Access Control Policy

OverSiteAI, LLC

Document Version:	2.0
Effective Date:	January 1, 2025
Last Updated:	June 25, 2025
Last Reviewed:	June 27, 2025
Classification:	Restricted
Owner:	Chief Technology Officer
Approved By:	Chief Executive Officer

Table of Contents

Access Control Policy

OversiteAI, LLC

Document Version: 2.0

Effective Date: January 1, 2025

Last Updated: June 25, 2025

Last Reviewed: June 27, 2025

Classification: Restricted

Owner: Chief Technology Officer

Approved By: Chief Executive Officer

1. Purpose and Scope

1.1 Purpose

NIST Controls: AC-1, AC-2

The Access Control Policy establishes OversiteAI's comprehensive framework for managing access to our information systems, applications, and data. As a small but security-conscious software company, we recognize that effective access control forms the foundation of our security posture. This policy ensures that access rights are granted based on legitimate business need, properly authenticated through modern security mechanisms, regularly reviewed to maintain least privilege, and promptly revoked when no longer required.

Our approach balances security requirements with operational efficiency, acknowledging that as a company of fewer than 20 employees, we must implement controls that are both effective and manageable. We leverage Azure's built-in security features extensively, allowing us to achieve enterprise-grade security without the overhead of complex manual processes or dedicated security staff.

This policy directly supports our architectural advantage: since our software runs entirely on customer premises with no access to customer data, our access control needs focus primarily on protecting our intellectual property, development systems, and corporate infrastructure. This design significantly reduces our risk profile and allows us to concentrate our security efforts where they matter most.

1.2 Scope

NIST Controls: AC-1, PL-2

This policy applies comprehensively across our entire technology landscape. It governs access to all OversiteAI information systems and applications, whether hosted in Azure, accessed through SaaS providers, or running on company-provided devices. The policy covers all users including full-time employees, contractors, consultants, and any third parties who require access to our systems for business purposes.

We address all access methods within this policy, from standard user authentication to API integrations and service accounts. Both logical access (system logins, application permissions, data access) and physical access (device security, home office controls) fall under this policy's purview. The policy applies equally to all environments - production, development, test, and corporate - with appropriate controls scaled to the sensitivity and criticality of each environment.

Importantly, this policy explicitly excludes customer environments where our software is deployed. By architectural design, OversiteAI has no access to customer-deployed instances of our software. This separation is a fundamental security principle that eliminates entire categories of risk and compliance requirements. Customers maintain complete control over access to their deployments, with our support limited to providing documentation and guidance.

1.3 Key Principles

NIST Controls: AC-1, AC-3, AC-6

Our access control implementation follows five fundamental principles that guide all decisions and implementations:

Least Privilege forms our primary access philosophy. Every user receives only the minimum access required to perform their assigned duties. We implement this through role-based access control, regular reviews, and a default-deny approach to permissions. For our small team, this means carefully crafted roles that match actual job functions rather than broad administrative access. We resist the temptation to grant excessive permissions for convenience, understanding that limited access protects both the company and the individual user.

Separation of Duties ensures that critical business functions require multiple people to complete, reducing the risk of fraud or error. Despite our small size, we maintain separation between development and deployment, financial approval and execution, and security configuration and audit. Where true separation isn't feasible due to team size, we implement compensating controls such as enhanced logging and regular review of privileged actions.

Need-to-Know restricts information access based on business necessity rather than curiosity or convenience. This principle applies particularly to sensitive areas such as customer contracts, financial data, and security configurations. We foster a culture of professional curiosity bounded by respect for confidentiality, ensuring team members understand why certain information requires restricted access.

Defense in Depth drives us to implement multiple layers of access controls rather than relying on any single security measure. Authentication, authorization, network controls, and monitoring work together to protect our resources. If one control fails or is compromised, others continue to provide protection. This layered approach is especially important for a small company where we cannot afford dedicated security operations.

Zero Trust guides our modern approach to security, assuming no implicit trust based on network location or previous authentication. Every access request is verified, every session is authenticated, and every action is logged. We've moved beyond perimeter-based security to embrace a model where trust is continuously verified, not assumed. Azure's conditional access and continuous authentication capabilities make this practical even for our small team.

2. Access Control Framework

2.1 Access Control Model

NIST Controls: AC-2, AC-3, AC-5

OversiteAI implements Role-Based Access Control (RBAC) as our primary access management model. This approach assigns permissions to roles rather than individuals, significantly simplifying administration while ensuring consistent access policies. As employees join, move between positions, or leave the company, we simply adjust their role assignments rather than managing hundreds of individual permissions.

Our RBAC implementation leverages Azure Active Directory's sophisticated role management capabilities, allowing us to define granular permissions that precisely match job functions. Roles are designed based on actual business requirements rather than technical possibilities, ensuring that each role grants necessary access without over-provisioning. We regularly review and refine these roles based on usage patterns and changing business needs.

Access categories within our framework are organized into four distinct levels. **System Access** controls the ability to log into systems and applications, forming the first gate of our security model. **Data Access** manages read and write permissions to different data classifications, ensuring sensitive information remains protected. **Function Access** governs the ability to perform specific operations within applications, such as approving changes or initiating deployments. **Administrative Access** provides privileged system functions necessary for IT operations but requiring additional controls and monitoring.

This structured approach allows us to maintain clear accountability and auditability. Every access decision can be traced back to a specific role assignment, which in turn links to a documented business need and proper approval. For our small team, this clarity is essential - we cannot afford ambiguity in access rights when every team member plays a critical role in our operations.

2.2 Access Zones

NIST Controls: AC-4, SC-7, SC-32

Our infrastructure is logically divided into distinct access zones, each with appropriate security controls and access restrictions. This segmentation provides defense in depth while remaining manageable for our small IT team through heavy use of Azure's native segmentation capabilities.

The **Production Environment** receives our highest level of security controls. Access is strictly limited to operations staff with a demonstrated need, and all activities are comprehensively logged and monitored. Every change requires formal change control approval, and we maintain complete audit trails of all actions. Production access is treated as privileged, requiring additional authentication factors and generating alerts for security review. We've architected this environment to be largely self-managing through Azure PaaS services, minimizing the need for direct access.

Our **Development Environment** provides necessary access for our engineering team while maintaining appropriate controls. Developers receive access to source code repositories, development tools, and test systems as required by their roles. We maintain strict separation between development and production, with no customer data ever permitted in development systems. This environment encourages innovation and rapid development while protecting production stability and security.

The **Corporate Environment** encompasses our business operations infrastructure including email, collaboration tools, documentation systems, and business applications. All employees receive appropriate access to these systems based on their roles. We leverage Microsoft 365's built-in security features extensively, benefiting from Microsoft's massive security investments while maintaining central control through Azure AD.

Most uniquely, the **Customer Environment** represents systems where we have zero access by design. Our software operates entirely on customer infrastructure, and we've architected our solution to require no callbacks, no data transmission, and no remote access. This fundamental design decision eliminates entire categories of security risks and compliance requirements. When customers need support, they control exactly what information to share, maintaining complete sovereignty over their data and systems.

3. User Access Management

3.1 Account Lifecycle

NIST Controls: AC-2, PS-4, PS-5

Managing user accounts throughout their lifecycle requires careful orchestration of people, processes, and technology. Our approach emphasizes automation where possible while maintaining human oversight for critical decisions.

Account Creation begins when a manager submits an access request through our IT ticketing system, typically as part of onboarding a new employee or contractor. HR validates the employment status and start date, ensuring we don't create accounts for individuals who haven't completed our hiring process. IT reviews the request against our standard role templates, confirming that the requested access aligns with the position's requirements.

Once approved, we create accounts using predefined role templates that ensure consistency and completeness. New users receive initial credentials through a secure channel, with mandatory password change required on first login. Multi-factor authentication enrollment happens immediately, before any access to sensitive systems is granted. New users must complete security awareness training within their first week, reinforcing the security responsibilities that come with system access.

Account Maintenance continues throughout the user's tenure with regular reviews and updates. Managers complete quarterly access reviews for their team members, validating that current permissions remain appropriate. We conduct annual recertification of all access rights, providing a comprehensive audit opportunity. Role changes trigger immediate access reviews, ensuring permissions align with new responsibilities. Our monitoring systems watch for unusual activity patterns that might indicate compromised credentials or insider threats.

Account Termination represents a critical security moment requiring swift, comprehensive action. When HR initiates the termination process, whether for voluntary or involuntary separation, our response is immediate and thorough. Access is disabled within two hours of notification, preventing any post-termination system access. VPN certificates are revoked, email access is suspended with appropriate forwarding configured, and all sessions are terminated.

We follow a detailed checklist ensuring nothing is missed: equipment return is tracked, knowledge transfer is documented, and data preservation complies with legal requirements. For involuntary terminations, we accelerate this process with immediate

access suspension followed by careful review to ensure no backdoors remain. Our small size allows us to respond quickly and personally to each termination, but we maintain strict process discipline to ensure consistency and completeness.

3.2 Standard Access Roles

NIST Controls: AC-2, AC-3, AC-5

Our role definitions reflect the reality of a small, highly skilled team where individuals often wear multiple hats while maintaining appropriate separation of duties. Each role is carefully crafted to provide necessary access without over-privileging users.

The **Developer Role** forms our baseline technical access, providing Azure DevOps repository access for source code management, development environment access for building and testing, and read access to technical documentation. Developers explicitly do not receive production access, maintaining our crucial separation between development and operations. This role suits junior developers and contractors who need to contribute code without broader system access.

Senior Developer Role extends developer permissions with additional responsibilities. These team members can review and merge code, providing quality control over our codebase. They receive limited production read access for troubleshooting purposes, carefully scoped to logs and metrics without the ability to modify production systems. Senior developers can also write and maintain architecture documentation, sharing knowledge across the team.

Our **DevOps Engineer Role** bridges development and operations with carefully controlled production access. These individuals manage our Azure infrastructure, maintain deployment pipelines, and monitor production systems. Their access includes configuration management capabilities, but all changes flow through our change control process. We've designed this role to support our automation-first approach, encouraging infrastructure as code over manual changes.

The **Support Role** enables customer assistance without compromising security. Support staff access our ticketing system, customer communication tools, and knowledge base. They receive limited log access for troubleshooting but cannot access customer data or production systems. This role demonstrates our commitment to helping customers while respecting the architectural boundaries of our zero-access design.

Administrative Roles provide business application administration capabilities. These roles manage user provisioning, review audit logs, and approve policy exceptions within

defined limits. We've distributed administrative functions across multiple specialized roles rather than creating broad "admin" access, ensuring that business administration remains separate from technical infrastructure control.

3.3 Access Request Process

NIST Controls: AC-2, AC-3

Our access request process balances security requirements with the operational reality of a small, fast-moving company. We've designed workflows that provide appropriate oversight without creating bureaucratic delays that would impact productivity.

Standard Access Requests follow a streamlined workflow optimized for common needs. Users submit requests through our IT ticketing system, selecting from predefined access types and providing business justification. The system automatically routes requests to the appropriate approver - typically the user's manager - and notifies IT once approved. For standard role assignments, IT provisions access within two business days using automated workflows where possible. Users receive notification when their access is active, along with any necessary instructions or training requirements.

Privileged Access Requests require additional scrutiny given their potential impact. These requests demand detailed written justification explaining not just what access is needed, but why existing permissions are insufficient. IT performs a risk assessment, considering the sensitivity of the requested access and potential for misuse. The CTO must approve all privileged access requests, ensuring senior leadership visibility into high-risk permissions. Where possible, we grant time-limited access that automatically expires, reducing the risk of permission creep. Enhanced monitoring accompanies privileged access, with activities logged and reviewed for anomalies.

Emergency Access procedures recognize that business sometimes can't wait for formal processes. In true emergencies, verbal approval from a manager allows IT to grant immediate access, with formal documentation required within 24 hours. We scrutinize these requests afterward, determining whether permanent access is needed or if the emergency was a one-time event. All emergency access generates audit trails for later review, ensuring accountability even in urgent situations.

4. Authentication Standards

4.1 Password Policy

NIST Controls: IA-5, AC-7

Our password policy reflects modern security understanding, moving beyond outdated complexity rules to focus on password strength and usability. We've aligned with NIST's latest guidance while adapting to our specific environment and threat model.

Password Requirements emphasize length over complexity, recognizing that longer passwords provide better security than short, complex ones. We require a minimum of 14 characters for all accounts, encouraging users to create memorable passphrases rather than cryptic combinations. While we don't mandate specific character types, our policy encourages mixing uppercase, lowercase, numbers, and special characters for additional entropy.

We explicitly prohibit common weak patterns: dictionary words used alone, personal information like names or birthdays, company name variations that might be guessed, keyboard patterns like "qwerty" or "123456", and any password previously used within the last 12 iterations. These restrictions prevent the most common password attacks while allowing users flexibility in creating strong, memorable credentials.

Password Management practices support security without creating undue burden. Initial passwords are system-generated and must be changed on first use, ensuring that no default or shared passwords persist. Regular users change passwords every 180 days, while privileged users rotate every 90 days, reflecting their higher risk profile. Service accounts, which can't be used for interactive login, rotate annually through a managed process.

We actively encourage password manager use, providing licenses for a commercial password manager to all employees. This tool enables strong, unique passwords for every account without the memorization burden that leads to weak or reused passwords. We prohibit password sharing absolutely - any collaboration needs are met through proper access provisioning, not credential sharing. Documentation systems are regularly scanned for embedded passwords, which are removed and replaced with proper references to our secure credential storage.

Account Lockout provides defense against brute force attacks while minimizing user frustration. After 5 failed attempts, accounts lock for 30 minutes before automatically unlocking. This threshold balances security with usability - high enough to accommodate genuine mistakes but low enough to thwart automated attacks. Users can request manual unlock through IT support if needed urgently, creating an audit trail of the event. Repeated lockouts trigger investigation, as they may indicate a compromised password, targeted attack, or user struggling with our authentication systems.

4.2 Multi-Factor Authentication (MFA)

NIST Controls: IA-2, IA-5

Multi-factor authentication serves as a critical defense against password compromise, and we've made it mandatory across all systems and users without exception. Our MFA implementation leverages Azure AD's sophisticated capabilities while remaining user-friendly and supportable by our small IT team.

MFA Requirements are non-negotiable: every user must enroll in MFA before receiving access to any company systems. We require MFA for all cloud service access, recognizing that cloud systems are exposed to global attack surfaces. VPN connections mandate MFA, ensuring that remote access receives appropriate protection. Administrative operations require MFA even when performed from trusted locations, acknowledging the high value of privileged access to attackers.

Approved MFA Methods are selected for security and usability. We prefer authenticator apps like Microsoft Authenticator, Google Authenticator, or Authy, which provide time-based one-time passwords without the vulnerabilities of SMS. These apps work offline, support multiple accounts, and resist common attack vectors. SMS serves only as a backup method for standard users, with full awareness of SIM swapping risks - privileged accounts cannot use SMS under any circumstances. For high-privilege users, we provide hardware tokens like FIDO2 keys or YubiKeys, offering phishing-resistant authentication for our most sensitive access.

MFA Enrollment integrates into our onboarding process seamlessly. New users enroll during their first day, guided by IT through the process. We require two distinct MFA methods for redundancy - typically an authenticator app and SMS backup for standard users. Self-service recovery options reduce IT burden while maintaining security, allowing users to manage their own MFA devices within policy constraints. Annual verification ensures that registered devices remain under user control and that contact information stays current.

4.3 Session Management

NIST Controls: AC-11, AC-12

Proper session management prevents unauthorized access through abandoned or hijacked sessions while balancing user productivity needs. Our controls adapt to the sensitivity of accessed resources and the security of the connection environment.

Session Controls implement defense in depth through multiple mechanisms. Automatic logout after 30 minutes of inactivity prevents abandoned sessions from remaining accessible. Maximum session duration of 8 hours forces periodic re-authentication, limiting the window for session hijacking. Sensitive operations like administrative changes require re-authentication regardless of session age, ensuring that critical actions receive fresh identity verification. We prohibit concurrent administrative sessions, preventing privilege escalation through multiple simultaneous connections. For our highest-risk access, we implement session recording, creating an audit trail of all actions for later review if needed.

Remote Session Security addresses the unique risks of distributed work. All remote sessions are clearly identified to users, showing connection source and time to detect unauthorized access. Users receive notification when sessions start, alerting them to potentially malicious access. Our systems provide self-service ability to review all active sessions and terminate suspicious connections. Every session creates detailed audit logs including source IP, authentication method, and resources accessed. These controls become especially important for our fully remote workforce, where "remote" is the normal state rather than an exception.

5. Authorization Management

5.1 Access Rights Assignment

NIST Controls: AC-3, AC-5, AC-6

Authorization management determines what authenticated users can actually do within our systems. Our approach emphasizes explicit grants, regular review, and clear documentation of all access decisions.

Access Assignment Principles guide every authorization decision. We operate on a default-deny basis - no access exists unless explicitly granted through proper channels. Every access grant requires documented approval from an authorized individual, creating accountability for access decisions. Where business needs are temporary, we implement time-limited access that automatically expires, reducing the accumulation of unnecessary permissions over time. Regular reviews ensure that all access remains appropriate, with cleanup of permissions no longer needed. Every access decision is documented, from initial request through approval to eventual revocation.

Segregation of Duties remains challenging but essential for a small company. We enforce separation between code development and production deployment, ensuring that those who write code don't unilaterally push it to production. User creation and

access approval require different individuals, preventing any single person from creating and authorizing accounts. Security configuration and audit functions are separated, ensuring independent review of security controls. Backup creation and restoration require different authorizations, protecting against unauthorized data access or destruction. Financial approvals follow defined thresholds, with larger amounts requiring additional approvers regardless of the requester's seniority.

