Human Resources Security and Governance Policy

OversiteAI, LLC

Document Version:	1.0
Effective Date:	January 1, 2025
Classification:	Internal
Owner:	Chief Executive Officer
Approved By:	

Table of Contents

Human Resources Security and Governance Policy

OversiteAI, LLC

Document Version: 1.0

Effective Date: January 1, 2025

Last Review Date: January 1, 2025

Next Review Date: January 1, 2026

Classification: Internal

Owner: Chief Executive Officer

Domain: oversiteai.io

1. Purpose and Scope

1.1 Purpose

This Human Resources Security and Governance Policy establishes OversiteAI's comprehensive framework for managing personnel-related security risks, defining acceptable use standards, and maintaining appropriate corporate governance while acknowledging our size as a small, remote-first software company. The policy ensures that our human resources practices align with security objectives and that our organization maintains proper oversight without creating unnecessary administrative burden.

As a company that develops client-hosted data collection and correlation solutions, we recognize that our employees are both our greatest asset and a potential security risk. This policy addresses that duality by establishing clear expectations, providing appropriate training, and implementing controls scaled to our size and risk profile. We leverage automation and cloud-native features wherever possible to maintain security without requiring dedicated security staff.

The policy serves multiple purposes within our security program. It establishes the foundation for personnel security throughout the employment lifecycle, defines acceptable behavior for system and resource usage, creates a framework for security awareness and training, and provides governance structures appropriate for a company of our size. By integrating these elements, we create a cohesive approach to human-centered security risks.

Control Mapping: CC1.4, CC1.5, CC2.1, CC2.2, CC9.2

1.2 Scope

This policy applies to all OversiteAI personnel, including full-time employees, part-time employees, contractors, consultants, interns, and any other individuals granted access to our systems or information. The policy covers all stages of the employment relationship from pre-employment screening through post-termination obligations.

The scope encompasses several key areas of human resources security and governance. Personnel security controls apply throughout the employment lifecycle, acceptable use standards govern all company resources and systems, security awareness requirements apply to all personnel regardless of role, and governance structures provide appropriate oversight for our operations. These elements work together to create a comprehensive approach to managing human-related risks.

Geographic scope reflects our remote-first structure, with the policy applying to all personnel regardless of physical location. As a fully remote company operating across multiple jurisdictions, we maintain consistent security standards while respecting local employment laws and regulations. The policy provides the flexibility needed to accommodate different legal requirements while maintaining our security posture.

Control Mapping: CC1.4, CC2.3, CC9.1

1.3 Policy Principles

Our approach to human resources security and governance reflects several key principles that guide implementation across all areas. We believe in implementing controls appropriate to our size and risk profile, leveraging technology to automate processes where practical, maintaining transparency in our expectations and procedures, and fostering a security-conscious culture through positive reinforcement rather than fear.

These principles recognize the realities of operating as a small software company. We cannot afford dedicated security staff or complex approval hierarchies, so we design our controls to be manageable by existing personnel. We emphasize prevention through good hiring practices and clear expectations rather than extensive monitoring. We trust our employees while verifying through appropriate controls.

The balance between security and usability remains critical to our success. Overly restrictive policies lead to workarounds and shadow IT, while insufficient controls expose us to unacceptable risks. This policy seeks the middle ground appropriate for our business model, implementing essential controls while avoiding unnecessary barriers to productivity.

Control Mapping: CC2.1, CC2.2, CC2.3

2. Human Resources Security

2.1 Pre-Employment Screening

Our pre-employment screening process provides appropriate verification of candidate qualifications and background while respecting privacy and maintaining efficiency. We implement screening measures scaled to the sensitivity of each role, recognizing that excessive screening creates unnecessary delays and costs without meaningful security benefits.

For all positions, we require identity verification, employment eligibility confirmation, and professional reference checks. Background checks include criminal history review for the past seven years, verification of previous employment, and confirmation of educational credentials where relevant to the position. We conduct these checks through a reputable third-party provider that maintains appropriate privacy controls and compliance with applicable laws including the Fair Credit Reporting Act (FCRA).

Positions with access to financial systems or sensitive financial data undergo additional screening including credit history review, though we recognize that financial difficulties alone do not disqualify candidates. We evaluate each situation individually, considering the nature of any issues, their relevance to the position, and evidence of rehabilitation or changed circumstances. For positions requiring special trust or accessing particularly sensitive systems, we may conduct extended background checks or request additional references.

The screening process begins only after a conditional offer of employment, ensuring compliance with employment law and avoiding unnecessary expense. Candidates receive clear communication about the screening requirements and their rights under applicable law. Any adverse findings trigger our individualized assessment process, where we consider the nature and gravity of any issues, time elapsed since occurrence, and relevance to the position's duties.

Control Mapping: CC1.4, CC1.5, CC9.2

2.2 Employment Terms and Agreements

Employment relationships at OversiteAI begin with comprehensive written agreements that establish clear expectations for security responsibilities and post-employment obligations. Our employment agreements include perpetual confidentiality obligations that survive termination, intellectual property assignment provisions ensuring company ownership of work product, and non-solicitation clauses protecting our workforce and customer relationships for one year post-employment.

Security responsibilities form an integral part of every employment agreement. Employees acknowledge their obligation to protect company information, comply with security policies, report security concerns promptly, and return all company property upon termination. These provisions create legal enforceability for our security requirements while setting clear expectations from the start of employment.

Contractor and consultant agreements receive equal attention to security provisions. Our Master Service Agreement template includes comprehensive confidentiality

requirements, specific security obligations aligned with our policies, insurance requirements including cyber liability coverage where appropriate, and clear limitations on access and authorized activities. We require all contractors to sign these agreements before receiving any access to our systems or information.

The agreement structure provides flexibility for different types of working relationships while maintaining consistent security standards. Whether engaging full-time employees, part-time staff, or project-based contractors, our agreements ensure that security obligations remain clear and enforceable. Regular legal review ensures these agreements remain current with changing laws and business needs.

Control Mapping: CC1.4, CC9.2, PI1.4

2.3 Onboarding Process

Our security-focused onboarding process ensures new personnel receive appropriate training, access, and equipment while creating a positive first impression of our security culture. The process begins before the first day with preparation of accounts, equipment, and access requirements based on the principle of least privilege.

The onboarding checklist drives consistent implementation across all new hires. HR or the hiring manager ensures completion of employment agreements and policy acknowledgments, submittal of access requests with appropriate approvals, configuration and delivery of company-issued devices, completion of initial security training, enrollment in multi-factor authentication systems, and collection of emergency contact information. This systematic approach prevents security gaps while avoiding overwhelming new employees.

First-day security training introduces our security program in an accessible, engaging manner. Rather than lengthy policy readings, we focus on practical security behaviors including password and MFA setup with hands-on assistance, recognition of phishing attempts using real examples, proper handling of confidential information relevant to their role, incident reporting procedures with emphasis on our no-blame culture, and physical security practices for home offices. This training establishes security as a normal part of our operations rather than an impediment to productivity.

The onboarding process extends through the first 30 days with progressive introduction of more complex security topics. We monitor completion of required training, provide mentorship on security practices, gather feedback on the onboarding experience, and adjust access permissions based on actual job requirements. This graduated approach helps new employees develop strong security habits without overwhelming them during

their initial adjustment period.

Control Mapping: CC1.4, CC1.5, CC2.2, CC9.2

2.4 Termination Process

Our termination process balances security requirements with respectful treatment of departing employees. Whether voluntary or involuntary, all terminations follow a consistent process designed to protect company assets while maintaining professional relationships where possible.

Time-critical actions occur within two hours of termination notification. These include disabling system access across all platforms, revoking VPN certificates and network access, removing email access while preserving data, revoking any physical access controls, implementing legal holds on relevant data, and securing any company equipment in the employee's possession. Our use of centralized identity management through Azure Active Directory enables rapid, comprehensive access revocation without manual intervention across multiple systems.

The complete exit process addresses both security and business continuity needs. Departing employees participate in knowledge transfer sessions to document critical information, return all company property including devices and access tokens, complete exit interviews to gather feedback and identify concerns, receive final compensation and benefits information, and acknowledge post-employment obligations including confidentiality and non-solicitation agreements. We approach these activities professionally, recognizing that today's departing employee might be tomorrow's customer, partner, or returning team member.

Post-termination activities ensure smooth transitions while maintaining security. Email forwarding remains active for 30 days to prevent business disruption, with automated responses informing senders of the employee's departure and providing alternative contacts. We retain employee data according to our retention policies and legal requirements. Clear communication about our reference policy helps departing employees understand what information we will and won't share with future employers.

Control Mapping: CC6.1, CC6.2, CC6.3, CC9.2

3. Acceptable Use Policy

3.1 General Use Standards

Our acceptable use policy establishes clear boundaries for the use of company resources while acknowledging the realities of modern work-life integration. We trust our employees to use good judgment while providing specific guidance on acceptable and prohibited activities.

Acceptable uses of company resources include all business activities and communications necessary for job performance, professional development activities that enhance job-relevant skills, limited personal use that doesn't interfere with job duties or consume excessive resources, and approved open-source contributions that don't conflict with company interests. We recognize that absolute prohibition of personal use is both unrealistic and counterproductive in a remote work environment.

Prohibited activities focus on uses that create legal, security, or reputational risks. These include any illegal activities regardless of jurisdiction, harassment or discrimination in any form, unauthorized access to systems or data beyond assigned privileges, using company resources for personal profit or outside business ventures, political campaigning or religious proselytization, accessing gambling or adult content sites, cryptocurrency mining or other resource-intensive personal projects, and installing unauthorized software that could introduce security risks.

The policy acknowledges gray areas and encourages employees to seek guidance when uncertain. We prefer questions before action rather than apologies after incidents. Managers receive training on how to address acceptable use questions consistently while considering context and business needs.

Control Mapping: CC6.1, CC6.6, CC6.7, CC9.2

3.2 Information Systems Use

Secure use of information systems requires clear standards that employees can reasonably follow. Our requirements focus on essential security behaviors while avoiding overly complex rules that encourage workarounds.

Authentication and access control standards emphasize practical security. Strong passwords remain mandatory, with complexity requirements enforced by our systems rather than relying on user compliance. Automatic screen locking protects unattended devices without requiring users to remember to lock manually. We absolutely prohibit credential sharing, with technical controls preventing password reuse across systems.

Any attempts to bypass security controls trigger immediate investigation, though we distinguish between malicious intent and user frustration with poorly designed systems.

Email and internet use policies reflect professional standards while acknowledging personal needs. We expect professional communication in all business contexts, prohibit spam or chain letters that waste resources and spread malware, require caution with attachments and links through both training and technical controls, and maintain separation between business and personal email accounts. Our email security gateway provides technical enforcement of many policies, reducing reliance on user compliance.

Data handling requirements integrate with our broader data classification scheme. Employees must protect confidential information according to its classification, use only approved methods for data transfer and storage, report any suspected data breaches immediately, and maintain appropriate backups of critical work. We provide secure, user-friendly tools for these activities, recognizing that security controls that impede productivity will be circumvented.

Control Mapping: CC6.1, CC6.2, CC6.3, CC6.7, CC7.2

3.3 Social Media Guidelines

Our social media guidelines acknowledge the blurred lines between personal and professional online presence while protecting company interests. We encourage responsible social media use that enhances both personal and company brands.

Professional social media use, particularly on LinkedIn, supports business objectives. Employees may share company successes and achievements that are already public, represent their professional expertise and company affiliation accurately, network with industry peers and potential partners, and participate in professional discussions relevant to our business. We provide guidance on effective professional social media use without mandating participation.

Personal social media use requires appropriate boundaries to protect company interests. Employees must not claim to officially represent the company unless authorized, share confidential information even inadvertently, disparage the company, colleagues, customers, or partners, or engage in behavior that reflects poorly on our professional reputation. We trust employees to use good judgment while providing clear examples of problematic posts.

The distinction between personal opinion and company position requires careful navigation. Employees speaking on industry topics should clarify when expressing

personal views, especially on controversial subjects. We support employee thought leadership while protecting against unauthorized company commitments or positions.

Control Mapping: CC6.7, CC9.2, PI1.3

3.4 Remote Work Standards

As a fully remote company, our remote work standards form the foundation of our security program rather than an exception to office-based policies. We design all controls with remote work as the default, avoiding the security gaps that plague hybrid approaches.

Home office security begins with the physical workspace. Employees must maintain a secure, private workspace where confidential conversations and data remain protected. This includes using password-protected WiFi networks with current security protocols, educating family members about not accessing company devices, taking precautions when visitors are present, securing physical documents when not in use, and using appropriate backgrounds or blur features during video calls to prevent information disclosure.

Device management in remote environments requires clear policies that employees can realistically follow. We provide company-issued devices for all business data processing, completely prohibiting BYOD for accessing company systems beyond basic communication tools. Personal devices may only be used for email access with enforced security policies, Slack participation without file sharing capabilities, and multi-factor authentication applications. This clear separation between personal and company data reduces both security risks and employee privacy concerns.

Public space work creates unique vulnerabilities requiring specific controls. While we prefer employees work from secure home offices, we recognize that occasional public space work is inevitable. Requirements include using screen privacy filters to prevent shoulder surfing, avoiding confidential calls in public spaces, connecting only through company VPN or verified secure networks, maintaining physical control of devices at all times, and minimizing exposure of sensitive information. These controls balance security with the flexibility our employees need.

Control Mapping: CC6.1, CC6.6, CC6.7, CC6.8

4. Security Awareness Training

4.1 Training Program Structure

Our security awareness training program provides practical, relevant education scaled to our size and risk profile. Rather than generic, checkbox compliance training, we deliver targeted content that helps employees protect themselves and the company.

Initial training for new employees occurs within their first 30 days, integrated with the onboarding process. The curriculum covers security fundamentals in accessible language, company-specific policies and procedures, data protection requirements relevant to their role, incident reporting with emphasis on our learning culture, phishing recognition using real-world examples, and physical security for remote work environments. We deliver this training through a combination of interactive modules, live sessions with experienced team members, and hands-on exercises that reinforce key concepts.

Annual refresher training maintains security awareness without becoming repetitive. Each year's curriculum incorporates updates based on policy changes and new threats, lessons learned from security incidents without blame, changes to tools or processes, evolving compliance requirements, and emerging threats relevant to our industry. We vary delivery methods and content to maintain engagement, recognizing that repetitive training loses effectiveness.

Specialized training addresses role-specific security needs. Developers receive secure coding training aligned with our technology stack, DevOps team members learn cloud security best practices for Azure, personnel handling sensitive data receive privacy training, and incident response team members practice response procedures. This targeted approach ensures relevant, actionable training without wasting time on irrelevant topics.

Control Mapping: CC1.4, CC1.5, CC2.2, CC2.3

4.2 Awareness Activities and Reinforcement

Security awareness extends beyond formal training through ongoing activities that reinforce good security behaviors. Our program uses multiple channels and approaches to maintain security visibility without becoming background noise.

Monthly security tips delivered through Slack provide bite-sized reminders of important security practices. These tips address seasonal concerns like tax scam awareness, emerging threats affecting our industry, lessons learned from public breaches, and

practical advice for home office security. We keep messages brief, actionable, and relevant to daily work.

Quarterly phishing simulations test and reinforce email security awareness. We design simulations to reflect actual threats targeting software companies rather than generic templates. Employees who fall for simulations receive immediate, non-punitive education explaining the warning signs they missed. Those who correctly identify and report simulations receive positive recognition. Our target failure rate of less than 10% reflects realistic expectations for a small company without dedicated security staff.

Knowledge sharing creates a collaborative security culture. We encourage employees to share security articles, discuss security challenges in team meetings, propose security improvements, and celebrate security wins. This approach positions security as everyone's responsibility rather than an imposed requirement from leadership.

Control Mapping: CC1.4, CC1.5, CC2.2

4.3 Training Metrics and Effectiveness

Measuring training effectiveness ensures our program delivers value beyond mere compliance. We track multiple metrics to assess both participation and behavior change.

Participation metrics include completion rates for required training with a target of 100%, time to completion for new hire training, engagement rates for optional security content, and attendance at security awareness events. These quantitative measures ensure basic compliance while identifying potential issues with training delivery or relevance.

Effectiveness metrics focus on behavior change and risk reduction. We measure phishing simulation failure rates over time, security incident frequency and types, self-reported near-misses and concerns, and security-related support requests. Improvement in these metrics indicates true awareness rather than just training completion.

