Incident Response Plan

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

Incident Response Plan

OversiteAI, LLC

Document Version: 2.0

Effective Date: January 1, 2025

Last Updated: June 25, 2025

Last Reviewed: June 27, 2025

Classification: Restricted

Owner: Chief Technology Officer

Approved By: Chief Executive Officer

1. Purpose and Scope

1.1 Purpose

NIST Controls: IR-1, IR-8

This Incident Response Plan serves as the cornerstone of OversiteAI's security operations, establishing comprehensive procedures for detecting, responding to, and recovering from security incidents that could impact our operations, assets, or reputation. As a small, cloud-native software company whose primary asset is our intellectual property (source code), we've designed this plan to be both thorough and practical. Our unique architecture - where software runs entirely on customer premises without any access to customer data - significantly reduces certain risk categories while elevating the importance of protecting our codebase and development infrastructure. The plan acknowledges that our team members wear multiple hats while ensuring we can respond effectively when security incidents occur.

We've learned from experience that effective incident response requires more than just technical procedures – it demands clear communication, rapid decision-making, and coordinated action across our entire organization. This plan provides that framework, ensuring everyone understands their role when incidents occur and that we can minimize damage while reducing recovery time and costs. Given our size and resources, we've focused on creating procedures that leverage automation and cloud-native capabilities rather than assuming dedicated security staff that we cannot yet afford.

1.2 Scope

NIST Controls: IR-1, IR-4

Our incident response procedures encompass all information security incidents affecting OversiteAI systems, regardless of whether they originate from external threats or internal issues. This comprehensive scope includes source code breaches or unauthorized access to our development repositories, system compromises targeting our Azure infrastructure or development environments, malware infections that could potentially inject malicious code into our software products, supply chain attacks through compromised dependencies or build systems, and corporate data breaches affecting employee information or business operations. We also address physical security incidents that could affect development workstations containing source code, as well as third-party incidents that might impact our software delivery pipeline. Notably, our architecture eliminates customer data breach risks since we never access, store, or process customer data - our software runs entirely on customer infrastructure.

This broad scope reflects the interconnected nature of modern software development where a security incident in one area can quickly cascade to affect our entire supply chain and ultimately our customers' trust. We've deliberately included edge cases and emerging threats in our planning, recognizing that as a software company, our intellectual property (source code) represents our primary value and faces unique risks from sophisticated attackers, insider threats, and supply chain compromises. The scope explicitly covers both our development environments where our codebase resides and our corporate infrastructure that supports business operations, understanding that compromises in either area could have severe business impact. However, customer data incidents are explicitly out of scope since our architecture prevents any access to customer environments or data.

1.3 Objectives

NIST Controls: IR-1, IR-8

Our incident response objectives balance multiple competing priorities while acknowledging the constraints of a small business. First and foremost, we aim to protect our intellectual property and prevent unauthorized access to our source code, which represents our entire business value. We ensure rapid containment of any breach that could compromise our codebase integrity or allow malicious code injection that might affect our customers. While we don't handle customer data directly, we maintain customer trust by ensuring our software remains secure and uncompromised.

Beyond immediate response, we ensure proper evidence collection and preservation to support potential legal proceedings, insurance claims, or regulatory investigations. Meeting legal and regulatory notification requirements within mandated timeframes protects us from additional liability while demonstrating our commitment to transparency. Perhaps most importantly, we commit to learning from every incident to prevent recurrence, treating each event as an opportunity to strengthen our security posture. Throughout all response activities, we work to maintain stakeholder confidence through professional handling and clear communication, knowing that how we handle incidents can impact our reputation as much as the incidents themselves.

2. Incident Response Team (IRT)

2.1 Team Structure

NIST Controls: IR-2, IR-3, IR-7

Our Incident Response Team structure reflects the reality of a small company where everyone wears multiple hats. Rather than maintaining a dedicated security team that

would be economically unfeasible at our size, we've designated primary and backup responders from our existing staff who can quickly pivot to incident response when needed. The CTO serves as our Incident Commander, bringing both technical depth and strategic thinking to critical decisions during incidents. This dual technical-business perspective ensures we balance security response with business continuity, especially important when we can't afford extended downtime.

The Incident Commander role encompasses overall incident coordination, making strategic decisions during active incidents, approving all external communications to ensure consistent messaging, and allocating resources effectively given our constraints. We've learned that having clear authority concentrated in this role prevents dangerous delays when quick decisions are needed. The DevOps Lead serves as backup, ensuring coverage during vacations or when the CTO is unavailable, and bringing deep infrastructure knowledge that complements the CTO's broader perspective.

Our Technical Lead, primarily filled by our Senior Developer with the DevOps Engineer as backup, handles the hands-on aspects of incident response. This includes technical investigation and analysis to understand attack vectors and impact, implementing containment and eradication actions to stop ongoing damage, collecting evidence while maintaining proper chain of custody, and managing system recovery to restore normal operations. The technical depth in this role ensures we can respond to sophisticated attacks while the backup provides infrastructure expertise for cloud-specific incidents.

The Communications Lead role, filled by our CEO with the Customer Success Lead as backup, manages the critical human elements of incident response. This encompasses internal communications to keep our team informed and coordinated, customer notifications that balance transparency with avoiding unnecessary alarm, media and public relations if incidents become public, and regulatory notifications to meet our compliance obligations. Having the CEO in this role ensures authority for critical communications while demonstrating executive commitment to security.

Our Documentation Lead can be filled by any available team member, acknowledging that during incidents we need flexibility in role assignment. This role maintains the incident timeline to support investigations and reporting, tracks action items ensuring nothing falls through the cracks, catalogs evidence for legal and insurance purposes, and prepares comprehensive reports for stakeholders and regulators. This distributed approach to documentation ensures we capture necessary information without bottlenecking on a single person.

2.2 Extended Team

NIST Controls: IR-2, IR-7, SA-9

Recognizing our size limitations, we've established relationships with external partners who extend our capabilities during major incidents. Our legal counsel, maintained on retainer, provides immediate access to legal advice on notification requirements, regulatory compliance guidance for multi-jurisdictional incidents, and liaison services with law enforcement when criminal activity is suspected. This relationship, established before incidents occur, ensures we can get rapid legal guidance without scrambling to find appropriate counsel during crisis situations.

We maintain a pre-identified relationship with an external security firm specializing in incident response for mid-market companies. This firm provides advanced forensics capabilities we cannot maintain internally, specialized incident response expertise for sophisticated attacks, and overflow capacity when incidents exceed our team's availability. The retainer ensures guaranteed response times and negotiated rates, making enterprise-grade capabilities accessible within our budget constraints.

Our infrastructure is hosted on Microsoft Azure, and we make use of the support and resources available through our account. This includes access to technical documentation, best-practice guidance, and support channels for resolving platform-specific issues. While we retain full responsibility for the security, availability, and operation of our application stack, Azure support can be engaged when appropriate to assist with cloud infrastructure questions or to resolve underlying service concerns. This approach ensures efficient issue resolution without creating operational dependency on external parties.

2.3 Contact Information

NIST Controls: IR-2, IR-3

Role	Primary	Backup	Contact
Incident Commander	CTO	DevOps Lead	-
Technical Lead	Sr Dev	DevOps Eng	-
Communications	CEO	-	-
Azure Support	-	-	-

Our escalation tree ensures rapid activation regardless of when incidents occur. The on-call engineer serves as the first point of contact during after-hours incidents, with authority to begin initial response and escalate as needed. They immediately contact the Technical Lead for any confirmed security incident, who assesses severity and activates the Incident Commander for Severity 1 or 2 incidents. The CEO receives direct escalation only for Severity 1 incidents that threaten business continuity or require executive decisions on public communications or significant resource allocation.

3. Incident Classification

3.1 Severity Levels

NIST Controls: IR-4, IR-5, IR-6

Our severity classification system provides clear criteria for prioritizing response efforts and allocating resources appropriately. We've designed four severity levels that reflect both technical impact and business consequences, ensuring rapid mobilization for critical incidents while avoiding alert fatigue from over-classification of minor events.