Where our small size makes complete separation impractical, we implement compensating controls. Enhanced logging captures all actions by users with combined duties. Regular reviews examine these logs for inappropriate activity. We rotate responsibilities periodically where feasible, preventing any individual from becoming indispensable. Most importantly, we maintain a culture of professional integrity where team members understand and respect these boundaries even when technical controls might permit circumvention.

5.2 Privileged Access Management

NIST Controls: AC-2, AC-3, AC-6

Privileged access represents our highest-risk permissions, requiring our strongest controls. We've implemented a comprehensive privileged access management program scaled appropriately for our size and resources.

Privileged Account Types are clearly defined and strictly controlled. Break-glass accounts exist for emergency access when normal authentication systems fail, with use triggering immediate alerts and investigation. Service accounts run automated processes with passwords managed programmatically and no interactive login permitted. Administrative accounts provide system management capabilities, always separate from users' standard accounts. Root or Administrator access represents ultimate system control, limited to absolute minimum use and maximum monitoring.

Privileged Access Controls layer multiple protections around high-risk permissions. Every privileged user maintains separate accounts for regular and administrative use, enforcing clear boundaries between routine work and sensitive operations. Enhanced authentication is mandatory, typically requiring hardware tokens or other phishing-resistant methods. All privileged activities generate detailed logs feeding our security monitoring systems. Quarterly certification reviews ensure privileged access remains appropriate and necessary. Where possible, we implement just-in-time access that grants privileges only when needed for specific tasks. For the most sensitive operations, we require use of Privileged Access Workstations (PAW) - specially configured systems with additional security controls.

Azure Privileged Roles require special attention given their power over our infrastructure. Global Administrator access is limited to maximum 2 users - typically the CTO and CEO - recognizing this role's ability to override all other controls. Subscription Owner rights belong only to the DevOps team, and only for subscriptions they actively manage. Security Administrator privileges rest solely with the CTO, ensuring centralized control over security configurations. Key Vault Administrator access is limited to 3 users who manage our secrets and certificates. These restrictions might seem severe for a small company, but the power of these roles demands proportional control.

5.3 Service Account Management

NIST Controls: AC-2, AC-3, IA-2

Service accounts present unique challenges - they can't participate in interactive authentication, often require high privileges, and run continuously without human oversight. Our management approach addresses these challenges through technical and procedural controls.

Service Account Standards ensure consistent security across all automated access. Every service account has a documented purpose explaining why it exists and what it accomplishes. A designated owner takes responsibility for each account's security and appropriate use. Passwords are complex (minimum 20 characters) and randomly generated, never following predictable patterns. These passwords are stored exclusively in Azure Key Vault, never in configuration files or documentation. Interactive login is technically prohibited through policy settings, preventing human use of these powerful accounts. Permissions follow least-privilege principles even more strictly than user accounts, since service accounts can't exercise judgment about appropriate use. Annual reviews verify that each service account remains necessary and appropriately configured.

Service Account Monitoring provides continuous oversight of these unattended accounts. We track all login attempts, whether successful or failed, to detect potential compromise. Usage patterns are baselined using Azure's analytics capabilities, with deviations triggering security alerts. Any anomaly - unusual login times, unexpected source systems, or atypical resource access - receives immediate investigation. Password rotation follows a regular schedule managed through Azure Automation, ensuring no password ages beyond acceptable limits. When service accounts are no longer needed, we decommission them promptly to prevent orphaned accounts from becoming security vulnerabilities.

6. Access Control Mechanisms

6.1 Network Access Controls

NIST Controls: AC-4, SC-7, SC-8

Network segmentation provides fundamental protection by limiting the scope of potential breaches and preventing lateral movement by attackers. Our implementation leverages Azure's software-defined networking to create granular controls without complex hardware management.

Network Segmentation divides our infrastructure into security zones with controlled interconnections. Production networks remain completely isolated from development, with no direct routing between environments. This separation prevents development mistakes or compromises from affecting customer-facing systems. Administrative networks exist separately, accessible only through jump boxes or PAWs with enhanced monitoring. Guest WiFi, used by visitors to our home offices, remains completely isolated from corporate resources. Azure Network Security Groups provide micro-segmentation within each zone, limiting communication to explicitly required paths. Where possible, we implement application-level segmentation, with each service communicating only with its required dependencies.

Remote Access security becomes critical for our distributed workforce. VPN connections are mandatory for accessing any internal resources, with no exceptions for convenience. We use certificate-based authentication in addition to passwords and MFA, providing defense against credential theft. Device compliance checking ensures that only company-managed devices with current security updates can establish VPN connections. Split-tunneling is disabled, routing all traffic through our security controls while users are connected to corporate resources. Automatic disconnect after 8 hours prevents forgotten sessions from remaining open indefinitely, requiring users to re-authenticate for extended work sessions.

6.2 Application Access Controls

NIST Controls: AC-3, AC-4, IA-2

Modern applications require sophisticated access controls that go beyond simple login credentials. Our approach leverages industry standards and Azure's capabilities to provide secure, user-friendly application access.

Single Sign-On (SSO) through Azure AD integration provides enormous security and usability benefits. Users authenticate once to access multiple applications, reducing

password fatigue and the temptation to reuse credentials. SAML and OAuth protocols are preferred, with legacy authentication methods phased out wherever possible. Centralized authentication enables consistent policy enforcement - MFA requirements, conditional access rules, and session policies apply uniformly across all integrated applications. The improved user experience actually enhances security by making the secure path the easy path. Enhanced monitoring becomes possible when all authentication flows through a central point, enabling detection of anomalous access patterns across applications.

API Access Control addresses programmatic access with appropriate security measures. API keys provide service integration capabilities, with each key scoped to minimum necessary permissions. OAuth enables user context propagation for APIs that act on behalf of users, maintaining auditability. Rate limiting prevents abuse while ensuring fair resource allocation across consumers. Our API gateway provides centralized monitoring of all API activity, detecting potential attacks or misuse. Regular key rotation ensures that compromised credentials have limited lifespan, with automated rotation preferred where applications support it.

