Asset Management and Data Protection 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

Asset Management and Data Protection 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: CM-1, CM-8, MP-1, SC-1

The Asset Management and Data Protection Policy establishes OversiteAI's comprehensive framework for identifying, classifying, protecting, and managing information assets throughout their lifecycle. This policy ensures that our company's valuable assets, particularly our source code and intellectual property, receive appropriate protection while maintaining operational efficiency suitable for our size and business model.

As a software company that provides client-hosted data collection and correlation solutions, we recognize that our primary assets are our intellectual property and the infrastructure that supports our development efforts. This policy addresses the unique challenges of protecting these assets while respecting our architectural design principle that customer data never enters our environment.

1.2 Scope

NIST Controls: CM-1, MP-1, PL-2

This policy applies to all OversiteAI information assets, including but not limited to hardware devices, software applications, cloud resources, source code, documentation, and any other resources that support our business operations. The policy covers all employees, contractors, and third parties who have access to company assets.

The scope specifically encompasses asset identification and inventory management, data classification and handling procedures, encryption standards for data protection, security configuration baselines, vulnerability management processes, and endpoint and network security controls. While our software operates entirely within customer environments, this policy focuses exclusively on protecting OversiteAI's corporate assets and does not address customer data, which by design never enters our systems.

1.3 Policy Objectives

NIST Controls: PM-1, PM-11

Through implementation of this policy, OversiteAI aims to maintain accurate inventory of all company assets, ensure appropriate protection based on asset value and

sensitivity, prevent unauthorized access or disclosure of confidential information, comply with relevant regulatory and contractual requirements, and optimize asset utilization while managing associated risks. These objectives support our broader information security goals while remaining practical for a small software company.

2. Policy Statement

2.1 Management Commitment

NIST Controls: PM-1, PM-2, SA-4

OversiteAI is committed to protecting its information assets through a risk-based approach that balances security requirements with operational needs. Management recognizes that our source code, development infrastructure, and intellectual property represent our competitive advantage and require robust protection. We leverage cloud-native security features and automation wherever possible to achieve enterprise-grade security without the overhead of traditional approaches.

Our asset management philosophy emphasizes simplicity and automation. Rather than maintaining complex manual processes, we utilize Azure's built-in capabilities for asset discovery, classification, and protection. This approach allows our small team to maintain security visibility without dedicating personnel solely to asset management tasks.

2.2 Core Principles

NIST Controls: CM-2, SC-28, SI-12

Our asset management and data protection practices are guided by several key principles. First, we maintain complete visibility of all company assets through automated discovery and regular reconciliation. Second, we classify information based on its sensitivity and business impact, applying protection measures proportionate to the classification level. Third, we enforce encryption for all sensitive data, both at rest and in transit, using industry-standard algorithms and key management practices.

Additionally, we implement defense-in-depth through layered security controls, maintain secure baseline configurations for all systems, and conduct regular vulnerability assessments with timely remediation. These principles ensure comprehensive protection while avoiding unnecessary complexity that could hinder our development velocity.

2.3 Privacy by Design

NIST Controls: SC-7, PL-8, AR-5

A fundamental aspect of our asset management approach is our privacy-by-design architecture. Our software operates exclusively within customer environments, meaning customer data never enters our infrastructure. This architectural decision eliminates entire categories of data protection requirements and allows us to focus our security efforts on protecting our intellectual property and corporate information. This design choice represents a significant security advantage that we maintain through strict architectural governance.

3. Asset Management Program

3.1 Asset Categories and Identification

NIST Controls: CM-8, PM-5

OversiteAI maintains a comprehensive inventory of assets across four primary categories, each with specific tracking and protection requirements. Our hardware assets include all company-provided laptops, workstations, and mobile devices used by employees for development and business activities. Given our fully remote workforce, this category also encompasses home office network equipment that connects to company resources. Each hardware asset is uniquely identified through serial numbers and asset tags, with ownership and location tracked in our central inventory system.

Software assets comprise our licensed applications, development tools, security software, and SaaS subscriptions that support our operations. We maintain particular focus on development tools and integrated development environments (IDEs) that directly interact with our source code. Cloud assets represent a critical category given our Azure-centric infrastructure, including all subscriptions, virtual machines, storage accounts, container instances, and networking resources. These assets are dynamically tracked through Azure Resource Manager tags and governance policies.

Our most valuable asset category is information assets, primarily consisting of our source code, algorithms, technical documentation, and architectural designs. This category also includes customer contracts, internal procedures, and other business-critical documentation. Each information asset is classified according to its sensitivity and business impact, ensuring appropriate protection measures are applied consistently.

3.2 Asset Inventory Management

NIST Controls: CM-8, CM-3, PM-5

We maintain our asset inventory through a combination of automated discovery and periodic reconciliation processes. For hardware assets, we utilize a centralized spreadsheet that captures essential details including serial numbers, assignment information, purchase dates, warranty status, and configuration specifications. This inventory is reconciled monthly against active directory records and VPN access logs to ensure all devices accessing company resources are properly tracked and authorized.

Cloud resource tracking leverages Azure's native capabilities extensively. We enforce a comprehensive tagging strategy through Azure Policy, requiring all resources to be tagged with environment designation (Development, Testing, or Production), owner identification, project association, and cost center allocation. Azure Resource Manager continuously monitors our infrastructure, providing real-time visibility into resource deployment, configuration, and utilization. We supplement this automated tracking with quarterly optimization reviews that identify underutilized resources, ensure proper tagging compliance, and validate that resources align with approved projects.

Software license management follows a structured approach to ensure compliance and optimize costs. We maintain a central license registry that tracks all software subscriptions, including purchase details, license counts, assignment records, and renewal dates. This registry integrates with our calendar system to provide advance notice of upcoming renewals, allowing time for usage evaluation and negotiation. Quarterly compliance checks validate that deployed software matches our license entitlements, with any discrepancies investigated and resolved promptly.

3.3 Asset Lifecycle Management

NIST Controls: CM-2, CM-3, SA-4, SA-10

Our asset lifecycle management process encompasses four distinct phases, each with specific controls and requirements. During the procurement phase, all asset acquisitions require documented business justification and budget approval according to established spending limits. New software undergoes security review before approval, including evaluation of vendor security practices, data handling requirements, and integration risks. Hardware procurement follows standardized configurations to ensure consistency and security.

The deployment phase emphasizes security from the start. All assets receive appropriate security configurations before being placed into service, including

encryption enablement, security software installation, and hardening according to our baseline standards. Assets are properly tagged and recorded in our inventory systems, with clear ownership assignment and access controls configured. We provide necessary training to users, ensuring they understand their responsibilities for protecting assigned assets.

Throughout the maintenance phase, we ensure assets remain secure and functional through regular updates, continuous monitoring, and periodic reviews. Our patch management process, integrated with change control procedures, ensures security updates are applied according to risk-based timelines. Performance monitoring helps identify assets requiring upgrade or replacement, while security scanning validates continued compliance with our standards.

The disposal phase receives particular attention given the sensitive nature of our information assets. All storage devices undergo secure data sanitization following NIST 800-88 guidelines, with certificates of destruction obtained for devices containing sensitive data. We update asset records to reflect disposal, ensuring our inventory remains accurate. For cloud resources, we follow documented decommissioning procedures that ensure all data is properly migrated or destroyed before resource deletion.

4. Data Classification and Handling

4.1 Classification Framework

NIST Controls: RA-2, SC-8, MP-2

OversiteAI employs a four-tier data classification system that provides clear guidance on protection requirements while remaining simple enough for all employees to understand and apply. Our classification levels reflect the potential business impact of unauthorized disclosure, with specific handling requirements scaled appropriately to our organization's size and risk profile.