Severity 1 - Critical incidents demand immediate response 24/7 and include confirmed source code breaches or repository compromises, successful supply chain attacks that could inject malicious code, ransomware attacks encrypting development systems or code repositories, and insider theft of intellectual property. These incidents threaten our entire business model since our code represents our sole product. We've learned that the difference between a major incident and a business-ending event often comes down to response speed, making immediate action non-negotiable for Severity 1 events.

Severity 2 - High incidents require response within one hour and encompass suspected but unconfirmed source code access, development environment compromises affecting isolated systems, build pipeline anomalies that might indicate supply chain attacks, and critical vulnerabilities in our software dependencies being actively exploited. These incidents balance urgency with measured response, allowing time for proper assessment while ensuring we don't delay containment of serious threats. The one-hour response time acknowledges that our small team might not be immediately available while ensuring we mobilize quickly enough to prevent escalation.

Severity 3 - Medium incidents allow response within four hours and include isolated security incidents affecting single systems or users, attempted but failed attacks that demonstrate threat actor interest, non-critical system compromises that don't impact

customer operations, and policy violations with potential security impact. This classification recognizes that many security events require attention but don't demand dropping everything else. The four-hour window allows us to handle these during business hours or schedule response during the next business period for after-hours detection.

Severity 4 - Low incidents can be addressed the next business day and cover routine security events like detected scans or probes from automated tools, minor policy violations without security impact, and false positives from our monitoring systems that need tuning. These events require documentation and potential system tuning but don't warrant emergency response. By clearly defining this category, we avoid burnout from treating every security event as urgent while ensuring nothing gets completely ignored.

3.2 Incident Types

*NIST Controls: IR-4, IR-5, IR-6, IR-8, IR-9, AC-7, AC-17, IA-5, SI-3, SI-4, SI-7, SI-12, SI-13, CP-10, PE-3, PE-6, MP-5, MP-6

We maintain a proactive posture toward security, identifying and classifying potential incidents to ensure appropriate controls, rapid response, and continuous mitigation efforts. While incidents often span multiple categories, our approach is rooted in anticipating attack vectors and limiting impact through layered defenses and procedural readiness.

Data Incidents

These involve compromise or exposure of sensitive internal information, including source code, employee data, and intellectual property. Although our systems are architected to avoid handling customer data—eliminating a major regulatory risk—we remain vigilant in protecting internal assets through access control, configuration reviews, and routine audits.

Access Incidents

These focus on unauthorized access, including credential theft, account compromise, privilege escalation, and authentication bypass. As access issues can serve as precursors to larger breaches, we enforce MFA, monitor access logs, and apply strict privilege separation. We are especially cautious with Azure AD privileged accounts due to their broad scope.

Malware Incidents

Malicious software, including ransomware, spyware, and code injection, poses risks to both operations and product integrity. We prioritize protection of development systems to prevent tampering with our software supply chain, applying endpoint protection, secure build practices, and regular code integrity checks.

Availability Incidents

Disruptions such as denial-of-service attacks, crashes, or resource exhaustion directly affect service reliability. Our cloud-based architecture provides inherent scalability and fault tolerance, but we also implement alerting, monitoring, and response plans to maintain availability and mitigate impact quickly.

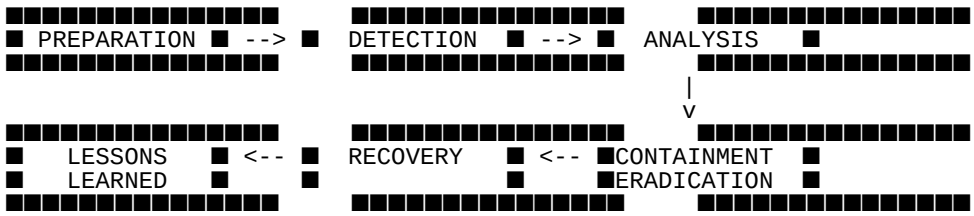
Physical Incidents

Though rare in a cloud-native environment, physical threats—like device theft or workspace breaches—can still expose sensitive assets. We mitigate these risks with full-disk encryption, remote wipe, access controls, and preparedness for environmental and hardware failures affecting developer systems.

4. Incident Response Process

4.1 Response Phases

NIST Controls: IR-4, IR-5, IR-6, IR-7



Our incident response process follows the industry-standard phases while adapted for our small team reality. This circular process emphasizes that incident response is ongoing, with lessons learned feeding back into preparation for the next incident. We've found this systematic approach prevents panic-driven responses while ensuring we don't skip critical steps under pressure.

4.2 Preparation Phase (Ongoing)

NIST Controls: IR-1, IR-2, IR-3

Preparation forms the foundation of effective incident response, requiring continuous effort to maintain readiness. Our technical preparations ensure we have the right tools

and systems in place before incidents occur. This includes maintaining incident response tools in ready state with current licenses and updated signatures, keeping contact lists current with quarterly reviews and immediate updates for personnel changes, updating playbooks based on new threats and lessons learned, verifying backup systems through monthly restoration tests, and configuring monitoring to detect the incidents we're most concerned about. We've learned that scrambling to deploy tools during an incident wastes precious time and often fails under pressure.

Team preparation acknowledges that incident response is a human process requiring clear understanding and regular practice. We ensure roles are assigned and understood through explicit documentation and regular discussion, training is completed with annual requirements and ongoing skill development, tabletop exercises conducted quarterly test our procedures without system impact, and on-call schedules maintained fairly across qualified team members. This human element often determines response success more than technical capabilities, particularly in our small team where confusion about roles could paralyze response.

Documentation readiness means having critical information immediately accessible when stress is high and time is short. We maintain response procedures in easily accessible formats with offline copies, evidence collection forms ready to ensure legal admissibility, communication templates pre-approved by legal counsel, and regulatory requirements matrices to avoid missing critical notifications. This preparation transforms complex requirements into simple checklists usable under pressure.

4.3 Detection and Analysis Phase

NIST Controls: IR-4, IR-5, SI-4

Detection begins our active response, coming from various sources that we monitor continuously. Azure Security Center provides our primary automated detection for infrastructure threats, while endpoint detection alerts catch threats on individual systems. Employee reports often identify issues our automated systems miss, particularly social engineering attacks. Customer notifications alert us to service issues they experience, while third-party notifications might inform us of breaches affecting our supply chain. Our monitoring system alerts aggregate various security signals into actionable intelligence. This multi-layered detection approach compensates for our inability to maintain 24/7 security monitoring.

Initial triage must occur within 15 minutes of detection to prevent minor incidents from escalating into major breaches. During this critical window, we validate whether the incident is real or a false positive to avoid wasting resources, determine the appropriate

severity level to trigger proper response, activate the response team based on severity and required expertise, begin documentation to capture crucial early evidence, and preserve initial evidence before it's overwritten or destroyed. This rapid triage process relies on clear criteria and practiced decision-making rather than lengthy analysis.

Detailed analysis extends over 1-2 hours as we develop comprehensive understanding of the incident. We work to determine the scope of incident including all affected systems and data, identify specific systems and data affected to understand business impact, establish a timeline to understand attack progression and identify patient zero, collect additional evidence while maintaining chain of custody, and assess business impact to inform response priorities and communications. Throughout analysis, we ask key questions: What happened and how? When did it occur and how long has it been ongoing? How was it discovered and why didn't we detect it sooner? What systems are affected and what's the blast radius? Is it ongoing or have we contained the active threat? What is the business impact in terms of data, availability, and reputation?

4.4 Containment Phase

NIST Controls: IR-4, IR-6

Immediate containment focuses on stopping the bleeding before the incident spreads further. We rapidly isolate affected systems using network segmentation and security group changes, disable compromised accounts to prevent further unauthorized access, block malicious IPs and domains at multiple network layers, revoke compromised credentials including API keys and service accounts, and enable additional monitoring to detect lateral movement or repeated attacks. This phase prioritizes speed over completeness, accepting that we might over-contain initially and relax restrictions as we understand the incident better.

Short-term containment implements more sustainable controls while we work toward full eradication. We patch vulnerabilities that enabled the incident when patches are available, increase logging verbosity to capture additional forensic data, deploy temporary fixes like Web Application Firewall rules for zero-days, reroute traffic if needed to maintain service availability, and backup affected systems before making changes that might destroy evidence. These actions balance incident response with business continuity, particularly important when full remediation might take days or weeks.

