

ขั้นตอนการปฏิบัติงานการบริหารจัดการระบบป้องกันการบุกรุกทางเครือข่าย (Firewall)

สำหรับบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

ขั้นตอนการปฏิบัติงาน

ขั้นตอน	ผังการทำงาน	ระยะเวลา
<p>๑. รับแจ้งปัญหาหรือคำร้องขอ</p> <p>๒. ตรวจสอบวิเคราะห์ปัญหาและผลกระทบด้านความปลอดภัย</p> <p>๓. กรณี Policy ใหม่</p> <p> ๓.๑ กำหนดค่า Zone, IP Address Application, Service และ Profile</p> <p>๔. กรณี Policy เดิมใช้งานไม่ได้</p> <p> ๔.๑ ตรวจสอบเส้นทางการจราจรทางเครือข่าย (Traffic log)</p> <p> ๔.๒ กำหนดค่าเพิ่มเติม</p> <p> ๔.๓ ประสานงานสำนักบริการคอมพิวเตอร์เปิดการเชื่อมต่อ</p> <p>๕. แจ้งผลการดำเนินงาน</p> <p>๖. บันทึกสถิติ</p>	<pre> graph TD Start([เริ่ม]) --> Receive[รับแจ้งปัญหา/คำร้อง] Receive --> Check[ตรวจสอบและวิเคราะห์ผลกระทบด้านความปลอดภัย] Check --> Decision{กฎใหม่?} Decision -- Yes --> Define[กำหนดค่า] Define --> Test[Testการใช้งานตามกฎ Rule ที่กำหนดค่า] Test --> Notify[แจ้งผล] Notify --> Record[บันทึกผลการปฏิบัติงาน] Record --> End([จบ]) Decision -- No --> CheckPath[ตรวจสอบเส้นทางการจราจรทางเครือข่าย] CheckPath --> AddDef[กำหนดค่าเพิ่มเติม] AddDef --> Connect[ประสานงาน สบค. เปิดการเชื่อมต่อ] Connect --> Test </pre>	<p>๒๐ นาที - ๓ วัน</p>

หมายเหตุ : ระยะเวลาดำเนินการขึ้นอยู่กับกระบวนการติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้อง