

# Access Review and Revocation Process

---

## Overview

This document outlines the process for regularly reviewing and revoking access privileges to ensure that only authorized personnel have access to organizational resources.

## Review Schedule

- **Quarterly Access Reviews:** Conducted every 3 months
- **Emergency Reviews:** Conducted immediately upon employee termination or role change

## Process Steps

### 1. Quarterly Access Review

**When:** First week of each quarter (January, April, July, October)

**Who:** IT Administrator and Department Managers

**Steps:**

1. Generate user access reports from all systems:

- Google Cloud Platform (GCP) IAM
- Amazon Web Services (AWS) IAM
- Kubernetes RBAC
- Database access (PostgreSQL)
- Storage bucket permissions
- Doppler (secrets management)
- Docker Hub (container registry)
- Central (document management)
- Slack workspaces
- OneLeet (compliance platform)
- Any third-party services

2. Review each user's access against their current role

### 3. Identify users who:

- No longer need access to specific systems
- Have changed roles and need different permissions
- Are no longer with the organization

### 4. Document findings in access review spreadsheet

## 2. Access Revocation Process

### Immediate Revocation (Employee Termination)

1. Disable user accounts in all systems within 24 hours
2. Remove from all Google Cloud IAM roles
3. Remove from AWS IAM roles and policies
4. Remove Kubernetes service accounts and RBAC bindings
5. Revoke database access
6. Remove from storage bucket permissions
7. Remove from Doppler projects and secrets access
8. Remove from Docker Hub organization
9. Remove from Central document access
10. Deactivate Slack accounts
11. Remove from OneLeet compliance platform
12. Document revocation with timestamp and reason

### Regular Revocation (Role Changes)

1. Review current permissions vs. new role requirements
2. Remove unnecessary permissions
3. Add required permissions for new role
4. Test access to ensure functionality
5. Document changes with approval from manager