Regular program evaluation incorporates employee feedback, incident analysis, industry benchmarking, and emerging threat assessment. We adjust our training program based on these inputs, maintaining relevance and effectiveness. Annual surveys gather detailed feedback on training quality, relevance, and suggested improvements.

Control Mapping: CC2.1, CC2.2, CC5.1, CC5.2

5. Corporate Governance

5.1 Governance Structure

Our governance structure provides appropriate oversight for a company of our size without creating bureaucratic impediments. We implement a streamlined approach that ensures accountability while maintaining agility.

Board oversight of security matters occurs through quarterly updates and as-needed escalations. The board receives reports on significant security incidents and responses, annual risk assessment results and treatment plans, security budget requirements and resource allocation, strategic security initiatives and major changes, and compliance status including audit results. Board members with relevant expertise provide guidance on security strategy without micromanaging operational decisions.

Executive management maintains hands-on involvement in security governance. The CEO holds overall accountability for security program success, the CTO manages day-to-day security operations and technical controls, and the CFO (when applicable) oversees financial controls and risk management. This direct involvement ensures security remains a business priority without requiring a separate security organization.

Our Security Governance Committee operates informally but effectively. Monthly meetings include the CEO, CTO, and rotating senior team members who review security metrics and trends, discuss recent incidents and lessons learned, approve policy changes and new initiatives, coordinate security efforts across teams, and plan upcoming security activities. Minutes document decisions and action items without creating excessive paperwork.

Control Mapping: CC1.1, CC1.2, CC1.3, CC1.4, CC2.1

5.2 Business Ethics Program

Our business ethics program establishes clear standards for conduct while acknowledging the realities of operating a small company without a dedicated compliance department. We focus on practical ethics that employees can understand and follow.

The Code of Conduct addresses core ethical principles in plain language. Requirements include honest and ethical behavior in all business dealings, compliance with applicable laws and regulations, prompt disclosure of conflicts of interest, fair dealing with customers, partners, and competitors, protection of company assets including intellectual property, maintenance of confidentiality, and creation of a respectful,

inclusive workplace. We provide examples and scenarios to clarify expectations without creating a legalistic document that no one reads.

Ethics reporting mechanisms balance accessibility with practicality for our size. Employees can report concerns directly to their manager or any executive, use our anonymous reporting email that routes to the CEO and board chair, or escalate directly to board members for executive-level concerns. We maintain a strict no-retaliation policy with regular reinforcement that reporting concerns is both welcomed and expected.

Ethics investigations follow a consistent process scaled to issue severity. Upon receiving a report, we conduct an initial assessment to determine scope and urgency, investigate thoroughly while maintaining confidentiality, document findings and recommendations, implement appropriate corrective actions, and communicate outcomes to relevant parties. Serious issues receive immediate board notification and potential external investigation support.

Control Mapping: CC1.1, CC1.4, CC2.1, CC9.2

5.3 Compliance Management

Our compliance management approach focuses on practical implementation of requirements rather than checkbox exercises. We maintain compliance with applicable laws, regulations, and contractual obligations through risk-based prioritization.

Compliance assessments occur annually or when significant changes arise. We review applicable legal and regulatory requirements, assess current compliance status honestly, identify gaps requiring remediation, prioritize based on risk and resource availability, and implement improvements iteratively. This pragmatic approach acknowledges that perfect compliance is neither achievable nor necessary for a company of our size.

Third-party compliance forms an essential component given our reliance on cloud services and external providers. We assess vendor security practices during selection, include appropriate security requirements in contracts, monitor performance through available reports and certifications, and conduct annual reviews of critical vendors. Our vendor management process scales scrutiny to criticality, avoiding excessive diligence on low-risk relationships.

Regulatory change monitoring leverages external resources rather than attempting comprehensive internal tracking. We subscribe to relevant security and privacy newsletters, participate in industry associations for our sector, engage legal counsel for

significant changes, and update policies and procedures as needed. This approach provides adequate awareness without dedicating full-time resources to compliance monitoring.

Control Mapping: CC1.2, CC1.3, CC1.5, CC2.1, CC3.1, CC3.2, CC3.3, CC3.4

6. Security Organization

6.1 Security Roles and Responsibilities

Our security organization embeds responsibilities throughout the company rather than creating a separate security department we cannot afford. This distributed model aligns with our size while ensuring comprehensive coverage.

The Chief Technology Officer serves as our de facto security leader, developing and maintaining security strategy, creating and updating security policies, managing the security budget within IT allocations, leading incident response efforts, and reporting to the board on security matters. This combination with technology leadership ensures security considerations integrate with technical decisions from the start.

Development team members carry specific security responsibilities including implementing secure coding practices, participating in security code reviews, identifying and reporting security concerns, maintaining security of development environments, and contributing to security tool selection. By making security part of normal development activities rather than a separate gate, we achieve better outcomes with less friction.

DevOps personnel manage infrastructure security as part of their operational responsibilities. This includes configuring and maintaining cloud security controls, implementing infrastructure as code with security built in, monitoring for security events and anomalies, maintaining compliance with security policies, and responding to infrastructure security incidents. The integration of security with operations creates more resilient systems.

All employees regardless of role share fundamental security responsibilities. These include protecting confidential information according to classification, following security policies and procedures, reporting security concerns promptly, completing required security training, and maintaining physical security of company assets. This universal participation creates a stronger security culture than relying on a few specialists.

