# การรักษาความมั่นคงปลอดภัยด้านข้อมูลและทรัพย์สินของ กฟภ. (Cyber Security)

9.1 Security Architecture

9.1.1 ผู้รับจ้างต้องระบุขอบเขตเครือข่ายของระบบ OMS การเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง และการให้บริการผู้ใช้งาน โดยจัดทาเป็นแผนผังระบบเครือข่าย (Network Diagram) หรือเอกสาร ที่ระบุองค์ประกอบทั้งหมดของระบบ OMS (ทั้งที่เป็น Physical และ Virtual) และอินเทอร์เฟซที่เป็นจุดเชื่อมโยงข้อมูล หรือจุดให้บริการผู้ใช้งาน รวมทั้งอุปกรณ์หรือระบบที่ใช้ควบคุม เผ้าระวัง ป้องกันการเข้าถึงเครือข่ายภายในของระบบ OMS

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

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

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

9.1.5 แอปพลิเคชัน OMS บนเวิร์กสเตชัน, เว็บแอปพลิเคชัน (Web Application), และบนอุปกรณ์เคลื่อนที่ (Mobile Device) สาหรับให้บริการผู้ใช้งาน ต้องทางานแบบ High Availability (HA) โดยหาก Process ที่ให้บริการแอปพลิเคชัน เว็บแอปพลิเคชัน และ/หรือ API หยุดการทางาน ผู้ใช้ต้องสามารถใช้งานระบบ OMS ต่อได้โดยไม่หยุดชะงัก

9.1.6 การเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง ต้องมีการเข้ารหัสลับ (Encryption) โดยใช้อัลกอริทึมที่ปลอดภัยและได้รับความเห็นขอบจาก กฟภ. ในกรณีที่ไม่สามารถใช้การเข้ารหัสลับได้ ผู้รับจ้างต้องกาหนดแนวทางในการตรวจสอบความถูกต้องหรือป้องกันการเปลี่ยนแปลงของข้อมูลระหว่างส่ง

9.1.7 ระบบ OMS ต้องรองรับการพิสูจน์ตัวตน (Authentication) ก่อนการเชื่อมโยงข้อมูลกับระบบที่เกี่ยวข้อง รวมทั้งรองรับการพิสูจน์ตัวตนของผู้ใช้งานแอปพลิเคชัน OMS บนเวิร์กสเตชัน, เว็บแอปพลิเคชัน (Web Application), และบนอุปกรณ์เคลื่อนที่ (Mobile Device)

9.1.8 ระบบ OMS ต้องรองรับการกาหนดสิทธิ์ผู้ใช้งานแบบ Role–Based Access Control (RBAC) โดยต้องสามารถกาหนดให้ผู้ใช้งานเข้าถึงฟังก์ชันต่างๆ ในระบบได้เท่าที่จาเป็น (Least Privileges) และตามหน้าที่ความรับผิดชอบ (Separation of Duties)

9.1.9 (Optional) ระบบ OMS ต้องรองรับการกาหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน โดยคานึงถึงระดับชั้นความลับของข้อมูล (Confidentiality) ความจาเป็นที่ต้องใช้ข้อมูลนั้นในการปฏิบัติงาน (Need-to-know) และความเป็นส่วนตัวของเจ้าของข้อมูล (Privacy)

9.1.10 (Optional) เครื่องเซิร์ฟเวอร์และเวิร์กสเตชันของระบบ OMS ต้องติดตั้งโปรแกรมป้องกันมัลแวร์ หรือ Endpoint Detection and Response (EDR) หรือมีการทา Application Allowlisting เพื่อป้องกันการโจมตี ติดตั้ง หรือเรียกใช้ซอฟต์แวร์ที่เป็นอันตรายต่อระบบ

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

9.1.12 ระบบ OMS ต้องมีการรวบรวม จัดเก็บข้อมูล Log ด้านความมั่นคงปลอดภัยไซเบอร์ของระบบปฏิบัติการ อุปกรณ์เครือข่าย และแอปพลิเคชันต่างๆ เป็นเวลาไม่น้อยกว่า 90 วัน และต้องสามารถส่งต่อข้อมูล Log ดังกล่าวไปยังอุปกรณ์ Log Collector หรือ SIEM ของ กฟภ. ได้

9.2 Security Testing

9.2.1 กฟภ. จะทา Vulnerability Assessment (VA) องค์ประกอบทั้งหมดของระบบ 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

9.2.2 กฟภ. จะทา Penetration Testing (Pentest) องค์ประกอบทั้งหมดของระบบ OMS (ฮาร์ดแวร์, ซอฟต์แวร์, ระบบปฏิบัติการ, เครื่องคอมพิวเตอร์เสมือน, อุปกรณ์เครือข่าย, เว็บแอปพลิเคชัน ฯลฯ) ก่อนการส่งมอบระบบ หรือในระหว่างระยะเวลารับประกัน เพื่อค้นหาช่องโหว่หรือจุดอ่อนที่อาจถูกใช้ในการโจมตีระบบ OMS จากผู้ไม่ประสงค์ดี และผู้รับจ้างต้องทาการแก้ไขช่องโหว่ที่ค้นพบ (Correction) หรือหาวิธีบรรเทาโอกาสที่จะถูกโจมตีหรือผลกระทบจากช่องโหว่นั้น (Mitigation) โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

9.3 Security Operation

9.3.1 ผู้รับจ้างต้องจัดทา Software Bill of Materials (SBOM) โดยระบุไลบรารีและ Third–Party Software ต่างๆ ที่มีการใช้งานในระบบ OMS เพื่อเป็นข้อมูลให้ กฟภ. ในการบริหารจัดการช่องโหว่ด้าน Supply Chain

9.3.2 ผู้รับจ้างต้องจัดหาสิทธิ์การใช้งาน (License) หรือ Subscription ขององค์ประกอบต่างๆ ในระบบ OMS ให้ครอบคลุมการใช้งานตลอดระยะเวลารับประกัน