Information Security Roles and Responsibilities Policy

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

Statement of Policy

VIMBuild, LLC is committed to conducting business in compliance with all applicable laws, regulations, and company policies. VIMBuild, LLC has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy and associated guidance establish the roles and responsibilities within VIMBuild, LLC, which are critical for effective communication of information security policies and standards. Clearly defined roles help ensure responsibility and coordination in protecting information assets.

Applicability

This policy applies to all VIMBuild, LLC infrastructure, network segments, systems, employees, and contractors who provide security and IT functions.

Audience

This policy applies to all VIMBuild, LLC employees and contractors involved with the Information Security Program. Other agents with access to company information and infrastructure, including partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers, must also comply with this policy.

Roles and Responsibilities

Role	Responsibilities
Board of Directors	- Provides oversight of cyber-risk and internal control for information security, privacy, and compliance. - Consults with Executive Leadership to align business, IT, and security objectives.
CEO	- Approves capital expenditures for Information Security and Privacy programs.
President	- Communicates security objectives to the CEO, Board of Directors, and Administrator
Administrator	- Oversees execution of the information security risk management program. - Provides security training and evaluates employee adherence to company policies.

Role	Responsibilities
IT Managers	- Implements information security controls for IT infrastructure. - Conducts IT risk assessments and maintains the risk register. - Develops and enforces information security policies and standards. - Coordinates security awareness programs and liaises with internal stakeholders. - Maintain confidentiality, integrity, and availability of assigned systems. - Approve access and change requests for systems under their control.
Head of Product	- Oversees security in the software development process. - Implements security controls in development and cloud hosting environments. - Ensures risk management in software development aligns with company goals.
Head of Finance	- Reviews vendor service contracts.
Employees & Contractors	- Follow security best practices and company policies. - Report security incidents and risks. - Help identify areas where risk management practices should be applied.

Policy Compliance

The Administrator will measure compliance with this policy through reports, internal/external audits, and feedback to policy owners.

Exceptions

Exceptions to this policy must be approved by the Administrator in advance.

Violations & Enforcement

Non-compliance with this policy will be addressed with management and Human Resources and may result in disciplinary action, up to and including termination of employment.