ข้อกำหนดการบริหารจัดการระบบป้องกันการบุกรุกทางเครือข่าย (Firewall)

สำหรับบุคลากรฝ่ายเทคโนโลยีสารสนเทศ

---

๑) ต้องตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒) ต้องตรวจสอบ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๓) ต้องมีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำทุกๆ ๓ เดือน

๔) ต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำหรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๕) ต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

   (๑) ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

   (๒) การขอใช้งานพอร์ตพิเศษนอกเหนือจากการใช้งานปกติจะต้องได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น

๖) กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อและแก้ไขปัญหาที่เครื่องหรืออุปกรณ์นั้นๆ ทันที

๗) ต้องกำหนดให้มีการบันทึกการทำงานบนระบบเครือข่าย (Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง