Supply Chain Policy for IT and Software Assets (OPS-SUPPLY-001)

Department: Operations, Legal & Finance
Version: 1.0
Date: 2025-10-01

1. Scope and Risk Management

This policy governs the acquisition, use, and disposal of all IT hardware (servers, networking equipment, user devices) and third-party software/cloud licenses utilized by NexaCore. The primary risk mitigated is the introduction of compromised or non-compliant components.

2. Hardware Supply Chain Security

- **Authorized Sourcing:** All critical hardware (e.g., firewall devices, data center servers) must be sourced directly from approved, tier-1 manufacturers or authorized regional distributors. No "grey market" or unverified sources are permitted.
- **Tamper-Evident:** Upon receipt, Operations personnel must inspect packaging for signs of tampering. Any suspicious package must be quarantined and reported to the IT Security Officer.
- **Secure Disposal:** Hardware reaching end-of-life must be destroyed by a certified asset disposal vendor. Data-bearing devices (SSDs, HDDs) must undergo mandatory physical destruction and provide a certificate of destruction.

3. Software Licensing and Vendor Compliance

- **License Management:** All commercial software must be tracked in the Centralized Asset Management (CAM) system. Licenses must be renewed preemptively to avoid service interruption.
- **Open Source Governance:** The R&D team must provide a Software Bill of Materials (SBOM) for all production builds. Open-source licenses must be reviewed by Legal to ensure compatibility with our SaaS model.
- **Third-Party Code Audit:** For any third-party code library that handles client data or authentication, a basic security audit (e.g., static analysis) must be performed by R&D before integration.

4. Regional Sourcing and Compliance

- **Vendor Vetting:** Priority is given to vendors that can provide evidence of regional compliance and local support presence in the MENA region.
- **Customs and Export Control:** Operations is responsible for ensuring all imported hardware complies with UAE and regional export/import control regulations. All

documentation must be retained for years.