Confidential data represents our most sensitive information, including source code, proprietary algorithms, security configurations, credentials, employee personal information, and detailed customer contracts. This classification requires the highest level of protection, as unauthorized disclosure could significantly damage our competitive position or violate legal obligations. All Confidential data must be encrypted at rest and in transit, with access restricted to individuals with documented business need and appropriate authorization.

Restricted data encompasses information that could moderately impact our operations if disclosed, such as internal procedures, system architecture documentation, customer configuration templates, and detailed project plans. While not as sensitive as Confidential data, Restricted information still requires access controls and should only be shared with employees and authorized contractors who need it for their job functions. This data must be protected when transmitted over public networks and stored only in approved company systems.

Internal data includes general business information intended for employee use but not public distribution, such as company announcements, meeting notes, training materials, and general correspondence. While this data doesn't require encryption, it should be protected from unauthorized external access and clearly marked to prevent inadvertent public disclosure. Public data comprises information explicitly intended for external distribution, including marketing materials, public documentation, job postings, and press releases, requiring no special protection measures beyond ensuring accuracy and appropriate approval before release.

4.2 Data Handling Procedures

NIST Controls: MP-4, MP-5, SC-8, SC-28

Our data handling procedures are designed to be practical and enforceable within our small team environment while ensuring appropriate protection for each classification level. For Confidential data, we mandate storage exclusively in encrypted repositories such as Azure Key Vault for secrets and credentials, encrypted Git repositories for source code, and BitLocker-encrypted local storage for temporary work files. Access requires multi-factor authentication plus explicit need-to-know authorization, with all access logged for audit purposes. We retain Confidential data for seven years to meet potential legal and contractual obligations.

Restricted data may be stored in our standard collaboration platforms including Azure DevOps, SharePoint, and Microsoft Teams, with role-based access controls enforced. While encryption at rest is provided by these platforms, we require additional encryption for any Restricted data transmitted outside our corporate environment. Access is limited to employees and contractors with relevant job functions, with quarterly reviews to remove unnecessary permissions. We maintain Restricted data for three years unless specific regulatory requirements dictate longer retention.

The handling of Internal and Public data follows more relaxed procedures appropriate to their sensitivity. Internal data can be stored in any company-approved system and shared freely among employees, though we prohibit storage on personal devices or

unapproved cloud services. Public data requires only verification of accuracy and appropriate approval before external distribution, with version control maintained for all published materials.

4.3 Data Transmission Security

NIST Controls: SC-8, SC-13, AC-4

Our approach to data transmission security recognizes both our small team dynamics and our architectural advantage of never handling customer data. For Confidential data, we enforce encryption for all transmissions using TLS 1.2 or higher for network communications and encrypted email for sensitive attachments. Source code commits require SSH key authentication with encrypted transport, while API keys and credentials must never be transmitted via email or instant messaging, instead using secure secret sharing tools.

Restricted data transmission requirements vary by context. Within our corporate environment, platform-provided encryption suffices. However, when Restricted data must traverse public networks or be shared with external parties, we require explicit encryption through VPN connections, encrypted email, or secure file transfer services. We prohibit the use of personal email accounts or consumer file-sharing services for any company data.

A critical aspect of our data protection strategy is our complete prohibition on physical media for data transfer. We do not accept or provide data on USB drives, optical media, or any other removable storage devices. This policy eliminates an entire category of data loss risks while aligning with modern cloud-based workflows. All data transfers occur through approved electronic channels with appropriate encryption and access controls.

5. Encryption Standards

5.1 Encryption Requirements

NIST Controls: SC-8, SC-13, SC-28

OversiteAI implements comprehensive encryption standards that leverage cloud-native capabilities while ensuring consistent protection across all data states. Our encryption strategy emphasizes automation and platform integration to minimize administrative overhead while maintaining strong security.

For data at rest, we mandate full disk encryption on all endpoint devices using platform-native solutions: BitLocker for Windows systems and FileVault for macOS devices. These solutions integrate with our device management approach, allowing remote verification of encryption status without requiring dedicated endpoint management infrastructure. In our Azure environment, we enable Storage Service Encryption for all storage accounts and Transparent Data Encryption for databases, providing automatic encryption without application changes. All backups receive additional encryption with keys managed separately from the data they protect.

Data in transit protection relies on modern cryptographic protocols with TLS 1.2 as our minimum standard for all network communications. We configure Perfect Forward Secrecy where supported, ensuring that compromise of long-term keys cannot decrypt past communications. VPN connections for remote access employ AES-256 encryption with certificate-based authentication preferred over passwords. All web services enforce HTTPS with HTTP Strict Transport Security headers, preventing downgrade attacks.

5.2 Key Management Practices

NIST Controls: SC-12, SC-17

Our key management approach balances security with operational practicality, leveraging Azure Key Vault as our primary key management system. Production encryption keys reside in a dedicated Key Vault with Hardware Security Module backing for our most critical keys. Development and test environments use separate Key Vaults to ensure complete isolation between environments. This segregation prevents accidental exposure of production keys during development activities.

Key rotation follows a risk-based schedule that considers both security requirements and operational impact. We rotate data encryption keys annually through Azure's key versioning capabilities, allowing transparent rotation without service disruption. Service account passwords rotate every 90 days using Azure AD's automated rotation features where possible, with manual rotation procedures documented for legacy systems. API keys rotate every 180 days with overlap periods to ensure smooth transitions. SSL certificates renew before expiration with automated monitoring providing 30-day advance warnings.

Access to encryption keys follows strict least-privilege principles enforced through Azure's role-based access control. Production keys remain accessible only to designated production systems and break-glass emergency accounts. We maintain comprehensive audit trails for all key access, with alerts configured for unusual access patterns. Our

key recovery procedures include secure backup of key material in geographically distributed Key Vaults, documented restoration procedures tested quarterly, and clear escalation paths for emergency access.

5.3 Customer Environment Considerations

NIST Controls: SC-7, SC-13

While our encryption standards apply strictly to OversiteAI infrastructure, we recognize our responsibility to enable strong encryption within customer environments where our software operates. Our software includes built-in encryption capabilities that customers can configure according to their security requirements. We provide comprehensive documentation on encryption configuration options, recommended key management practices, and integration with customer key management systems.

Importantly, our architectural design ensures we never possess the ability to decrypt customer data, as we never have access to customer encryption keys or data. This separation provides an additional layer of security beyond technical controls, eliminating the risk of insider threats or external compromise of OversiteAI systems leading to customer data exposure.

6. Security Configuration Management

6.1 Configuration Standards Development

NIST Controls: CM-1, CM-2, CM-6

OversiteAI maintains security configuration baselines that reflect industry best practices adapted to our operational reality as a small software company. Rather than implementing complex configuration management databases, we leverage Infrastructure as Code principles and cloud-native governance features to ensure consistent, secure configurations across our environment.

Our configuration standards derive from multiple authoritative sources including CIS Benchmarks, Azure Security Baseline recommendations, and vendor security guidance, filtered through our risk assessment process to identify controls appropriate to our size and threat model. We prioritize configurations that can be automated and monitored through platform capabilities, avoiding manual processes that don't scale with our lean team structure. Each baseline configuration undergoes testing in our development environment to validate functionality and identify potential impacts on developer productivity before production implementation.

