System Access & Authorization Control Policy

Each Reveal employee, contractor, and associate has limited access to Reveal systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis.

Employee Access to Reveal Systems

Access to Reveal systems and third-party accounts owned by Reveal will only be granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of that position.

Access control and management is divided into multiple phases of an account lifecycle: creation, privilege management, authorization, password management, audit, and revocation.

Authorization: Role Based Access Control

- In most cases, Reveal employees are granted access to Reveal systems according to their role and/or team.
- The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members.
- If a Reveal employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the policy outlined in “access requests” below.

Creation: Access Requests

- Access requests for Reveal employees are made by Jira.
- Access requests should be made to the Reveal employee or employees who manage the relevant resource(s).
- Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.
- When granting access, employees will ensure grants are scoped to the minimum breadth and duration to complete the relevant business task. Root access will not be granted unless absolutely necessary to perform the job function.
- In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted.

Privilege Management

- Reveal’s CTO will determine and maintain appropriate assignment of privilege within Reveal’s production, development and test applications and environments.
- Reveal’s CTO will determine and maintain appropriate assignment of privilege within Reveal’s databases.
- Reveal’s CTO will determine and maintain appropriate assignments within supporting infrastructure.

Account Audit

- The responsible team will conduct quarterly audits of accounts, privileges and password management, and is required to document findings and changes.

Revocation: Role Changes & Termination

- Managers must notify Reveal's CTO if an employee has been terminated or changes role.
- In the case of termination, the former employee’s access is required to be revoked within reasonable timelines as defined by company procedural commitments in Vanta.
- In the case of a role change, the employee’s access should be revised within reasonable timelines as defined by company procedural commitments in Vanta.
- In some cases, access will be revoked as a disciplinary measure for policy violation.

Employee Authentication to Reveal Systems

Authentication

Each Reveal employee has a unique user ID and password that identifies them as the user of a Reveal IT asset or application. All assets, applications and vetted third party platforms may be required to have two-factor authentication configured.

Password, Key, and Certificate Management

As specified in the Acceptable Use Policy and Password Policy, Reveal employees must use complex passwords and multi-factor authentication for all Reveal-related accounts. User passwords must conform with the restrictions set forward in the Reveal Password Policy. Please see Acceptable Use Policy and Password Policy for further details and guidance.

Reveal's CTO is responsible for issuing and revoking SSH keys in all environments.

Reveal's CTO is responsible for issuing, renewing, and revoking public web and internal SSL certificates.

Customer Data

Employees that require access to customer data must have an individual account. This account, as well as actions performed with it, will be subject to additional monitoring at the discretion of the management team and subject to applicable regulations and third-party agreements.

At a minimum, employees with access to customer data can expect that their actions in customer-data systems (e.g. an internal admin tool) will be logged, with the logs stored centrally for at least 1 year.

Guest Access to Reveal Systems

Occasionally, guests will have a legitimate business need for access to the corporate network. When such need is demonstrated, temporary guest access to company systems is permitted. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest’s work is completed.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee’s offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations that lead to security incidents, employees may face severe disciplinary actions up to and including termination.
- Reveal employees will not be disciplined for surfacing deficiencies or misconfigurations that contradict this policy.

Responsibility

Each Reveal employee is responsible for surfacing technical misconfigurations and deficiencies to the CTO for immediate resolution.

The CTO is responsible for ensuring this policy is followed.

Last updated: 2021-10-19