Access Control Policy

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

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All VIMBuild, LLC information systems that process, store, or transmit confidential data as defined in the VIMBuild, LLC Data Management Policy. This policy applies to all employees of VIMBuild, LLC and to all external parties with access to VIMBuild, LLC networks and system resources.

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

VIMBuild, LLC shall determine the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by VIMBuild, LLC's business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

VIMBuild, LLC's primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

Access to Networks and Network Services

The following security standards shall govern access to VIMBuild, LLC networks and network services:

- Technical access to VIMBuild, LLC networks must be formally documented including the standard role or approver, grantor, and date.
- Only authorized VIMBuild, LLC employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the VIMBuild, LLC production networks and resources.
- VIMBuild, LLC guests may be granted access to guest networks after registering with office staff without a documented request.
- Remote connections to production systems and networks must be encrypted.

User Access Management

VIMBuild, LLC requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed. If a password is compromised or suspected of compromise, the incident should be escalated to the IT Team immediately and the password must be changed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new users, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or VIMBuild, LLC management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any VIMBuild, LLC security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

Users shall be promptly disabled or removed when users leave the organization or contract work ends in accordance with SLAs.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any VIMBuild, LLC production systems until after they have completed all HR onboarding tasks.
- Access should be restricted to only what is necessary to perform job duties.
- No access may be granted earlier than the official employee start date.
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or management.
- Records of all permission and privilege changes shall be maintained for no less than one year.

Management of Privileged Access

Granting of administrative rights shall be strictly controlled and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of VIMBuild, LLC assets.

Password Policy

- Minimum 8 characters, including one uppercase letter and one number.
- Initial passwords must be set to a unique value and changed after first login.
- No use of security questions as sole password reset requirement.
- Require email verification for password changes.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required.

Access to Program Source Code

Access to program source code and associated items shall be strictly controlled to prevent unauthorized functionality from being introduced into software and to protect VIMBuild, LLC intellectual property.

Exceptions

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

Violations & Enforcement

Any known violations of this policy should be reported to the Administrator. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.