ResolvX

Access Control Policy

Topic-Specific Policy — Identity, Authentication & Access

POL-003 · v1.0 · 2026 · Internal — Restricted

Document Information

Policy ID	POL-003
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	IT Admin
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Frameworks	ISO 27001:2022 A5.15–A5.18, A8.2–A8.3 · NIST 800-53B AC-1–AC-17, IA-1–IA-12 · SOC 2 CC6.1–CC6.3

ResolvX — Access Control Policy

1. Purpose

This Access Control Policy establishes the requirements for controlling physical and logical access to ResolvX's information assets, systems, infrastructure, and data. It defines how access is granted, managed, reviewed, and revoked, ensuring that personnel have access only to what they need to perform their role, and no more.

The policy implements the principle of **least privilege** as the foundational access control model across all systems and environments.

2. Scope

This policy applies to:

- All access to ResolvX systems such as cloud infrastructure (AWS), corporate applications (Okta-managed SaaS), internal tools, databases, and APIs.
- All account types such as user accounts, service accounts, privileged accounts, shared accounts, and system-to-system accounts.
- All personnel - employees, contractors, consultants, and third-party vendors with system access
- All environments - Production, Staging, and Development

3. Access Control Principles

ResolvX implements access control based on the following principles:

Principle	Definition	Application at ResolvX
Least Privilege	Access granted is the minimum required for the business function	Default to read-only; write/admin access requires justification
Need-to-Know	Access to information is limited to those with a documented business need	Production data access restricted to engineering; client data access restricted by role
Separation of Duties	No single individual controls all aspects of a critical transaction or process	Finance approvals require two parties; production deployments require peer review
Zero Trust	No user or system is trusted by default — all access is verified	MFA enforced for all users; short-lived credentials used where possible
Default Deny	Access is denied unless explicitly granted	AWS IAM default deny; Okta no access until provisioned

4. Identity and Access Management

4.1 Identity Provider

ResolvX uses **Okta** as the central Identity Provider (IdP) for all corporate systems. All user accounts must be federated through Okta SSO. Direct application logins that bypass Okta are not permitted for corporate applications unless technically unavoidable and approved by IT Admin.

4.2 Account Provisioning

Access is provisioned through a formal Joiner/Mover/Leaver (JML) process:

Joiners:

- Hiring manager submits access request to IT Admin before start date, specifying role and required systems.
- IT Admin creates Okta account and assigns to appropriate role-based access groups within 1 business day of start.
- New hire receives MFA setup instructions as first login step.
- Access is documented in the access inventory.

Movers (role changes):

- Manager notifies IT Admin and GRC Lead of role change.
- Previous role access is revoked within 2 business days.
- New role access is provisioned per the new role's access profile.
- Access review triggered within 30 days of the change.

Leavers:

- HR notifies IT Admin and GRC Lead on the day of departure decision (not day of departure).
- All access is revoked within 4 hours of the departure date and time including Okta, AWS, GitHub, and all SaaS applications.
- Corporate devices are collected and remotely wiped via Jamf.
- IT Admin confirms deprovisioning is complete and documents confirmation.

4.3 Account Types

Account Type	Description	Requirements
Standard User	Day-to-day business system access	MFA required; Okta provisioned
Privileged User	Admin access to systems, cloud console, databases	MFA required; PAM controls; usage logged; quarterly review
Service Account	System-to-system authentication	No interactive login; rotating credentials; documented owner
Shared Account	Shared by multiple users	Prohibited unless no technical alternative; approved by CISO; fully logged
Emergency / Break-glass	Emergency access bypassing normal controls	Approval required; time-limited; all usage reviewed post-incident

Shared accounts are strongly discouraged. Where technically unavoidable, they must be approved by the CISO, have all activity logged, and be reviewed at each quarterly access review.

5. Authentication Requirements

5.1 Multi-Factor Authentication (MFA)

MFA is mandatory for all accounts without exception. There are no exemptions to this requirement.

Account Type	MFA Requirement
All standard users	TOTP or push notification via Okta Verify
Privileged users	Hardware security key (FIDO2/WebAuthn) preferred; TOTP minimum
AWS root account	Hardware security key required; root usage prohibited for daily operations
API / service accounts	Certificate-based or long-lived API key with rotation schedule

5.2 Password Requirements

Enforced by Okta:

- Minimum 14 characters
- Complexity: upper, lower, number, special character required
- No reuse of last 12 passwords
- No maximum age requirement (per NIST SP 800-63B guidance ; frequent rotation leads to weaker passwords)
- Immediate reset required upon suspected compromise

5.3 Session Management

- Browser sessions: 8-hour idle timeout; 24-hour absolute timeout
- CLI / API sessions: Tokens expire after 1 hour; refresh tokens expire after 24 hours
- Privileged console sessions: 1-hour absolute timeout with re-authentication required

5.4 Account Lockout

- 5 failed login attempts triggers a 15-minute lockout
- After 10 failed attempts, account is locked until IT Admin manually resets
- Lockout events are logged and reviewed for potential brute-force patterns

6. Role-Based Access Control (RBAC)

ResolvX implements RBAC across all systems. Access is assigned to roles, not individuals. Individuals inherit access by virtue of their role assignment.

