# Information Security Standard – Identification, Authorization, and Access Control

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the minimum controls for Identification, Authorization and Access 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 systems shall conform to the requirements outlined in the {Company} Information Classification Standard for the level of authentication required based on the information stored on the system.
2. All users shall have separate and unique accounts for user access and administrative access. Accounts used for administrative access should only be used for that purpose, and only have the minimum level of access required for the employee to accomplish the requirements of their job or role. Wherever possible, separation of duties principles shall be used to prevent single individuals from accumulating excessive access.
3. Temporary or emergency accounts are not allowed on {Company} systems.
4. Administrative access to production systems is limited to those employees directly involved in maintaining, updating, and supporting the production systems. All access to the production systems shall be via a two-factor VPN connection and terminate on a bastion host. Direct access to the production environment from end-user workstations is specifically proscribed. Direct ‘root’ access is never allowed; all employees are first required to connect via their user accounts and then use sudo or equivalent to achieve the level of access required.
5. At a minimum, all systems used to access {Company}’s non-public information assets shall conform to the following:
   1. Anti-malware software that is running continually, configured to automatically update at least daily, and performs full system scans weekly.
   2. Unique usernames for all users of the system
   3. Strong passwords for all users (>12 characters, with at least 1 number, capital, and symbol), that are changed at least every 90 days
   4. Hard drives that provide encryption of at least the user’s directories on the host
   5. Remote management software installed that can lock or erase the system in the event of loss
   6. Screen lock after 15 minutes of inactivity.
   7. Are not left unattended in an insecure area.
6. Any accounts that have not been logged into or otherwise seen active use shall be programmatically disabled after 30 days.
7. All accounts with administrative access to production and Internet-facing systems are to be reviewed for accuracy every 30 days by the appropriate system administrator. This shall include but is not limited to Admins, Service Accounts, Sudoers, and Database accounts. All other accounts shall be reviewed at least every 180 days.
8. All Admin account access to production systems/environments is limited to those CS and Engineering staff providing direct support to customers or part of the on-call rotation. Two-Factor Authentication is required for all interactive Admin access.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 20 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |