# Access Management Policy

| | |
|---|---|
| **Version number** | 2.2 |
| **Last Approved** | Apr 21, 2025 |
| **Classification** | PUBLIC |

## Overview

This Access Management policy describes provisioning, management, monitoring, and de-provisioning of user accounts and privileges, operating under the principle of least privilege.

### Applicability

The applicability of this statement falls under purview of the Security Documentation Overview .

### Purpose

Access management controls are key to ensuring that the correct employees and contractors have access to the correct data and systems with the correct level. The Company's access controls are guided by the principle of least privilege and need-to-know to ensure security and privacy. The Access Management Policy shall outline the Company's standard for user access management across all systems.

### Scope

This policy applies to employee/contractor access to systems that process or store customer data.

# Access Management Policy

***Principle of Least Privilege***

Access controls must be allocated on the basis of business need and ‘Least Privilege’. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

### User Access Account Management

User account management procedures must be implemented for user provisioning, modification, and de-provisioning on all Company systems.

Procedures shall be established for all information systems to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organization.

All additions, deletions, suspensions and modifications to user accesses should be captured in an audit log showing who took the action and when.

### Access Monitoring

User access management reviews will be conducted quarterly for in-scope systems.

Access reviews will validate the consistency and effectiveness of access provisioning and deprovisioning processes for all in scope systems including the appropriate allocation of roles and privileges.

All user accounts that have not been accessed for a period of inactivity appropriate for the systems, without prior arrangement, must be disabled.

### Authentication

All access to Company information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user’s identity. Additional authentication requirements are detailed within the Password Policy.

Access to networks occurs through MFA and VPN, controlled by various user access groups.

### Unique Account Identifiers

All individual user IDs must be unique for each user.

Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorized by

appropriate Management.

Shared accounts are prohibited by default. Exceptions must be authorized by appropriate management.

### Privileged Access

All administrative/privileged user accounts must be based upon job function and authorized by the appropriate management, prior to access being given. All changes to privileged accounts must be logged and regularly reviewed.

User accounts for privileged access must be separate from a user's normal user account (for non-privileged access).

Passwords for privileged user accounts must be rotated at least annually where MFA is in place and quarterly without MFA.

### Management Oversight

#### VP of Information Security

The VP of Information Security is responsible for ensuring that the requirements of this policy are implemented within any program, projects, systems or services for which they are responsible.

The VP of Information Security is responsible for ensuring that a robust checking regimen is in place and complied with to ensure that legitimate user access is not abused.

The VP of Information Security may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regimen.

#### Managers

Managers are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job and comply with role-based access principles.

#### System Custodians

System Custodians are privileged users responsible for administering system access. Custodians are responsible for collaborating with Managers to determine how to appropriately define and allocate roles and permissions to Users.

System Custodians are empowered to make access approval and exception decisions within the scope of the systems they administer.

System Custodians are responsible for ongoing monitoring of user access to the systems they administer, independently of formalized quarterly access reviews.

Users

Users must only access Company systems and data for legitimate use as required by their job and role.

## Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview .

---

## Document control

> This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

| | | |
|---|---|---|
| **Document Owner** | @Art Machado | |
| **Author(s)** | @Art Machado | |
| **Required Approver(s) and Approval Date** | @Art Machado - VP Information Security | Apr 21, 2025 |
| | | |
| **Review cycle** | ANNUAL | |
| **Next review date** | Feb 20, 2026 | |

### Version History

| Date | Author(s) | Version | Changes |
|---|---|---|---|
| Apr 21, 2025 | @Art Machado @angelina.kilmer | 2.2 | Added details regarding System Custodian responsibilities. |
| Mar 3, 2025 | @Art Machado | 2.1 | Privileged account update |

| | | | |
|---|---|---|---|
| Feb 21, 2025 | @Art Machado @Paul Gordon @angelina.kilmer | 2.0 | Annual Review |
| Nov 01, 2024 | @angelina.kilmer | 1.6 | Updated Policy classification from Confidential to Public |
| Mar 12, 2024 | @Art Machado, @Sarah Zwicker (Unlicensed) @Paul Gordon | 1.5 | Annual review |
| Dec 4, 2023 | @Sarah Zwicker (Unlicensed) | 1.4 | Linked Password Policy |
| Aug 29, 2023 | @Sarah Zwicker (Unlicensed) | 1.3 | Removed ISO Annex control language |
| Feb 23, 2023 | @Art Machado, @Sarah Zwicker (Unlicensed) | 1.2 | Annual review + logo updated |
| Apr 13, 2022 | @Sarah Zwicker (Unlicensed) | 1.1 | Initial Review and Approval |

| | | | |
|---|---|---|---|
| Mar 31, 2022 | @Art Machado, @Sarah Zwicker (Unlicensed) | 1.0 | Original version |