Operations Security Policy

Policy Owner: VIMBuild, LLC
Author: Martin Ashton
Effective Date: 02/06/2025

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All VIMBuild, LLC information systems that are business-critical and/or process, store, or transmit company data. This policy applies to all employees of VIMBuild, LLC and other third-party entities with access to VIMBuild, LLC networks and system resources.

Operations Security

Documented Operating Procedures

Both technical and administrative operating procedures shall be documented as needed and made available to all users who require them.

Change Management

Changes to business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment shall be tested, reviewed, and approved prior to deployment. All significant changes must be documented.

Change management processes shall include:

- Planning and testing of changes, including remediation measures.
- Managerial approval before proceeding with significant changes affecting security or operations.
- Advance communication of changes, including schedules and anticipated effects, provided to relevant stakeholders.
- Documentation of all emergency changes and subsequent reviews.
- A process for remediating unsuccessful changes.

Capacity Management

System processing resources and storage shall be monitored and adjusted to meet VIMBuild, LLC availability and performance requirements. Human resource availability and capacity shall also be reviewed as part of the annual risk assessment process.

Separation of Development, Staging, and Production Environments

Development and staging environments shall be strictly segregated from production environments to reduce risks of unauthorized access or changes. Confidential production customer data must not be used in development or test environments without explicit approval from the Administrator.

Systems and Network Configuration, Hardening, and Review

Systems and networks shall be configured and maintained in accordance with security standards (refer to **Appendix A**). Firewalls and network access controls shall be used to regulate production network traffic.

Production network access configuration rules shall be reviewed annually. Changes require documented approval.

Protection from Malware

To safeguard infrastructure against malware, detection, prevention, and recovery controls shall be implemented, along with user awareness programs.

- Anti-malware protections must be utilized on all company-issued devices.
- Threat detection software shall be deployed for company email.
- Malware incidents must be reported as security incidents.

Information Backup

Backups shall be maintained and periodically tested to ensure recoverability. Security measures shall be applied in accordance with data confidentiality.

- Backups must be stored separately from production data.
- Restore tests shall be performed at least annually.

Logging & Monitoring

Production infrastructure shall produce detailed logs, including:

- User log-in and log-out events.
- CRUD (create, read, update, delete) operations.
- Logs containing user ID, IP address, timestamps, action type, and affected objects.
- Logs must be stored for at least 30 days.

Administrator and operator activities shall be logged and reviewed periodically.

Clock Synchronization

All relevant information processing systems shall synchronize clocks to network time servers using reputable sources.

File Integrity Monitoring and Intrusion Detection

Production systems shall monitor, log, and alert on suspicious changes to critical system files. Unauthorized intrusions and access attempts shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow documented change management requirements.

Technical Vulnerability Management

Vulnerabilities shall be identified, evaluated, and remediated in accordance with risk levels:

Severity	Remediation Time
Critical	7 Days
High	7 Days
Medium	14 Days
Low	30 Days
Informational	As needed

Vulnerability scans shall be performed at least quarterly.

Restrictions on Software Installation

Rules governing software installation shall be enforced per VIMBuild, LLC's Information Security Policy.

Information Systems Audit Considerations

Audit activities shall be planned to minimize disruptions to business processes.

Systems Security Assessment & Requirements

Security risks shall be assessed before acquiring new systems, technologies, or services. Third-party services shall be evaluated in accordance with the **Third-Party Management Policy**.

The company shall conduct an annual network security assessment.

Exceptions

Requests for exceptions to this policy must be submitted to the Administrator for approval.

Violations & Enforcement

Violations of this policy must be reported to the Administrator. Non-compliance can result in suspension of system access or disciplinary action, up to termination of employment.

Appendix A – Configuration and Hardening Standards

Configuration and hardening standards shall be maintained in the internal documentation portal. Relevant resources:

- Azure Compliance Resources
- NIST Security Standards