Access Control Policy

Purpose

The purpose of this policy is to establish the principles and guidelines for controlling access to systems owned by <Company Name>.

Scope

The policy applies to all employees and contractors, and the accounts they use in connection with fulfilling their responsibilities to <Company Name>.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

Access to systems at <Company Name> must be controlled to ensure only authorized users and applications can access customer and corporate data. Access and access controls must abide by the following principles:

- Deny-by-default: Access must be denied by default. Gaining access requires an explicit configuration step
- Least-privilege: Users and processes must be granted the lowest permission level necessary to perform their role
- Auditability: Access grants are explicitly requested and approved, and an audit trail is persisted

Least-privilege access

Access to sensitive systems and resources is granted based on the principle of least privilege.

The Principle of Least Privilege states that a subject should be given only the privileges needed to complete their task or responsibility. If a subject does not need an access right, the subject should not have that right. In addition, the assignment of rights to a subject should be based on that subject's function and role, rather than the subject's identity or rank.

Each <Company Name> employee and contractor has limited access to <Company Name> systems, data and applications. Access is always provisioned to the minimum necessary for the individual to perform their duties and serve the business purpose of their role.

The Principle of Least Privilege is applied not only to user accounts, but also to application-to-application service accounts, machine roles, operating system permissions, private interfaces, as well as the entire publicly-accessible surface of <Company Name>'s systems. Each permission context is reviewed to ensure that only the minimum required rights are granted.

In order to refine access grants over time, and bolster the initial role-based approach, automated tools may be used to continuously monitor access privileges and flag unused ones to be reviewed for revocation.

Role-based access control

Defined permission roles are utilized to assign and segregate access privileges to data and systems.

In a role-based access control approach, access to resources is determined based on roles that reflect a user's set of responsibilities, rather than granted individually for each user. A role-based approach reduces permission customization, improves scalability as teams grow, reduces the likelihood of misconfigured permission settings, and simplifies the access review process.

A default least-privilege role allows for easy onboarding of new users, and reduces the likelihood that users are granted more access than they need.

<Company Name> employees are granted access to systems according to their role and their team.

If a <Company Name> employee requires access outside of that provided by their role or team, the employee initiates an access request following the policy outlined in the "requesting and approving access" section.

Requesting and approving access

Access to systems is requested by filing an internal access request ticket specifying the need for the access. Access is approved by the respective manager and granted by administrators based on a least-privilege principle.

Initial access to systems is granted as part of the employee onboarding process, which is documented in full in <Company Name>'s internal knowledge base. Access requests for new employees are typically filed by the employee's manager. The ticket trail must contain an explicit approval by the owner of the respective system.

Temporary access

Additional access with privileges exceeding those necessitated by regular duties may be granted on a temporary basis. Each temporary access grant must be accompanied by a valid business purpose, such as an ongoing incident or an operational alert that may lead to an incident if not resolved.

In all cases, access must be revoked immediately once the original business need for the grant no longer exists.

Temporary access grants must be treated as an exception and kept to a minimum. Recurring exceptions must be investigated, and the necessary tooling must be created to alleviate the need for repeated privilege escalation.

Termination process

Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.

To ensure access is revoked immediately, Human Resources or the manager of the departing employee or contractor must file an offboarding ticket as soon as access is no longer needed.

Role changes

An equivalent access revocation checklist is executed when employees change roles within <Company Name>. New roles may require substantially different access profiles, so it is important that such an event is handled consistently.