

Access Control Policy

Standards for Logical Access, Authentication, and Identity Governance

ORGANIZATION

Northwind Labs, Inc. (14 Personnel)

DOCUMENT OWNER

Head of Security & Infrastructure

VERSION / STATUS

Version 1.0 • Active & Approved

EFFECTIVE DATE

October 1, 2026

CORE INFRASTRUCTURE

AWS • Okta Identity Engine • GitHub

TARGET AUDIT SCOPE

SOC 2 Type II (Security / Availability)

1. Purpose

SOC 2: CC6.1, CC6.2, CC6.3

The purpose of this Access Control Policy is to establish binding technical and operational standards for granting, maintaining, reviewing, and revoking logical access to Northwind Labs, Inc. ("Northwind Labs") information systems, customer data repositories, cloud infrastructure, and internal networks. This policy enforces the foundational security principles of least privilege, role-based access control (RBAC), and defense-in-depth to protect Northwind Labs and customer data from unauthorized disclosure, modification, or compromise.

2. Scope

This policy applies to:

- All users authorized to access Northwind Labs information systems, including full-time employees, part-time staff, contractors, advisors, and authorized third-party vendors.

- All information systems, cloud accounts on Amazon Web Services (AWS), identity platforms (Okta Identity Engine), code repositories (GitHub Enterprise Cloud), production databases, and internal SaaS tools operated by or on behalf of Northwind Labs.
- All endpoints (company-managed laptops and workstations) connecting to production or corporate resources.

3. Roles and Responsibilities

SOC 2: CC1.3, CC6.2

- **Head of Security & Infrastructure (Security Owner):** Establishes access control architectures, approves access policy exceptions, oversees quarterly user access reviews, and ensures RBAC role definitions align with business needs.
- **Lead Cloud Infrastructure Engineer (Technical Administrator):** Manages provisioning and deprovisioning operations, enforces technical authentication controls on AWS IAM Identity Center and GitHub, configures identity integrations, and monitors administrative account activity.
- **People Operations / HR:** Provides advance written notification to the Security Owner and Technical Administrator regarding personnel changes, status updates, role transfers, or employment terminations.
- **Department Managers & Team Leads:** Reviews and formally approves access requests for direct reports; certifies quarterly access rosters during periodic user access reviews.
- **All Personnel:** Responsible for safeguarding individual authentication credentials, utilizing the approved password manager (1Password Business), adhering strictly to multi-factor authentication (MFA) requirements, and immediately reporting suspected credential theft or unauthorized access.

4. Policy Statements

4.1 Principle of Least Privilege and Role-Based Access Control (RBAC)

SOC 2: CC6.1, CC6.3

- **Least Privilege:** Access to systems, networks, applications, production datastores, and sensitive data is restricted to the minimum permissions necessary for personnel to perform their assigned job responsibilities.

- **Role-Based Access Control (RBAC):** Permissions are provisioned according to standardized functional roles managed centrally within Okta Identity Engine and AWS IAM Identity Center. Ad-hoc, individual permission grants that deviate from standard role definitions are prohibited without documented approval from the Head of Security & Infrastructure.
- **Production Data Isolation:** Access to production infrastructure and databases containing customer data is strictly limited to authorized engineering personnel whose job functions explicitly require direct production troubleshooting. Non-technical staff (including Sales, Marketing, and General Administration) are never granted access to production datastores.

4.2 Account Provisioning and Onboarding

SOC 2: CC6.2

- **Formal Access Request:** Access to systems, repositories, and administrative tools must be requested by the hiring manager through the internal ticketing system and approved by the Head of Security & Infrastructure or a designated administrator prior to provisioning.
- **Unique Identification:** Every user is provisioned a unique account tied directly to their individual corporate email identity (`first.last@northwindlabs.example`). Shared, generic, or group accounts (e.g., `admin@northwindlabs.example`, `dev@northwindlabs.example`) are strictly prohibited for interactive logins.
- **Initial Password Issuance:** Temporary credentials issued during onboarding must be transmitted via an encrypted, out-of-band communication channel (e.g., encrypted 1Password temporary share link). Passwords must be forced to rotate upon initial authentication.

4.3 Account Deprovisioning and Offboarding

SOC 2: CC6.2

- **Timely Deprovisioning:** When an employee or contractor concludes their working relationship with Northwind Labs:
 - **Standard Voluntary Departures:** All logical access across Okta Identity Engine, AWS, GitHub Enterprise Cloud, 1Password Business, Google Workspace, and connected SaaS applications must be revoked within twenty-four (24) hours of the formal departure date.
 - **Involuntary Departures:** All logical access must be revoked immediately prior to or concurrently with the termination notification meeting.
- **Account Disablement over Deletion:** Accounts are immediately suspended, active web and API sessions terminated, and authentication tokens revoked rather than deleting account

records outright, ensuring audit log integrity and traceability.

- **Asset Return:** All company-managed hardware, physical security keys, and corporate credentials must be surrendered to People Operations on or before the departure date.

4.4 Periodic User Access Reviews

SOC 2: CC6.2, CC6.3

- **Review Cadence:** The Head of Security & Infrastructure and Lead Cloud Infrastructure Engineer conduct formal user access reviews at least **quarterly**.
- **Scope of Review:** Access audits encompass:
 - AWS IAM Identity Center permission sets and AWS account memberships.
 - Okta group assignments, application entitlements, and directory administrative roles.
 - GitHub Enterprise Cloud repository write/admin privileges and organization owners.
 - Production database connection credentials, SSH bastion access, and Cloudflare Zero Trust policies.
- **Remediation SLAs:** Any identified orphaned accounts, unnecessary administrative privileges, or transferred employees retaining obsolete permissions must be revoked within three (3) business days of identification.
- **Audit Evidence Retention:** Dated review sign-off sheets, exported access rosters, and corresponding remediation tickets are archived securely and retained for a minimum of one (1) year to serve as audit evidence.

Tailoring Note for Startups: Quarterly access reviews are one of the most heavily scrutinized areas in SOC 2 Type II audits. Northwind Labs' policy specifies a 3-day remediation SLA and 1-year evidence retention to provide an unambiguous, auditable artifact for external auditors.

4.5 Authentication and Password Standards

SOC 2: CC6.1

- **Centralized Identity & Single Sign-On (SSO):** All company applications, internal tools, and cloud environments must authenticate through Okta Identity Engine via SAML 2.0 or OIDC. Direct, per-application local account creation is prohibited where SSO integration is supported.

- **Password Requirements:** Corporate master passwords and local administrative passwords must adhere to the following standards:
 - Minimum length of sixteen (16) characters.
 - Passwords must contain a combination of uppercase letters, lowercase letters, numbers, and symbols, or consist of an approved high-entropy multi-word passphrase of at least twenty (20) characters.
 - Passwords must not contain easily guessable patterns, dictionary words, company names, or personal details.
 - In accordance with NIST SP 800-63B guidelines, passwords are not subjected to mandatory periodic expiration unless there is evidence or suspicion of compromise.
- **Password Manager Utilization:** All personnel are required to use Northwind Labs' managed password vault (1Password Business) to generate, store, and autofill corporate credentials. Storing passwords in web browsers, unencrypted local files, text notes, or spreadsheets is strictly forbidden.

4.6 Multi-Factor Authentication (MFA) Requirements

SOC 2: CC6.1, CC6.6

- **Mandatory MFA:** Multi-Factor Authentication is universally mandatory across all personnel and external collaborators accessing Northwind Labs systems, without exception.
- **Covered Surfaces:** MFA is technically enforced at the identity layer on:
 - Corporate identity provider and single sign-on portal (Okta Identity Engine).
 - Cloud infrastructure consoles, CLI sessions, and APIs on Amazon Web Services.
 - Source code management and CI/CD pipelines (GitHub Enterprise Cloud).
 - Company password manager (1Password Business).
 - Production database bastion jump hosts and telemetry dashboards.
- **Approved Factors:** Approved secondary authentication factors include:
 - FIDO2 / WebAuthn hardware security keys (e.g., YubiKey 5 Series).
 - Managed mobile authenticator apps with push verification and number matching (Okta Verify, 1Password TOTP).
 - SMS and voice-based verification are strictly prohibited as primary authentication factors and may only be enabled as an emergency recovery fallback where hardware or TOTP

authenticators are technically unsupported.

4.7 Privileged and Administrative Access Management

SOC 2: CC6.1, CC6.3

- **Separation of Administrative Accounts:** Engineering staff with administrative rights on AWS or Okta must use standard, unprivileged accounts for routine activities (email, web browsing, internal communication) and assume elevated roles only when performing specific administrative tasks.
- **Prohibition of Direct Root Access:** Direct interactive login to the AWS root account is prohibited. The AWS root user is secured with a hardware-bound security key kept in dual-custody physical storage, with continuous CloudTrail alerting configured for any root login event.
- **Break-Glass Emergency Access:** A dedicated, vaulted break-glass administrator account is maintained for disaster recovery. Access credentials are split between the Head of Security & Infrastructure and VP of Engineering in 1Password. Invocation of break-glass credentials automatically alerts security monitoring channels and triggers an immediate post-incident audit review.

4.8 Remote Access and Network Perimeter Security

SOC 2: CC6.6, CC6.7

- **Cryptographic Transmission:** All network traffic connecting to Northwind Labs production infrastructure, administrative portals, or databases must utilize secure cryptographic protocols (TLS 1.3 or TLS 1.2 minimum; SSHv2). Unencrypted protocols (e.g., plain HTTP, Telnet, unencrypted FTP) are blocked at the perimeter.
- **Zero Trust Network Access:** Production environment access is governed by Cloudflare Zero Trust (Access). Engineers must authenticate through Okta SSO with device posture checks validated before accessing internal endpoints.
- **No Direct Database Exposure:** Production databases and internal microservices are isolated inside private AWS VPC subnets with no public IPv4 addresses assigned. Direct inbound connections from the public internet are architecturally blocked.

4.9 Machine Accounts, Service Credentials, and Secrets

SOC 2: CC6.1

- **Service Accounts:** Programmatic access between internal services, CI/CD runners, and cloud infrastructure must use dedicated IAM roles (AWS IAM Roles for Service Accounts / IRSA) or machine service accounts configured with strictly bounded permissions.
- **Prohibition of Hardcoded Secrets:** API keys, database connection strings, SSH private keys, and cryptographic certificates must never be hardcoded into application source code or committed to GitHub repositories.
- **Secrets Management:** Secrets must be stored and dynamically injected into runtime environments using AWS Secrets Manager or GitHub Actions encrypted repository secrets. Automated pre-commit scanning (TruffleHog / GitGuardian) is enforced across all engineering repositories.

5. Enforcement

Compliance with this Access Control Policy is mandatory for all personnel. Violations—including credential sharing, intentional circumvention of MFA, unauthorized granting of system privileges, or hardcoding production secrets—will result in disciplinary action up to and including immediate termination of employment or contract, and potential civil or criminal legal recourse.

6. Exceptions Process

Exceptions to this policy (e.g., temporary access required for emergency vendor integration) must be submitted via the Security Exception Form and require:

1. Documented technical justification, scope, and specific system inventory.
2. Verified compensating controls (e.g., strict IP restriction, enhanced session logging).
3. Formal written risk acceptance signed by both the Head of Security & Infrastructure and the VP of Engineering.
4. An explicit expiration date not to exceed ninety (90) calendar days.

7. Review Cadence

This policy is reviewed annually by the Head of Security & Infrastructure and updated as necessary to reflect changes in Northwind Labs' infrastructure, team structure, regulatory

obligations, and threat landscape.

8. Revision History

VERSION	DATE	AUTHOR / ROLE	SUMMARY OF CHANGES
1.0	October 1, 2026	Head of Security & Infrastructure	Initial policy adoption