Privacy and Data Protection Addendum

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

Privacy and Data Protection Addendum

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. Executive Summary

Purpose and Scope

This Privacy and Data Protection Addendum establishes OversiteAI's commitment to privacy through architectural design and clarifies how our unique business model—where software operates entirely on customer premises—fundamentally eliminates traditional privacy risks. This document supplements our Information Security Policy and provides transparency about our privacy-by-design approach.

Key Privacy Principles

OversiteAI operates under a revolutionary privacy model: we have architected our solutions to make customer data access technically impossible, not merely restricted by policy. Our software runs exclusively within customer-controlled environments, ensuring complete data sovereignty remains with our customers. This architectural decision represents the strongest possible privacy protection—stronger than any procedural control or contractual commitment could provide.

Document Applicability

This addendum applies to all OversiteAI operations, employees, contractors, and business processes. It clarifies the distinction between the minimal business data we process for our operations and the complete absence of customer data processing in our business model. All team members must understand and support this privacy-first architecture.

Control Mapping: SOC 2 CC1.2, CC1.3, CC1.4, CC1.5, P1.1 | NIST PM-1, AR-1

2. Privacy Architecture Statement

2.1 Fundamental Privacy Design

OversiteAI's approach to privacy represents a paradigm shift from traditional software companies. Rather than implementing complex privacy controls, consent mechanisms, and data processing agreements, we have eliminated the need for these measures through architectural design. Our software operates as a completely isolated system within customer environments, with no capability to transmit data back to OversiteAI.

This design philosophy emerged from our founding principle: the most secure and private data is data we never see. By architecting our solutions to operate entirely on

customer premises without any phone-home functionality, telemetry collection, or cloud dependencies, we've created a system where customer data privacy is guaranteed by the laws of physics and network architecture, not just by policy promises.

Our commitment to this model extends throughout our product lifecycle. When designing new features, the first question is always: "Can this be implemented without any data leaving the customer environment?" If the answer is no, we either redesign the feature or decline to implement it. This unwavering commitment to local-only processing has shaped every aspect of our product development.

2.2 Technical Implementation of Privacy

The technical architecture that enables our privacy-by-design approach consists of several key components. First, our software is distributed as self-contained packages that require no external dependencies or cloud services to function. All processing, analysis, and correlation happen within the customer's network perimeter using only their computational resources.

Second, we've deliberately excluded any telemetry, analytics, or usage tracking from our software. While this means we lack the product insights that many modern software companies rely on, it ensures absolute privacy for our customers. We gather product feedback through voluntary customer advisory boards and support interactions, never through automated data collection.

Third, our update mechanism operates on a pull-only basis. Customers check for updates when they choose to, download them from our secure distribution site, and apply them within their environment. No automatic updates, no forced connections, and no opportunity for data exfiltration exists in this model.

2.3 Privacy Advantages of Our Model

Our architectural approach provides several unique privacy advantages. Data residency is absolute—customer data never moves, so there are no complex questions about international transfers, data localization, or jurisdictional conflicts. Data minimization is maximized—we collect zero customer data, which is the ultimate form of data minimization.

Privacy compliance becomes significantly simpler for our customers. They don't need to evaluate our privacy practices, review our subprocessors, or worry about our compliance with various privacy regulations regarding their data. Since we never touch their data, we can't compromise it, lose it, or misuse it. This dramatically reduces their vendor risk assessment burden and simplifies their own privacy compliance efforts.

Control Mapping: SOC 2 CC1.1, CC3.1, CC6.1, P1.1, P2.1 | NIST AR-1, AR-2, AR-7, UL-2

3. Scope of Data Processing

3.1 Data We Process

While our architecture ensures we never process customer data, we do process limited categories of business data necessary for our operations. Understanding this scope is crucial for transparency and helps clarify the boundaries of our privacy commitments.

Employee Data: We maintain standard human resources records for our employees, including contact information, compensation data, performance records, and benefits information. This data is processed in accordance with employment law requirements and our Employee Privacy Notice. We use Azure Active Directory for identity management and Microsoft 365 for productivity tools, ensuring enterprise-grade security for this sensitive information.

Business Contact Data: We maintain a customer relationship management (CRM) system containing business contact information for sales prospects, customers, and partners. This includes names, business email addresses, company affiliations, and interaction history. We process this data based on legitimate business interest and provide clear opt-out mechanisms for all marketing communications.

Operational Data: Our business operations generate standard operational data including financial records, contracts, support tickets (without customer data), and general business correspondence. This data is processed as necessary for business operations and retained according to legal and business requirements.

3.2 Data We Do Not Process

It's equally important to be explicit about what we do not process. We have no access to, visibility into, or ability to process:

- Customer production data of any kind
- End-user personal information from customer deployments
- Data collected, processed, or analyzed by our software
- Log files or diagnostic information from customer installations
- Performance metrics or usage patterns from deployed software
- Any data that resides within customer environments

This limitation is not a policy choice that could be overridden by management decision or customer request—it is a fundamental architectural constraint. Even if a customer wanted to share their data with us, our software provides no mechanism to do so.

3.3 Data Processing Principles

For the limited business data we do process, we adhere to core privacy principles. We practice data minimization by collecting only what is necessary for specific business purposes. We ensure purpose limitation by using data only for the stated purposes at collection. We maintain data accuracy through regular updates and verification processes.

We implement appropriate retention periods based on legal requirements and business needs, not indefinite retention. We ensure data security through comprehensive technical and organizational measures detailed in our Information Security Policy. We provide transparency through this document and our privacy notices about what data we process and why.

Control Mapping: SOC 2 CC3.1, CC3.2, P2.1, P3.1, P3.2 | NIST DI-1, DM-1, SE-1, UL-1

4. Customer Data Responsibilities

4.1 Customer Control and Sovereignty

Our architectural model places complete data control and sovereignty with our customers. This isn't merely a contractual arrangement—it's a technical reality. Customers maintain absolute authority over their data because it never leaves their environment. They implement their own access controls, determine their own retention periods, and manage their own backup and recovery processes.

This level of control extends to all aspects of data governance. Customers decide which privacy regulations apply to their data processing, how to handle data subject requests, what consent mechanisms to implement, and how to manage international data transfers. Our software provides the technical capabilities, but all privacy decisions remain with the customer who actually controls the data.

We support this customer sovereignty by providing comprehensive documentation about our software's capabilities and limitations. We're transparent about what our software does with data (processes it locally) and what it doesn't do (transmit it anywhere). This enables customers to make informed decisions about their privacy posture and compliance requirements.

4.2 Support Model and Privacy

Supporting customers while maintaining our zero-data-access architecture requires innovative approaches. We've developed a support model that provides effective assistance without ever requiring access to customer data. This model demonstrates that privacy and quality support are not mutually exclusive.

When customers encounter issues, we work with synthetic data and sanitized reproductions. Customers can create test cases using non-production data that reproduce their issues. We maintain test environments with synthetic datasets that mirror common customer scenarios. This allows us to diagnose and resolve issues without ever seeing real customer data.

For complex troubleshooting, we may engage in screen-sharing sessions where customers maintain complete control. They can share their screens while controlling what is visible, redact sensitive information in real-time, and terminate the session at any moment. We never request remote control access, and our support tools are designed to be effective with view-only access.

4.3 Customer Privacy Obligations

While we eliminate privacy risks through architecture, we recognize that our customers still have privacy obligations to their own users. We support these obligations by providing clear documentation about our software's data handling, generating audit logs that remain within customer control, and enabling privacy-preserving configurations.

Our software includes features that help customers meet their privacy obligations. Configurable data retention policies allow automatic deletion after specified periods. Role-based access controls enable principle of least privilege. Audit trails track all data access and modifications. These features operate entirely within the customer environment, maintaining our zero-access model while supporting customer compliance.

Control Mapping: SOC 2 CC1.2, CC2.1, CC6.1, P1.1, P4.1 | NIST AP-2, IP-1, DM-3

5. Business Operations Privacy

5.1 Marketing and Sales Privacy

Our marketing and sales operations represent the primary area where we process external personal data, albeit in a very limited scope. We maintain a disciplined approach to marketing data collection, focusing exclusively on business-to-business relationships and avoiding any consumer data collection.

Our website (oversiteai.io) uses minimal analytics to understand traffic patterns and improve user experience. We've specifically chosen privacy-respecting analytics that don't track individual users across sites or build behavioral profiles. Cookie usage is limited to essential functions and anonymous analytics, with clear notice and easy opt-out options.

When potential customers express interest in our solutions, we collect only business contact information necessary to facilitate the sales process. This typically includes name, business email, company name, and role. We don't purchase contact lists, engage in mass email campaigns to purchased lists, or use aggressive tracking technologies. Our sales philosophy aligns with our privacy philosophy—respectful, minimal, and transparent.

5.2 Support Operations Privacy

Support operations require careful balance between helping customers effectively and maintaining our privacy commitments. Our support ticket system is configured to discourage customers from including sensitive data. Ticket forms include prominent warnings about not including production data, and our support team is trained to immediately flag and request removal of any sensitive information accidentally included.

We maintain knowledge base articles based on sanitized, generalized versions of support interactions. When a support case provides valuable learnings, we extract the technical essence while removing all customer-specific details. This allows us to build institutional knowledge without compromising privacy.

Support metrics are tracked at an aggregate level only. We monitor overall response times, resolution rates, and customer satisfaction scores without building detailed profiles of individual customer support patterns. This provides the operational visibility we need while respecting customer privacy.

5.3 Internal Operations Privacy

Our internal business operations follow privacy-by-design principles similar to our product architecture. Employee monitoring is limited to security purposes and clearly disclosed. We don't engage in excessive surveillance or behavioral analytics of our own team. Access to business systems follows least-privilege principles with regular reviews.

We maintain clear boundaries between different types of business data. HR data is accessible only to those with specific need-to-know. Financial data is restricted to finance team members. Customer contact data is available to sales and support teams but not to development teams. This segmentation reduces privacy risks from both accidental exposure and potential breaches.

Control Mapping: SOC 2 CC1.3, CC2.1, P2.1, P5.1, P6.1 | NIST DM-2, SE-1, UL-1

6. Privacy Rights Framework

6.1 Rights for Direct Contacts

Despite processing minimal personal data, we fully support privacy rights for individuals whose information we do process. We've implemented streamlined processes to handle rights requests efficiently, recognizing that simplicity in our data processing makes rights fulfillment straightforward.

Right of Access: When individuals request information about data we hold about them, we can quickly search our limited systems and provide comprehensive results. Our simple data architecture means we can confidently state whether we have any information about a requester and provide it in a portable format within days, not weeks.

Right to Rectification: Accuracy is maintained through simple update processes. When someone notifies us of incorrect information, we update it immediately across our limited systems. We don't have complex data propagation challenges because we don't maintain elaborate data ecosystems.

Right to Erasure: Deletion requests are straightforward to fulfill because we know exactly where data resides. Business contacts can be removed from our CRM system, marketing lists, and support systems quickly and completely. We maintain a suppression list to ensure deleted contacts aren't inadvertently re-added.

Right to Object and Restrict Processing: Marketing opt-outs are processed immediately and permanently. We don't engage in profiling or automated decision-making, so restrictions on processing are simple to implement—we just stop processing the data for optional purposes while maintaining any legally required records.

6.2 Supporting Customer End-User Rights

While we cannot directly fulfill data subject requests from customer end-users (since we have no data about them), we actively support our customers in meeting their obligations. We provide template language customers can use in their privacy notices to explain our role and data processing model.

Our documentation includes clear explanations customers can adapt for their users about how our software processes data locally, why data subject requests should be directed to the customer not to us, and what technical controls are available for privacy protection. We also provide technical documentation about data flows, storage locations, and processing activities within our software to help customers respond to detailed inquiries.

When customers receive data subject requests, we're available to provide attestations about our zero-access architecture. These attestations can help customers demonstrate to regulators or data subjects that vendor risk is minimized through architectural controls.

6.3 Rights Request Process

For individuals who wish to exercise privacy rights regarding data we process, we maintain a simple, accessible process. Requests can be submitted to privacy@oversiteai.io with basic identity verification. We don't require extensive documentation or complex forms—a simple email stating the request and providing basic verification information suffices.

We commit to acknowledging requests within 48 business hours and fulfilling them within 30 days, though our simple data architecture typically allows much faster response. We don't charge fees for rights requests and don't have complex eligibility requirements. If we cannot fulfill a request (for example, because we don't have any data about the requester), we clearly explain this rather than creating obstacles.

Control Mapping: SOC 2 P6.1, P6.2, P6.3, P6.4, P6.5, P6.6, P6.7 | NIST IP-2, IP-3, IP-4, DI-2

7. International Data Transfers

7.1 Our Operating Model

OversiteAI operates with a straightforward international data approach: we're a United States-based company with all operations in the US. This simplicity eliminates many complex international data transfer considerations that challenge global organizations. All our employees work from the United States, our infrastructure resides in US Azure regions, and our business operations are conducted under US law.

This focused geographic approach means that any personal data we process for our business operations remains within the United States. We don't have international subsidiaries requiring data transfers, offshore development centers accessing code repositories, or follow-the-sun support models that might require data access from multiple jurisdictions.

For the limited scenarios where we might process data from international contacts (such as a European company interested in our software), we rely on appropriate legal mechanisms. Standard contractual clauses are available when needed, though our minimal data processing and privacy-first approach typically make complex transfer mechanisms unnecessary.

7.2 Customer Deployment Flexibility

While our operations are US-based, our software architecture provides complete flexibility for customer deployments worldwide. Customers can deploy our software in any geographic location they choose, subject to their own compliance requirements. The software functions identically whether deployed in the US, EU, Asia, or any other region.

This deployment flexibility extends to data residency requirements. Since our software operates entirely within customer environments with no phone-home capability, customers achieve perfect data residency compliance. Data processed by our software in Germany stays in Germany. Data processed in Singapore stays in Singapore. We enable compliance through architecture, not through complex contractual arrangements.

Customers operating across multiple jurisdictions can deploy separate instances in each region, maintaining complete data segregation. Our software's architecture naturally supports this model without requiring special configuration or additional controls. Each deployment is an island, processing data locally without any cross-border data flows.

7.3 Cross-Border Support

Supporting international customers while maintaining our zero-access architecture requires careful consideration. Our support model works identically regardless of customer location—we never see customer data whether they're in San Francisco or Frankfurt. Time zone differences are handled through asynchronous support tickets and scheduled calls, not through offshore support centers.

When international customers require contractual commitments regarding data protection, we provide our standard zero-access attestations. These documents explain that international data transfer provisions are unnecessary when no data transfer capability exists. This architectural approach often simplifies customer procurement processes by eliminating complex data transfer impact assessments.

Control Mapping: SOC 2 CC1.4, P2.1, P5.2 | NIST UL-4, AC-20

8. Privacy Incident Response

8.1 Incident Scope and Types

Given our architectural model, the scope of potential privacy incidents is dramatically reduced compared to traditional software companies. We cannot have customer data breaches because we don't have customer data. However, we maintain robust incident response procedures for the types of privacy incidents that could affect our operations.

Potential privacy incidents in our environment might include unauthorized access to our employee records, breach of our CRM system containing business contacts, website compromise affecting visitor analytics, or exposure of support tickets (though these shouldn't contain sensitive data). Each scenario requires different response actions, but all are manageable within our simplified data environment.

Our incident response procedures integrate with our general Information Security Incident Response Plan but include specific provisions for privacy-related incidents. The key difference is the notification requirements—privacy incidents may trigger legal notification obligations that security incidents without personal data impact do not.

8.2 Response Procedures

When a potential privacy incident is detected, our response follows a structured approach optimized for our lean organization. The discovering employee immediately notifies the CEO, who serves as our de facto privacy officer. Given our small size, we can achieve rapid communication and decision-making without complex escalation hierarchies.

Initial assessment focuses on determining what data might be affected, how many individuals might be impacted, and whether the incident is ongoing or contained. Because we maintain minimal personal data in well-defined systems, this assessment can typically be completed within hours, not days. We don't have to search through complex data lakes or distributed systems to understand impact.

Containment actions leverage our simple architecture. Affected systems can be quickly isolated, compromised credentials can be reset across our limited platforms, and unauthorized access can be definitively terminated. Our small scale becomes an advantage—we can implement containment faster than large organizations with complex infrastructures.

8.3 Notification and Communication

If a privacy incident affects personal data we process, we commit to transparent and timely notification. Affected individuals are notified within 72 hours of confirmation that their data was impacted. Our notifications are clear, jargon-free explanations of what happened, what data was involved, and what steps we're taking.

For business contacts, notification is straightforward through email. For employees, we provide both written notice and direct discussion. We don't hide behind complex legal language or minimize the impact—our notifications clearly state the facts and our response actions.

Regulatory notifications follow applicable requirements. While we're US-based, we recognize that privacy laws like GDPR may apply if we process data from covered individuals. We maintain template notifications that can be quickly customized for specific incidents, ensuring we meet tight regulatory deadlines without sacrificing accuracy.

8.4 Learning and Improvement

Every privacy incident, even minor ones, triggers a lessons-learned review. Our small size allows everyone involved to participate directly in these reviews. We examine not just the technical failures but also process gaps that allowed the incident to occur.

Improvements are implemented rapidly. Unlike large organizations that might take months to roll out changes, we can update procedures, implement new controls, and retrain staff within days. This agility helps us continuously improve our privacy posture based on real-world experience.

Control Mapping: SOC 2 CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, P6.6 | NIST SE-2, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8

9. Third-Party Privacy Management

9.1 Vendor Privacy Standards

While our zero-access architecture eliminates traditional data processor relationships, we still engage vendors for business operations. Each vendor relationship is evaluated for privacy impact, though most process only our business data, not customer-related information. We maintain high standards for vendor privacy practices proportionate to the data they might access.

For critical vendors like Microsoft (Azure and Office 365), we rely on their enterprise privacy commitments and certifications. These major providers maintain SOC 2, ISO 27001, and other relevant certifications. We review their privacy practices annually and monitor for significant changes that might affect our risk posture.

For smaller vendors, we conduct proportionate due diligence. A vendor providing development tools that never touch personal data requires minimal privacy review. A vendor with access to employee data (like our benefits provider) undergoes more thorough evaluation. This risk-based approach ensures we focus effort where privacy impact is greatest.

9.2 Contractual Protections

Our vendor contracts include privacy provisions scaled to the relationship. All vendors with potential access to personal data sign agreements including confidentiality obligations, restrictions on data use, security requirements, and cooperation with privacy rights. We don't require complex Data Processing Agreements (DPAs) for vendors that never touch personal data, maintaining proportionality in our approach.

Key contractual terms focus on practical protections rather than legal complexity. Vendors must notify us of any breaches potentially affecting our data, allow us to audit privacy practices (though we rarely exercise this right with trusted vendors), delete our data upon termination, and use subcontractors only with our awareness. These terms provide protection without creating administrative burden for either party.

9.3 No Fourth-Party Processing

One of our strongest privacy positions is our complete absence of fourth-party data processing. We don't use subcontractors for development, support, or any function that might access personal data. All work is performed by our direct employees, eliminating complex chains of data access that complicate privacy management.

This position extends to our product development. We don't outsource development to third parties who might embed tracking or telemetry. We don't use external support vendors who might need customer data access. We don't engage marketing agencies that might process contact data on our behalf. This direct control model significantly simplifies our privacy management.

When vendors ask about subprocessor lists or fourth-party management, we can confidently state: there are none. This often accelerates customer procurement processes, as they don't need to evaluate complex processing chains or worry about data flowing to unknown fourth parties.

Control Mapping: SOC 2 CC3.3, CC9.1, CC9.2, P4.1, P4.2, P4.3 | NIST AR-3, UL-2, UL-3

10. Privacy Documentation and Transparency

10.1 Customer-Facing Documentation

Transparency about our privacy model helps customers understand and trust our approach. We maintain comprehensive documentation that clearly explains our zero-access architecture, including technical architecture diagrams showing data flow boundaries, security whitepapers detailing our controls, and compliance attestations like this SOC 2 report.

Our documentation uses clear, non-technical language where possible. While we provide technical details for security teams, we also offer executive summaries that business leaders can understand. Key messages are consistent across all documents: we can't access your data because our architecture prevents it.

We regularly update documentation to reflect product changes, though our fundamental privacy model remains constant. Version control ensures customers can see what has changed and when. We proactively notify customers of significant documentation updates that might affect their compliance programs.

10.2 Privacy Notices

We maintain two primary privacy notices, each tailored to its specific audience and purpose. Our website privacy notice covers visitors to oversiteai.io, explaining our minimal analytics, cookie usage, and how we handle contact form submissions. It's written in plain language, avoiding legal jargon where possible.

Our employee privacy notice provides comprehensive information about how we process employee data. It covers recruitment data, employment records, monitoring activities, and employee rights. New employees receive this notice during onboarding, and we review it annually with all staff to ensure continued awareness.

Both notices follow privacy-by-design principles themselves—they're concise, well-organized, and actually readable. We avoid the common practice of burying important information in lengthy legal text. Key information appears prominently, and we use formatting to improve readability.

10.3 Transparency Reports

While large technology companies publish transparency reports about government data requests, our report would be simple: we've never received a request for customer data, and couldn't comply if we did because we don't have any. Nevertheless, we commit to transparency about any requests for the limited data we do process.

Annually, we publish a simple transparency statement covering government requests for data (typically zero), privacy rights requests received and fulfilled, significant privacy incidents (hopefully zero), and changes to our privacy program. This report demonstrates our commitment to transparency even when there's little to report.

Control Mapping: SOC 2 CC1.1, CC1.2, CC1.3, CC2.1, CC2.2, CC2.3, P1.1 | NIST TR-1, TR-2, TR-3

11. Regulatory Compliance

11.1 Applicable Regulations

Our simplified data processing model significantly reduces regulatory complexity. For our business operations, we primarily fall under US privacy laws. California Consumer Privacy Act (CCPA) applies to our California employee data and any California business contacts. We maintain compliant notices and honor all CCPA rights requests.

General Data Protection Regulation (GDPR) would apply if we process data from EU individuals. While we don't actively market in the EU, we may occasionally interact with

EU-based businesses interested in our solutions. For these limited interactions, we maintain GDPR-compliant practices including lawful basis for processing, appropriate notices, and rights fulfillment capabilities.

Sector-specific regulations like HIPAA or FERPA don't apply to us directly—we're not a covered entity or business associate because we never access protected data. However, we enable our customers' compliance by ensuring our software can be deployed in compliant environments. Our architecture supports customers who need to meet these strict requirements.

11.2 Compliance Approach

Rather than maintaining complex compliance matrices for numerous regulations, we follow privacy best practices that generally exceed regulatory requirements. By processing minimal data, being transparent about our practices, honoring all rights requests, and maintaining strong security, we meet or exceed most privacy law requirements.

This principled approach serves us well as new privacy laws emerge. When new state privacy laws come into effect, we typically find we're already compliant because our practices exceed their requirements. We monitor legal developments but rarely need significant changes because our privacy-first model inherently aligns with regulatory goals.

For customers concerned about specific regulatory compliance, we provide clear documentation about our practices that they can include in their compliance assessments. Our zero-access architecture often simplifies their compliance by eliminating vendor risk considerations for customer data processing.

11.3 Future Regulatory Preparedness

As privacy regulations continue to evolve globally, we're well-positioned to maintain compliance. Our architectural decisions provide future-proofing against increasingly strict requirements. Regulations may require stronger consent mechanisms, increased individual rights, or stricter cross-border controls—none of which affect us significantly given our model.

We participate in industry discussions about privacy regulation and software architecture. By sharing our approach, we hope to influence the industry toward privacy-by-design architectures. We believe regulations should incentivize architectural privacy rather than just procedural controls.

When new regulations emerge, our compliance review is straightforward: Do we process covered data? Usually, the answer is no for customer data, and minimal for business operations. This allows us to focus on substantive compliance for the data we do process rather than complex applicability analyses.

Control Mapping: SOC 2 CC1.4, CC1.5, CC2.1, P1.1, P8.1 | NIST AR-5, AR-8

12. Privacy Training and Awareness

12.1 Employee Privacy Education

Every OversiteAI employee receives privacy training tailored to our unique model. Rather than generic privacy training, we focus on understanding our architectural advantages and the responsibilities they create. New employees learn why we've chosen this model and how to articulate its benefits to customers and prospects.

Training covers both theoretical principles and practical applications. Employees understand concepts like data minimization and privacy by design, but more importantly, they learn how these apply to their daily work. Support staff know never to request customer data. Developers understand why telemetry features are forbidden. Sales teams can explain our privacy advantages confidently.

We conduct annual privacy refreshers that aren't just compliance checkboxes. These sessions include real scenarios employees might encounter, updates on privacy trends and regulations, and reinforcement of our privacy-first culture. Given our small size, these are interactive discussions, not passive presentations.

12.2 Role-Specific Training

Different roles require different privacy knowledge depths. Developers receive additional training on secure coding practices that maintain our zero-access architecture. They learn to recognize and resist feature requests that would compromise our privacy model, no matter how seemingly valuable.

Sales and marketing staff receive specialized training on privacy-compliant outreach. They understand the boundaries of acceptable business development, the importance of honoring opt-out requests immediately, and how to position our privacy advantages without overstating them. They also learn to recognize and properly route privacy-related customer inquiries.

Leadership team members receive comprehensive privacy training covering regulatory landscapes, strategic privacy decisions, and the business value of our privacy model.

They understand that privacy isn't just compliance—it's a competitive advantage that differentiates us in the market.

12.3 Privacy Culture

Beyond formal training, we cultivate a privacy-aware culture through daily practices. Privacy considerations are standard in product planning discussions. "How does this affect privacy?" is a routine question in design reviews. We celebrate decisions that enhance privacy, even when they might limit functionality.

We maintain open channels for privacy questions and concerns. Any employee can raise privacy issues directly with leadership without fear of negative consequences. We've created an environment where protecting privacy is everyone's responsibility, not just assigned to a privacy officer.

Success stories reinforce our privacy culture. When we win deals because of our zero-access architecture, we share these wins company-wide. When we help customers solve complex compliance challenges through our architecture, we celebrate. These positive reinforcements maintain enthusiasm for our privacy-first approach.

Control Mapping: SOC 2 CC1.1, CC1.2, CC2.2, CC2.3, CC2.4, P1.1 | NIST AR-4, AT-1, AT-2, AT-3, AT-4

13. Privacy Impact Assessments

13.1 Assessment Methodology

While our zero-access architecture eliminates privacy risks for most initiatives, we maintain a lightweight Privacy Impact Assessment (PIA) process for changes that might affect the limited personal data we do process. Our PIA methodology is proportionate to our scale and risk profile, focusing on practical risk identification rather than bureaucratic documentation.

Any initiative that might process new personal data, change how we process existing personal data, or engage new vendors with data access triggers a PIA. Given our lean operations, this might occur only a few times annually. The assessment examines what data would be processed, the purpose and legal basis, potential risks to individuals, and mitigation measures.

Our PIA template is a simple questionnaire that can be completed in under an hour for most initiatives. It asks straightforward questions like: Will this process personal data? Is there another way to achieve the goal without personal data? What happens if this

data is breached? Who needs access to this data? The simplicity encourages honest assessment rather than compliance theater.

13.2 Product Development PIAs

For product development, PIAs serve a crucial gatekeeping function. Any proposed feature that would collect, transmit, or process data undergoes assessment. In most cases, the assessment is brief: "Does this feature maintain our zero-access architecture? Yes? Approved from a privacy perspective." This simplicity allows rapid development while maintaining privacy standards.

Occasionally, valuable features might require data collection. For example, customers might request usage analytics to optimize their deployments. Our PIA process forces us to explore privacy-preserving alternatives: Could analytics be generated locally and viewed by the customer only? Could we provide tools for customers to analyze their own usage without data leaving their environment? These assessments often lead to innovative solutions that provide value while maintaining privacy.

When features absolutely would require data collection, our PIA process usually results in declining to build them. We document these decisions to explain to customers why certain seemingly standard features aren't available. This transparency helps customers understand that missing features are deliberate privacy choices, not technical limitations.

13.3 Operational PIAs

PIAs for operational changes focus on our business data processing. When evaluating new vendors, changing business processes, or implementing new internal tools, we assess privacy impact proportionate to risk. A new project management tool that processes employee names requires minimal assessment. A new HR system processing sensitive employee data requires comprehensive evaluation.

The PIA process integrates with our vendor management and change control processes. Privacy assessment isn't a separate bureaucratic step but part of holistic evaluation. This integration ensures privacy considerations don't slow down necessary business changes while still receiving appropriate attention.

Results of PIAs are documented simply—often just an email thread or a brief document. We focus on capturing decisions and rationales rather than generating extensive paperwork. This documentation proves valuable when similar proposals arise later or when explaining our decisions to auditors or customers.

Control Mapping: SOC 2 CC1.3, CC3.1, CC3.2, P1.1, P2.1, P8.1 | NIST AR-2, CM-4

14. Data Protection by Design and Default

14.1 Architectural Privacy Implementation

Data protection by design isn't an add-on feature for OversiteAI—it's the fundamental principle that shaped our entire business model. From our earliest architectural decisions, we chose designs that make privacy violations impossible rather than merely prohibited. This approach requires more upfront design effort but eliminates entire categories of privacy risks.

Our implementation of privacy by design extends through every layer of our technology stack. At the network layer, our software doesn't open outbound connections that could leak data. At the application layer, we don't include libraries or frameworks with telemetry capabilities. At the data layer, all processing happens in-memory or in customer-controlled storage. Each architectural decision reinforces our privacy model.

Default configurations prioritize privacy over functionality. While our software could theoretically be modified by sophisticated customers to add telemetry, the default installation provides no such capability. Optional features that might have privacy implications are disabled by default with clear documentation about their impact if enabled. We make privacy the easy path, not the difficult one.

14.2 Privacy in Feature Design

When designing new features, privacy by design principles guide our decisions. We start with the assumption that no data should leave the customer environment and work backward from there. If a feature seems to require external data transmission, we challenge ourselves to redesign it for local operation.

This constraint drives innovation. When customers requested collaborative features, traditional design would involve cloud synchronization. Instead, we developed peer-to-peer synchronization options that work within customer networks. When benchmarking capabilities were requested, we created local benchmark generation rather than centralized comparison databases. These privacy-preserving innovations often provide additional benefits like better performance and reliability.

Feature requests undergo privacy review before development begins. This isn't a bureaucratic gate but a design collaboration. Developers work with privacy considerations from the start rather than trying to bolt on privacy controls later. This approach results in cleaner, more elegant solutions that naturally preserve privacy.

14.3 Default Privacy Settings

Our software ships with privacy-maximizing defaults throughout. Logging is configured to capture operational data without personal information. Access controls default to least-privilege rather than open access. Data retention defaults to shorter periods rather than indefinite storage. These defaults can be adjusted by customers but start from a privacy-first position.

Documentation clearly explains the privacy implications of any configuration changes. If a customer wants to enable more detailed logging for troubleshooting, we explain what additional data might be captured and how to minimize privacy impact. We provide configuration templates for common scenarios that maintain privacy while meeting operational needs.

The principle of data protection by default extends to our business operations. New employees don't automatically get access to all systems—they receive only what their role requires. Marketing tools don't automatically capture maximum data—they're configured for minimal collection. Privacy isn't something we add when regulations require it; it's the starting point we relax only when necessary.

Control Mapping: SOC 2 CC1.1, CC3.1, CC6.1, P1.1, P2.1 | NIST AR-7, SC-8

15. Privacy Governance

15.1 Organizational Structure

Our privacy governance structure reflects our lean organization while ensuring appropriate oversight. The CEO serves as our executive privacy sponsor, demonstrating top-level commitment to privacy. This direct leadership involvement ensures privacy considerations receive appropriate weight in strategic decisions.

Rather than a dedicated Data Protection Officer (which our scale doesn't warrant), privacy responsibilities are distributed across leadership team members. The CEO handles strategic privacy decisions and regulatory relationships. The head of engineering ensures technical privacy controls. The head of operations manages operational privacy practices. This distributed model ensures privacy expertise where decisions are made.

Privacy governance integrates with our regular business operations rather than creating parallel structures. Privacy topics appear on leadership team agendas when relevant. Privacy metrics are reviewed alongside other operational metrics. Privacy risks are evaluated within our standard risk management framework. This integration

makes privacy governance sustainable for our small team.

15.2 Decision Rights and Accountability

Clear decision rights prevent privacy from becoming nobody's responsibility. Product features affecting privacy require CEO approval, ensuring strategic alignment. Vendor relationships potentially involving personal data require operations head approval. Privacy-affecting technical changes require engineering head approval. These clear boundaries enable rapid decisions while maintaining oversight.

Accountability mechanisms are straightforward in our small organization. Each leader owns privacy outcomes in their area. Performance discussions include privacy protection alongside other objectives. Privacy failures would be treated as seriously as security breaches or financial mismanagement. This accountability is cultural, not just procedural.

Regular privacy reviews ensure ongoing attention. Quarterly, we review privacy incidents (hopefully none), rights requests received, regulatory changes, and improvement opportunities. These reviews are brief, focused discussions, not lengthy presentations. Action items are assigned and tracked like any other business commitment.

15.3 Continuous Improvement

Our privacy program evolves based on experience and changing requirements. We monitor privacy trends through industry associations, regulatory updates, and customer feedback. When new privacy challenges emerge in the industry, we proactively assess our readiness rather than waiting for direct impact.

Improvement initiatives focus on practical enhancements rather than theoretical perfection. If we identify a privacy gap, we implement proportionate controls. If customers consistently ask about certain privacy features, we evaluate adding them. If regulations introduce new requirements, we assess efficient compliance approaches. Each improvement is evaluated for both privacy benefit and operational impact.

We measure privacy program effectiveness through simple, meaningful metrics: Number of privacy incidents (target: zero), time to fulfill rights requests (target: under 5 days), privacy-related customer concerns (target: decreasing trend), and employee privacy training completion (target: 100%). These metrics drive real improvements rather than creating measurement burden.

Control Mapping: SOC 2 CC1.1, CC1.2, CC1.3, CC1.4, CC1.5, CC2.1, P1.1 | NIST AR-1, AR-8, PM-2

16. Contact Information

Privacy Inquiries

We maintain accessible channels for privacy-related communications. Our primary privacy contact (privacy@oversiteai.io) is monitored daily by operations team members trained in privacy request handling. We commit to acknowledging privacy inquiries within one business day and providing substantive responses within five business days.

Escalation Path

For urgent privacy-related matters or escalations, individuals may contact our Data Protection Team at privacy@oversiteai.io. This channel ensures timely review and appropriate handling of sensitive data protection issues.

OverSiteAI is committed to upholding transparency and supporting the responsible exercise of privacy rights without unnecessary delay or complexity.

Regulatory Communications

For regulatory authorities needing to contact us regarding privacy matters, we provide direct access to decision-makers. Our CEO serves as the primary regulatory contact, ensuring authoritative responses to official inquiries. We maintain positive relationships with privacy regulators through transparency and responsiveness.

Control Mapping: SOC 2 CC1.1, CC2.1, P1.1, P6.7 | NIST IP-4

17. Document Control

Control Mapping: NIST PM-4, SA-5, CM-3

Version	Date	Author	Changes
1.0	January 1, 2025	CTO	Initial comprehensive version
2.0	Jun 25, 2025	CTO	Updated NIST control mappings throughout document

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: NIST Control Mapping

This appendix provides a comprehensive mapping of NIST Privacy Controls and SOC 2 criteria to specific sections within this Privacy and Data Protection Addendum. The mapping demonstrates how our privacy program addresses relevant control requirements through our architectural approach and operational practices.

Note on NIST Privacy Controls: The NIST Privacy Control families referenced below are derived from NIST Special Publication 800-53, Revision 5, Appendix J (Privacy Control Catalog). These controls supplement security controls with privacy-specific requirements. Control mappings indicate where each section's content addresses the intent of specific NIST controls, though implementation may vary based on our organization's size and architectural model.

Privacy Control Families Addressed

Authority and Purpose (AP)

- AP-1: Authority to Collect - Section 3 (Scope of Data Processing)
- AP-2: Purpose Specification - Sections 3, 4 (Data Processing & Customer Responsibilities)

Authority and Responsibility (AR)

- AR-1: Governance and Privacy Program - Sections 2, 15 (Architecture & Governance)
- AR-2: Privacy Impact and Risk Assessment - Sections 2, 13 (Architecture & PIAs)
- AR-3: Privacy Requirements for Contractors - Section 9 (Third-Party Management)
- AR-4: Privacy Monitoring and Auditing - Section 12 (Training and Awareness)
- AR-5: Privacy Awareness and Training - Section 11 (Regulatory Compliance)

- AR-7: Privacy-Enhanced System Design - Sections 2, 14 (Architecture & Design)
- AR-8: Accountability, Audit, and Risk Management - Section 15 (Governance)

Data Quality and Integrity (DI)

- DI-1: Data Quality - Section 3 (Scope of Data Processing)
- DI-2: Data Integrity and Integrity Board - Section 6 (Rights Framework)

Data Minimization and Retention (DM)

- DM-1: Minimization of Personally Identifiable Information - Section 3 (Scope)
- DM-2: Data Retention and Disposal - Section 5 (Business Operations)
- DM-3: Minimization of PII Used in Testing - Section 4 (Customer Responsibilities)

Individual Participation and Redress (IP)

- IP-1: Consent - Section 4 (Customer Responsibilities)
- IP-2: Individual Access - Section 6 (Rights Framework)
- IP-3: Redress - Section 6 (Rights Framework)
- IP-4: Complaint Management - Sections 6, 16 (Rights & Contact)

Security (SE)

- SE-1: Inventory of Personally Identifiable Information - Section 5, Appendix B
- SE-2: Privacy Incident Response - Section 8 (Privacy Incident Response)

Transparency (TR)

- TR-1: Privacy Notice - Section 10 (Documentation and Transparency)
- TR-2: System of Records Notices and Privacy Act - Section 10 (Documentation)
- TR-3: Dissemination of Privacy Program Information - Section 10 (Documentation)

Use Limitation (UL)

- UL-1: Internal Use - Section 3 (Scope of Data Processing)
- UL-2: Information Sharing with Third Parties - Sections 2, 9 (Architecture & Third Parties)
- UL-3: Information Sharing - Section 9 (Third-Party Management)
- UL-4: Information Sharing with Foreign Countries - Section 7 (International Transfers)

Program Management (PM)

- PM-1: Information Security Program Plan - Section 1 (Executive Summary)
- PM-2: Senior Information Security Officer - Section 15 (Governance)
- PM-4: Plan of Action and Milestones Process - Section 17 (Document Control)

System and Services Acquisition (SA)

- SA-5: Information System Documentation - Section 17 (Document Control)

Configuration Management (CM)

- CM-3: Configuration Change Control - Section 17 (Document Control)
- CM-4: Security Impact Analysis - Section 13 (Privacy Impact Assessments)

Access Control (AC)

- AC-20: Use of External Information Systems - Section 7 (International Transfers)

Incident Response (IR)

- IR-1 through IR-8: Incident Response Planning and Handling - Section 8

Awareness and Training (AT)

- AT-1 through AT-4: Security Awareness and Training - Section 12

System and Communications Protection (SC)

- SC-8: Transmission Confidentiality and Integrity - Section 14 (By Design)

SOC 2 Privacy Criteria Mapping by Section

Section	Primary SOC 2 Criteria	Supporting NIST Controls
1. Executive Summary	CC1.2-CC1.5, P1.1	PM-1, AR-1
2. Privacy Architecture	CC1.1, CC3.1, CC6.1, P1.1, P2.1	AR-1, AR-2, AR-7, UL-2
3. Scope of Data Processing	CC3.1-CC3.2, P2.1, P3.1-P3.2	DI-1, DM-1, SE-1, UL-1
4. Customer Responsibilities	CC1.2, CC2.1, CC6.1, P1.1, P4.1	AP-2, IP-1, DM-3
5. Business Operations	CC1.3, CC2.1, P2.1, P5.1, P6.1	DM-2, SE-1, UL-1
6. Privacy Rights	P6.1-P6.7	IP-2, IP-3, IP-4, DI-2
7. International Transfers	CC1.4, P2.1, P5.2	UL-4, AC-20
8. Privacy Incident Response	CC7.1-CC7.5, P6.6	SE-2, IR-1 through IR-8

9. Third-Party Management	CC3.3, CC9.1-CC9.2, P4.1-P4.3	AR-3, UL-2, UL-3
10. Documentation	CC1.1-CC1.3, CC2.1-CC2.3, P1.1	TR-1, TR-2, TR-3
11. Regulatory Compliance	CC1.4-CC1.5, CC2.1, P1.1, P8.1	AR-5, AR-8
12. Training and Awareness	CC1.1-CC1.2, CC2.2-CC2.4	AR-4, AT-1 through AT-4
13. Privacy Impact Assessments	CC1.3, CC3.1-CC3.2, P1.1, P2.1, P8.1	AR-2, CM-4
14. Privacy by Design	CC1.1, CC3.1, CC6.1, P1.1, P2.1	AR-7, SC-8
15. Privacy Governance	CC1.1-CC1.5, CC2.1, P1.1	AR-1, AR-8, PM-2
16. Contact Information	CC1.1, CC2.1, P1.1, P6.7	IP-4
17. Document Control	N/A	PM-4, SA-5, CM-3

Control Family Coverage Summary

NIST Control Family	Primary Sections	Secondary Sections
Authority and Purpose (AP)	3, 4	-
Authority and Responsibility (AR)	2, 9, 11, 12, 13, 14, 15	1
Data Quality and Integrity (DI)	3, 6	-
Data Minimization and Retention (DM)	3, 4, 5	-
Individual Participation (IP)	4, 6, 16	-
Security (SE)	5, 8	3
Transparency (TR)	10	-
Use Limitation (UL)	2, 3, 5, 7, 9	-

Program Management (PM)	1, 15, 17	-
System Acquisition (SA)	17	-
Configuration Management (CM)	13, 17	-
Access Control (AC)	7	-
Incident Response (IR)	8	-
Awareness and Training (AT)	12	-
System Protection (SC)	14	-

Appendix B: Data Inventory

Category 1: Employee Data

- **Data Types**: Names, addresses, SSNs, compensation, benefits, performance
- **Purpose**: Employment administration
- **Retention**: Per legal requirements + 7 years
- **Access**: HR function only
- **Systems**: Azure AD, Microsoft 365, payroll provider

Category 2: Business Contacts

- **Data Types**: Names, business emails, companies, roles
- **Purpose**: Sales, marketing, support
- **Retention**: Until opt-out + 2 years for support
- **Access**: Sales, marketing, support teams
- **Systems**: CRM, support ticket system

Category 3: Website Visitors

- **Data Types**: Anonymous analytics, contact form submissions
- **Purpose**: Website improvement, lead generation
- **Retention**: Analytics: 90 days, Contacts: see Category 2
- **Access**: Marketing team
- **Systems**: Privacy-respecting analytics, web forms

Appendix C: Vendor Privacy Matrix

Vendor	Data Access	Privacy Controls	Risk Level
Microsoft (Azure/365)	Employee data, infrastructure	SOC 2, ISO 27001, DPA	Low
Payroll Provider	Employee compensation data	SOC 2, specialized agreements	Medium
CRM Provider	Business contacts	SOC 2, data isolation	Low
Support Ticket System	Support interactions (no customer data)	Cloud security standards	Low
Analytics Provider	Anonymous website data	Privacy-focused design	Low

Appendix D: Privacy Incident Response Quick Reference

Hour 1: Immediate Response

- Notify CEO
- Contain if possible
- Preserve evidence
- Begin impact assessment

Hours 2-24: Assessment

- Determine data affected
- Identify individuals impacted
- Evaluate legal obligations
- Prepare notifications

Hours 24-72: Notification

- Notify affected individuals
- Submit regulatory notifications if required
- Implement immediate fixes
- Begin root cause analysis

Week 1-4: Remediation

- Complete root cause analysis
- Implement permanent fixes

- Update procedures
- Conduct lessons learned

Appendix E: Template Privacy Responses

Access Request Response Template:

"We have located the following information associated with your email address: [list data]. This represents all personal data OversiteAI processes about you. If you need this in a different format, please let us know."

Deletion Request Response Template:

"We have deleted your personal data from our systems as requested. You have been added to our suppression list to prevent re-addition. Please note that we may retain minimal data required for legal compliance, such as records of this deletion request."

Marketing Opt-Out Confirmation:

"You have been unsubscribed from all OversiteAI marketing communications. You may still receive transactional emails if you are a current customer. This preference has been permanently recorded."

Appendix F: Annual Privacy Review Checklist

- [ ] Review and update privacy notices
- [ ] Audit vendor privacy practices
- [ ] Test rights request procedures
- [ ] Update privacy training materials
- [ ] Review privacy incidents and near-misses
- [ ] Assess new regulatory requirements
- [ ] Evaluate privacy control effectiveness
- [ ] Update risk assessments
- [ ] Refresh employee privacy training
- [ ] Publish transparency report