# Information Security Standard – Personnel and Separation of Duties

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the personnel security controls to be implemented across all of {Company}’s systems.

## Applicability

Compliance with the controls outlined in this document is mandatory for all {Company} employees, contractors, vendors, and guests.

## Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

## Scope

The requirements of this standard to all systems that store, process, or transmit {Company} information; or are used to connect to those systems that are used to store, process, or transmit {Company}’s information.

## Controls

1. All {Company} personnel must be properly vetted and assigned appropriate roles and permissions, and those permissions periodically reviewed through both automated and manual means.
2. All {Company} personnel shall be subject to the same stringent screening requirements upon hire, and all positions are treated as equal in business risk and potential impact. Personnel shall only be assigned access to those systems required to perform their role.
3. Personnel shall be screened before starting their role, and every 5 years thereafter, with the following minimum checks to occur:
   1. SSN Trace
   2. Multi-State ICC
   3. Statewide search for 7 years with address verification
   4. Education verification
   5. Employment verification.
4. All non-FTE staff must provide equivalent background check documentation to {Company} before having access granted to any {Company} systems or information.
5. Managers shall follow the IT-Designated termination process immediately upon learning that personnel will be separating from the company. Those separating from the company shall be reminded of their contractual and legal responsibilities to protect {Company} data and systems, even after separation.
6. Personnel transferring between roles shall have their access to systems associated with their previous role revoked and new access permissions based on the requirements for their new role granted.
7. All employees shall conform to the Rules of Behavior and acknowledge their understanding annually.
8. Separation of Duties shall be followed as outlined below:
   1. The {Company} Platform’s role-based access controls allow customers to enforce a separation of duties within the common workflows. Managing overall access and role mappings to the site is limited to those with Administrator privileges. Implementation of these separations is the responsibility of the customer.
   2. Within the {Company} organization, separation of duties is implemented through the management of accounts based on role. As a general guideline, software engineers have system-level access, managers and select leads may additionally provision accounts, while operations and security also have infrastructure access including knowledge of infrastructure accounts where necessary. Information technology staff have access to systems used for account provisioning and user management.
   3. Shared accounts or systems with a single login are managed via LastPass, with credentials rotated every 60 days.
9. Training - All personnel should receive general information security training upon hire and at least annually thereafter. Additionally, specialized role-specific training should be provided annually for all developers and personnel with elevated levels of access to production systems or code repositories.

## Roles

### Software Engineers

Software engineers are responsible for building, operating, and maintaining {Company}’s platform. In this role, they are granted system-level access to the underlying information system (for example, through SSH and VPN) via individual user accounts. Privileged system operations are performed by elevating access through the use of the sudo command; such access is centrally logged as part of the common audit logging infrastructure. Individuals are responsible for all activity related to their user ID.

Software engineers are granted access to 3rd party services that support {Company} systems and operations via individual accounts, or where multiple accounts are not supported by a provider, via shared credentials managed via LastPass and rotated every 60 days.

### 

### Engineering Managers and Select Engineers

Engineering Managers and Select Engineers (as approved by a Director or higher-level leader in engineering) have permissions to provision approved user access where systems allow for the distinction. For example, granting access to {Company} repositories to other employees and provisioning system-level access via SSH. These employees are expected to adhere to these guidelines when provisioning accounts.

### Operations and Security Team Members

Operations and Security Team members are responsible for managing the underlying infrastructure at {Company}. They are granted administrative access to infrastructure accounts including DNS management, SSL, root, firewall administration, and AWS.

### 

### Information Technology Staff

Information Technology staff are responsible for central account provisioning and have Administrative access to centralize services including account management and LastPass.

### Support Staff

Support staff are responsible for customer user account management and troubleshooting customer issues. In this role, they have elevated access to the {Company} portal and may be granted system-level access to the underlying information system (for example, through SSH and VPN) via individual user accounts. Privileged system operations are performed by elevating access through the use of the sudo command; such access is centrally logged as part of the common audit logging infrastructure. Individuals are responsible for all activity related to their user ID.

Support staff are granted access to 3rd party services that support {Company} systems and operations via individual accounts, or where multiple accounts are not supported by a provider, via shared credentials managed via LastPass and rotated every 60 days.

### Professional Services Staff

Professional Services staff are responsible for onboarding customers as well as providing support and assistance for troubleshooting customer issues. In this role, they have elevated access to the {Company} portal and may be granted system-level access to the underlying information system (for example, through SSH and VPN) via individual user accounts. Privileged system operations are performed by elevating access through the use of the sudo command; such access is centrally logged as part of the common audit logging infrastructure. Individuals are responsible for all activity related to their user ID.

Support staff are granted access to 3rd party services that support {Company} systems and operations via individual accounts, or where multiple accounts are not supported by a provider, via shared credentials managed via LastPass and rotated every 60 days.

### Non-engineering Staff

Read-only or no access to production infrastructure. Any exceptions due to job requirements are made on a case-by-case basis with approval from the Security team and their managers.

### Platform User Roles

{Company} has documented the procedures for managing user roles at {insert location}. Any policies are specific to, and the responsibility of, the individual customer.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.1 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |