Access Onboarding and Termination Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.2, CC6.3

1 Purpose and Scope

a. The purpose of this policy is to define procedures to onboard and offboard users to technical infrastructure in a manner that minimizes the risk of information loss or exposure.

b. This policy applies to all technical infrastructure within the organization.

c. This policy applies to all full-time and part-time employees and contractors.

2 Background

a. In order to minimize the risk of information loss or exposure (from both inside and outside the organization), the organization is reliant on the principle of least privilege. Account creation and permission levels are restricted to only the resources absolutely needed to perform each person's job duties. When a user's role within the organization changes, those accounts and permission levels are changed/revoked to fit the new role and disabled when the user leaves the organization altogether.

3 Policy

a. *During onboarding:*

   i. Hiring Manager informs HR upon hire of a new employee.

   ii. HR emails IT to inform them of a new hire and their role.

   iii. IT creates a checklist of accounts and permission levels needed for that role.

   iv. The owner of each resource reviews and approves account creation and the associated permissions.

   v. IT works with the owner of each resource to set up the user.

b. *During offboarding:*

   i. Hiring Manager notifies HR when an employee has been terminated.

   ii. HR notifies IT immediately (within 4 hours) upon confirmation of employee termination. For involuntary terminations, IT is notified before or at the time of termination.

   iii. IT terminates all access within 24 hours of receiving notification. For involuntary terminations or security-related separations, access must be revoked immediately (within 4 hours).

c. *When an employee changes roles within the organization:*

   i. Hiring Manager will inform HR of a change in role.

ii. HR and IT will follow the same steps as outlined in the onboarding and offboarding procedures.

d. *Review of accounts and permissions:*

i. Each month, IT and HR will review all accounts and permission levels for accuracy.

ii. Privileged accounts (admin, root, and any account with elevated system access) must undergo a separate quarterly access review. Results must be documented and stored as audit evidence.

iii. Any accounts identified as unnecessary or incorrectly provisioned during reviews must be remediated within 5 business days of discovery.

4 API Authorization Requirements

a. Every GraphQL query, mutation, and REST endpoint that returns or modifies merchant, lender, loan, payment, or personal data must enforce **both** authentication and **role-based authorization**. Authentication alone is not sufficient: a valid session establishes *who* is calling, not *what they may see*.

b. Resolvers must declare their required role explicitly. Where a role guard is omitted, the effective audience is **every authenticated user of every role**, including consumers.

c. Queries returning a model that contains any credential, secret, or token field must apply an explicit field selection or a restricted response type rather than returning the full record. A dedicated public or restricted type should be used where a subset of fields is needed by a lower-privilege caller.

d. Credentials, secrets, and tokens must not be exposed as API fields at all unless a documented business need requires reading them back.

e. **Known exception.** The single-merchant lookup enforces authentication only, with no role restriction, while every sibling merchant operation is restricted to administrators. It returns the complete merchant record including the stored POS credential. **Any authenticated user of any role can read a merchant's live POS access credential.** *Owner: Technical function. Severity: Critical. Target date: [TBD].*

f. Prior to SOC 2 fieldwork, a **complete authorization review of every API operation** should be performed to confirm that no other operation omits a role restriction or returns unselected sensitive fields.