We document our configuration standards in version-controlled runbooks that serve both as implementation guides and compliance references. These runbooks include specific settings with security justification, implementation commands or scripts, validation procedures to confirm correct application, and rollback instructions for cases where configurations cause issues. This approach ensures consistency while maintaining flexibility to adapt configurations as our environment evolves.

6.2 Implementation and Enforcement

NIST Controls: CM-2, CM-6, CM-7

Configuration deployment follows our Infrastructure as Code methodology, with all production configurations defined in version-controlled templates and scripts. For Azure resources, we use ARM templates and Azure Policy to enforce configurations at deployment time, preventing non-compliant resources from being created. This proactive approach proves more effective than retroactive remediation and aligns with our preference for automation over manual intervention.

Endpoint configurations leverage platform-specific tools to maintain consistency. Windows systems receive configurations through PowerShell Desired State Configuration scripts that establish security baselines including BitLocker encryption settings, Windows Defender configurations, firewall rules, and user rights assignments. MacOS systems use configuration profiles distributed through our MDM-lite approach, enforcing FileVault encryption, Gatekeeper settings, firewall enablement, and screen lock requirements. For the few Linux systems in our environment, we maintain Ansible playbooks that configure security settings while preserving the flexibility developers need.

Our cloud configurations benefit from Azure's extensive governance capabilities. We implement Azure Policy initiatives that enforce encryption requirements, network security rules, diagnostic logging settings, and resource tagging standards. These policies operate in enforcement mode for production resources while using audit mode for development environments, balancing security with developer flexibility. Azure Security Center provides continuous monitoring of configuration compliance, generating alerts for drift detection and offering remediation guidance.

6.3 Configuration Monitoring and Drift Management

NIST Controls: CM-3, CM-4, SI-7

Configuration drift represents a significant security risk, particularly in dynamic cloud environments. We address this through continuous monitoring that leverages platform

capabilities rather than building custom solutions. Azure Security Center serves as our primary configuration monitoring tool, providing real-time visibility into compliance status across our Azure resources. We configure automated alerts for high-priority deviations such as encryption disabled on storage accounts, network security groups modified to allow unrestricted access, diagnostic logging disabled on critical resources, or unapproved software installed on endpoints.

Our response to configuration drift depends on the severity and scope of the deviation. For critical security configurations, we implement automated remediation where possible, such as re-enabling encryption or restoring network security rules. Non-critical deviations generate tickets for manual review, allowing us to determine whether the change was intentional and requires baseline updates or represents unauthorized modification requiring remediation. This graduated response prevents alert fatigue while ensuring serious issues receive immediate attention.

Monthly configuration reviews supplement our continuous monitoring, providing opportunity to validate that our baselines remain appropriate and identify patterns in drift that might indicate need for baseline adjustments. During these reviews, we examine Azure Policy compliance reports, Security Center recommendations, endpoint configuration summaries, and change logs from our configuration management tools. Findings feed into our continuous improvement process, helping refine our standards to better balance security with operational needs.

7. Vulnerability Management

7.1 Vulnerability Identification

NIST Controls: RA-3, RA-5, SI-2

Our vulnerability management program takes a pragmatic approach appropriate to our size while ensuring comprehensive coverage of our attack surface. We employ multiple identification methods that leverage automated tools and cloud-native capabilities to maintain visibility without requiring dedicated security personnel.

Azure Security Center provides continuous vulnerability assessment for our cloud infrastructure, automatically scanning for misconfigurations, missing patches, and security recommendations. This platform-native approach requires no additional agents or scanners, delivering actionable findings directly integrated with our Azure environment. For web applications, we utilize OWASP ZAP in our CI/CD pipeline, performing automated security testing with each build. This shift-left approach identifies vulnerabilities during development when they're easiest and least expensive

to fix.

Dependency scanning represents a critical component given modern software's reliance on open-source components. We employ GitHub's Dependabot for automated vulnerability detection in our code dependencies, receiving immediate alerts when new vulnerabilities are disclosed in packages we use. This proactive approach has prevented several potential security incidents by identifying vulnerable components before they reached production. Additionally, we conduct annual penetration testing through qualified third parties, providing an external perspective on our security posture and validating our internal assessments.

7.2 Risk Assessment and Prioritization

NIST Controls: RA-3, RA-5, PM-9

Not all vulnerabilities pose equal risk to our organization, and our small team cannot address every finding immediately. We therefore implement a risk-based approach to vulnerability prioritization that considers both technical severity and business context. Our prioritization framework uses the Common Vulnerability Scoring System (CVSS) as a starting baseline but adjusts priorities based on factors specific to our environment.

Critical vulnerabilities (CVSS 9.0-10.0) affecting internet-facing systems or core infrastructure receive immediate attention, with remediation required within 7 days. These might include remote code execution vulnerabilities in web applications, authentication bypasses in critical systems, or data exposure risks in production databases. High-severity vulnerabilities (CVSS 7.0-8.9) require remediation within 14 days, while medium severity (CVSS 4.0-6.9) allows 30 days for resolution. Low-severity findings (CVSS 0.1-3.9) are addressed within 90 days or during regular maintenance windows.

However, we adjust these timelines based on compensating controls and actual exploitability. For instance, a critical vulnerability in a system isolated within our internal network might receive a lower practical priority than a medium vulnerability in an internet-facing application. We document these risk-based decisions in our vulnerability tracking system, ensuring auditors understand our reasoning and demonstrating mature security thinking despite our small size.

7.3 Remediation Process

NIST Controls: SI-2, SI-5, CA-5

Our remediation process balances speed with stability, recognizing that rushed fixes can cause more damage than the vulnerabilities they address. For each identified vulnerability, we follow a structured approach that begins with validation and impact assessment. We verify the vulnerability's presence in our environment and determine affected systems, potential business impact, and required remediation effort.

Remediation planning considers multiple options including patching, configuration changes, compensating controls, or in rare cases, risk acceptance. We prefer automated patching through Azure Update Management for infrastructure components and automated dependency updates for code libraries. When patches aren't immediately available, we implement compensating controls such as network isolation, increased monitoring, or temporary functionality restrictions. All remediation activities follow our change management process, with expedited procedures for critical vulnerabilities.

Post-remediation validation ensures fixes are effective without introducing new issues. We rescan remediated systems to confirm vulnerability resolution, validate that business functionality remains intact, and update our vulnerability database with remediation details. This closed-loop process provides evidence of our vulnerability management effectiveness and helps identify patterns that might indicate systemic issues requiring broader attention.

8. Endpoint Security

8.1 Endpoint Protection Strategy

NIST Controls: SI-3, SI-4, SC-7

Our endpoint security approach recognizes that our fully remote workforce operates from diverse locations without traditional network perimeters. We therefore implement strong endpoint protections that function regardless of network location while remaining manageable for our small IT team. Our strategy emphasizes platform-native security features supplemented with carefully selected third-party tools that integrate with our existing infrastructure.

For Windows endpoints, we standardize on Windows Defender Antivirus and Windows Defender for Endpoint, providing anti-malware protection, behavioral analysis, and endpoint detection and response (EDR) capabilities. These Microsoft solutions integrate seamlessly with our Azure infrastructure, providing centralized visibility through Azure Security Center without requiring separate management consoles. MacOS endpoints utilize XProtect and Gatekeeper for baseline protection, supplemented with

CrowdStrike Falcon for advanced threat detection. This combination provides platform-appropriate security while maintaining consistent EDR capabilities across operating systems.

Beyond anti-malware, our endpoint protection encompasses full disk encryption, host-based firewalls configured to default-deny incoming connections, automatic security updates with deferral options for testing, and application control preventing unauthorized software installation. We enforce these protections through a combination of Group Policy for Windows systems and configuration profiles for macOS, with compliance monitoring through our asset management processes.

8.2 Device Compliance and Monitoring

NIST Controls: CM-8, SI-4, PM-6

Maintaining visibility into endpoint compliance without enterprise-scale management tools requires creative approaches. We implement a lightweight compliance framework that leverages cloud services and automation to provide necessary oversight without overwhelming our team. Each endpoint must meet baseline compliance requirements before accessing company resources, with ongoing monitoring to detect deviations.

Our compliance requirements include encryption enabled and verified, operating system fully patched within 30 days of release, anti-malware active with current definitions, firewall enabled with approved configuration, screen lock configured for 5-minute timeout, and strong authentication (password or biometric) required. We validate compliance through monthly automated scans using PowerShell scripts for Windows and shell scripts for macOS, with results aggregated in our SharePoint-based compliance dashboard.

Non-compliant devices trigger graduated responses based on the severity of non-compliance and duration. Initial non-compliance generates email notifications to device owners with self-remediation instructions. Continued non-compliance after 48 hours escalates to IT team intervention and potential access restrictions. Critical non-compliance, such as disabled encryption or anti-malware, results in immediate VPN access suspension until remediation. This automated enforcement reduces manual intervention while ensuring security standards are maintained.

8.3 Mobile Device Management

NIST Controls: AC-19, AC-20, MP-7

Our mobile device approach reflects our security principles while acknowledging the realities of a small, distributed team. Rather than implementing complex Mobile Device Management (MDM) solutions, we maintain a clear separation between corporate and personal devices. Company-issued mobile devices, provided when role requirements justify, receive basic security configurations including device encryption, strong passcode requirements, remote wipe capability, automatic lock after 5 minutes, and restriction to approved applications.

We explicitly prohibit storing or accessing company data on personal mobile devices, eliminating the complexity of Bring Your Own Device (BYOD) programs. Employees can access email and collaboration tools through web interfaces on personal devices, but cannot install corporate applications or download sensitive data. This clear boundary simplifies our security model while respecting employee privacy. For roles requiring mobile access to sensitive systems, we provide dedicated company devices with appropriate protections.

Remote wipe capabilities for company devices are managed through Azure AD integration, allowing IT administrators to remotely wipe lost or stolen devices. We test these capabilities quarterly and maintain clear procedures for employees to report device loss. Our incident response plan includes specific provisions for mobile device compromise, ensuring rapid response to potential data exposure.

9. Network Security

9.1 Network Architecture and Segmentation

NIST Controls: SC-7, SC-20, AC-4

OversiteAI's network architecture reflects our cloud-first, fully remote operational model. We maintain no traditional corporate network infrastructure, instead relying on cloud-native networking capabilities and zero-trust principles. This approach eliminates the complexity of managing physical network devices while providing superior security through software-defined controls.

Our Azure infrastructure implements comprehensive network segmentation through Virtual Networks (VNets) and Network Security Groups (NSGs). Production resources operate in isolated VNets with no direct connectivity to development or testing environments. Management access occurs through Azure Bastion or Just-In-Time VM access, eliminating persistent management connections that could be exploited. We implement hub-and-spoke network topology where shared services reside in a central hub VNet, with environment-specific resources in spoke VNets connected through

Azure VNet peering with appropriate route filtering.

Network Security Groups enforce granular traffic control at both subnet and network interface levels. We follow a default-deny approach, explicitly allowing only required communications. Production NSGs restrict inbound traffic to specific ports and source IPs, while development environments allow slightly more permissive rules to facilitate debugging and testing. All NSG changes require change management approval and are logged for audit purposes. We review NSG rules quarterly to remove unnecessary permissions and ensure continued alignment with the principle of least privilege.

9.2 Remote Access Security

NIST Controls: AC-17, IA-2, SC-8

Our fully remote workforce necessitates robust remote access controls that provide security without impeding productivity. We implement a multi-layered approach to remote access that begins with endpoint compliance validation, requires strong authentication, and provides monitored access to corporate resources.

VPN access serves as our primary remote connectivity method, utilizing Azure VPN Gateway with certificate-based authentication supplementing username/password credentials. We configure split-tunneling as disabled, ensuring all traffic flows through our monitored infrastructure when connected to corporate resources. VPN connections automatically terminate after 12 hours of continuous connection or 30 minutes of inactivity, requiring re-authentication to maintain access. This approach balances security with usability for our distributed team.

Multi-factor authentication is mandatory for all remote access, including VPN connections, Azure portal access, and critical SaaS applications. We utilize Azure AD Multi-Factor Authentication, providing flexible second-factor options including mobile app notifications, SMS codes, and hardware tokens for high-privilege accounts. Conditional access policies enforce additional requirements based on risk signals, such as requiring re-authentication when accessing sensitive resources from new locations or devices.

9.3 Network Monitoring and Threat Detection

NIST Controls: SI-4, AU-12, IR-4

Network visibility in a cloud environment requires different approaches than traditional network monitoring. We leverage Azure-native capabilities extensively, supplemented with targeted third-party solutions where platform capabilities fall short. This approach

provides comprehensive visibility while avoiding the complexity of managing separate SIEM infrastructure.

Azure Network Watcher provides packet capture, flow logs, and connection monitoring across our Azure infrastructure. We enable NSG flow logs for all production network security groups, with logs forwarded to Log Analytics for analysis and long-term retention. Azure Traffic Analytics processes these flow logs, providing visualizations of traffic patterns and automatic detection of suspicious activities such as unusual data transfers, connections from unexpected geographic locations, or communication with known malicious IPs.

For advanced threat detection, we rely on Azure Sentinel's cloud-native SIEM capabilities. Sentinel aggregates signals from across our environment including Azure activity logs, sign-in logs, endpoint telemetry, and third-party services. We configure detection rules for common attack patterns while avoiding false-positive-prone generic rules that would overwhelm our small team. Custom analytics rules focus on behaviors specific to our environment, such as source code repository access from unusual locations or mass file downloads that could indicate data exfiltration.

10. Compliance and Audit

10.1 Compliance Framework

NIST Controls: CA-2, CA-7, PM-9

OversiteAI's compliance approach focuses on meeting SOC 2 Type II requirements while maintaining flexibility for future compliance needs. Rather than implementing heavyweight compliance management systems, we build compliance into our operational processes and leverage automation to reduce manual compliance efforts.

Our compliance framework maps security controls to SOC 2 Trust Service Criteria, with clear documentation of how each control addresses specific criteria. We maintain this mapping in a simple spreadsheet that links policies, procedures, and technical controls to relevant TSC requirements. This straightforward approach allows us to demonstrate compliance without creating administrative burden. Where our small size prevents implementation of traditional enterprise controls, we document compensating controls that achieve equivalent risk reduction through alternative means.

Regular compliance assessments validate our control effectiveness. We conduct quarterly internal reviews focusing on different control areas each quarter, ensuring complete coverage annually. These assessments use standardized checklists derived

from our control mappings, with evidence collection automated where possible. For example, Azure Policy compliance reports provide automatic evidence of configuration control effectiveness, while PowerShell scripts gather endpoint compliance data. This automation-first approach ensures consistent evidence collection without requiring extensive manual effort.

