Risk Management Policy

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

Purpose

To define actions to address VIMBuild, LLC information security risks and opportunities. This policy establishes a framework for achieving information security and privacy objectives.

Scope

This policy applies to all VIMBuild, LLC IT systems that process, store, or transmit confidential, private, or business-critical data. It also extends to all employees, consultants, contractors, business partners, vendors, suppliers, outsourced service providers, and other third parties with access to VIMBuild, LLC networks and system resources.

Risk Management Statement

Inadequate IT risk management exposes VIMBuild, LLC to security threats, cyberattacks, legal issues, and reputational damage. VIMBuild, LLC ensures that risk management is integral to organizational governance and business operations at strategic and operational levels.

Risk Management Strategy

VIMBuild, LLC has established processes to identify and mitigate risks that could hinder the achievement of strategic and operational objectives. This strategy ensures that:

- The risk management policy is applied across the organization.
- The policy and its operational application are regularly reviewed.
- Non-compliance is reported to appropriate company officers.

Risk Categories

VIMBuild, LLC classifies risks into the following categories:

- **Reputational**
- **Contractual**
- **Regulatory/Compliance**
- **Economic/Financial**
- **Fraud**
- **Privacy**
- **Environmental & Sustainability**
- **Impact on People**
- **Operational Capacity**

Each risk is assessed based on **likelihood** (scale of 1-5) and **impact** (scale of 1-5).

Risk Criteria

Risk is determined by evaluating:

- Likelihood and impact of adverse events affecting confidentiality, availability, and integrity.
- Organizational and customer information security risks.
- Regulatory compliance risks related to privacy and data protection.

Risk Response, Treatment, and Tracking

Risks are prioritized and maintained in a risk register. Risk responses include:

- **Modify:** Implement actions to reduce the risk.
- **Accept:** Monitor the risk while taking no immediate action.
- **Transfer:** Pass the risk to another party (e.g., insurance, contractual agreements).
- **Avoid:** Cease the activity or change processes to eliminate the risk.

Where applicable, a **Risk Treatment Plan** is developed for mitigation.

Risk Management Procedures

1. Maintain a **Risk Register** and **Treatment Plan**.
2. Rank risks by likelihood and impact.
3. Evaluate risks to estimate potential monetary loss where possible.
4. Respond to risks based on priority and available resources.
5. Provide regular risk management reports to senior leadership.

Risk Acceptance Criteria and Levels

Role	Responsibility
CEO	Approves risk acceptance and treatment decisions.
President	Authorizes risk avoidance, remediation, or transference.
Administrator	Identifies and develops treatment plans for IT security risks. Communicates risks to management.

Risk Assessment Process (Appendix A)

This process follows **NIST 800-30** guidelines:

1. **Prepare**: Establish risk assessment scope and purpose.
2. **Conduct**: Identify threats, vulnerabilities, and likelihood of occurrence.
3. **Communicate**: Share findings with leadership for decision-making.
4. **Maintain**: Continuously monitor and update risk assessments.

Risk Assessment Matrix (Appendix B)

Risk Calculation

Risk Score = **Likelihood** × **Impact**

Risk Level	Description
Low (1-4)	Limited adverse impact.
Medium (5-12)	Serious but manageable adverse impact.
High (15-25)	Severe impact requiring immediate response.

Likelihood Scale

Likelihood Level	Description
1 (Very Unlikely)	< 5% chance in 5-10 years.
2 (Unlikely)	6-20% chance in 2-5 years.
3 (Somewhat Likely)	21-50% chance in 1-2 years.
4 (Likely)	51-80% chance in 1 year.
5 (Very Likely)	> 80% chance in 1 year or less.

Impact Scale

Impact Level	Description
1 (Very Low)	Minimal impact on operations.
2 (Low)	Some disruptions, but primary functions remain intact.
3 (Medium)	Significant degradation of mission capability.
4 (High)	Major financial or operational damage.
5 (Very High)	Severe consequences for organization-wide operations.

Exceptions

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

Violations & Enforcement

Any violations should be reported to the Administrator. Non-compliance can result in disciplinary actions, including termination.