

**การไฟฟ้าส่วนภูมิภาค**

**PROVINCIAL ELECTRICITY AUTHORITY**

โครงการจัดหา พัฒนา ติดตั้ง และบำรุงรักษา

ระบบริหารไฟฟ้าขัดข้อง Outage Management System (OMS)

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

**Appendix H: การรักษาความมั่นคงปลอดภัยด้านข้อมูลและทรัพย์สินของ กฟภ. (Cyber Security)**

# **การรักษาความมั่นคงปลอดภัยด้านข้อมูลและทรัพย์สินของ กฟภ. (Cyber Security)**

# Security Architecture

# ผู้รับจ้างต้องระบุขอบเขตเครือข่ายของระบบบริหารไฟฟ้าขัดข้อง (OMS) การเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง และการให้บริการผู้ใช้งาน โดยจัดทำเป็นแผนผังระบบเครือข่าย (Network Diagram) หรือเอกสาร ที่ระบุองค์ประกอบทั้งหมดของระบบบริหารไฟฟ้าขัดข้อง (OMS) (ทั้งที่เป็น Physical และ Virtual) และอินเทอร์เฟซที่เป็นจุดเชื่อมโยงข้อมูล หรือจุดให้บริการผู้ใช้งาน รวมทั้งอุปกรณ์หรือระบบที่ใช้ควบคุม เผ้าระวัง ป้องกันการเข้าถึงเครือข่ายภายในของระบบบริหารไฟฟ้าขัดข้อง (OMS)

# เครือข่ายภายในของระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องออกแบบโดยแยกกลุ่มเครือข่าย (Network Zone) ออกจากกันตามความจาเป็นในการทางาน และระดับความสำคัญต่อการให้บริการของระบบ (เช่น Production, Pre-Production, Management, De-militarized Zone (DMZ), ฯลฯ) และข้อมูลที่วิ่งผ่านระหว่างกลุ่มเครือข่าย ต้องมีการควบคุมโดย Next-Generation Firewall และระบบ Intrusion Prevention System

# อินเทอร์เฟซที่เป็นจุดเชื่อมโยงข้อมูล หรือให้บริการผู้ใช้งาน ต้องมีการป้องกันโดย Next–Generation Firewall และระบบ Intrusion Prevention System (IPS) ที่สามารถรองรับปริมาณข้อมูลของผู้ใช้งานตามจานวนที่ระบุในสถาปัตยกรรมโครงสร้างพื้นฐานและการเชื่อมโยง

# (Optional) เว็บแอปพลิเคชัน (Web Application) และ/หรือ API สาหรับอุปกรณ์เคลื่อนที่ (Mobile Device) สาหรับให้บริการผู้ใช้งาน ต้องมีการป้องกันโดย Web Application Firewall (WAF) และ/หรือ API Firewall ที่สามารถรองรับปริมาณข้อมูลของผู้ใช้งานตามจำนวนที่ระบุในสถาปัตยกรรมโครงสร้างพื้นฐานและการเชื่อมโยง

# แอปพลิเคชัน OMS บนเวิร์กสเตชัน, เว็บแอปพลิเคชัน (Web Application), และบนอุปกรณ์เคลื่อนที่ (Mobile Device) สำหรับให้บริการผู้ใช้งาน ต้องทำงานแบบ High Availability (HA) โดยหาก Process ที่ให้บริการแอปพลิเคชัน เว็บแอปพลิเคชัน และ/หรือ API หยุดการทำงาน ผู้ใช้ต้องสามารถใช้งานระบบบริหารไฟฟ้าขัดข้อง (OMS) ต่อได้โดยไม่หยุดชะงัก

# การเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง ต้องมีการเข้ารหัสลับ (Encryption) โดยใช้อัลกอริทึมที่ปลอดภัยและได้รับความเห็นขอบจาก กฟภ. ในกรณีที่ไม่สามารถใช้การเข้ารหัสลับได้ ผู้รับจ้างต้องกำหนดแนวทางในการตรวจสอบความถูกต้องหรือป้องกันการเปลี่ยนแปลงของข้อมูลระหว่างส่ง

# ระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องรองรับการพิสูจน์ตัวตน (Authentication) ก่อนการเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง รวมทั้งรองรับการพิสูจน์ตัวตนของผู้ใช้งานแอปพลิเคชัน OMS บนเวิร์กสเตชัน, เว็บแอปพลิเคชัน (Web Application), และบนอุปกรณ์เคลื่อนที่ (Mobile Device)

# ระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องรองรับการกำหนดสิทธิ์ผู้ใช้งานแบบ Role–Based Access Control (RBAC) โดยต้องสามารถกาหนดให้ผู้ใช้งานเข้าถึงฟังก์ชันต่าง ๆ ในระบบได้เท่าที่จำเป็น (Least Privileges) และตามหน้าที่ความรับผิดชอบ (Separation of Duties)

