Sample Access Control Policy

DRAFT · Policy AC-01 / Version 0.1

All people, accounts, configurations, review outcomes and implementation statements in this kit are invented for training. No CUI, export-controlled information, real contract data or credentials are included. Do not submit these files to SPRS, an assessor or a contracting officer as evidence of real implementation.

Purpose · 3.1.1 and 3.1.8

Limit access to authorized users and establish a documented response to unsuccessful logon attempts. Applies only to the fictional Apex Lab Workspace.

Authorization workflow

1. IT lead records the requested role and business reason.
2. Owner documents approval before provisioning.
3. IT lead applies least privilege and retains the authorization record.
4. Consultant reviews the register and flags missing approvals.
5. Owner makes the decision to remove or approve unresolved access through an authorized change process.

Sample login standard

For this exercise only: 5 failed attempts within 15 minutes trigger a 15-minute lockout. This is a fictional organization-selected setting, not a universal compliance threshold. Real systems require an appropriate documented policy and functional verification.

Review evidence

Retain approvals, dated reviews, sanitized configuration exports and functional test records. A policy expresses intent; implementation cannot be established from policy text alone. No policy signature is included: this document is AI-DRAFTED and unapproved.