Control Mapping: CC1.2, CC1.4, CC2.2, CC2.3

6.2 External Security Support

Recognizing our size limitations, we strategically engage external security expertise where internal capabilities are insufficient or specialized skills are required. This approach provides access to deep expertise without the overhead of full-time specialists.

Security advisory services supplement our internal capabilities through annual security assessments by qualified firms, penetration testing of critical systems and applications, incident response support for complex situations, compliance guidance for evolving requirements, and strategic security consulting for major initiatives. We select partners who understand small business constraints and can provide practical recommendations.

Key security vendors form an essential part of our extended team. We maintain relationships with legal counsel experienced in data security and privacy, an incident response firm on retainer for major events, forensics capabilities through our IR partner, security training providers for specialized content, and compliance auditors familiar with our industry. These relationships ensure rapid access to expertise when needed.

Vendor selection criteria emphasize practical value over prestigious names. We evaluate expertise relevant to our size and industry, ability to provide actionable recommendations, cost structures appropriate for small businesses, cultural fit with our organization, and references from similar companies. Long-term relationships with vendors who understand our business provide better value than constantly switching providers.

Control Mapping: CC1.2, CC2.1, CC9.1, CC9.2

7. Environmental and Social Governance (ESG)

7.1 Environmental Responsibility

Our environmental responsibility program leverages the inherent efficiency of our cloud-first, remote-work model while implementing additional measures where practical. We recognize that good environmental practices often align with good business practices.

Green IT practices begin with our fundamental architecture choices. Our cloud-first strategy leverages Azure's efficient data centers with renewable energy commitments, advanced cooling systems, and optimized hardware utilization. By avoiding on-premises infrastructure, we eliminate inefficient server rooms, reduce electronic waste, and benefit from Microsoft's economies of scale in environmental management.

Remote work provides substantial environmental benefits beyond IT efficiency. Eliminating daily commutes for all employees significantly reduces transportation emissions. Home offices typically consume less energy than traditional office spaces when allocated per employee. We avoid the environmental costs of maintaining physical offices including HVAC, lighting, and cleaning. Virtual meetings replace business travel for most interactions, reducing aviation emissions.

Additional environmental measures demonstrate commitment within our capabilities. We maintain a paperless office with rare exceptions for legal requirements, properly recycle electronic equipment through certified programs, select energy-efficient equipment when purchasing, encourage employees to use renewable energy at home where available, and offset carbon emissions from necessary business travel. These actions show environmental consciousness without creating undue burden.

Control Mapping: CC2.1, CC3.1

7.2 Social Responsibility

Our social responsibility efforts focus on areas where a small software company can make meaningful contributions without overextending limited resources. We emphasize quality over quantity in our social initiatives.

Diversity and inclusion form core values reflected in our practices. As an equal opportunity employer, we actively work to eliminate bias in hiring through structured interviews and diverse hiring panels. We provide reasonable accommodations for employees with disabilities, create an inclusive culture welcoming all backgrounds and perspectives, and address any discrimination or harassment immediately. Our remote work model inherently supports inclusion by eliminating geographic barriers and providing flexibility for different life circumstances.

Community engagement leverages our technical expertise for broader benefit. We contribute to open source projects aligned with our mission, support local tech communities through speaking and mentoring, offer internships when resources permit to develop new talent, and share non-proprietary knowledge through blog posts and presentations. These activities build our reputation while contributing to the broader

ecosystem.

Employee wellbeing initiatives recognize that sustainable performance requires work-life balance. We offer flexible working hours to accommodate different schedules and time zones, encourage employees to take vacation time and disconnect, provide mental health support through our benefits program, support professional development within budget constraints, and maintain reasonable workload expectations. These practices reduce burnout and turnover while improving security through engaged, alert employees.

Control Mapping: CC1.1, CC2.1

7.3 Corporate Responsibility

Our corporate responsibility program demonstrates ethical business practices appropriate for our size and industry. We focus on doing business the right way rather than elaborate CSR programs we cannot sustain.

Responsible business practices guide all our operations. We conduct business ethically even when no one is watching, treat vendors fairly with prompt payment and reasonable terms, respect customer privacy beyond mere compliance, communicate transparently about our capabilities and limitations, and pursue sustainable growth over short-term gains. These principles build trust with stakeholders while reducing legal and reputational risks.

Customer-centric responsibility acknowledges our unique position providing security infrastructure. We design products with privacy and security by default, provide clear documentation and support, respond promptly to security concerns, maintain transparency about our security practices, and never compromise customer security for business advantage. Our success depends entirely on maintaining customer trust.

Partner and vendor relationships reflect our values through fair dealing. We negotiate contracts in good faith, pay invoices promptly according to terms, provide honest feedback on performance, respect intellectual property rights, and maintain confidentiality of partner information. These practices create a positive ecosystem supporting our growth.

Control Mapping: CC1.1, CC2.1, CC9.1

8. Independent Oversight

8.1 Internal Audit Function

Our internal audit function provides independent assessment scaled to our size and resources. Rather than a full internal audit department, we implement a practical approach providing necessary oversight without excessive overhead.

Audit activities focus on high-risk areas and regulatory requirements. Annual control assessments evaluate the design and effectiveness of key controls, quarterly spot checks verify ongoing compliance with critical policies, process effectiveness reviews identify improvement opportunities, and special audits address specific concerns or incidents. This risk-based approach maximizes value from limited audit resources.

Independence measures ensure objectivity despite our small size. The audit function reports directly to the CEO and board, maintains unrestricted access to systems and information, receives protected budget allocation for activities, and avoids operational responsibilities that create conflicts. When internal resources lack independence for specific reviews, we engage external parties.

Audit findings receive appropriate attention through formal reporting and tracking. We document all findings with risk ratings and recommendations, obtain management responses with remediation commitments, track remediation progress through completion, report status to leadership and board, and incorporate lessons learned into control improvements. This systematic approach ensures audit value beyond mere compliance checking.

Control Mapping: CC4.1, CC4.2, CC4.3, CC5.1, CC5.2, CC5.3

8.2 External Validation

External validation provides independent verification of our security program effectiveness. We engage qualified third parties for assessments that internal resources cannot perform objectively or lack expertise to complete.

Third-party assessments follow a regular schedule aligned with business needs. Annual SOC 2 Type 2 audits provide comprehensive control validation, penetration testing identifies technical vulnerabilities, security assessments evaluate overall program maturity, and targeted compliance reviews address specific requirements. We select assessors based on relevant expertise, industry recognition, and cost-effectiveness.

Transparency in sharing results demonstrates confidence in our security program. We provide SOC 2 reports to customers under NDA, share penetration test executive summaries showing remediation, communicate openly about security improvements underway, and acknowledge areas requiring enhancement. This openness builds trust while maintaining appropriate confidentiality for detailed vulnerabilities.

Continuous improvement drives our response to external findings. We treat all findings as improvement opportunities rather than failures, prioritize remediation based on risk and resources, implement systematic fixes rather than point solutions, measure effectiveness of remediation efforts, and share lessons learned across the organization. This approach transforms audits from compliance exercises into value-generating activities.

Control Mapping: CC4.1, CC4.2, CC4.3, CC5.1

9. Visitor Management

9.1 Physical Visitor Management

While operating as a fully remote company, we maintain visitor management procedures for situations where physical meetings occur, such as team gatherings, client meetings, or co-working space usage.

When meeting in temporary physical spaces, we implement appropriate visitor controls. All visitors sign in with contact information for potential contact tracing, remain escorted by an OversiteAI employee at all times, receive temporary identification if required by the facility, stay restricted from any areas containing sensitive information, and sign out upon departure. These basic controls provide accountability without elaborate systems.

Co-working space usage requires additional precautions given the shared environment. Employees must verify visitor identity before admitting to reserved spaces, avoid displaying sensitive information on screens, use privacy screens when working in open areas, secure devices when stepping away, and conduct confidential calls in private rooms. These practices balance collaboration needs with security requirements.

Home office visits follow special guidelines to protect both security and privacy. Client or partner visits to home offices require advance approval, confidential materials must be secured before visits, video calls should use blurred backgrounds to prevent information disclosure, and family members should understand basic security expectations. We respect employee privacy while maintaining necessary controls.

Control Mapping: CC6.4, CC7.1

9.2 Virtual Visitor Management

Virtual meetings constitute our primary interaction mode, requiring robust controls that don't impede collaboration. Our virtual visitor management balances security with usability for daily operations.

Video conferencing security starts with platform configuration. We enable waiting rooms to control meeting access, require meeting passwords for all external meetings, control screen sharing permissions appropriately, provide notice before recording any sessions, and verify participant identity for sensitive discussions. These settings provide baseline security without making meetings cumbersome.

Meeting hygiene practices protect against common virtual meeting risks. Employees must verify all participants before discussing confidential information, use unique meeting IDs rather than personal rooms for external meetings, end meetings properly to prevent lingering participants, avoid sharing meeting details on public forums, and report any suspicious meeting behavior immediately. Regular reminders reinforce these practices.

Virtual event security scales these practices for larger gatherings. Webinars and all-hands meetings require registration for attendance tracking, use of platform security features like attendee controls, dedicated moderators for chat and Q&A; management, clear recording notices and consent processes, and post-event access controls for recordings. These measures maintain security without limiting valuable interactions.

Control Mapping: CC6.4, CC6.6, CC6.7

10. Enforcement and Violations

10.1 Policy Violation Response

Our approach to policy violations emphasizes learning and improvement while maintaining accountability. We recognize that in a small company, overly punitive approaches damage culture and trust without improving security.

The investigation process balances thoroughness with practicality. When violations are reported or detected, we conduct an initial assessment to understand scope and severity, investigate facts without prejudgment, document findings objectively, determine appropriate responses considering context, and implement actions focused

on preventing recurrence. Throughout this process, we maintain confidentiality and treat individuals with respect.

Progressive discipline provides proportional responses to violations. Verbal warnings address minor first offenses with coaching, written warnings document repeated or more serious violations, performance improvement plans help employees correct ongoing issues, suspension occurs only for serious violations requiring investigation, and termination remains reserved for severe breaches or failure to improve. Legal action may follow criminal activity or serious harm to the company.

The context surrounding violations influences our response. We consider whether the violation was intentional or accidental, the employee's history and overall performance, potential harm or actual damage caused, the employee's response when confronted, and likelihood of recurrence. This nuanced approach maintains fairness while protecting company interests.

Control Mapping: CC1.4, CC1.5, CC9.2

10.2 Positive Reinforcement

Positive reinforcement for good security behaviors proves more effective than punishment alone. Our program recognizes and rewards employees who strengthen our security posture.

Security champion recognition celebrates employees who go beyond basic compliance. We acknowledge those who identify and report security vulnerabilities, propose effective security improvements, help colleagues with security challenges, maintain perfect records in phishing simulations, and demonstrate security leadership in their teams. Recognition includes public acknowledgment, small rewards, and consideration in performance reviews.

Innovation in security receives particular encouragement. Employees who develop tools or processes improving security, identify creative solutions to security challenges, contribute to security automation efforts, or share valuable security knowledge receive both recognition and support for further development. This approach transforms security from a burden into an opportunity for professional growth.

Team celebrations for security achievements build collective ownership. When we achieve security milestones like clean penetration tests, successful audit results, incident-free quarters, or high training completion rates, we celebrate as a company. These celebrations reinforce that security is everyone's responsibility and success.

Control Mapping: CC1.4, CC2.2

11. Metrics and Reporting

11.1 HR Security Metrics

Human resources security metrics focus on measurable outcomes that indicate program effectiveness. We track key indicators without creating excessive measurement burden.

Access management metrics ensure timely privilege changes. We measure time from termination to access revocation with a target under 2 hours, percentage of access reviews completed on schedule, number of unauthorized access attempts detected, and time to provision appropriate new user access. These metrics identify potential gaps in our joiner-mover-leaver processes.

Training and awareness metrics gauge program participation and effectiveness. Key measures include training completion rates by deadline, average time to complete new hire security training, phishing simulation failure rates over time, security incident reports per employee, and security-related help desk tickets. Trends in these metrics show whether our awareness efforts achieve desired behavior changes.

Compliance metrics track adherence to HR security policies. We monitor background check completion before access provisioning, percentage of employees with current signed agreements, policy violation frequency and types, exit process completion rates, and post-termination obligation acknowledgments. These measures ensure consistent policy implementation.

Control Mapping: CC2.1, CC4.1, CC5.1, CC5.2

11.2 Governance Metrics

Governance metrics demonstrate oversight effectiveness and organizational maturity. We select metrics that provide actionable insights without creating bureaucracy.

Leadership engagement metrics confirm appropriate oversight. We track board meeting security discussion frequency, executive participation in security initiatives, time to leadership decision on security matters, security budget approval timeliness, and strategic initiative progress. Strong leadership engagement correlates with program success.

Ethics and compliance metrics indicate organizational culture health. Important measures include ethics hotline usage and case resolution times, conflict of interest disclosures and management, compliance assessment findings and remediation, third-party compliance scores, and employee satisfaction with ethical culture. These metrics provide early warning of cultural issues.

Continuous improvement metrics show program maturation. We measure audit finding remediation rates and timeliness, repeat finding frequency across audits, self-identified issues versus external findings, process improvement implementation rates, and stakeholder satisfaction scores. Positive trends demonstrate a learning organization.

Control Mapping: CC1.3, CC2.1, CC4.3, CC5.1, CC5.2, CC5.3

11.3 Reporting Framework

Our reporting framework delivers relevant information to appropriate audiences without overwhelming recipients or creating excessive reporting burden. We tailor content and frequency to stakeholder needs.

Board reporting occurs quarterly with additional updates for significant events. Reports include executive summaries highlighting key risks and achievements, trending metrics with commentary on significant changes, major incident summaries and remediation status, upcoming initiatives requiring board awareness, and resource needs or constraints affecting security. Visual dashboards supplement detailed reports for quick comprehension.

Management reporting provides operational detail for decision-making. Monthly reports to executives include detailed metrics with trend analysis, incident reports with root cause analysis, project status for security initiatives, resource utilization and needs, and emerging risks requiring attention. These reports support tactical and strategic planning.

Team-level reporting maintains front-line engagement. Weekly or bi-weekly updates share relevant metrics for each team, recent security events and lessons learned, upcoming security activities affecting the team, recognition for security achievements, and reminders of security practices. This communication keeps security visible without becoming noise.

Control Mapping: CC2.1, CC4.1, CC4.2, CC5.1, CC5.2

12. Policy Maintenance

12.1 Review and Update Process

Regular policy review ensures continued relevance and effectiveness. Our annual review cycle examines policy content for accuracy, completeness, and alignment with current practices.

The review process incorporates multiple inputs including regulatory and legal requirement changes, security incident lessons learned, audit findings and recommendations, industry best practice evolution, organizational changes affecting security, technology changes requiring policy updates, and employee feedback on policy effectiveness. This comprehensive approach identifies necessary updates while avoiding change for change's sake.

Update procedures maintain document control while enabling timely changes. Minor updates correcting typos or clarifying language follow expedited approval, moderate changes affecting procedures require security committee review, and major changes affecting multiple stakeholders need executive approval. All changes include clear documentation of what changed and why.

Communication of policy changes ensures organization-wide awareness. We announce updates through standard communication channels, highlight significant changes requiring action, provide training on new requirements, update related procedures and guidelines, and verify understanding through acknowledgment processes. This systematic approach prevents policies from becoming shelfware.

Control Mapping: CC1.3, CC2.1, CC5.3

12.2 Exception Management

Policy exceptions acknowledge that one-size-fits-all approaches don't work for every situation. Our exception process provides flexibility while maintaining control and accountability.

Exception requests require documented business justification including the specific policy requirement requiring exception, business reason the requirement cannot be met, proposed alternative controls mitigating risks, duration of the exception needed, and approval from appropriate management. This documentation ensures thoughtful consideration rather than casual circumvention.

The approval process scales to exception risk and scope. Low-risk temporary exceptions receive manager approval, medium-risk or extended exceptions require security committee review, and high-risk or permanent exceptions need executive approval. All exceptions undergo documented risk assessment considering potential impact and compensating controls.

Exception tracking maintains visibility and accountability. We maintain a central register of all approved exceptions, review exceptions quarterly for continued necessity, revoke exceptions when no longer justified, analyze exception patterns for policy improvement, and report exception status to leadership. This systematic approach prevents exception accumulation while identifying policy improvement opportunities.

Control Mapping: CC1.3, CC2.1, CC3.4, CC5.3

13. Related Documents

The following documents provide additional detail on specific aspects of our security program:

- **Information Security Policy**: Master framework for our security program
- **Access Control Policy**: Detailed authentication and authorization requirements
- **Risk Management Policy**: Risk assessment and treatment procedures
- **Incident Response Plan**: Security event handling procedures
- **Asset Management and Data Protection Policy**: Asset and data security controls
- **Change Management and Business Continuity Policy**: Change control and resilience
- **Privacy and Data Protection Addendum**: Privacy-specific requirements
- **Employee Handbook**: General employment policies and procedures
- **Code of Conduct**: Detailed ethical standards and expectations

These documents work together to create comprehensive security coverage while avoiding duplication. Regular cross-referencing ensures consistency and completeness.

14. Definitions

Acceptable Use: Authorized activities using company resources consistent with business purposes and policy requirements

Background Check: Verification of employee history including criminal records, employment, and education as appropriate to position sensitivity

BYOD (Bring Your Own Device): Personal devices used for business purposes - prohibited for accessing company systems at OversiteAI

Governance: System of rules, practices, and processes for organizational direction and control

Onboarding: Systematic process of integrating new employees including security requirements

Phishing Simulation: Controlled tests of employee ability to recognize malicious emails

Security Champion: Employee demonstrating exceptional security awareness and leadership

Termination: End of employment relationship requiring systematic security control changes

Visitor: Any non-employee granted physical or virtual access to company resources

Document Control

Version	Date	Author	Changes
1.0	January 1, 2025	CEO	Initial comprehensive policy

Review and Approval:

- **Document Owner**: Chief Executive Officer
- **Technical Review**: Chief Technology Officer
- **Legal Review**: [External Legal Counsel]
- **Board Approval**: [Board Chair]

Review Schedule:

- Last Review: January 1, 2025
- Next Review Due: January 1, 2026
- Review Frequency: Annual

Distribution:

This document is classified as Internal and is available to all OversiteAI employees through our standard documentation repository. The current version supersedes all

previous versions.

Appendices

Appendix A: Code of Conduct Acknowledgment Form

I acknowledge that I have read and understood the OversiteAI Code of Conduct and Human Resources Security and Governance Policy. I agree to comply with all provisions contained herein and understand that violation may result in disciplinary action up to and including termination.

Employee Information:

- Name: _____
- Title: _____
- Department: _____
- Date: _____

Acknowledgments:

- [ ] I have received a copy of the Code of Conduct
- [ ] I have read and understood the policy requirements
- [ ] I have had the opportunity to ask questions
- [ ] I agree to comply with all provisions
- [ ] I understand the consequences of violations

Employee Signature: _____

Date: _____

Appendix B: Security Training Completion Record

Employee Name: _____

Initial Security Training

- Information Security Overview: _____ (Date)
- Data Classification: _____ (Date)
- Acceptable Use Policy: _____ (Date)
- Password and MFA Setup: _____ (Date)
- Incident Reporting: _____ (Date)
- Physical Security: _____ (Date)

Annual Refresher Training

- Year 20**:** _____ (Date)
- Year 20**:** _____ (Date)
- Year 20**:** _____ (Date)

Specialized Training (as applicable)

- Secure Coding: _____ (Date)
- Cloud Security: _____ (Date)
- Privacy Training: _____ (Date)
- Incident Response: _____ (Date)

Training Coordinator: _____

Date: _____

Appendix C: Termination Security Checklist

Employee Information

- Name: _____
- Title: _____
- Termination Date: _____
- Type: [ ] Voluntary [ ] Involuntary

Immediate Actions (Within 2 hours)

- [ ] System access disabled (Time: _____)
- [ ] VPN certificates revoked (Time: _____)
- [ ] Email access removed (Time: _____)
- [ ] Building access revoked (Time: _____)
- [ ] Legal hold check completed
- [ ] Manager notified

Exit Process

- [ ] Knowledge transfer documented
- [ ] Company property returned
  - [ ] Laptop/Desktop
  - [ ] Mobile devices
  - [ ] Access cards/tokens
  - [ ] Other: _____

- [ ] Exit interview conducted
- [ ] Final compensation processed
- [ ] Benefits information provided
- [ ] Post-employment obligations reviewed

Post-Termination

- [ ] Email forwarding configured (30 days)
- [ ] Data archived per retention policy
- [ ] Reference policy explained
- [ ] Alumni status updated

Completed By: _____

Date: _____

Verified By: _____

Date: _____

Appendix D: Security Incident Reporting Form

See Incident Response Plan for detailed incident reporting procedures and forms.

Appendix E: Policy Exception Request Form

Exception Request Information

Requestor: _____

Date: _____

Department: _____

Policy Reference

- Policy Name: _____
- Section: _____
- Specific Requirement: _____

Exception Details

- Duration Requested: [ ] Temporary (End date: _____) [ ] Permanent
- Business Justification:

Risk Assessment

- Potential Risks:
- Compensating Controls:

Approvals

- Manager: _____ **Date:** ____
- Security Committee: _____ **Date:** ____
- Executive (if required): ___ **Date:** ____

Exception ID: _____ (Assigned by Security Committee)

Review Dates:

- 90 Day Review: _____
- Annual Review: _____

Appendix F: Visitor Access Log Template

Date: _____

Physical Visitors

Time In	Visitor Name	Company	Host	Purpose	Time Out
Time	Meeting Title	External Participants	Hosts	Sensitive Topics	Recording
					Y/N
					Y/N

Completed By: _____

Review: _____

End of Human Resources Security and Governance Policy