6.3 Data Access Controls

NIST Controls: AC-3, AC-4, SC-8

Data access controls ensure that information is available to authorized users while remaining protected from unauthorized access or modification. Our implementation spans from file systems to databases, with consistent principles throughout.

File System Permissions leverage Active Directory groups for scalable management. We never assign permissions to individual users, which would create administrative nightmares as people change roles. Instead, users are added to appropriate groups, and groups receive permissions. Inheritance is used thoughtfully - default permissions flow down directory structures, with exceptions only where specifically needed. Regular permission reviews identify and remediate permission creep, where access accumulates over time. Every permission change generates an audit trail, enabling investigation of how inappropriate access might have been granted.

Database Access follows strict security principles given the sensitivity of structured data. Application service accounts provide the only path to production databases - no direct user access is permitted. This design ensures that all data access flows through application logic with appropriate business rules and audit trails. Read-only access for reporting purposes uses separate credentials with query-only permissions. All connections are encrypted using TLS, preventing eavesdropping on database traffic.

Query logging captures all database operations for security analysis and troubleshooting, though we carefully manage these logs given their sensitive nature.

7. Access Reviews and Certification

7.1 Periodic Access Reviews

NIST Controls: AC-2, AU-6, CA-7

Regular access reviews ensure that permissions remain appropriate as roles and responsibilities evolve. Our review program balances thoroughness with the practical limitations of a small team, focusing effort where risk is highest.

Quarterly Reviews focus on high-risk access that requires frequent validation. Managers review all user access for their team members, confirming that current permissions align with job responsibilities. The CTO personally reviews all privileged access, given its critical nature and limited distribution. Service account owners verify that their accounts remain necessary and appropriately scoped. We generate exception reports highlighting unusual access patterns - dormant accounts, excessive privileges, or access anomalies - for focused investigation. Any orphaned accounts discovered are immediately disabled pending investigation of why they weren't properly terminated.

Annual Certification provides comprehensive validation of our entire access control environment. This thorough review examines all systems and applications, not just high-risk areas covered in quarterly reviews. We verify that role definitions remain appropriate for current business operations. Compliance with access control policies is validated through sampling and testing. The results are compiled into a board-level report demonstrating our security posture and any identified areas for improvement. This annual cycle aligns with our policy reviews, enabling updates based on observed patterns and emerging needs.

7.2 Review Process

NIST Controls: AC-2, AU-6

Our review process is designed for efficiency and effectiveness, recognizing that lengthy, complex reviews often go uncompleted or become rubber-stamp exercises.

Manager Review Steps follow a clear workflow that respects managers' time while ensuring thoroughness. Managers receive an access report for their team via secure email, formatted for easy review with clear indicators of changes since the last review. They verify each user's need for current access, considering whether job

responsibilities have changed. Role assignments are confirmed as appropriate, with any needed changes flagged for IT action. The certification is completed through a simple web interface, with automated reminders for overdue reviews. IT implements approved changes within 2 business days, with automated workflows handling common changes. The entire process is designed to take less than 30 minutes per quarter for a typical manager, ensuring compliance without excessive burden.

Automated Reviews supplement human oversight with continuous monitoring. Our systems detect dormant accounts that haven't been used within expected timeframes, flagging them for investigation. Excessive privilege alerts identify users with permissions beyond their peer group, potentially indicating permission creep. Access anomaly detection uses Azure's machine learning capabilities to identify unusual patterns that might indicate compromise or misuse. Compliance dashboards provide real-time visibility into our access control posture, enabling proactive management rather than reactive cleanup. Trend analysis helps identify systemic issues - if multiple users repeatedly need the same additional access, perhaps our role definitions need updating.

7.3 Access Metrics

NIST Controls: AC-2, AU-6, PM-14

Metrics drive improvement by making abstract security concepts concrete and measurable. We track key performance indicators that reflect both security effectiveness and operational efficiency.

Key Performance Indicators are selected for their relevance to our access control objectives. Time to provision access measures our responsiveness to business needs - target is 2 business days for standard requests. Time to revoke access indicates our risk exposure window - target is 2 hours from termination notice. Percentage of reviews certified on time shows process compliance - target is 95% within deadline. Number of exceptions reflects policy appropriateness - too many suggests overly restrictive policies. Orphaned accounts found indicates termination process effectiveness - target is zero. Failed login attempts are monitored for potential attacks - baselines are established with deviations investigated. Privilege escalations are tracked to ensure they follow proper procedures - all should have corresponding approvals.

These metrics are reviewed monthly by IT leadership and quarterly by executive management. Trends are more important than point-in-time values - we look for continuous improvement rather than perfection. When metrics indicate problems, we investigate root causes rather than just addressing symptoms. This data-driven

approach ensures our access control program evolves based on evidence rather than assumptions.

8. Physical Access Controls

8.1 Home Office Security

NIST Controls: PE-3, PE-5, PE-6

As a fully distributed company, traditional physical security controls don't apply - we have no corporate offices or data centers to protect. Instead, our physical security focuses on protecting company assets and data in home office environments.

Requirements for home offices balance security with the reality of residential settings. We encourage dedicated work spaces when possible, recognizing that physical separation improves both security and work-life balance. Screen privacy filters are available upon request for employees who work in shared spaces or public locations. Lockable storage for any printed sensitive documents is required, with lockable file cabinets provided by the company. Device security cables are provided to prevent opportunistic theft of laptops or other equipment. Clean desk practices are mandatory - sensitive information must be secured when not actively in use, not left visible to family members or visitors.

Best Practices guide employees in maintaining security without creating unworkable requirements. Screen locking when stepping away is mandatory, with automatic lock configured for 5-minute idle periods. Video call backgrounds should be professional and not reveal sensitive information visible in the home office. Employees must maintain awareness of who might overhear sensitive calls or see confidential information on screens. Document disposal requires shredding for any printed sensitive information, with home shredders provided by the company. Device placement should consider both ergonomics and security - screens positioned away from windows or high-traffic areas of the home.

