Firstsource Risk / InfoSec — Access Control SOP (v1.0)

Document ID: FS-SEC-AC-SOP
Owner: Information Security
Effective Date: 04 Nov 2025
Review Cycle: Annual

0. Purpose & Scope

This SOP defines how access to Firstsource systems and data is requested, approved, provisioned, reviewed, and revoked to reduce risk and meet regulatory obligations.
In scope: workforce identities (employees, contractors, interns), service accounts, SaaS, VPN, databases, production infra, data stores (Internal/Confidential/Restricted).
Out of scope: physical/door access, public marketing sites.

AC-1 Governance & Principles

- **AC-1.1 Least Privilege:** Grant only the minimum access required for job tasks. Elevated access must be time-bound and monitored.
- **AC-1.2 Separation of Duties (SoD):** High-risk actions (e.g., production writes, approvals of financial postings) require at least two distinct roles; no one can both request and approve.
- **AC-1.3 Time-Bound Access:** Temporary/elevated access **must** include explicit start and end times.
- **AC-1.4 Break-Glass:** Emergency admin access is allowed only during incidents/outages with on-call Security approval; all actions must be logged and reviewed post-incident within 3 business days.

AC-2 Identity Lifecycle (Joiner/Mover/Leaver)

- **AC-2.1 New Hires:** Access requires manager approval and mapping to a standard role profile before provisioning.
- **AC-2.2 Contractors & Interns:** Access is **temporary** and expires automatically after **90 days** unless renewed with documented justification.
- **AC-2.3 Role Changes (Movers):** Access must be reviewed and updated within **3 business days** of a role change; remove orphaned access.
- **AC-2.4 Leavers/Terminations:** Disable **all** logical access (SSO, VPN, email) **no later than end-of-day** on termination date.
- **AC-2.5 Transfers:** Remove access not required in the target role within **5 business days**.

AC-3 Authentication & MFA

- **AC-3.1 MFA Required:** MFA is required for SSO, VPN, production consoles, and admin portals.

- **AC-3.2 Service Accounts:** Must use key/secret or certificate authentication; rotate credentials every **90 days**; never use personal MFA.
- **AC-3.3 Shared Credentials:** Prohibited except under **AC-1.4** (break-glass) and must be vaulted.

AC-4 Data Access Levels

- **AC-4.1 Public:** No auth; internal publication allowed.
- **AC-4.2 Internal:** Auth required; least privilege applies.
- **AC-4.3 Confidential:** Requires **manager and data owner** approval; read-only by default; write requires security review.
- **AC-4.4 Restricted:** Requires **Security review**, **data owner approval**, and **access review every 30 days**. Access is typically read-only; write requires CAB approval (see AC-6.2).

AC-5 Network & Remote Access

- **AC-5.1 VPN:** Granted to employees; contractors allowed with business justification and **90-day maximum term** (renewable with AC-8.1).
- **AC-5.2 Production Networks:** Prohibited for interns and contractors unless **AC-1.4** (break-glass) is invoked with incident reference.
- **AC-5.3 Third-Party Access:** Must be isolated to dedicated network segments and reviewed every **30 days**.

AC-6 System & Database Access

- **AC-6.1 Prod DB Read-Only:** Requires data owner approval; ticket must describe the business purpose; access is time-boxed.
- **AC-6.2 Prod Write Access:** Requires CAB approval, SoD per **AC-1.2**, and logging.
- **AC-6.3 Break-Glass DB Accounts:** Disabled by default and vaulted; usage requires incident or change ticket; post-use review within 3 business days.

AC-7 Reviews, Monitoring & Logging

- **AC-7.1 Quarterly Access Reviews:** Managers and system owners must certify user access to their apps/systems quarterly.
- **AC-7.2 Elevated Access Reviews:** Admin/root roles reviewed **monthly**.
- **AC-7.3 Logging & Retention:** All grants, changes, revocations, and privileged actions must be logged and retained for **1 year** minimum.

AC-8 Exceptions & Risk Acceptance

- **AC-8.1 Exception Process:** Document the business justification, scope, controls, risk acceptance by Security, and explicit expiry date.
- **AC-8.2 Legal/Regulatory:** No exception may violate legal/regulatory requirements; when unsure, consult Legal & Compliance.

AC-9 Request & Approval Workflow

- **AC-9.1 Request Ticket:** All access requests must be raised in the service desk with:
    - user identity, role, manager, system(s), data classification, requested level (read/write/admin), and justification;
    - for temporary access: start/end timestamps (see **AC-1.3**).
- **AC-9.2 Approvals:**
    - Internal data → **Manager** (minimum)
    - Confidential → **Manager + Data Owner** (**AC-4.3**)
    - Restricted → **Security Review + Data Owner** (**AC-4.4**)
    - VPN for contractors → **Manager + Security** (**AC-5.1**)
    - Prod write → **CAB + SoD** (**AC-6.2**)
- **AC-9.3 Provisioning:** Performed by IAM/Platform team only after approvals; changes logged (**AC-7.3**).
- **AC-9.4 Revocation:** IAM/Platform team must revoke access at or before expiry/end-of-employment; ensure removal from all systems (see **AC-2.4**).

AC-10 SoD Examples (Non-Exhaustive)

- **AC-10.1** A developer with deploy/write access to production may not approve their own changes (SoD per **AC-1.2**).
- **AC-10.2** A finance operator posting journal entries cannot approve the same entries.
- **AC-10.3** A DBA with break-glass may not close the incident review on their own actions.

AC-11 Enforcement & Non-Compliance

- **AC-11.1** Violations may result in access removal, incident creation, and disciplinary action.
- **AC-11.2** Systems found with orphaned access must be remediated within **5 business days** (see **AC-2.5**).

Appendix A — Approval Matrix (Quick Reference)

- **Employee – VPN:** Manager ✅ / Security ⛔ (MFA enforced) → **Allowed**
- **Contractor – VPN:** Manager ✅ + Security ✅ → **Max 90 days** (**AC-5.1**, **AC-2.2**)
- **Intern – Production Network: Not allowed** (see **AC-5.2**)
- **Prod DB Read-Only:** Data Owner ✅; time-boxed (**AC-6.1**)
- **Prod DB Write:** CAB ✅ + SoD; logging (**AC-6.2**, **AC-7.3**)
- **Restricted Data Access:** Security review ✅ + Data Owner ✅; 30-day review (**AC-4.4**)

Appendix B — Glossary

- **CAB:** Change Advisory Board
- **Data Owner:** Role accountable for a dataset/system
- **SoD:** Separation of Duties
- **Break-Glass:** Emergency access under **AC-1.4**

Revision History

- **v1.0 (04 Nov 2025):** Initial release