# (Optional) ระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องรองรับการกำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน โดยคานึงถึงระดับชั้นความลับของข้อมูล (Confidentiality) ความจาเป็นที่ต้องใช้ข้อมูลนั้นในการปฏิบัติงาน (Need-to-know) และความเป็นส่วนตัวของเจ้าของข้อมูล (Privacy)

# (Optional) เครื่องเซิร์ฟเวอร์และเวิร์กสเตชันของระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องติดตั้งโปรแกรมป้องกันมัลแวร์ หรือ Endpoint Detection and Response (EDR) หรือมีการทำ Application Allowlisting เพื่อป้องกันการโจมตี ติดตั้ง หรือเรียกใช้ซอฟต์แวร์ที่เป็นอันตรายต่อระบบ

# องค์ประกอบทั้งหมดของระบบบริหารไฟฟ้าขัดข้อง (OMS) (ฮาร์ดแวร์, ซอฟต์แวร์, ระบบปฏิบัติการ, เครื่องคอมพิวเตอร์เสมือน, อุปกรณ์เครือข่าย, เว็บแอปพลิเคชัน ฯลฯ) ต้องมีการออกแบบและควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ โดยอ้างอิงตามมาตรฐานสากลหรือ Best Practice เช่น CIS Critical Security Controls V8 และ OWASP Top 10 2021 เป็นต้น

# ระบบบริหารไฟฟ้าขัดข้อง (OMS) ต้องมีการรวบรวม จัดเก็บข้อมูล Log ด้านความมั่นคงปลอดภัยไซเบอร์ของระบบปฏิบัติการ อุปกรณ์เครือข่าย และแอปพลิเคชันต่างๆ เป็นเวลาไม่น้อยกว่า 90 วัน และต้องสามารถส่งต่อข้อมูล Log ดังกล่าวไปยังอุปกรณ์ Log Collector หรือ SIEM ของ กฟภ. ได้

# Security Testing

# กฟภ. จะทำ Vulnerability Assessment (VA) องค์ประกอบทั้งหมดของระบบบริหารไฟฟ้าขัดข้อง (OMS) (ฮาร์ดแวร์, ซอฟต์แวร์, ระบบปฏิบัติการ, เครื่องคอมพิวเตอร์เสมือน, อุปกรณ์เครือข่าย, เว็บแอปพลิเคชัน ฯลฯ) ก่อนการส่งมอบระบบ เพื่อค้นหาช่องโหว่หรือจุดอ่อน โดยอ้างอิงตามมาตรฐานสากลหรือ Best Practice เช่น OWASP Top 10 2021 และ CIS Benchmarks เป็นต้น และผู้รับจ้างต้องทาการแก้ไขช่องโหว่ที่ตรวจพบ (Correction) หรือหาวิธีบรรเทาโอกาสที่จะถูกโจมตีหรือผลกระทบจากช่องโหว่นั้น (Mitigation) โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

# กฟภ. จะทา Penetration Testing (Pentest) องค์ประกอบทั้งหมดของระบบบริหารไฟฟ้าขัดข้อง (OMS) (ฮาร์ดแวร์, ซอฟต์แวร์, ระบบปฏิบัติการ, เครื่องคอมพิวเตอร์เสมือน, อุปกรณ์เครือข่าย, เว็บแอปพลิเคชัน ฯลฯ) ก่อนการส่งมอบระบบ หรือในระหว่างระยะเวลารับประกัน เพื่อค้นหาช่องโหว่หรือจุดอ่อนที่อาจถูกใช้ในการโจมตีระบบบริหารไฟฟ้าขัดข้อง (OMS) จากผู้ไม่ประสงค์ดี และผู้รับจ้างต้องทำการแก้ไขช่องโหว่ที่ค้นพบ (Correction) หรือหาวิธีบรรเทาโอกาสที่จะถูกโจมตีหรือผลกระทบจากช่องโหว่นั้น (Mitigation) โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

# Security Operation

# ผู้รับจ้างต้องจัดทำ Software Bill of Materials (SBOM) โดยระบุไลบรารีและ Third–Party Software ต่าง ๆ ที่มีการใช้งานในระบบบริหารไฟฟ้าขัดข้อง (OMS) เพื่อเป็นข้อมูลให้ กฟภ. ในการบริหารจัดการช่องโหว่ด้าน Supply Chain

# ผู้รับจ้างต้องจัดหาสิทธิ์การใช้งาน (License) หรือ Subscription ขององค์ประกอบต่าง ๆ ในระบบบริหารไฟฟ้าขัดข้อง (OMS) ให้ครอบคลุมการใช้งานตลอดระยะเวลารับประกัน