**Purpose and Scope**

This Access Control and Termination Policy defines requirements for access and removal of access to [Organization Name] data, systems, facilities, and networks. From time to time, [Organization Name] may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to [Organization Name] including applicable laws and regulations.

 This policy applies to all [Organization Name] assets or approved devices utilized by personnel acting on behalf of [Organization Name] or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept, and follow all [Organization Name] policies and procedures.

**Access Control Requirements**

**Principle of Least Privilege**

[Organization Name] adheres to the principle of least privilege, specifying that users of [Organization Name] systems will be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user. Access to systems will be provisioned via a deny-all methodology - users will only gain access to a system upon receiving formal independent approval.

Administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access. Authorized individuals with administrative access shall be listed in the “Authorized Administrative Access” form.

Access to systems and applications must be controlled by a secure log-on process to prove the identity of the user.

**Unique Accounts**

Users of [Organization Name] systems and applications will be provided with unique credentials (System user names, IDs, keys, etc.) that can be used to trace activities to the individual responsible for that account. Shared user accounts shall only be utilized in circumstances where there is a clear business benefit and when user functions do not need to be traced. Shared account password shall only be stored in a [Organization Name] approved password manager.

[Organization Name] shall disable or delete all default users on all organizational systems before those systems are deployed for use.

**Password Security**

Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with multiple users. Where possible, all user and system account passwords must be a minimum of eight characters and complex. All accounts must use unique passwords not used elsewhere.

**Rotation Requirements**

 If an account is suspected to be compromised, the password should be reset and the security team should be immediately notified.

**Storing Passwords**

Passwords must only be stored using a [Organization Name] approved password manager. [Organization Name] does not hard code passwords or embed credentials in static code.

**Multi-Factor Authentication**

When available, multi-factor authentication should be used. Multi-factor authentication must be used for access to company email, version control tool and cloud infrastructure.

**Onboarding Procedures**

In order to onboard new personnel, the following steps should be taken and documented:

1. Any [Organization Name] devices provided to the new hire must be inventoried in accordance with [Organization Name] policy
2. A new hire email or ticket must be sent to the appropriate team to inform them of new personnel
3. IT/Engineering and the new personnel’s manager must document a checklist of accounts, groups and permission levels needed for that hire
4. The applicable team must set up each user with the appropriate access, both logical and physical
5. All of the onboarding processes must be appropriately documented via ticketing or other document management tools

**Offboarding Procedures**

In order to offboard an employee or contractor, the following steps must be taken:

1. An offboarding email or ticket must be sent to IT/Engineering when personnel has been terminated or resigned informing IT/Engineering of the team members’ last day
2. IT/Engineering must review and perform action against the appropriate revocation checklist to revoke access to [Organization Name] systems, applications, and physical access points (as applicable) within 24 hours of the last day with the company or sooner if necessary
3. Any [Organization Name] devices provided must be collected and accounted for in accordance with [Organization Name] policy
4. All of the offboarding processes must be appropriately documented via [Organization Name] ticketing or other document management tools

**Change to Access**

Requests for changes to access level(s), such as in the cases of a change in job duties or an emergency requiring elevated permissions, must be documented and approved by the appropriate manager.

A documented request must be sent to the appropriate department when an employee or contractor role changes to evaluate whether access privileges should be changed. When accounts are no longer required, user access rights must be reviewed and reallocated as necessary prior to changes being made.

Such changes must be tracked using the [Organization Name] ticketing or other document management tools.

**Processes Acting on Behalf of Users**

[Organization Name] shall track all processes acting on behalf of users and their access levels in the “Authorized Processes” form.

**Quarterly Access Reviews**

A team manager must review, audit, and document user accounts and associated privileges of at least high-risk, critical systems and contractual file systems at least quarterly to ensure that access is documented and restricted appropriately.

IT/Engineering must review and audit the documented system accounts and associated privileges listed in the “Access Control Policy” form for all system accounts.