6.1 Standard Role Profiles

Role Profile	Systems	Access Level
Engineering	GitHub, AWS Dev/Staging, Jira, Confluence, internal APIs	Read/write on dev/staging; read-only on production config
Engineering Lead	All Engineering + AWS Production console (limited)	As above + production read; deploy via CI/CD pipeline only
Customer Success	CRM, support portal, case management system	Client-facing systems only; no infrastructure access
Finance	Accounting system, expense management	Finance systems only; no engineering or client data access
HR	HRIS, Workday, employee records	HR systems only
GRC / Compliance	All systems (read-only), risk tools, audit evidence	Read access across all; write access to GRC tooling
IT Admin	Okta admin, Jamf MDM, all corporate IT systems	Admin on IT infrastructure; requires PAM for privileged operations
Head of Cloud Ops	AWS Production (full), security tooling, monitoring	Full AWS access; all changes logged; privileged session recording

6.2 Access Beyond Standard Profile

Any access requirement beyond the standard role profile must be:

- Requested by the employee's manager in writing to IT Admin
- Justified with a documented business reason
- Time-limited where possible (default 90 days with renewal)
- Logged in the Access Exception Register

7. Privileged Access Management (PAM)

Privileged access including AWS console admin access, database admin access, and Okta admin access is subject to enhanced controls:

- Just-in-Time access: Privileged access is elevated for specific tasks and expires automatically; standing privileged access is not permitted.
- Session recording: All privileged session activity is logged; AWS CloudTrail captures all API calls.
- Dual approval: Production environment changes require peer review and approval; no self-approval.
- Dedicated privileged accounts: Privileged tasks use dedicated admin accounts, not day-to-day user accounts.
- Privileged account inventory: Maintained by IT Admin; reviewed quarterly.
- AWS root account: Locked away; MFA hardware key required; usage triggers immediate review; only used for account-level operations that cannot be delegated.

8. Access Reviews

8.1 Quarterly Access Reviews

IT Admin, in coordination with the GRC Lead, conducts a formal access review every quarter. The review covers:

- All user accounts and their current access levels
- All privileged accounts and their usage logs
- All service accounts and their owners
- All exceptions and their justifications

Managers confirm that their direct reports' access remains appropriate for their current role. Unjustified access is revoked within 5 business days of the review.

8.2 Triggered Reviews

In addition to the quarterly cycle, access reviews are triggered by:

- Personnel changes (promotion, role change, department transfer)
- Termination (immediate full revocation)
- Security incident involving compromised credentials
- Significant system changes

8.3 Access Review Records

All access review outcomes are documented and retained for a minimum of 3 years as audit evidence.

9. Remote Access

- All remote access to ResolvX systems must be via Okta-authenticated SSO with MFA
- VPN is required when accessing internal-only systems from untrusted networks
- Remote desktop or direct SSH access to production systems must use the designated bastion host and is subject to session logging
- Direct production database access from outside the AWS VPC is prohibited

10. Third-Party and Vendor Access

Third-party access to ResolvX systems must be:

- Approved in advance by the IT Admin and GRC Lead
- Scoped to the minimum access required for the engagement
- Time-limited to the duration of the engagement
- Subject to MFA
- Documented in the vendor access register
- Revoked immediately upon completion of the engagement

Vendors must sign a Non-Disclosure Agreement (NDA) and, where applicable, a Data Processing Agreement (DPA) before access is granted.

11. Physical Access

Physical access to ResolvX office space is managed by building access controls. Server infrastructure is hosted on AWS hence there is no on-premises data centre. Physical security of AWS facilities is managed by AWS and is covered by AWS's ISO 27001 certification and SOC 2 reports.

Personnel must not allow tailgating through secure areas or share physical access credentials (e.g., key cards).

12. Access Logging and Monitoring

- All authentication events (successful and failed) are logged in Okta
- All AWS API activity is captured by CloudTrail
- All privileged session activity is logged
- Logs are retained for a minimum of 12 months
- Anomalous access patterns (after-hours access, access from unusual locations, excessive failed logins) are reviewed by the GRC Lead and Head of Cloud Ops

13. Compliance and Enforcement

Violations of this policy including sharing credentials, bypassing MFA, accessing systems without authorisation, or retaining access after a role change are treated as serious policy violations and may result in immediate access revocation, formal disciplinary action, or termination.

14. Document Control

Field	Detail
Policy ID	POL-003
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	IT Admin
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Framework References	ISO/IEC 27001:2022 A5.15, A5.16, A5.17, A5.18, A8.2, A8.3 · NIST SP 800-53B AC-1 to AC-17, IA-1 to IA-12 · NIST CSF 2.0 PR.AA-01 through PR.AA-06 · SOC 2 TSC CC6.1, CC6.2, CC6.3
Related Policies	POL-001 (IS Policy), POL-002 (AUP), Controls Owners Register

ResolvX GRC Program — Internal Use Only — v1.0 — 2026

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	