We recognize that home environments vary widely and avoid prescriptive requirements that might be impossible in some living situations. Instead, we focus on principles and outcomes, trusting our professionals to implement appropriate controls for their specific circumstances while providing the tools and support they need to do so effectively.

8.2 Device Access Controls

NIST Controls: AC-3, AC-7, IA-2

Device-level controls provide critical protection given that laptops and mobile devices contain gateways to all our corporate resources. These controls must be effective yet not so burdensome that users attempt to circumvent them.

Device Security implements multiple layers of protection. Biometric authentication (fingerprint or face recognition) is preferred where hardware supports it, providing convenient yet secure access. PIN or password protection is mandatory on all devices, with complexity requirements matching our general password policy. Auto-lock engages after 5 minutes of inactivity, balancing security with usability during active work sessions. Full disk encryption protects data at rest, using BitLocker on Windows and FileVault on macOS. Remote wipe capability through Intune enables data protection even if devices are lost or stolen. Find My Device features are enabled to assist in recovery of misplaced equipment and to verify devices haven't left expected locations.

BYOD Policy takes a clear stance: personal devices are not permitted for company data access. This policy simplifies our security management enormously - we don't need to manage the complexity of personal devices with unknown security states. Company devices are provided to all employees who need them, eliminating any business justification for BYOD. While personal use of company devices is acceptable within reason, users understand that these devices are subject to company monitoring and management. Security software is centrally managed and mandatory, with compliance checks preventing non-compliant devices from accessing corporate resources. Regular compliance scans ensure devices maintain required security configurations and updates.

9. Monitoring and Compliance

9.1 Access Monitoring

NIST Controls: AU-2, AU-3, AU-6, AU-12

Continuous monitoring transforms our access controls from preventive to detective, enabling rapid response to security incidents. Our monitoring strategy leverages Azure's built-in capabilities extensively, providing enterprise-grade visibility without enterprise-grade complexity.

Real-time Monitoring focuses on events most likely to indicate security issues. Failed authentication attempts are tracked across all systems, with patterns analyzed for brute force or password spray attacks. Privilege escalations generate immediate alerts, ensuring all use of administrative rights receives scrutiny. After-hours access is

monitored against normal patterns - while our distributed team works various hours, significant deviations warrant investigation. Geographic anomalies like impossible travel (logins from distant locations within unrealistic timeframes) trigger automatic investigation. Concurrent sessions from different locations suggest compromised credentials. Data access patterns are baselined and monitored for unusual bulk downloads or access to typically unused resources.

Alert Thresholds are tuned to balance detection with false positives. Five failed logins trigger account lockout, preventing brute force while accommodating genuine mistakes. Ten failed logins generate security alerts for investigation, as this suggests targeted attack rather than user error. Privileged access use is logged always, with all administrative actions captured for review. New location access generates user notifications, allowing quick identification of unauthorized access. Impossible travel scenarios trigger immediate investigation and potential account suspension pending verification. These thresholds are regularly reviewed and adjusted based on observed patterns and false positive rates.

9.2 Compliance Auditing

NIST Controls: AU-6, CA-2, CA-7

Regular auditing verifies that our controls operate as designed and identifies areas for improvement. Our audit program is scaled appropriately for our size while maintaining rigor where it matters most.

Internal Audits follow a risk-based schedule focusing effort on high-impact areas. Monthly privileged access audits review all administrative actions for appropriateness and policy compliance. Quarterly user access reviews verify that managers are completing certifications and that identified changes are implemented. Semi-annual policy compliance assessments test whether documented procedures are being followed in practice. Annual comprehensive audits examine our entire access control environment, providing input for strategic improvements and policy updates.

Evidence Collection supports both internal audits and external assessments. Access provisioning forms document the request and approval chain for every access grant. Approval documentation is retained electronically, linked to the accounts or permissions granted. Review completion records prove that periodic certifications occurred as required. Exception approvals are tracked centrally with business justifications and expiration dates. Training records demonstrate that users received required security awareness education. This evidence is organized and retained according to our records retention policy, ensuring availability when needed while

managing storage costs.

9.3 Violation Handling

NIST Controls: AC-2, AU-14, IR-5

Clear consequences for policy violations ensure that our access controls are taken seriously while remaining fair and proportionate to the offense.

Violation Types are categorized by severity and intent. Password sharing is strictly prohibited and easily detected through concurrent login analysis. Unauthorized access attempts indicate either malicious intent or serious misunderstanding of policies. Policy circumvention, such as using personal accounts to avoid controls, suggests intentional misconduct. Access misuse involves using legitimate access for inappropriate purposes. Review non-completion by managers indicates failure to fulfill security responsibilities. Each category has defined detection methods and response procedures.

Consequences follow a progressive discipline model that emphasizes correction over punishment. First offenses typically result in a warning and mandatory security training, recognizing that mistakes happen and education often resolves issues. Second offenses trigger formal disciplinary action with HR involvement and documented performance impacts. Third offenses may result in access suspension pending investigation and potential termination. Severe violations - those involving malicious intent, data theft, or actions that place the company at significant risk - may result in immediate termination regardless of prior history. All actions are coordinated with HR to ensure consistency and legal compliance.

10. Exceptions

10.1 Exception Process

NIST Controls: AC-2, CA-5, PM-2

Despite our best efforts to create comprehensive policies, business needs sometimes require exceptions. Our exception process provides a controlled mechanism for deviating from standard policies when justified by business requirements.

Exception Request Requirements ensure that deviations are carefully considered. A clear business justification must explain why standard policies cannot be followed and what business objective requires the exception. Risk assessment identifies potential security impacts and how they'll be managed. Compensating controls must be proposed to mitigate risks introduced by the exception - we never accept risk without mitigation.

Time limitations are mandatory - all exceptions must have expiration dates, forcing periodic reconsideration. The approval authority depends on the risk level and scope of the exception.

