Information Security Policy

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

Overview

This Information Security Policy is intended to protect VIMBuild, LLC's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, web browsing, and file transfers, are the property of VIMBuild, LLC. These systems are to be used for business purposes in serving the interests of the company, its clients, and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every VIMBuild, LLC employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of VIMBuild, LLC's information and assets. These rules are in place to protect customers, employees, and VIMBuild, LLC from risks including virus attacks, compromise of network systems and services, financial and reputational risks, and legal and compliance issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct VIMBuild, LLC business or interact with internal networks and business systems, whether owned or leased by VIMBuild, LLC, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at VIMBuild, LLC and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with VIMBuild, LLC policies, standards, and local laws and regulations.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible using designated reporting channels.

Whistleblower Anonymous Fraud Reporting

VIMBuild, LLC encourages employees and others to raise serious concerns internally so that inappropriate conduct and actions can be addressed and corrected. Retaliation against employees who report ethics violations or suspected legal violations in good faith is strictly prohibited.

Anonymous reports may be submitted from a self-provisioned email address to the Administrator.

Mobile Device Policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening email attachments from unknown senders, which may contain malware.

Key requirements:

- Devices must be locked with a password or equivalent control (e.g., biometric) and auto-lock after 5 minutes of inactivity.
- Confidential information must not be stored on mobile devices or USB drives unless encrypted.
- Company-owned devices must be returned upon termination, and company data must be removed from personal devices.

Clear Screen/Clear Desk Policy

Users shall not leave confidential materials unsecured on their desks or workspaces and must ensure screens are locked when not in use.

Remote Access Policy

Laptops and other resources used to access the VIMBuild, LLC resources must conform to security requirements, including:

- Use of antivirus software with automatic updates enabled.
- Use of multi-factor authentication (MFA) for remote access.
- Prohibition of unauthorized remote access software.
- Secure public Wi-Fi usage policies.

Acceptable Use Policy

VIMBuild, LLC proprietary and customer information stored on computing devices, whether owned by VIMBuild, LLC, employees, or third parties, remains the sole property of VIMBuild, LLC. Employees are responsible for reporting theft, loss, or unauthorized disclosure of company information or equipment.

Unacceptable Use

The following activities are strictly prohibited:

- Violations of intellectual property laws, including unauthorized software distribution.
- Unauthorized access to company data or servers.
- Introduction of malicious programs (e.g., viruses, worms, Trojans).
- Sharing of account credentials.
- Engaging in fraudulent or deceptive activities using company resources.
- Security breaches or unauthorized network monitoring.
- Circumventing security controls or installing unauthorized remote access tools.

Email and Communication Activities

Employees must exercise caution when using company resources for communication. Prohibited activities include:

- Sending unsolicited bulk emails (spam).
- Harassment via email, phone, or messaging platforms.
- Forging email headers or impersonating others.
- Participating in chain letters, Ponzi schemes, or other fraudulent activities.

Exceptions

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

Violations & Enforcement

Any known violations should be reported to the Administrator. Violations may result in immediate withdrawal of system and network privileges and/or disciplinary action, up to and including termination.