10.2 Audit Preparation and Support

NIST Controls: AU-6, CA-2, PM-9

Preparing for external audits requires organized evidence management and clear documentation of our security practices. We maintain an audit evidence repository in SharePoint, organized by control objective and time period. This repository includes automated reports from security tools, screenshots of security configurations, change management records, training completion certificates, and incident response documentation. By maintaining this repository continuously rather than scrambling before audits, we reduce audit preparation stress and ensure evidence accuracy.

Our audit support process emphasizes transparency and education. We recognize that auditors may be unfamiliar with cloud-native security approaches or small company operational models. We therefore prepare clear explanations of how our automated controls achieve security objectives, why certain enterprise-style controls are inappropriate for our size, and how our compensating controls provide equivalent protection. This educational approach helps auditors understand our security posture and reduces likelihood of findings based on misunderstanding rather than actual control deficiencies.

During audit fieldwork, we designate a primary audit liaison who coordinates evidence requests and schedules interviews. This single point of contact prevents auditor requests from disrupting multiple team members while ensuring timely response to information needs. We maintain an audit communication log tracking all requests, responses, and open items, ensuring nothing falls through the cracks during the intensive audit period.

10.3 Continuous Compliance Improvement

NIST Controls: CA-5, PM-4, PM-31

Compliance is not a point-in-time achievement but an ongoing journey. We implement continuous improvement processes that incorporate lessons learned from audits, industry developments, and our own operational experiences. Each audit finding, whether from internal assessments or external audits, triggers root cause analysis to

identify systemic improvements rather than just point fixes.

Our improvement process includes quarterly control effectiveness reviews examining metrics and key performance indicators, annual policy and procedure updates reflecting operational changes and lessons learned, regular benchmarking against industry practices appropriate to our size, and proactive identification of emerging compliance requirements. We track improvements through our change management process, ensuring modifications to controls are properly tested and documented before implementation.

We also maintain awareness of evolving compliance requirements that might affect our business. While currently focused on SOC 2, we monitor developments in privacy regulations, industry-specific requirements, and customer compliance needs. This forward-looking approach allows us to build flexible controls that can adapt to new requirements without complete overhaul, protecting our investment in compliance infrastructure.

11. Metrics and Reporting

11.1 Key Performance Indicators

NIST Controls: PM-6, PM-11, CA-7

Effective security management requires measurable objectives that demonstrate control effectiveness and guide improvement efforts. Our metrics program focuses on actionable indicators that our small team can influence rather than vanity metrics that look impressive but provide little practical value. We select KPIs that directly relate to our risk profile and can be collected automatically or with minimal manual effort.

Our asset management metrics include asset inventory accuracy measured through monthly reconciliation, tracking the percentage of assets properly recorded with current information. We monitor unlicensed software instances detected during quarterly compliance scans, aiming for zero unauthorized installations. Hardware refresh compliance ensures devices are replaced before becoming security liabilities, with metrics tracking the percentage of devices within support lifecycle. Cloud resource utilization metrics help optimize costs while ensuring appropriate security controls, measuring the percentage of resources with proper tagging and security configurations.

Security operational metrics focus on vulnerability management effectiveness and configuration compliance. We track mean time to detect vulnerabilities through

automated scanning frequency and tool coverage percentages. Mean time to remediate measures our responsiveness, with separate tracking for each severity level. Patch compliance percentage indicates our success at maintaining current security updates within defined timelines. Configuration drift metrics reveal how well our automation maintains desired security states, measuring the percentage of systems matching approved baselines.

11.2 Reporting Structure

NIST Controls: AU-6, PM-11

Our reporting structure provides appropriate visibility to different stakeholder groups without creating reporting fatigue. We generate automated reports wherever possible, using Azure Monitor workbooks, Security Center dashboards, and PowerBI for data visualization. This automation ensures consistent reporting while minimizing manual effort that could be better spent on security improvements.

Monthly operational reports target IT and development teams, providing detailed metrics on vulnerability status by system and severity, patch compliance with specific systems requiring attention, configuration drift detection with remediation priorities, and license compliance status with upcoming renewals. These reports include specific action items and owners, ensuring findings translate into improvements rather than just documentation.

Quarterly management reports provide executive visibility into security program effectiveness. These reports emphasize trends rather than point-in-time data, highlighting improvement or degradation in key metrics. We include security incident frequency and impact analysis, compliance assessment results with remediation progress, security investment effectiveness measuring return on security spending, and risk landscape changes affecting our threat model. Graphics and trend lines make data accessible to non-technical executives while supporting appendices provide detail for those wanting deeper analysis.

11.3 Continuous Monitoring Dashboard

NIST Controls: CA-7, PM-6, SI-4

Beyond periodic reports, we maintain real-time security dashboards accessible to all team members. These dashboards aggregate data from multiple sources into unified views that provide immediate visibility into our security posture. We utilize Azure Sentinel workbooks as our primary dashboard platform, leveraging its native integration with our security tools and flexible visualization capabilities.

Our primary security dashboard displays current threat level based on active incidents and alerts, vulnerability counts by severity with age tracking, patch compliance percentage with systems requiring immediate attention, configuration compliance status with drift alerts, and active security incidents with response status. Color coding (green/yellow/red) provides at-a-glance status assessment, while drill-down capabilities allow investigation of specific issues. We review dashboard design quarterly, adjusting based on user feedback and changing priorities.

For development teams, we provide specialized dashboards focusing on application security metrics including dependency vulnerabilities in code repositories, security test results from CI/CD pipelines, code quality metrics related to security, and production deployment security validations. These development-focused dashboards integrate with existing developer workflows, displaying in tools developers already use rather than requiring separate security interfaces.

12. Roles and Responsibilities

12.1 Asset Owners

NIST Controls: CM-9, PM-2, PS-7

Asset owners bear primary responsibility for protecting assigned resources throughout their lifecycle. In our flat organizational structure, asset ownership typically aligns with functional responsibilities - developers own development systems, sales team members own their CRM access, and so forth. This direct ownership model ensures those most familiar with assets take responsibility for their protection.

Asset owner responsibilities include maintaining accurate asset information in our inventory systems, ensuring assigned assets receive required updates and patches, reporting any security concerns or incidents promptly, following data classification and handling procedures, completing required security training related to their assets, and supporting audit activities by providing evidence as needed. For critical assets like production systems or repositories containing source code, we designate primary and backup owners to ensure continuous coverage.

We recognize that security is not most employees' primary function, so we provide tools and automation to simplify their security responsibilities. Automated patching reduces manual update burden, clear classification guidelines eliminate guesswork about data handling, and self-service security tools allow owners to validate compliance without IT intervention. Regular training reinforces these responsibilities while building security awareness throughout our organization.

12.2 IT Team Responsibilities

NIST Controls: PM-2, PS-7, SA-11

Our IT team serves as the primary implementers and maintainers of security controls, translating policy requirements into technical reality. Given our small size, IT team members wear multiple hats, balancing security responsibilities with operational support, development infrastructure, and other technical needs. This reality shapes how we structure IT security responsibilities to be achievable alongside other duties.

Core IT security responsibilities include maintaining asset inventory systems with regular reconciliation, deploying and updating security configurations across all platforms, monitoring compliance through automated tools and dashboards, coordinating vulnerability remediation efforts, managing privileged access and authentication systems, responding to security alerts and incidents, and supporting audit activities with evidence collection. The IT team also serves as security subject matter experts, advising other teams on secure implementation approaches and evaluating new technologies for security implications.

To manage these responsibilities efficiently, we emphasize automation and platform integration. Rather than building custom security tools, we leverage Azure Security Center, Sentinel, and other platform features that provide enterprise capabilities without enterprise overhead. We document standard operating procedures for common security tasks, enabling any IT team member to execute critical processes. This cross-training ensures security operations continue even when specific team members are unavailable.

12.3 Management Responsibilities

NIST Controls: PM-1, PM-2, PS-7

Executive management demonstrates security commitment through active participation in the security program rather than mere policy approval. Our leadership team understands that security culture flows from the top, and their actions set the tone for organizational security behavior. This visible commitment proves particularly important in our small organization where executives interact directly with all team members.

Management responsibilities include establishing and communicating security policies and priorities, ensuring adequate resources for security initiatives, participating in risk assessment and acceptance decisions, reviewing security metrics and improvement plans, supporting security training and awareness programs, and demonstrating compliance with security policies in their own actions. During incidents, management

provides clear decision-making authority and supports the incident response team with necessary resources.

Our executives participate in quarterly security reviews, examining metrics, discussing significant risks, and approving improvement initiatives. These reviews balance security needs with business objectives, ensuring security enhances rather than hinders our business success. Management also maintains external relationships with auditors, customers, and partners regarding security matters, presenting our security posture and addressing concerns at the appropriate level.

12.4 All Employee Responsibilities

NIST Controls: AT-2, PS-7, PM-13

Every OversiteAI employee shares responsibility for protecting company assets and maintaining our security posture. We foster a security-conscious culture where employees understand that security is everyone's job, not just the IT team's responsibility. This distributed security model proves essential for small organizations that cannot afford dedicated security staff for every function.

Universal security responsibilities include protecting assigned assets from theft, loss, or unauthorized access; following data classification and handling procedures for all information they process; using strong, unique passwords with multi-factor authentication; reporting security incidents or concerns immediately without fear of blame; completing assigned security training within required timeframes; and maintaining awareness of social engineering and phishing attempts. Employees must also ensure visiting guests or contractors do not gain unauthorized access to systems or information.

We reinforce these responsibilities through regular security awareness communications, celebrating security successes, and creating an environment where security questions are encouraged. Our no-blame incident reporting culture ensures employees report mistakes promptly, allowing rapid response and learning from near-misses. By making security part of everyone's job description, we achieve better protection than organizations relying solely on technical controls.

13. Exceptions and Waivers

13.1 Exception Request Process

NIST Controls: CA-5, PM-2, RA-3

While our security policies reflect careful consideration of risks and operational needs, we recognize that legitimate business requirements sometimes conflict with security controls. Our exception process provides a formal mechanism for evaluating and potentially approving deviations from standard security requirements while maintaining appropriate oversight and risk management.

Exception requests must document the specific control requirement that cannot be met, the business justification for the exception, the duration for which the exception is needed, proposed compensating controls to mitigate risks, and potential impact if the exception is not granted. Requesters submit exceptions through our IT ticketing system using a standardized form that ensures consistent information capture. This formal process prevents informal workarounds that could create unmanaged security gaps.

Upon receipt, the IT team performs initial risk assessment, evaluating the technical implications of the requested exception. This assessment considers the criticality of the affected system, sensitivity of data involved, effectiveness of proposed compensating controls, and potential for exception to create precedent. The assessment results in a risk rating (low, medium, high) that determines the approval authority required and influences the decision process.

13.2 Approval Authority

NIST Controls: PM-2, RA-3

Our exception approval hierarchy reflects risk levels while remaining practical for our small organization. Low-risk exceptions, such as temporary delays in non-critical patching or minor configuration deviations in development environments, require only IT Manager approval. These exceptions typically involve minimal data exposure risk and include effective compensating controls.

Medium-risk exceptions require Chief Technology Officer approval. These might include extended delays in security updates for critical systems, deviations from encryption standards with strong compensating controls, or temporary use of non-standard tools for specific projects. The CTO evaluates these exceptions considering both technical risks and business impact, potentially requiring additional compensating controls before approval.

High-risk exceptions demand Chief Executive Officer approval, reflecting their potential impact on our overall security posture. Examples include any exception affecting customer-facing systems, deviations from core security principles like data isolation, or exceptions without viable compensating controls. These exceptions receive

intense scrutiny and are approved only when business necessity absolutely requires the deviation.

13.3 Exception Management and Review

NIST Controls: CA-5, CA-7, PM-14

Approved exceptions are not permanent variances but temporary accommodations requiring active management. We maintain a central exception registry tracking all approved exceptions with their business justification, risk assessment results, approval documentation, compensating controls implemented, and expiration dates. This registry provides visibility into our exception landscape and ensures temporary exceptions don't become permanent through neglect.

Exception owners must provide monthly status updates confirming compensating controls remain effective, progress toward exception remediation, and any changes in risk profile. These updates flow through our standard reporting channels, ensuring management visibility into outstanding exceptions. If circumstances change making the exception unnecessary or increasing its risk, owners must immediately notify the security team for re-evaluation.

All exceptions undergo formal review at least quarterly or upon expiration, whichever comes first. During review, we assess whether the business need continues, compensating controls remain effective, and progress toward elimination is satisfactory. Extensions require re-approval at the original level or higher if risk has increased. We track exception trends to identify systemic issues requiring policy updates or architectural changes, ensuring our security program evolves with business needs.

14. Policy Compliance

14.1 Compliance Monitoring

NIST Controls: CA-2, CA-7, PM-14

Ensuring adherence to this policy requires continuous monitoring that balances thoroughness with our operational constraints. We implement automated compliance monitoring wherever possible, leveraging platform capabilities and scripted checks to provide visibility without manual review burden. This automation-first approach ensures consistent monitoring while freeing our team for higher-value security activities.

Technical compliance monitoring utilizes Azure Policy for cloud resources, PowerShell Desired State Configuration for Windows endpoints, and custom scripts for application-specific requirements. These tools continuously or periodically assess compliance with our security baselines, generating alerts for deviations requiring attention. We aggregate monitoring data in Log Analytics, providing centralized visibility and enabling trend analysis across our environment.

Process compliance monitoring proves more challenging but equally important. We track completion of required security activities through our ticketing system, including vulnerability remediation within defined timelines, completion of security reviews for new software, and timely updates to asset inventory. SharePoint lists maintain training completion records and policy acknowledgments. Quarterly compliance reports synthesize technical and process monitoring results, providing management with clear visibility into policy adherence.

14.2 Non-Compliance Response

NIST Controls: IR-5, PM-14

When monitoring detects non-compliance, our response varies based on severity and scope. Technical non-compliance typically triggers automated or semi-automated remediation. For example, Azure Policy can automatically re-enable encryption on non-compliant storage accounts, while endpoint management scripts can reinstall missing security software. This immediate response contains risk while we investigate root causes.

Process non-compliance requires more nuanced responses. Initial violations typically result in coaching and re-training, recognizing that our small team may occasionally miss requirements despite best intentions. We document these conversations and provide specific guidance on achieving compliance. Repeated violations escalate through our management chain, potentially resulting in formal performance discussions. However, our focus remains on achieving compliance rather than punishment, working with employees to identify and address barriers to policy adherence.

For systemic non-compliance affecting multiple systems or processes, we initiate root cause analysis to understand underlying issues. These analyses often reveal policy requirements that prove impractical for our environment, unclear guidance requiring clarification, or missing tools preventing easy compliance. Findings feed into our policy update process, ensuring our requirements remain achievable while maintaining appropriate security.

14.3 Enforcement and Accountability

NIST Controls: AC-2, PS-8, PM-14

While we prefer cooperative approaches to compliance, clear enforcement mechanisms ensure policy requirements receive appropriate attention. Our enforcement strategy emphasizes prevention and detection over punishment, but includes defined consequences for willful non-compliance that threatens our security posture.

Technical enforcement occurs through preventive controls wherever possible. Azure Policy prevents creation of non-compliant resources, network security groups block unauthorized connections, and conditional access policies restrict access from non-compliant devices. These technical controls enforce policy requirements without relying on user compliance, providing consistent security regardless of human factors.

For areas where technical enforcement isn't feasible, we rely on detective controls with defined escalation procedures. First violations trigger automated notifications to asset owners with remediation instructions. Continued non-compliance escalates to management attention and potential access restrictions. Severe violations, such as intentional bypass of security controls or failure to report security incidents, may result in disciplinary action up to termination. However, our no-blame culture for honest mistakes ensures employees report issues without fear, improving our overall security through transparency.

15. Related Documents

15.1 Policy Framework Integration

NIST Controls: PL-4, PM-4

This Asset Management and Data Protection Policy operates within OversiteAI's broader information security framework, with critical dependencies on several related policies and procedures. Understanding these relationships ensures comprehensive security coverage while avoiding redundancy or conflicts between different policy requirements.

Our Information Security Policy serves as the master framework establishing overall security principles and governance structures that this policy implements for specific asset protection needs. The Access Control Policy defines authentication and authorization requirements that protect access to the assets identified and classified under this policy. Together, these policies ensure assets receive protection appropriate to their sensitivity throughout their lifecycle.

The Incident Response Plan provides procedures for responding to security events affecting assets covered by this policy, including data breaches, device theft, or unauthorized access to sensitive information. The Change Management Policy governs modifications to assets and their configurations, ensuring changes don't compromise security controls defined here. The Risk Management Policy guides risk-based decisions for asset protection levels and exception approvals.

15.2 Standard Operating Procedures

NIST Controls: SA-5, PM-4

While this policy establishes what must be done, separate standard operating procedures (SOPs) document how to implement policy requirements. These SOPs provide step-by-step instructions for common tasks, ensuring consistent execution regardless of who performs the activity. Key SOPs supporting this policy include Asset Onboarding Procedures for adding new hardware or software to inventory, Data Classification Guidelines with practical examples for each classification level, Encryption Implementation Guides for various platforms and scenarios, Vulnerability Remediation Workflows with tool-specific instructions, and Configuration Baseline Deployment for each supported platform.

We maintain these SOPs in our SharePoint document library, with version control ensuring teams always access current procedures. Each SOP includes prerequisite requirements, detailed steps with screenshots where appropriate, validation procedures to confirm successful completion, and troubleshooting guides for common issues. Regular reviews ensure SOPs remain accurate as our tools and processes evolve.

15.3 External References

NIST Controls: PM-7, SA-5

Our asset management and data protection practices draw from industry standards and best practices adapted to our organizational context. Key external references include NIST Special Publication 800-53 providing comprehensive security control guidance, CIS Controls offering prioritized security actions, Azure Security Baseline establishing cloud-specific security configurations, and NIST SP 800-88 guiding media sanitization procedures. While we don't implement these frameworks wholesale, we reference them to ensure our practices align with industry standards.

We also maintain relationships with security communities and vendor resources that inform our practices. Microsoft's Azure Security Center recommendations directly

influence our cloud security configurations. OWASP guidance shapes our application security approach. These external inputs ensure our security practices reflect current threats and defensive techniques while remaining achievable for our small team.

16. Definitions

NIST Controls: PM-7

Asset: Any resource of value to OversiteAI, including hardware devices, software applications, cloud resources, data, and intellectual property that requires protection from unauthorized access, use, disclosure, modification, or destruction.

Asset Owner: The individual assigned responsibility for protecting a specific asset throughout its lifecycle, including maintaining accurate inventory information, ensuring appropriate security controls, and supporting audit activities.

Configuration Baseline: A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Data Classification: The process of organizing data into categories based on sensitivity, criticality, and regulatory requirements to ensure appropriate protection levels are applied consistently.

Data at Rest: Information stored on any physical or virtual storage medium, including hard drives, solid-state drives, cloud storage, databases, and backup media.

Data in Transit: Information actively moving from one location to another, such as across the internet or through a private network, including data transfers between cloud services, email communications, and file uploads/downloads.

Encryption: The process of converting readable data into an unreadable format using cryptographic algorithms and keys, ensuring only authorized parties with the correct decryption key can access the original information.

Endpoint: Any device that connects to OversiteAI's network or systems, including laptops, desktops, smartphones, tablets, and IoT devices used for business purposes.

Hardening: The process of securing a system by reducing its attack surface through removing unnecessary software, disabling unused services, configuring security settings, and applying security patches.

Infrastructure as Code (IaC): The practice of managing and provisioning infrastructure through machine-readable definition files rather than physical hardware configuration or interactive configuration tools.

Key Management: The process of administering cryptographic keys throughout their lifecycle, including generation, distribution, storage, rotation, recovery, and destruction.

Network Segmentation: The practice of dividing a computer network into smaller parts to improve performance and security, typically implemented through VLANs, subnets, or software-defined networking.

Patch: A piece of software designed to update a computer program or its supporting data, to fix or improve it, including fixing security vulnerabilities and other bugs.

Remediation: The act of correcting, fixing, or otherwise addressing a security vulnerability, misconfiguration, or policy violation to eliminate or reduce risk.

Security Configuration: The security-relevant settings and parameters of an information system that affect its security posture and must be properly implemented to protect against threats.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source to compromise security.

Zero Trust: A security concept centered on the belief that organizations should not automatically trust anything inside or outside their perimeters and must verify anything and everything trying to connect to systems before granting access.

17. 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 G

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)

18. Appendices

Appendix A: Asset Inventory Template

Asset ID	Asset Type	Description	Owner	Location	Purchase Date	Classification	Encryption Status	Last Audit
[Unique ID]	[Hardware/Software/Cloud/Data]	[Detailed description]	[Name]	[Physical/Cloud location]	[MM/DD/YYYY]	[Confidential/Restricted/Internal/Public]	[Yes/No/N/A]	[MM/DD/YYYY]

Appendix B: Data Classification Quick Reference Guide

CONFIDENTIAL - Our Most Sensitive Data

- Source code and proprietary algorithms
- Security credentials and encryption keys
- Employee personal information (SSN, bank details)
- Detailed customer contracts with pricing
- Strategic plans and confidential financials

Handling: Encrypt always, strict access control, no sharing outside company

RESTRICTED - Important Business Information

- System architecture documentation
- Internal procedures and runbooks
- Customer configuration templates
- Project plans and timelines
- Internal meeting recordings

Handling: Internal use only, encrypt over public networks, role-based access

INTERNAL - General Company Information

- General announcements and updates
- Training materials and guides
- Non-sensitive meeting notes
- Team calendars and schedules
- General correspondence

Handling: Not for public sharing, standard corporate systems only

PUBLIC - Information for External Sharing

- Marketing materials and whitepapers
- Public API documentation
- Job postings and company descriptions
- Press releases and blog posts
- Open source contributions

Handling: No special requirements, ensure accuracy before publishing

Appendix C: Encryption Standards Summary

Encryption Algorithms:

- Symmetric Encryption: AES-256 (minimum AES-128)
- Asymmetric Encryption: RSA-2048 (minimum), ECC P-256
- Hashing: SHA-256 (minimum), SHA-384 preferred
- Key Derivation: PBKDF2, scrypt, or Argon2
- TLS Versions: 1.2 minimum, 1.3 preferred

Platform-Specific Requirements:

- Windows: BitLocker with TPM, AES-256
- macOS: FileVault 2, AES-256
- Linux: LUKS with AES-256
- Cloud Storage: Azure Storage Service Encryption
- Databases: Transparent Data Encryption (TDE)
- Backups: AES-256 with separate key management

Appendix D: Vulnerability Remediation Timeline Matrix

CVSS Score	Severity	Internet-Facing Systems	Internal Systems	Development Systems
9.0-10.0	Critical	48 hours	7 days	14 days
7.0-8.9	High	7 days	14 days	30 days
4.0-6.9	Medium	14 days	30 days	60 days
0.1-3.9	Low	30 days	90 days	Next release

Note: Timelines may be adjusted based on exploitability, compensating controls, and business impact

Appendix E: Security Configuration Checklist

Windows Endpoints:

- [ ] BitLocker enabled and recoverable
- [ ] Windows Defender active and current
- [ ] Firewall enabled with approved rules
- [ ] Automatic updates configured
- [ ] PowerShell execution policy restricted
- [ ] Screen lock at 5 minutes
- [ ] Local admin accounts disabled

macOS Endpoints:

- [ ] FileVault enabled
- [ ] Firewall turned on
- [ ] Gatekeeper enabled
- [ ] Automatic updates active
- [ ] Screen lock required

- [ ] SIP enabled
- [ ] Time Machine encrypted

Azure Resources:

- [ ] Storage encryption enabled
- [ ] Network Security Groups configured
- [ ] Diagnostic logging active
- [ ] Resource tags applied
- [ ] Azure Policy compliant
- [ ] Backup configured
- [ ] Access reviews scheduled

Appendix F: Incident Response Quick Reference

If You Suspect a Security Incident:

1. **STOP** - Don't try to fix it yourself
2. **SECURE** - Disconnect affected systems if safe to do so
3. **REPORT** - Contact IT immediately:
   - Email: security@oversiteai.io
   - Slack: #security-incidents
   - Phone: [Emergency Contact]

Information to Provide:

- What happened and when
- Systems or data affected
- Who else knows about it
- What actions you've taken
- Any error messages or screenshots

Remember: No blame for honest mistakes or being victim of an attack. Quick reporting allows quick response!

Appendix G: NIST Control Mapping

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

Access Control Family (AC)

- AC-2: Account Management - Section 14.3
- AC-4: Information Flow Enforcement - Sections 4.3, 9.1

- AC-17: Remote Access - Section 9.2
- AC-19: Access Control for Mobile Devices - Section 8.3
- AC-20: Use of External Information Systems - Section 8.3

Awareness and Training Family (AT)

- AT-2: Security Awareness Training - Section 12.4

Audit and Accountability Family (AU)

- AU-6: Audit Review, Analysis, and Reporting - Sections 10.2, 11.2
- AU-12: Audit Generation - Section 9.3

Security Assessment and Authorization Family (CA)

- CA-2: Security Assessments - Sections 10.1, 10.2, 14.1
- CA-5: Plan of Action and Milestones - Sections 7.3, 13.1, 13.3
- CA-7: Continuous Monitoring - Sections 10.1, 10.3, 11.3, 13.3, 14.1

Configuration Management Family (CM)

- CM-1: Configuration Management Policy and Procedures - Sections 1, 6.1
- CM-2: Baseline Configuration - Sections 2.2, 3.3, 6.1, 6.2
- CM-3: Configuration Change Control - Sections 3.2, 3.3, 6.3
- CM-4: Security Impact Analysis - Section 6.3
- CM-6: Configuration Settings - Sections 6.1, 6.2
- CM-7: Least Functionality - Section 6.2
- CM-8: Information System Component Inventory - Sections 1.1, 3.1, 3.2, 8.2
- CM-9: Configuration Management Plan - Section 12.1

Identification and Authentication Family (IA)

- IA-2: Identification and Authentication - Section 9.2

Incident Response Family (IR)

- IR-4: Incident Handling - Section 9.3
- IR-5: Incident Monitoring - Section 14.2

Media Protection Family (MP)

- MP-1: Media Protection Policy and Procedures - Sections 1.1, 1.2
- MP-2: Media Access - Section 4.1
- MP-4: Media Storage - Section 4.2
- MP-5: Media Transport - Section 4.2

- MP-7: Media Use - Section 8.3

Physical and Environmental Protection Family (PE)

- None specifically addressed (physical security handled in separate policy)

Planning Family (PL)

- PL-2: System Security Plan - Section 1.2
- PL-4: Rules of Behavior - Section 15.1
- PL-8: Information Security Architecture - Section 2.3

Personnel Security Family (PS)

- PS-7: Third-Party Personnel Security - Sections 12.1, 12.2, 12.3, 12.4
- PS-8: Personnel Sanctions - Section 14.3

Program Management Family (PM)

- PM-1: Information Security Program Plan - Sections 1.3, 2.1, 12.3
- PM-2: Senior Information Security Officer - Sections 2.1, 12.1, 12.2, 12.3, 13.1, 13.2
- PM-4: Plan of Action and Milestones Process - Sections 10.3, 15.1, 15.2, 17
- PM-5: Information System Inventory - Sections 3.1, 3.2
- PM-6: Information Security Measures of Performance - Sections 8.2, 11.1, 11.3
- PM-7: Enterprise Architecture - Sections 15.3, 16
- PM-9: Risk Management Strategy - Sections 7.2, 10.1, 10.2
- PM-11: Mission/Business Process Definition - Sections 1.3, 11.1, 11.2
- PM-13: Information Security Workforce - Section 12.4
- PM-14: Testing, Training, and Monitoring - Sections 13.3, 14.1, 14.2, 14.3
- PM-31: Continuous Process Improvement - Section 10.3

Risk Assessment Family (RA)

- RA-2: Security Categorization - Section 4.1
- RA-3: Risk Assessment - Sections 7.1, 7.2, 13.1, 13.2
- RA-5: Vulnerability Scanning - Sections 7.1, 7.2

System and Services Acquisition Family (SA)

- SA-4: Acquisition Process - Sections 2.1, 3.3
- SA-5: Information System Documentation - Sections 15.2, 15.3, 17
- SA-10: Developer Configuration Management - Section 3.3
- SA-11: Developer Security Testing and Evaluation - Section 12.2

System and Communications Protection Family (SC)

- SC-1: System and Communications Protection Policy and Procedures - Section 1.1
- SC-7: Boundary Protection - Sections 2.3, 5.3, 8.1, 9.1
- SC-8: Transmission Confidentiality and Integrity - Sections 4.1, 4.3, 5.1, 9.2
- SC-12: Cryptographic Key Establishment and Management - Section 5.2
- SC-13: Cryptographic Protection - Sections 4.3, 5.1, 5.3
- SC-17: Public Key Infrastructure Certificates - Section 5.2
- SC-20: Secure Name/Address Resolution Service - Section 9.1
- SC-28: Protection of Information at Rest - Sections 2.2, 4.2, 5.1

System and Information Integrity Family (SI)

- SI-2: Flaw Remediation - Sections 7.1, 7.3
- SI-3: Malicious Code Protection - Section 8.1
- SI-4: Information System Monitoring - Sections 8.1, 8.2, 9.3, 11.3
- SI-5: Security Alerts, Advisories, and Directives - Section 7.3
- SI-7: Software, Firmware, and Information Integrity - Section 6.3
- SI-12: Information Handling and Retention - Section 2.2

Privacy Controls Family (AR)

- AR-5: Privacy Impact Assessment - Section 2.3