืนระบบสารสนเทศในสภาวะเกิดจากผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ หรือภัยธรรมชาติ ตามแผน
 |  |  |  |  |  |  |  |  |  | มีการซักซ้อมทดสอบการกู้คืนระบบสารสนเทศในสภาวะเกิดจากผู้บุกรุก ความเสื่อมสภาพของฮาร์ดแวร์ หรือภัยธรรมชาติ ตามแผนการดำเนินการอย่างน้อยปีละ 1 ครั้ง | สำนักคอมพิวเตอร์ |
| 1. มีประเมินผล การวิเคราะห์ และรายงานผลการดำเนินงานประจำปี เพื่อนำมาแก้ไขปรับปรุงในแผนปีถัดไป
 |  |  |  |  |  |  |  |  |  | มีประเมินผล การวิเคราะห์ และรายงานผลการดำเนินงานประจำปี เพื่อนำมาแก้ไขปรับปรุงในแผนปีถัดไป  | สำนักคอมพิวเตอร์ |