

**การไฟฟ้าส่วนภูมิภาค**

**PROVINCIAL ELECTRICITY AUTHORITY**

โครงการจัดหา พัฒนา ติดตั้ง และบำรุงรักษา

ระบบริหารไฟฟ้าขัดข้อง Outage Management System (OMS)

* 1. **(2) ขอบเขตรายละเอียดของงาน (TOR)**

**Book 6 : Cyber Security Requirements**

# ข้อกำหนดความต้องการด้านความมั่นคงปลอดภัย

1. ผู้รับจ้างจะต้องดำเนินการให้สอดคล้องตามนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศของ กฟภ. รวมถึงคำสั่งและแนวปฏิบัติที่เกี่ยวข้อง
2. ห้ามมิให้ผู้รับจ้างนำอุปกรณ์ประมวลผลใด ๆ ต่อเข้ากับระบบงานหรือระบบเครือข่ายของ กฟภ. โดยมิได้ผ่านการตรวจสอบจากเจ้าหน้าที่ผู้รับผิดชอบของ กฟภ. และต้องได้รับการอนุญาตก่อนการติดตั้ง และ การเชื่อมต่ออุปกรณ์คอมพิวเตอร์ใด ๆ เข้ากับระบบคอมพิวเตอร์ของ กฟภ. ต้องทำการเชื่อมต่อเข้ากับ Port ที่ กฟภ. กำหนดเท่านั้น
3. ผู้รับจ้างต้องมีความตระหนักและการปฏิบัติเพื่อให้เกิดการมั่นคงความปลอดภัยในข้อมูลและทรัพย์สินของ กฟภ.
4. ผู้รับจ้างต้องรับผิดชอบในการจัดการด้านความปลอดภัยข้อมูล เช่น การจัดเก็บข้อมูล การโยกย้าย การทำสำเนา และการทำลาย ฯลฯ
5. ผู้รับจ้างต้องมีการจำกัดสิทธิบุคลากรของผู้รับจ้างในการเข้าใช้งานข้อมูลของ กฟภ. ให้สามารถใช้งานได้เฉพาะในส่วนที่เกี่ยวข้องกับงานที่บุคลากรนั้นเกี่ยวข้องเท่านั้น
6. ผู้รับจ้างต้องจัดให้มีระบบรักษาความปลอดภัยด้านซอฟต์แวร์และฮาร์ดแวร์และระบบเครือข่ายสำหรับอุปกรณ์ที่นำเสนอในโครงการนี้ รวมถึงการติดตั้งระบบเพื่อตรวจสอบเหตุการณ์ที่มีผลกระทบต่อ ความปลอดภัยของระบบในโครงการนี้ และต้องแจ้งให้หน่วยงานผู้รับผิดชอบของ กฟภ. ทราบทันทีที่เกิดเหตุการณ์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบงานและอุปกรณ์ในโครงการ
7. ห้ามมิให้ผู้รับจ้างนำข้อมูลของ กฟภ. หรือ Source Code ของโครงการออกจาก กฟภ. ไม่ว่าด้วยวิธีการ ใด ๆ เว้นเสียแต่จะได้รับอนุญาตจาก กฟภ. หากผู้รับจ้างละเมิดข้อห้ามดังกล่าวนี้ กฟภ. ขอสงวนสิทธิ์ในการคิดค่าปรับจากผู้รับจ้างตามสมควร หรือบอกเลิกสัญญาได้โดยผู้รับจ้างยังต้องรับผิดชอบต่อค่าเสียหายทั้งหมดที่เกิดขึ้น
8. กฟภ. ขอสงวนสิทธิ์ในการเข้าตรวจสอบการปฏิบัติงานของผู้รับจ้างได้ตามแต่ที่ กฟภ. จะเห็นสมควร
9. ผู้รับจ้างต้องแจ้งหน่วยงานที่ควบคุมดูแลการทำงานทันทีในกรณีที่เกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ
10. ผู้รับจ้างต้องทำเอกสารด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย การออกแบบและตั้งค่าเกี่ยวกับระบบเครือข่าย การตั้งค่าด้านระบบไฟร์วอล เอกสารเกี่ยวกับการเชื่อมต่อผ่านเครือข่ายคอมพิวเตอร์กับระบบซอฟต์แวร์ทุกระบบ อธิบายเนื้อหาของการเชื่อมโยงข้อมูล ระบุระดับของความจำเป็นหรือผลกระทบของการเชื่อมโยงข้อมูลนั้น รวมถึงต้องอธิบายแอดเดรสของทุกระบบที่เกี่ยวข้อง ทุกโปรโตคอลที่เกี่ยวข้อง
11. เพื่อความมั่นคงปลอดภัยทางไซเบอร์ของระบบ ผู้รับจ้างต้องทำการตรวจสอบและทบทวน อย่างน้อยตามกิจกรรมดังต่อไปนี้
    1. ทบทวนการอนุญาตและการตั้งค่าต่าง ๆ ว่าถูกต้องตามเอกสารและตามวัตถุประสงค์หรือไม่
    2. ตรวจสอบการบันทึกประวัติ (log) การรับส่งข้อมูลผ่านเครือข่ายว่าทำงานได้อย่างถูกต้อง
    3. ตรวจสอบว่าบริการหรือเซอร์วิสที่ไม่ได้ใช้ถูกเอาออกไปแล้วหรือไม่
    4. ตรวจสอบว่าซอฟต์แวร์ทุกตัวที่เกี่ยวข้องได้รับการปรับปรุงเวอร์ชันล่าสุดแล้วหรือไม่
    5. ดำเนินการแสกนไวรัสและมาลแวร์และตรวจสอบว่าซอฟต์แวร์แสกนไวรัสทำงานได้ดี
    6. ตรวจสอบว่าซอฟต์แวร์สนับสนุนอื่นที่ไม่ได้ใช้งานได้ถูกเอาออกไปหรือไม่
    7. สร้างไฟล์ซิกเนเจอร์ใหม่ (signature file) ทั้งหมดเพื่อความมั่นคงปลอดภัย
    8. ลบบัญชีผู้ใช้ที่เป็นค่าดีฟอลท์ (default) ออกทั้งหมด
    9. ตรวจสอบการให้สิทธิการเข้าถึงระบบและข้อมูลทั้งหมดถูกต้องเหมาะสมดีแล้ว
    10. ทบทวนการได้รับการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของเจ้าหน้าที่ผู้เกี่ยวข้องทั้งหมดรวมถึงเจ้าหน้าที่ของผู้รับจ้างตามโครงการต่างๆ ที่เกี่ยวข้อง
    11. สร้างสำเนาทั้งหมดของซอฟต์แวร์และข้อมูล เพื่อให้พร้อมกู้คืนได้เสมอ