Access Management Policy

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

# Purpose

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

# Scope

All [Company Name] information systems that process, store, or transmit confidential data as defined in the [Company Name] Data Management Policy. This policy applies to all employees of [Company Name] and to all external parties with access to [Company Name] engineering 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

[Company Name] grants access to systems on the “principle of least privilege.ˮ This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by [Company Name]ʼs business and security requirements.

[Company Name]'s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control RBAC. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party and documented within the ticketing system.

# All privileged access to production systems should use Multi-Factor Authentication MFA.

**Access to Networks and Network Services**

The following security standards shall govern access to [Company Name] networks and network services:

 [Company Name] 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 w/ SSL and TLS.

# User Access Management

[Company Name] leverages Okta for management of user access. Okta is subject to all access management policies.

[Company Name] requires that all personnel have a unique user identifier for system access, and that user credentials. 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.

# User Registration and De-registration

 Only authorized IT administrators shall be permitted to create new user IDs  User IDs shall be promptly disabled or removed when users leave the

organization or contract work ends. User IDs shall not be re-used.

# User Access Provisioning

 Access should be restricted to only what is necessary to perform job duties  Access shall be granted based on the access matrix. Additional permissions

requested will be documented within the ticketing system and approved by system owner.

# User Access Reviews

Administrators shall perform access rights reviews of production systems on at least a semi-annual basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

# 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 and documented within the company ticketing system. The maximum allowable time period for access termination is 24 business hours.

In the event an account is required to be active after the employee has been terminated, the request is noted within the off-boarding ticket.

In the event an account is required to be re-activated, the request is documented within a ticket.

# User Responsibility for the Management of Secret Authentication Information

Control and management of individual user passwords is the responsibility of all [Company Name] personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

# System and Application Access Information Access Restriction

Restrictions to applications is based on individual application requirements taking into account the risk of access and the requirements to perform job duties.

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all [Company Name] systems, devices, and infrastructure prior to deployment.

# 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.

# Password Management System

Systems for managing passwords should be interactive and assist [Company Name] personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible.

All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

# Exceptions

Requests for an exception to this Policy must be submitted to the Director of Security, Engineering or the Head of IT for approval.

# Violations & Enforcement

Any known violations of this policy should be reported to the Director of Security, Engineering or the Head of IT. 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.

# Appendix A Summary of Access Provisioning Procedure

During the onboarding process, a service ticket will be generated for access. IT will provision access dependent on role matrix and additional requests made by the manager. Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

# Related Documentation:

Access Matrix:

Default Role Access Matrix  Access Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** | **Approved by** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |