Third-Party Management Policy

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

Purpose

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers. This policy establishes baseline security controls for third parties interacting with VIMBuild, LLC confidential data.

Scope

This policy applies to all VIMBuild, LLC data and information systems that are business-critical and/or process, store, or transmit confidential data. It extends to all employees, consultants, contractors, business partners, vendors, suppliers, and other third-party entities with access to VIMBuild, LLC data, systems, networks, or system resources.

Policy

Information Security in Third-Party Relationships

Security requirements for third parties accessing the organization's assets must be documented and agreed upon before engagement.

For service providers who may access VIMBuild, LLC confidential data, systems, or networks, due diligence must be performed before provisioning access. Compliance with regulatory and certification standards such as **ISO 27001, SOC 2, PCI DSS, CCPA, and GDPR** must be documented.

Addressing Security in Agreements

Service agreements shall include:

- Security responsibilities for confidentiality, integrity, and availability.
- Regulatory compliance obligations.
- Access control requirements for customer and company data.

Technology Supply Chain Security

Risk assessments must be conducted on suppliers and service providers. Where warranted, agreements must specify security controls for protecting the supply chain.

Third-Party Service Delivery Management

- **Monitoring & Review:** High-risk third-party services shall be reviewed at least quarterly.

- **Change Management:** Changes to third-party services, agreements, or security measures shall be assessed for impact before implementation.

Third-Party Risk Management

No confidential data shall be shared with third parties without:

1. A **Third-Party Risk Assessment**.
2. A fully executed **written contract, statement of work, or service agreement**.
3. Defined security requirements and service levels.

Third-Party Security Standards

All third parties must maintain reasonable security controls. Assessments shall review compliance in the following areas:

Category	Requirement
Information Security Policy	Maintain policies supported by executive leadership.
Risk Assessment & Treatment	Implement ongoing risk evaluation and mitigation.
Operations Security	Conduct vulnerability testing, network protection, and security monitoring.
Access Control	Enforce strict user authentication and access policies.
Secure Development	Follow secure coding, change management, and review practices.
Physical Security	Comply with VIMBuild, LLC Physical Security Policy.
Human Resources	Conduct background checks on personnel handling confidential data.
Compliance & Legal	Protect customer data, ensure regulatory compliance.

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 may result in system access suspension or disciplinary action, up to termination.