Approval Levels match authority to risk. Standard exceptions within IT's normal purview can be approved by the IT Manager, streamlining common needs. Policy deviations that change how we implement security require CTO approval, ensuring technical leadership agrees with the approach. High-risk exceptions that could materially impact our security posture require CEO approval, involving business leadership in significant risk decisions. Exceptions to audit findings cannot be approved at all - these represent compliance requirements that must be addressed through remediation, not exceptions.

10.2 Exception Monitoring

NIST Controls: CA-7, PM-14

Exceptions require ongoing oversight to ensure they remain necessary and that compensating controls remain effective.

Central exception tracking in our IT service management system ensures nothing gets lost or forgotten. Every exception is recorded with its business justification, approval details, compensating controls, and expiration date. Quarterly exception reviews examine all active exceptions, verifying that business needs persist and compensating controls remain effective. Metrics on exception types and frequency identify patterns suggesting policy updates might be needed - frequent exceptions to the same policy indicate the policy might be too restrictive. Root cause analysis for repeated exceptions helps us understand whether our policies align with business reality. When patterns emerge, we consider policy updates rather than perpetual exceptions, keeping our policies relevant and achievable.

11. Technical Implementation

11.1 Azure AD Configuration

NIST Controls: AC-2, AC-3, IA-2

Azure Active Directory serves as our identity and access management foundation, providing sophisticated capabilities that would be impossible for our small team to build or maintain independently.

Security Settings are configured to maximize protection while maintaining usability. Conditional access policies enforce our security requirements consistently - MFA for all cloud access, compliant device requirements, and location-based restrictions where appropriate. Risk-based authentication leverages Microsoft's threat intelligence to identify suspicious logins, automatically requiring additional verification or blocking access entirely. Identity Protection continuously monitors for compromised credentials appearing in breach databases or showing suspicious patterns. Privileged Identity Management (PIM) enables just-in-time administrative access with approval workflows and time limitations. Access reviews are configured to automatically remind managers of certification requirements and track completion.

Integration Points extend Azure AD's protection across our environment. Azure DevOps inherits our authentication policies, ensuring source code receives the same protection as other resources. Microsoft 365 integration provides seamless user experience while maintaining security controls. Third-party applications integrate via SAML or OAuth where possible, extending single sign-on benefits. On-premises systems, where they exist, integrate through Azure AD Connect or application proxies. API management leverages Azure AD for OAuth token issuance and validation. This pervasive integration ensures consistent security policies regardless of which system users access.

11.2 Tools and Technologies

NIST Controls: AC-2, AC-3, IA-2

Our tool selection emphasizes cloud-native solutions that provide enterprise capabilities without enterprise complexity or cost.

Identity Management centers on Azure Active Directory for all user authentication and authorization. Azure AD B2B enables secure partner collaboration without creating security islands or shadow IT. Multi-Factor Authentication is provided natively through Azure AD with multiple options for user preference. Privileged Identity Management controls administrative access with sophisticated workflows. Identity Protection provides continuous security monitoring using Microsoft's global threat intelligence. These integrated tools work together seamlessly, providing defense in depth without integration headaches.

Access Control Tools extend beyond identity to protect resources and data. Azure RBAC provides granular permissions management for all Azure resources with inheritance and deny assignments. Key Vault centralizes secret management, eliminating passwords in code or configuration files. Conditional Access creates

dynamic access policies that adapt to risk levels and context. Just-In-Time Access reduces standing privileges by granting access only when needed. Azure Bastion eliminates exposed RDP/SSH endpoints while maintaining administrative access. Together, these tools implement our zero-trust principles without requiring extensive custom development.

12. Training Requirements

12.1 User Training

NIST Controls: AT-2, AT-3, AT-4

Effective access control requires users who understand both how to use our systems and why security measures exist. Our training program provides practical, relevant education without overwhelming non-technical staff.

All Users receive foundational security training covering essential topics. Password security training explains our requirements and provides practical tips for creating strong, memorable passwords. MFA usage training ensures everyone can successfully use their chosen authentication methods. Phishing awareness remains critical given that social engineering often targets credentials. The access request process is explained so users know how to get the access they need through proper channels. Security responsibilities are clearly communicated - users are our first line of defense, not passive consumers of IT services.

Managers receive additional training on their specific responsibilities. The access review process is demonstrated with hands-on practice to ensure comfort with the tools and procedures. Approval responsibilities are explained, emphasizing the security impact of carelessly approved access. Segregation of duties principles help managers understand why certain combinations of access create risks. Monitoring reports are explained so managers can identify concerning patterns in their teams. Compliance requirements are covered to ensure managers understand the regulatory and contractual obligations we must meet.

12.2 Specialized Training

NIST Controls: AT-3, AT-4

Technical staff and privileged users require deeper training commensurate with their enhanced access and responsibilities.

IT Staff receive comprehensive technical training on our tools and procedures. Azure AD administration covers the full lifecycle of user management and advanced features. Access provisioning procedures ensure consistency and security in how access is granted. Monitoring tools training enables proactive security management rather than reactive response. Incident response procedures prepare IT staff to handle security events effectively. Audit support training ensures IT can efficiently provide evidence for internal and external audits. This technical training is supplemented with ongoing education as our tools and threats evolve.

Privileged Users understand that with great power comes great responsibility. Enhanced security requirements are explained in detail - why privileged accounts need stronger controls. PAW usage training ensures these specialized workstations are used correctly for maximum protection. Incident indicators help privileged users recognize when their powerful access might be under attack. Evidence preservation procedures ensure that privileged users don't inadvertently destroy forensic data during incident response. Compliance obligations are emphasized, as privileged users can single-handedly cause compliance failures. Regular refresher training keeps these critical skills sharp.

