Secure Development Policy

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

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

This policy applies to all VIMBuild, LLC applications and information systems that are business-critical and/or process, store, or transmit confidential data. It also applies to all internal and external engineers and developers of VIMBuild, LLC software and infrastructure.

Policy

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled by formal change control procedures. These procedures shall ensure that development, testing, and deployment of changes are not performed by a single individual without approval and oversight. Significant code changes must be reviewed and approved before merging into production.

Software Version Control

All VIMBuild, LLC software shall be version-controlled. Access to repositories shall be restricted based on employee roles. All code shall be written, tested, and stored in a local repository before syncing to the central repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms change, business-critical applications must be reviewed and tested to ensure security and operational integrity.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be strictly controlled and limited to necessary changes.

Secure System Engineering Principles

Secure development principles shall be documented, maintained, and applied in all system implementation efforts, including:

- **Minimize attack surface area**
- **Establish secure defaults**

- **Least privilege access**
- **Defense in depth**
- **Fail securely**
- **Separation of duties**
- **Avoid security by obscurity**
- **Keep security simple**

Privacy-by-design principles shall also be applied, including:

- **Privacy as the default setting**
- **Privacy embedded into design**
- **End-to-end security**
- **Respect for user privacy**

Secure Development Environment

Development environments shall be logically or physically segregated into:

- Production
- Test / Staging
- Development

Outsourced Development

VIMBuild, LLC shall supervise outsourced system development and ensure compliance with internal security standards and policies.

System Security Testing

Security testing shall be performed throughout the development lifecycle. No code shall be deployed without documented successful test results and security remediation.

Application Vulnerability Management

- Application code shall be scanned before deployment.
- Vulnerability patches must be deployed within 90 days of discovery.

System Acceptance Testing

Acceptance testing shall be conducted before system deployments or major updates. A **Release Checklist** must be completed, showing the completion of all required tests and remediation.

Protection of Test Data

Test data shall be carefully selected and protected. Confidential customer data shall not be used for testing unless explicitly approved.

Acquisition of Third-Party Systems and Software

All acquisitions shall comply with VIMBuild, LLC's **Third-Party Management Policy**.

Developer Training

Developers shall receive annual secure development training, including prevention of:

- Authorization bypass attacks
- Injection attacks
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Use of insecure session IDs
- Use of vulnerable libraries

Exceptions

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

Violations & Enforcement

Violations of this policy should be reported to the Administrator. Non-compliance may result in disciplinary action, up to termination.