13. Related Documents

NIST Controls: PL-4, PM-4

This Access Control Policy operates within a broader security documentation framework. Related documents provide additional detail on specific topics:

- **Information Security Policy**: Establishes overall security governance and principles
- **Password Standards**: Detailed technical requirements for password construction and management
- **Incident Response Plan**: Procedures for handling security events including access violations
- **Acceptable Use Policy**: Defines appropriate use of access privileges once granted
- **Remote Work Policy**: Additional controls for our distributed workforce
- **Data Classification Policy**: Determines what access controls apply to different data types
- **Identity Management Procedures**: Step-by-step instructions for common access control tasks

14. Definitions

NIST Controls: PM-7

Clear definitions ensure consistent understanding across our organization:

Access Control: Technical and administrative means of restricting system and data access to authorized entities

Authentication: Process of verifying the claimed identity of a user, system, or service

Authorization: Granting of specific access rights after successful authentication

MFA (Multi-Factor Authentication): Authentication requiring two or more independent factors

Privilege: Ability to perform security-relevant functions that ordinary users cannot

RBAC (Role-Based Access Control): Access control model using roles as the primary grouping mechanism

Service Account: Non-interactive account used by applications or automated processes

SSO (Single Sign-On): Authentication scheme allowing one set of credentials for multiple systems

15. Document Control

NIST Controls: PM-4, SA-5

Version	Date	Author	Changes
1.0	January 1, 2025	CTO	Initial comprehensive version
2.0	Jun 25, 2025	CTO	Added NIST control mappings throughout document and new Appendix B

Review and Approval

- **Prepared By**: _____ **Date:** ____

- **Approved By**: _____ **Date:** ____

Next Review Date: January 1, 2026

Distribution:

- All Employees: Via company policy portal
- IT Team: Direct distribution for implementation
- Executive Team
- External Auditors (upon request)

16. Appendices

Appendix A: Access Request Form

User Information

- Full Name: _____
- Department: _____
- Manager: _____
- Start Date: _____
- Employee Type: [ ] Full-time [ ] Contractor [ ] Partner

Access Requested

- [ ] Email and Microsoft 365
- [ ] Azure DevOps Repository Access
- [ ] VPN Remote Access
- [ ] Specific Application: _____
- [ ] Other: _____

Role Assignment

- [ ] Developer
- [ ] Senior Developer
- [ ] DevOps Engineer
- [ ] Support Staff
- [ ] Administrative Staff
- [ ] Other: _____

Business Justification

Please explain why this access is needed:

_____

_____

_____

Time Limitation (if applicable)

- Start Date: _____
- End Date: _____
- Reason for temporary access: _____

Approvals

- Requesting Manager: _____ **Date:** __
- HR Verification: _____ **Date:** __
- IT Review: _____ **Date:** __
- CTO (if privileged): _____ **Date:** __

Appendix B: NIST Control Mapping

This policy addresses the following NIST SP 800-53 controls:

Access Control Family (AC)

- AC-1: Access Control Policy and Procedures - Sections 1, 13, 15
- AC-2: Account Management - Sections 3, 5, 7, 9, 10
- AC-3: Access Enforcement - Sections 1, 2, 5, 6, 8
- AC-4: Information Flow Enforcement - Sections 2, 6
- AC-5: Separation of Duties - Sections 2, 5
- AC-6: Least Privilege - Sections 1, 5
- AC-7: Unsuccessful Login Attempts - Sections 4, 8
- AC-11: Session Lock - Section 4
- AC-12: Session Termination - Section 4

Audit and Accountability Family (AU)

- AU-2: Audit Events - Section 9
- AU-3: Content of Audit Records - Section 9
- AU-6: Audit Review, Analysis, and Reporting - Sections 7, 9
- AU-12: Audit Generation - Section 9
- AU-14: Session Audit - Section 9

Identification and Authentication Family (IA)

- IA-2: Identification and Authentication - Sections 4, 6, 11
- IA-5: Authenticator Management - Section 4

Security Assessment Family (CA)

- CA-2: Security Assessments - Section 9
- CA-5: Plan of Action and Milestones - Section 10
- CA-7: Continuous Monitoring - Sections 7, 9, 10

Planning Family (PL)

- PL-2: System Security Plan - Section 1
- PL-4: Rules of Behavior - Section 13

Personnel Security Family (PS)

- PS-4: Personnel Termination - Section 3
- PS-5: Personnel Transfer - Section 3

Physical and Environmental Protection Family (PE)

- PE-3: Physical Access Control - Section 8
- PE-5: Access Control for Output Devices - Section 8
- PE-6: Monitoring Physical Access - Section 8

Program Management Family (PM)

- PM-2: Senior Information Security Officer - Section 10
- PM-4: Plan of Action and Milestones Process - Sections 13, 15
- PM-7: Enterprise Architecture - Section 14
- PM-14: Testing, Training, and Monitoring - Sections 7, 10, 12

System and Communications Protection Family (SC)

- SC-7: Boundary Protection - Section 2, 6
- SC-8: Transmission Confidentiality and Integrity - Section 6
- SC-32: Information System Partitioning - Section 2

System and Services Acquisition Family (SA)

- SA-5: Information System Documentation - Section 15

Awareness and Training Family (AT)

- AT-2: Security Awareness Training - Section 12

- AT-3: Role-Based Security Training - Section 12
- AT-4: Security Training Records - Section 12

Incident Response Family (IR)

- IR-5: Incident Monitoring - Section 9

Appendix C: Role Matrix

Role	System Access	Data Access	Administrative	Privileged
Developer	DevOps, Dev Environment	Source Code, Dev Data	None	No
Senior Developer	DevOps, Dev, Limited Prod	Source Code, Logs	Code Merge	No
DevOps Engineer	All Environments	Infrastructure Config	Deployment	Yes
Support Staff	Ticketing, Docs	KB Articles, Logs	Ticket Admin	No
Administrative Staff	Business Apps	Corporate Data	User Provisioning	Limited
Manager	Standard + Reports	Team Data	Approval Workflows	No
Executive	All Standard Systems	All Business Data	Policy Override	Limited

Legend:

- System Access: Which systems the role can log into
- Data Access: What types of data the role can view/modify
- Administrative: Any administrative functions available
- Privileged: Whether the role includes privileged access requiring enhanced controls