Evidence preservation throughout containment ensures we can support investigations, insurance claims, and potential legal proceedings. We create forensic images of affected systems before making changes, collect logs and artifacts that might be

overwritten during normal operations, document system state through screenshots and configuration exports, maintain chain of custody with proper forms and access controls, and secure physical evidence like affected devices in locked storage. This evidence collection occurs in parallel with containment, requiring coordination to avoid team members destroying evidence while trying to help.

4.5 Eradication Phase

NIST Controls: IR-4, IR-6

Removing the threat completely prevents reinfection and repeated incidents. We systematically delete malware from all affected systems using multiple scanning tools, close vulnerabilities through patching and configuration changes, remove unauthorized access by resetting credentials and reviewing all access grants, clean infected systems or rebuild from known-good sources when cleaning isn't trustworthy, and update security controls to detect and prevent similar attacks. This phase requires patience and thoroughness as rushed eradication often leaves backdoors that attackers exploit weeks later.

Verification of successful eradication prevents embarrassing reinfections that damage credibility. We scan for remaining threats using different tools than initial detection, verify patches applied successfully and didn't introduce new issues, confirm access removed by testing former attack paths, check for backdoors including scheduled tasks and startup items, and monitor for reinfection over several days before declaring victory. This verification process has caught persistent threats that would have survived our initial eradication efforts.

4.6 Recovery Phase

NIST Controls: IR-4, CP-10

System restoration returns us to normal operations while maintaining security improvements from the incident. We restore from clean backups after verifying they predate the infection, rebuild compromised systems from standard images when backups aren't suitable, reinstall applications using clean sources and updated versions, restore data after validation to ensure we're not reintroducing malware, and verify functionality through comprehensive testing before returning to production. This methodical approach prevents introducing new problems while fixing the original incident.

Enhanced monitoring during recovery catches problems before they affect users. We implement enhanced monitoring for the initial recovery period, watch specifically for

incident recurrence using indicators from our investigation, verify normal operations through synthetic transactions and user feedback, monitor performance to ensure recovery hasn't degraded service, and track user activity for anomalies that might indicate persistent compromise. This vigilance during early recovery has caught subtle persistent threats that evaded our eradication efforts.

Returning to normal operations requires careful orchestration to avoid confusion. We remove temporary controls that might impact performance or usability, restore normal access patterns after verifying user legitimacy, document final system state for future reference and compliance, close the incident ticket with comprehensive documentation, and send final communications to stakeholders confirming resolution. This orderly conclusion ensures everyone knows the incident is over while capturing lessons for improvement.

4.7 Lessons Learned Phase

NIST Controls: IR-4, IR-8

Post-incident review within one week ensures we capture insights while memories remain fresh. We conduct comprehensive timeline review to understand the complete incident lifecycle, assess decisions made during response to identify what worked and what didn't, evaluate process effectiveness to find gaps in our procedures, review communications to improve future stakeholder updates, and analyze tool performance to identify needed capabilities or training. This structured review transforms each incident into organizational learning.

Improvement actions from lessons learned strengthen our security posture incrementally. We update response procedures based on gaps identified during the incident, enhance security controls to prevent similar incidents, identify additional training needs for team members, implement tool improvements or acquire new capabilities, and update policies to address root causes. These improvements accumulate over time, making each incident response better than the last. Our small size allows rapid implementation of improvements without bureaucratic delays.

Comprehensive documentation preserves institutional knowledge as team members change. We produce final incident reports for executive review and compliance records, collect metrics for trending and program improvement, update our knowledge base with technical details and response procedures, improve playbooks with specific lessons from this incident type, and share learnings across the team to build collective expertise. This documentation investment pays dividends when similar incidents occur months or years later.

5. Communication Procedures

5.1 Internal Communications

NIST Controls: IR-4, IR-6

Effective internal communication during incidents ensures coordinated response without information silos. We use our private Slack #incident channel as the primary coordination point during active incidents, providing real-time updates visible to all responders. For Severity 1 and 2 incidents, we establish a voice bridge enabling rapid decision-making and complex technical discussions that would be cumbersome in text. Hourly email updates go to extended stakeholders who need awareness but aren't actively responding, while our status dashboard provides visual representation of incident progress and system status.

Stakeholder updates follow a tiered approach based on incident severity and organizational impact. The CEO receives immediate notification for Severity 1 incidents that have potential for business impact, while the broader leadership team gets updates within one hour to enable resource allocation and business decisions. All staff receive appropriate updates when incidents might affect their work or require their awareness for customer interactions. These defined timelines ensure consistent communication without overwhelming people with unnecessary details.

5.2 External Communications

NIST Controls: IR-6, IR-8

Customer notifications balance transparency with avoiding unnecessary alarm, following strict timelines based on severity. Since we don't handle customer data, our notifications primarily concern potential software integrity issues. Severity 1 incidents affecting code integrity require notification within 4 hours, as customers need to assess their deployment risk. Severity 2 incidents allow 8 hours for notification, providing time to verify whether distributed software was affected. Severity 3 incidents permit 24-hour notification windows, typically for issues that didn't affect released code. Severity 4 incidents get aggregated into monthly security bulletins. These timelines provide predictability while allowing proper impact assessment.

Our customer notification content follows a careful structure providing necessary information without creating additional risk. We explain what happened focusing on potential software integrity impacts, clearly state when the incident occurred and which software versions might be affected, describe whether their deployments could be compromised, outline actions we've taken to verify code integrity, provide clear next

steps such as integrity verification procedures, and include direct contact information for technical questions. Since our software runs on customer infrastructure, we include guidance on how to check their deployments for indicators of compromise. This structured approach ensures consistent, professional communications that maintain customer confidence.

Regulatory notifications follow strict legal requirements that vary by jurisdiction and incident type. While our architecture eliminates most data breach notification requirements since we don't process customer data, we still have obligations for employee data breaches under GDPR (72 hours for EU employee personal data) and various state laws. More relevant to our business model are potential requirements around software supply chain notifications, particularly if compromised code could affect critical infrastructure customers. Our cyber insurance requires notification within 24 hours for potential claims. We maintain a regulatory notification checklist ensuring we don't miss critical deadlines.

Media and public relations require special handling given the potential for incidents to damage our reputation. We maintain a strict policy that no team member provides comments without CEO approval, preventing inconsistent or damaging statements. Only prepared statements reviewed by legal counsel get released, ensuring accuracy and appropriate legal protection. All media interactions coordinate through legal counsel who understand the implications of public statements. We designate a single spokesperson (typically the CEO) for consistency. These controls prevent well-meaning but potentially harmful public communications during stressful incidents.

5.3 Communication Templates

NIST Controls: IR-6

Pre-drafted templates ensure rapid, consistent, and legally appropriate communications during incidents when time is critical. Our initial customer notification template provides the structure for rapid communication while allowing customization for specific incidents:

```
Subject: Important Security Update - [Date]

Dear [Customer Name],

We are writing to inform you of a security incident that
[may have affected/did not affect] the integrity of our software.

What Happened:
[Brief description without revealing attack vectors]

When:
[Timeline of events]
```

```
Software Versions Potentially Affected:
[Specific versions if any]

Impact Assessment:
[Whether deployed software could be compromised]

Our Response:
[Code integrity verification steps taken]

What You Should Do:
[Verification steps for your deployment]
[How to check for indicators of compromise]
[Update procedures if needed]

We take the security of our software seriously and apologize
for any concern this may cause. Our code integrity verification
shows [status of distributed software].

If you have questions, please contact:
[Contact Information]

Sincerely,
[Name], [Role]
OversiteAI
```

6. Specific Incident Playbooks

6.1 Source Code Breach Playbook

NIST Controls: IR-4, IR-5, IR-6, IR-8

Source code breaches represent our highest-risk incident type given that our code is our entire business value. Our immediate actions upon detecting potential unauthorized code access focus on understanding scope and preventing further exfiltration. We rapidly identify which repositories or code sections were accessed to understand the business impact. Determining whether code was merely viewed versus actually copied affects our response strategy. We work immediately to revoke compromised credentials and rotate all repository access tokens while preserving audit logs for investigation.

Our investigation for source code breaches follows specific lines of inquiry crucial for protecting our intellectual property. We must determine exactly what code was accessed, including specific repositories, branches, and commit history. Understanding whether code was cloned, downloaded, or merely viewed online affects both our response and potential business impact. Determining how long unauthorized access persisted helps scope potential theft and identify all affected code assets. Identifying the entry point prevents reoccurrence and may reveal additional vulnerabilities in our development infrastructure. Confirming whether systems remain compromised drives decisions about code integrity and the need for comprehensive security audits of our entire codebase.

6.2 Supply Chain Attack Playbook

NIST Controls: IR-4, SA-12, SR-3

Supply chain attacks targeting our development pipeline or dependencies pose extreme risk since they could compromise our software integrity at scale. Our immediate response to suspected supply chain compromise focuses on preventing malicious code from reaching our customers. We immediately freeze all builds and deployments to prevent distribution of potentially compromised software, audit recent releases for signs of tampering or unexpected changes, isolate build systems from production to prevent lateral movement, inventory all third-party dependencies for known compromises, and notify customers if released software might be affected.

Investigation of supply chain attacks requires deep technical analysis across our entire development ecosystem. Build log analysis reveals unauthorized changes or unexpected behavior during compilation. Dependency verification ensures all libraries match expected hashes and signatures. Source code diffs identify any unauthorized modifications between versions. Binary analysis of compiled artifacts can reveal injected malicious code. Container image scanning detects compromised base images or layers. This investigation often requires specialized expertise we may need to bring in externally.

Recovery from supply chain attacks demands extraordinary care to prevent reinfection. We rebuild entire development environments from known-clean sources, verify all dependencies against multiple sources before trusting them, implement additional signing and verification throughout our pipeline, enhance monitoring for build anomalies and unexpected changes, and carefully validate all software before resuming distribution. The reputational damage from distributing compromised software could destroy our business, making thorough remediation essential regardless of time or cost.

6.3 Ransomware Playbook

NIST Controls: IR-4, IR-5, SI-3

Ransomware attacks have evolved from simple encryption malware to sophisticated operations including data exfiltration and extortion. For OversiteAI, ransomware targeting our development infrastructure or code repositories represents an existential threat. Our immediate response to suspected ransomware focuses on preventing spread while preserving our ability to recover. We isolate infected systems within minutes using network segmentation, immediately verify the integrity and availability of our code repository backups, check if attackers accessed source code before encryption for potential extortion, preserve the ransom note and all attacker

communications, and maintain a firm policy against paying ransoms which only encourages future attacks.

Recovery from ransomware requires careful decision-making balancing technical capabilities with business needs. Our primary recovery method relies on restoring from backups, which requires validating backup integrity and ensuring they predate infection. When decryption keys are publicly available for older ransomware variants, we may attempt decryption, though this rarely succeeds with modern ransomware. Rebuilding systems from scratch becomes necessary when backups are unavailable or compromised. Seeking vendor assistance from security firms with ransomware expertise may provide options we haven't considered. Throughout recovery, we document time and costs for insurance claims and lessons learned.

Key decisions during ransomware incidents require executive involvement given potential business impact. Any consideration of ransom payment requires CEO approval and legal counsel consultation, though our policy strongly discourages payment. Law enforcement notification decisions balance potential assistance against delays and public disclosure. Cyber insurance claims must be filed promptly to ensure coverage for response costs and business interruption. Public disclosure approaches require careful consideration of customer impact, regulatory requirements, and reputational damage. These decisions often have no perfect answer, requiring judgment calls based on specific circumstances.

6.6 Account Compromise Playbook

NIST Controls: IR-4, AC-2, AC-7

Account compromises in our environment primarily concern developer accounts with repository access, administrative accounts with infrastructure control, and service accounts used in our build pipeline. Our immediate actions focus on preventing code theft or infrastructure damage. We disable compromised accounts within minutes, immediately audit recent repository access and code downloads, reset all related passwords including git credentials and API tokens, review infrastructure changes for backdoors or persistence, and check build logs for signs of pipeline manipulation.

Investigation of account compromises requires detailed analysis of authentication and authorization logs. Login history analysis reveals the timeline of compromise and potential data exposure window. We examine permission changes that might indicate privilege escalation or preparation for data theft. Data access logs show what information the attacker viewed or exfiltrated during their access. Email and file activity could reveal business email compromise or intellectual property theft. Evidence

of lateral movement to other accounts or systems indicates a more sophisticated attack requiring broader response. This investigation often reveals the compromise predated detection by weeks or months, emphasizing the importance of comprehensive logging.

Account compromise response must address both immediate threats and systemic weaknesses that enabled the attack. We implement additional authentication factors for affected account types, review and strengthen password policies that may have permitted weak credentials, enhance monitoring for unusual authentication patterns that might indicate future compromises, educate users about the attack vector to prevent recurrence, and assess whether architectural changes could prevent similar compromises. Our small size makes company-wide changes feasible that larger organizations couldn't implement quickly.

6.5 DDoS Attack Playbook

NIST Controls: IR-4, SC-5

While our customer-hosted architecture makes traditional DDoS attacks less impactful, attacks targeting our development infrastructure or software distribution channels could still disrupt operations. Our immediate actions leverage cloud-native protections while ensuring continued development productivity. We activate Azure DDoS protection for our development infrastructure, implement geographic filtering if attacks originate from unexpected regions, enable rate limiting on our package repositories and download servers, work to identify whether the DDoS masks other attack attempts, and ensure development teams can continue working through alternate access methods if needed.

Mitigation strategies for DDoS attacks combine technical controls with business decisions about acceptable trade-offs. Traffic filtering at multiple layers blocks malicious traffic while attempting to allow legitimate users, though perfect filtering rarely exists. Geographic blocking may be necessary if attacks originate from regions where we have no customers, accepting that we might block some legitimate traffic. CDN activation can absorb volumetric attacks by distributing load across global infrastructure. Capacity scaling in the cloud provides near-infinite resources but at potentially significant cost. ISP coordination becomes necessary for network-layer attacks that Azure cannot fully mitigate. Each mitigation strategy involves trade-offs between availability, cost, and potential collateral damage to legitimate users.

DDoS attacks often accompany other attack types, using availability issues to distract from data exfiltration or system compromise. We maintain vigilance for secondary attacks during DDoS response, ensure monitoring continues for other threat types,

preserve logs that might reveal the true attack objective, and prepare for extortion attempts following demonstration attacks. This multi-faceted view prevents tunnel vision on availability while missing more serious compromises.

6.4 Insider Threat Playbook

NIST Controls: IR-4, AU-6, PS-4

Insider threats pose unique risks in our environment where developers have legitimate access to our most valuable asset - source code. Our immediate actions when suspecting insider threats focus on quiet evidence preservation while preventing mass code exfiltration. We implement subtle monitoring of repository access patterns without alerting the suspected insider, temporarily limit large-scale code downloads through rate limiting rather than access revocation, preserve all git logs and access records before they can be modified, immediately consult legal counsel for employment law compliance, and prepare to quickly revoke access if exfiltration accelerates.

Special handling requirements for insider threats reflect their unique challenges compared to external attacks. Investigations must remain confidential to protect both the investigation integrity and the employee's reputation if suspicions prove unfounded. HR involvement from the start ensures employment law compliance and proper procedures. Legal considerations include potential criminal prosecution and civil litigation requiring careful evidence handling. Law enforcement involvement may be necessary for criminal cases but requires careful coordination. Chain of custody becomes critical as insider threat cases more often result in legal proceedings than external attacks. These requirements often conflict with our usual transparent culture, requiring careful navigation.

Insider threat investigations often reveal systemic issues beyond individual malicious actions. Excessive access permissions enabling unauthorized actions, inadequate segregation of duties allowing single individuals too much control, insufficient monitoring of privileged user activities, gaps in pre-employment screening or ongoing monitoring, and cultural issues that might drive insider actions all require attention. Addressing these systemic issues prevents future insider threats while improving overall security posture.

7. Evidence Collection and Handling

7.1 Evidence Types

NIST Controls: IR-4, AU-9

Effective incident response requires proper evidence collection to support investigations, legal proceedings, and lessons learned. Our cloud-native environment creates unique evidence challenges compared to traditional on-premises infrastructure. Digital evidence forms the bulk of our collection and includes system logs from Azure services and our applications providing detailed activity records, network traffic captures when available through Azure Network Watcher or application logs, memory dumps from compromised systems before remediation destroys volatile evidence, file system images captured through Azure disk snapshots or forensic tools, database logs showing data access and modifications, and email records that might reveal social engineering or data exfiltration.

Physical evidence remains relevant despite our cloud focus, particularly for insider threats or device compromises. Hard drives from compromised endpoints require proper handling to preserve evidence, mobile devices might contain cached credentials or company data, USB drives could introduce malware or exfiltrate data, printed materials might reveal information that doesn't exist digitally, and access logs or badge records correlate physical presence with digital activities. Our small office environment makes physical evidence collection manageable but requires the same rigor as digital evidence.

7.2 Collection Procedures

NIST Controls: IR-4, AU-9

Chain of custody procedures ensure evidence admissibility in legal proceedings while supporting internal investigations. We document comprehensive details for every piece of evidence including who collected it with full name and role, what exactly was collected with specific descriptions, when collection occurred with precise timestamps, where the evidence originated and where it's stored now, and how collection was performed including tools and procedures used. This documentation seems excessive during incidents but proves invaluable months later during legal proceedings or insurance claims.

Our technical collection procedures emphasize preservation of evidence integrity while maintaining practical efficiency. We use write-blockers when imaging physical drives to prevent accidental modification, create bit-for-bit copies rather than logical copies to capture all data including deleted files, generate and verify cryptographic hashes before and after transfer to prove integrity, use secure transmission methods like encrypted channels for evidence transfer, and store evidence with encryption at rest to prevent unauthorized access. These procedures come from painful lessons learned when improperly handled evidence was challenged in legal proceedings.

Evidence handling requires balancing competing needs for investigation access and integrity preservation. We maintain detailed access logs showing everyone who viewed or analyzed evidence, limit access to named individuals with specific need to know, use separate analysis systems to prevent contamination of evidence, document all analysis actions that might modify evidence, and maintain original copies separate from working copies. This approach enables thorough investigation while preserving admissibility.

7.3 Evidence Retention

NIST Controls: IR-4, AU-11

Our evidence retention policies balance legal requirements, storage costs, and practical needs for future reference. Incident evidence receives special handling with seven-year retention recognizing potential legal proceedings, insurance claims, and regulatory investigations that may emerge years after incidents. Normal operational logs retain for 90 days unless they become incident evidence, balancing storage costs with investigation needs. Legal hold requirements override all retention policies when litigation is anticipated or active. Secure destruction procedures ensure evidence doesn't leak after retention periods expire. Audit trails of all retention and destruction actions protect against claims of spoliation.

These retention policies reflect our assessment of realistic legal and business needs while acknowledging storage limitations as a small company. We've automated retention where possible to avoid manual errors while maintaining flexibility for special circumstances. Regular review ensures our policies remain aligned with changing regulations and business needs.

8. Training and Testing

8.1 Training Program

NIST Controls: IR-2, IR-3

Our training program builds incident response capabilities across our small team while acknowledging that security isn't anyone's primary role. We've structured training to be practical and immediately applicable rather than theoretical, ensuring time invested provides immediate value.

All staff receive foundational security awareness training that includes recognizing potential threats to our source code and development infrastructure, understanding the critical importance of protecting our intellectual property, knowing how to report suspicious repository access or build anomalies, and participating in regular security

exercises focused on code protection scenarios. This universal training ensures every employee understands that our code is our business and acts accordingly. Annual refresher training maintains awareness while introducing new supply chain threats and updating procedures based on lessons learned. that includes recognizing security incidents and the importance of rapid reporting, understanding basic incident types they might encounter, knowing how to report suspicious activities without fear of blame, and participating in regular phishing simulations that test and reinforce learning. This universal training ensures every employee can serve as a sensor in our detection network while building a security-conscious culture. Annual refresher training maintains awareness while introducing new threats and updating procedures based on lessons learned.

Incident Response Team members receive deeper training aligned with their response roles. This includes comprehensive incident response procedures tailored to our environment, hands-on evidence handling training to ensure legal admissibility, communication protocol practice for high-stress situations, and tool usage training for the specific technologies we employ. We emphasize scenario-based training that mirrors real incidents rather than abstract concepts. Annual certification requirements ensure skills remain current while providing career development opportunities for team members.

Specialized training addresses specific technical needs within our response capability. Technical responders receive forensics training appropriate for cloud environments, leadership team members practice crisis communication for public-facing incidents, and management receives legal and regulatory training for compliance requirements. This targeted approach ensures we have necessary skills without over-training people who won't use them. We leverage online training where possible to minimize cost while maintaining quality.

8.2 Testing Schedule

NIST Controls: IR-3, CA-2

Regular testing validates our procedures work as designed while identifying gaps before real incidents expose them. Our testing schedule balances thoroughness with the reality that everyone has primary jobs beyond incident response.

Monthly testing focuses on technical fundamentals that must work reliably. We verify automated tool functionality including detection and alerting systems, test communication trees to ensure contact information remains current, and validate backup integrity through restoration exercises. These quick tests catch degradation

before it impacts real response while requiring minimal time investment from team members.

Quarterly testing exercises our human and procedural elements. Tabletop exercises walk through incident scenarios without touching production systems, allowing us to test decision-making and communication in a safe environment. Playbook walkthroughs ensure procedures remain current with our evolving environment while building team familiarity. Team availability checks confirm we can assemble necessary resources within response time requirements. These exercises often reveal outdated assumptions or procedures that looked good on paper but fail in practice.

Annual testing provides comprehensive validation through realistic scenarios. Full simulation exercises test our entire response capability end-to-end, revealing integration issues between phases. Third-party assessments provide objective evaluation of our capabilities and recommendations for improvement. Purple team exercises combine internal and external perspectives to test both defense and response. These intensive exercises require significant investment but provide confidence in our real incident response capability.

8.3 Exercise Scenarios

NIST Controls: IR-3

Our exercise scenarios reflect realistic threats aligned with our risk assessment, focusing heavily on protecting our source code and development infrastructure. Each scenario teaches specific lessons while building general response capabilities relevant to a software company that doesn't handle customer data. aligned with our risk assessment rather than fantastical movie plots. Each scenario teaches specific lessons while building general response capabilities.

Source code theft simulations are our highest priority scenario given that code represents our entire business value. We practice rapid detection of unauthorized repository access, test our ability to identify what code was accessed or cloned, exercise decision-making around customer notifications for potential integrity issues, and practice code integrity verification across our entire codebase. These exercises have revealed the need for better repository access monitoring and more granular git permissions.

Supply chain attack exercises test our ability to detect and respond to compromises in our development pipeline. We practice identifying unusual build behavior or dependency changes, test our ability to verify the integrity of third-party libraries,

exercise customer notification procedures for potentially compromised software, and practice rolling back releases while maintaining customer trust. These scenarios have proven critical given recent industry supply chain attacks.

Other scenarios round out our preparedness including insider threat investigations focusing on developers with repository access, ransomware attacks targeting our development infrastructure, and compromised developer workstation scenarios that could expose credentials or code. Each scenario contributes specific skills while reinforcing that protecting our intellectual property is paramount. We rotate scenarios to maintain engagement while ensuring comprehensive coverage over time.

9. Integration with Other Plans

NIST Controls: CP-2, IR-4, PM-8

Our Incident Response Plan doesn't operate in isolation but forms part of an integrated resilience framework. Clear integration points with other organizational plans ensure coordinated response without duplication or gaps. This integration becomes particularly critical during major incidents that threaten business continuity beyond just security impacts.

9.1 Business Continuity Plan

NIST Controls: CP-2, CP-4

Security incidents often trigger business continuity concerns, requiring seamless handoff between plans. Our integration ensures that incident severity classifications align with business continuity activation triggers, avoiding confusion about when to escalate from security response to business continuity. We share communication procedures between plans, ensuring stakeholders receive consistent information regardless of which plan is active. Resource prioritization protocols prevent conflict when both security response and business recovery compete for the same limited resources. Recovery coordination mechanisms ensure security considerations are maintained during rapid business recovery efforts that might otherwise reintroduce vulnerabilities.

This integration reflects lessons learned when past incidents created business impacts we weren't prepared to handle through security response alone. By clearly defining escalation triggers and handoff procedures, we ensure smooth transition when incidents exceed security boundaries. Regular joint exercises between incident response and business continuity teams have refined these integration points, building

muscle memory for real events.

9.2 Disaster Recovery Plan

NIST Controls: CP-2, CP-10

Technical recovery often requires disaster recovery procedures, particularly for ransomware or destructive attacks. Our integration ensures system recovery procedures consider security requirements to avoid reinfecting cleaned systems, backup utilization includes validation to prevent restoring compromised data, alternative site activation maintains security controls despite emergency conditions, and data restoration includes integrity verification beyond simple functionality testing. This security-aware recovery prevents incidents from recurring due to rushed recovery efforts.

We've learned that pressure to restore service quickly can lead to bypassing security controls that seem unnecessary during emergencies. Our integrated procedures explicitly address this tendency, building security validation into recovery checklists rather than treating it as an afterthought. Joint exercises have proven invaluable for building understanding between security and operations teams about their mutual dependencies during recovery.

9.3 Crisis Management

NIST Controls: IR-4, PM-1

Major security incidents become organizational crises requiring executive leadership beyond technical response. Our crisis management integration addresses executive decision-making for issues beyond technical response authority, media relations when incidents become public knowledge, stakeholder management for investors and key customers, and reputation protection through coordinated communication strategies. These elements often determine long-term business impact more than technical response effectiveness.

Clear escalation criteria ensure smooth transition from technical incident response to executive crisis management. We've defined specific triggers including confirmed data breaches affecting customers, ransomware with significant business disruption, insider threats involving executives, and any incident likely to generate media attention. These triggers activate our crisis management team while maintaining technical response efforts, ensuring both technical and business aspects receive appropriate attention.

10. Metrics and Reporting

NIST Controls: IR-4, IR-8, PM-6

10.1 Key Metrics

NIST Controls: IR-5, PM-6

Meaningful metrics drive continuous improvement in our incident response program while demonstrating value to leadership. We focus on metrics that indicate actual capability rather than vanity numbers that look good but provide little insight.

Our response metrics measure the speed and effectiveness of our incident handling processes. Mean Time to Detect (MTTD) reveals how quickly our monitoring and detection capabilities identify incidents, with trends showing whether our detection is improving. Mean Time to Respond (MTTR) measures the gap between detection and active response, indicating our mobilization effectiveness. Mean Time to Contain (MTTC) shows how quickly we can stop active threats from causing additional damage. Mean Time to Recover (MTTR) captures total incident duration from detection to full service restoration. These time-based metrics, tracked by severity level, reveal whether our response is improving and where bottlenecks exist.

Quality metrics assess the accuracy and effectiveness of our processes beyond simple speed. False positive rate indicates whether our detection is properly tuned or crying wolf too often, causing alert fatigue. Incidents by type reveal patterns in our threat landscape, with particular attention to code repository access attempts and development infrastructure attacks. Source code integrity verification success rate measures our ability to confirm code hasn't been tampered with. Repeat incident tracking shows whether our remediation efforts truly address root causes or just symptoms. These quality indicators ensure we're not just responding quickly but effectively protecting our intellectual property. the accuracy and effectiveness of our processes beyond simple speed. False positive rate indicates whether our detection is properly tuned or crying wolf too often, causing alert fatigue. Incidents by type reveal patterns in our threat landscape and where to focus preventive efforts. Severity accuracy measures whether our initial classifications hold up through investigation or require adjustment. Repeat incident tracking shows whether our remediation efforts truly address root causes or just symptoms. These quality indicators ensure we're not just responding quickly but effectively.

Process metrics evaluate the human and procedural elements that often determine response success. Escalation effectiveness measures whether incidents reach the right

people quickly without unnecessary delays. Communication timeliness tracks whether stakeholders receive updates within defined windows. Evidence quality assessments ensure our collection procedures support potential legal needs. Implementation rate of lessons learned demonstrates whether we're actually improving based on experience or just documenting good intentions. These process measurements often reveal improvement opportunities that technical metrics miss.

10.2 Reporting

NIST Controls: IR-8, AU-6, PM-14

Regular reporting transforms raw metrics into actionable intelligence for different audiences. We've structured our reporting cadence to provide timely information without overwhelming recipients or creating busywork.

Monthly reports target operational leadership with tactical information for immediate improvements. These include incident summaries with enough detail to understand patterns without compromising confidentiality, metrics dashboards showing trends with clear visual indicators of improvement or degradation, trend analysis highlighting emerging threats or process issues requiring attention, and specific improvement actions with owners and deadlines. This frequency ensures issues receive attention before they become systemic while respecting leadership time constraints.

Quarterly reports provide strategic analysis for executive decision-making. These comprehensive documents include detailed analysis of incident patterns and their business implications, process improvement recommendations with cost-benefit analysis, training status updates ensuring our team maintains necessary capabilities, and budget utilization analysis demonstrating fiscal responsibility. The quarterly cadence aligns with business planning cycles while providing sufficient data for meaningful analysis.

Annual reports assess program maturity and set strategic direction. These include comprehensive program maturity assessments against industry frameworks, strategic recommendations for capability improvements aligned with business growth, resource requirement projections based on threat landscape and company evolution, and industry comparisons showing how our capabilities stack up against similar companies. This annual strategic view ensures our incident response capabilities evolve with business needs rather than stagnating.

11. Resource Requirements

NIST Controls: IR-2, PM-3, SA-2

11.1 Tools and Technology

NIST Controls: IR-2, IR-7

Effective incident response requires appropriate tools, but our small size demands careful selection to maximize capability within budget constraints. We focus on tools that provide multiple capabilities, integrate with our existing environment, and don't require dedicated specialists to operate.

Our core toolset leverages Azure-native capabilities supplemented by best-of-breed solutions where necessary. Azure Sentinel serves as our SIEM platform, providing log aggregation, correlation, and automated response capabilities within our existing Azure environment. The native integration reduces complexity while providing enterprise-grade capabilities at a cost scaled to our usage. Our EDR solution protects endpoints with behavioral detection and response capabilities beyond traditional antivirus. The forensics toolkit includes both cloud-native and traditional tools for evidence collection and analysis. Our communication platform (currently Slack) provides secure, auditable incident coordination with integration to other tools. Documentation systems capture institutional knowledge and satisfy compliance requirements. This integrated stack provides comprehensive capability without overwhelming complexity.

Additional resources extend our capabilities for scenarios exceeding internal capacity. Our incident response retainer provides guaranteed access to expertise and resources during major incidents, converting unpredictable emergency costs into manageable operational expenses. Legal counsel retainer ensures immediate access to legal guidance for breach notifications and privileged investigations. Threat intelligence feeds enhance our detection and response with contextual information about emerging threats. Training budget maintains team capabilities through continuous education. Equipment refresh cycles ensure our tools remain current and supported. These investments reflect our recognition that incident response readiness requires ongoing commitment, not just emergency spending.

11.2 Documentation

NIST Controls: IR-2, AU-11

Proper documentation forms the foundation of effective and legally defensible incident response. Our documentation requirements balance thoroughness with practicality, ensuring we capture necessary information without creating bureaucratic burden during high-stress incidents.

We maintain standardized forms and templates that guide consistent response while reducing cognitive load during incidents. Incident response forms capture essential information systematically, ensuring nothing gets forgotten in the heat of response. Evidence bags and tags maintain physical chain of custody with pre-printed fields for required information. Chain of custody forms document digital evidence handling with legally sufficient detail. Communication templates ensure rapid, consistent, and appropriate notifications. Contact lists provide immediate access to critical resources without searching through systems. This documentation infrastructure transforms complex requirements into simple checklists, enabling effective response even when stress is high and experience is limited.

12. Maintenance

NIST Controls: IR-1, IR-3, PM-4

12.1 Plan Updates

NIST Controls: IR-3, CA-5

Living documents require regular maintenance to remain effective, and our Incident Response Plan is no exception. We've established a maintenance schedule that ensures currency without creating excessive overhead for our small team.

Annual comprehensive reviews examine every aspect of the plan for accuracy and effectiveness. These reviews consider changes in our business model, technology stack, threat landscape, and regulatory environment. We assess whether our procedures still match operational reality, roles remain assigned to appropriate people, and contact information stays current. This annual deep dive often reveals assumptions that no longer hold true and procedures that have informally evolved beyond documentation.

Trigger-based updates supplement scheduled reviews when significant changes demand immediate attention. Major incidents often reveal procedure gaps requiring prompt correction to prevent recurrence. Regulatory changes might impose new notification requirements we must incorporate. Organizational changes like key personnel transitions or structural reorganizations necessitate role reassignment. Technology changes including new tools or platforms require procedure updates. These

trigger-based updates ensure our plan remains aligned with reality rather than becoming a compliance artifact.

12.2 Continuous Improvement

NIST Controls: IR-4, CA-7

Beyond basic maintenance, we pursue continuous improvement to strengthen our incident response capabilities over time. This improvement process transforms each incident and exercise into organizational learning that enhances future response.

Lessons learned from actual incidents provide the most valuable improvement insights. We systematically capture what worked well to reinforce effective procedures, what failed to identify necessary corrections, what was missing to address capability gaps, and what surprised us to update threat models. These lessons get incorporated into updated procedures, new training requirements, and tool enhancements. Our small size enables rapid implementation of improvements without bureaucratic delays that plague larger organizations.

External inputs complement internal lessons to ensure we don't develop tunnel vision. Industry best practices from frameworks and peer organizations highlight capabilities we should consider. Threat landscape evolution informs new scenarios we must prepare for. Stakeholder feedback reveals external perspectives on our response effectiveness. Audit findings identify gaps from compliance perspectives. These external inputs challenge our assumptions and drive improvements we might not identify internally.

13. Legal and Regulatory Requirements

13.1 Overview

NIST Controls: IR-6, AU-10, AU-16

While our architecture eliminates most data protection regulations since we don't process customer data, we still face several categories of legal requirements during incident response. State breach notification laws still apply to our employee personal information, requiring careful handling of HR data breaches. Industry-specific regulations may apply when our software is used in regulated industries, particularly if code compromise could affect healthcare or financial services customers. International privacy laws like GDPR affect our EU employee data, though not customer data we never access. Contractual obligations with enterprise customers often include security incident notification requirements regardless of data involvement. Intellectual property

law becomes critical when source code theft occurs, requiring different handling than data breaches. These requirements shape our response procedures while remaining proportional to our actual regulatory exposure.

13.2 Legal Coordination

NIST Controls: AU-2, AU-10, IR-6

Legal counsel involvement from the earliest stages of significant incidents ensures appropriate protection while meeting obligations. We've established clear triggers for legal engagement including any suspected source code theft, incidents potentially affecting regulated industry customers, employee data breaches triggering notification requirements, and any incident likely to result in litigation. This early engagement enables privileged communications that protect sensitive investigation details while ensuring compliant response.

Attorney-client privilege considerations shape our investigation procedures for serious incidents. Initial assessments occur under legal direction to maintain privilege, investigation teams include legal counsel for privileged communications, documentation procedures capture facts while protecting legal strategy, and we maintain separate channels for privileged discussions to avoid contaminating operational communications. This approach enables effective response while preserving legal protections.

13.3 Regulatory Reporting Procedures

NIST Controls: IR-6, AU-16, PM-16

When incidents trigger regulatory reporting, accuracy and timeliness are critical. Our procedures ensure we meet obligations without admitting liability unnecessarily.

Notification preparation involves careful coordination between multiple stakeholders. Legal counsel leads drafting with technical input on facts and scope, leadership input on business impact, communications expertise for messaging consistency, and compliance knowledge for regulatory requirements. Standard notification elements include the nature of the incident described factually without speculation, types of information potentially involved with specific data categories, number of individuals affected based on conservative estimates, discovery and containment timeline showing responsible response, mitigation measures implemented to prevent recurrence, contact information for affected individuals' questions, and resources like credit monitoring when appropriate. We maintain pre-reviewed templates for common scenarios, updated quarterly by counsel to reflect regulatory changes.

Submission procedures vary by jurisdiction, requiring careful attention to detail. Some jurisdictions require online portal submissions with specific formatting requirements we document carefully. Others demand physical mail using certified delivery with return receipts for proof. Many want email to designated addresses with specific subject line formats. Some require sample consumer notification letters for approval before sending. We maintain detailed checklists for each jurisdiction where we have employees or significant customers, recognizing that missing technical requirements can result in violations despite substantive compliance.

Documentation requirements anticipate regulatory investigations that often follow notifications. We prepare comprehensive packages including complete incident timelines with supporting evidence, documentation of security measures in place before the incident, demonstration of reasonable response once we detected the issue, proof of notification compliance including delivery confirmations, and evidence of remediation efforts to prevent recurrence. Organizing this documentation proactively during incidents rather than scrambling during investigations significantly improves outcomes while reducing legal costs.

13.4 Cyber Insurance Coordination

NIST Controls: PM-13, SA-9, CM-10

Our cyber insurance policy provides crucial financial protection and access to expert resources during incidents. Effective coordination maximizes these benefits while ensuring coverage remains valid.

Policy coverage relevant to incidents includes broad categories we must understand to utilize effectively. Incident response costs cover forensics, legal, and public relations expenses that can quickly overwhelm our budget. Business interruption losses compensate for revenue impact during outages. Cyber extortion coverage addresses ransomware and similar threats, though our policy against payment limits this use. Regulatory fines and penalties coverage where insurable varies by jurisdiction. Customer notification costs can be substantial for large breaches. Third-party liability protects against customer lawsuits. Understanding these coverages ensures we activate appropriate benefits while maintaining compliance with policy terms.

Notification requirements in our policy demand prompt action to preserve coverage. We must notify our carrier within 48 hours of potential claims, including any Severity 1 incident regardless of apparent insurance impact, incidents with potential third-party effects that might generate liability, regulatory investigation notices that could lead to fines, extortion attempts even if we don't intend payment, and anticipated response

costs exceeding $10,000. The CFO manages insurance relationships but all incident commanders understand requirements to prevent coverage gaps through late notification.

Insurance panel resources provide pre-vetted expertise at negotiated rates. Incident response firms offer immediate deployment with carrier relationships, forensics specialists bring advanced capabilities we lack internally, legal counsel experienced in breaches understand notification complexity, public relations firms manage reputational impact professionally, and customer notification services handle large-scale mailings efficiently. Using panel resources often provides better outcomes than finding vendors during crisis while reducing costs through pre-negotiated rates.

Documentation for claims requires attention during incidents when other priorities compete. We track incident timelines meticulously to support coverage arguments, document response costs through project codes enabling accurate billing, calculate business interruption impacts with financial precision, demonstrate mitigation efforts showing we acted reasonably to minimize damage, and document prior security measures proving due care that affects coverage. This contemporaneous documentation significantly improves claim success compared to after-the-fact reconstruction.

Coverage limitations shape our response strategies to remain within policy bounds. Waiting periods before coverage applies mean initial costs may be ours. Sub-limits for specific costs like forensics require careful management. Exclusions for certain attack types might leave gaps we must cover. Requirements to use panel vendors limit flexibility but ensure quality. Security warranty impacts mean our controls must match application statements. Understanding these limitations prevents surprise coverage denials while enabling maximum utilization of available benefits.

14. Resource Management

14.1 Budget and Financial Considerations

NIST Controls: PM-3, SA-2, PM-11

Incident response capabilities require ongoing investment balanced against our small company constraints. Our resource management ensures readiness without overwhelming operational budgets. We've structured our spending to provide maximum capability while maintaining financial sustainability.

Our annual incident response budget allocates $75,000 across critical capabilities, representing approximately 1.5% of revenue - a reasonable investment given our risk profile. Retainers and insurance consume $25,000 annually, providing access to expertise and financial protection we couldn't afford during actual incidents. Tools and technology require $15,000 beyond base Azure services, enabling advanced detection and response capabilities. Training and exercises need $10,000 to maintain team readiness through continuous education. External validation exercises cost $5,000 annually but provide objective assessment of our capabilities. We maintain a $20,000 contingency reserve for actual incident costs, ensuring response isn't delayed by procurement processes. Board approval for this budget demonstrates governance support while establishing clear expectations.

Incident cost tracking during events supports insurance claims and improvement analysis. We capture internal labor using time tracking with special project codes, multiply hours by loaded rates including benefits and overhead. External consultant costs get coded separately for forensics versus legal versus public relations. Technology costs include emergency licenses and additional infrastructure scaling. Business disruption costs encompass lost productivity and delayed project delivery. Customer impact costs cover service credits and potential lost business. This detailed tracking reveals true incident costs often hidden in general operations, supporting future budget justifications.

Emergency spending authority prevents bureaucratic delays during critical response moments. The Incident Commander can authorize up to $10,000 without additional approval, enabling immediate consultant engagement or tool procurement. CEO approval extends authority to $50,000, covering most incident response needs while maintaining oversight. Expenses above $50,000 require board notification though not pre-approval, balancing fiduciary duty with response needs. This tiered authority, tested through exercises, ensures money never delays necessary response while preventing runaway spending during crisis.

14.2 Technology Stack

NIST Controls: SA-9, CM-7, SC-36

Our incident response technology leverages cloud-native capabilities supplemented by specialized tools where necessary. This approach maximizes capability while minimizing management overhead that our small team cannot support.

Core platform capabilities come from Azure-native services integrated with our infrastructure. Azure Security Center provides continuous assessment and threat

detection across our resources without additional agents or complex deployment. Azure Sentinel serves as our SIEM with automated response capabilities through playbooks we've customized for our environment. Azure Monitor enables comprehensive logging and alerting using the same platform that runs our services. Microsoft 365 Defender protects endpoints and identities with coordinated response across devices and accounts. Azure Backup provides immutable backups crucial for ransomware recovery with native cloud integration. These tools, included or minimally priced with our Azure commitment, provide enterprise capabilities without enterprise costs or complexity.

Supplemental tools address specific gaps where Azure-native capabilities fall short. ServiceNow provides incident ticket tracking and workflow automation beyond basic task lists. Recorded Future API integration enriches indicators with threat intelligence context. Magnet AXIOM cloud enables remote forensic collection when we can't access physical devices. VirusTotal Enterprise analyzes suspicious files with multiple engines and historical context. Slack maintains incident communication channels with full retention for post-incident review. These carefully selected tools each solve specific problems without duplicating existing capabilities, keeping total monthly costs under $1,500.

Build versus buy decisions reflect our constraints and expertise realistically. We default to Azure native tools when they meet requirements adequately, avoiding tool sprawl. Building internal tools only makes sense for company-specific integrations no vendor provides. Complex tool operation requiring dedicated specialists gets rejected regardless of capabilities. Free or open source alternatives receive consideration when commercial tools don't provide sufficient additional value. Multi-use tools that provide value beyond incident response get preference in purchasing decisions. This pragmatic approach has created a manageable stack providing necessary capabilities without overwhelming complexity or cost.

14.3 External Partnerships

NIST Controls: SA-9, IR-7, PS-7

Strategic partnerships multiply our capabilities without adding permanent overhead. We've carefully selected partners who understand small business constraints while providing enterprise-grade expertise when needed.

Our incident response retainer transforms unpredictable emergency costs into manageable operational expenses. The retained firm provides 24/7 hotline access ensuring we can always reach expertise, 10 pre-paid hours annually for preparedness activities like tabletop exercises, reduced hourly rates during actual incidents making

response affordable, access to specialized expertise in areas like forensics and malware analysis, and tooling and infrastructure we couldn't justify purchasing. The retainer firm specializes in mid-market companies, understanding our resource constraints while providing capabilities that would cost millions to build internally.

Legal partnerships ensure rapid access to specialized counsel without maintaining expensive in-house expertise. Primary counsel on monthly retainer handles general security and privacy questions, contract reviews for security terms, and initial incident assessment. Breach counsel specialists engage for actual incidents requiring notification expertise, multi-jurisdictional coordination, and regulatory defense. International counsel networks provide local expertise for jurisdiction-specific requirements without maintaining global relationships. These layered relationships provide appropriate expertise when needed without excessive ongoing costs.

Technology vendor relationships extend beyond normal support to security partnership. Microsoft Premier support includes security escalation paths and dedicated account team understanding our architecture. GitHub enterprise security team access enables rapid response to repository concerns. AWS security review services help when multi-cloud scenarios arise. These relationships, negotiated into enterprise agreements, provide expert assistance during incidents without additional cost. We've learned that vendors want to help during security incidents - we just need established relationships to access that help quickly.

Community relationships provide free resources that complement commercial partnerships. Information Sharing and Analysis Centers (ISACs) enable threat intelligence sharing with peer companies. Local FBI cyber task force relationships facilitate law enforcement coordination when needed. CISA provides alerts and free services designed for small businesses. Security community Slack and Discord channels offer peer support and real-time threat discussions. These community resources, requiring only time investment, often provide insights unavailable through commercial channels.

14.4 Scalability Planning

NIST Controls: PM-2, SA-2, CM-14

Our resource model must scale with company growth without linear cost increases. Planning ensures smooth scaling rather than reactive scrambling when growth overwhelms current capabilities.

Scaling triggers indicate when resource model changes become necessary. Employee count exceeding 50 suggests dedicated security resources become justified. Revenue surpassing $10M enables increased security investment while demanding better protection. International expansion requiring local presence complicates incident response coordination. Regulatory changes might impose requirements exceeding current capabilities. Incidents demonstrating capability gaps provide clear evidence for resource increases. Each trigger initiates comprehensive resource review examining whether existing tools scale or need replacement, if dedicated security staff becomes necessary, whether partnerships can handle increased demand, and what new capabilities growth makes necessary.

Our scaling strategy provides a roadmap while maintaining flexibility for business realities. From 0-50 employees, our current model with external partnerships remains appropriate. At 50-100 employees, a part-time security analyst and enhanced tools become necessary. From 100-200 employees, a full-time security team with internalized basic incident response becomes justified. Above 200 employees, a dedicated SOC with 24/7 monitoring becomes standard. This roadmap sets expectations with leadership while acknowledging actual scaling depends on business conditions beyond simple employee count.

Investment prioritization when scaling ensures maximum impact from limited resources. Detection capabilities take priority to see more as attack surface grows. Automation handles volume increases without linear staffing growth. Training builds internal expertise reducing external dependency. Tools enhance team effectiveness multiplying human capability. Staffing comes only after maximizing the above, avoiding premature hiring. This approach maintains lean operations while systematically building security maturity aligned with business growth.

15. Document Maintenance

15.1 Review and Update Procedures

NIST Controls: CA-5, PM-4, PL-2

This Incident Response Plan requires regular updates to remain effective. Our maintenance procedures ensure the plan evolves with our business, threat landscape, and lessons learned while avoiding the common pitfall of plans becoming shelfware that looks good for auditors but fails during real incidents.

Scheduled reviews follow a tiered approach balancing thoroughness with effort. Quarterly reviews focus on contact information and quick reference guides that change

frequently and cause immediate problems when outdated. Semi-annual reviews examine playbooks and technical procedures ensuring they match our current tooling and cloud infrastructure. Annual comprehensive reviews assess every plan section for accuracy, effectiveness, and alignment with business changes. Ad-hoc reviews triggered by significant incidents or organizational changes ensure we don't wait for scheduled reviews when immediate updates are needed. Review assignments rotate among team members, building familiarity with the plan while distributing maintenance workload.

Each reviewer uses a standard checklist ensuring consistent, thorough evaluation. Contact details get verified through test calls and messages. Procedures get walked through mentally or in tabletop exercises to verify they match current reality. Recent incidents get analyzed for gaps they revealed in our procedures. Role assignments get confirmed with current organization structure and responsibilities. External dependencies like vendor contacts and service agreements get validated. This systematic approach catches issues that ad-hoc reviews miss while building reviewer expertise.

Update triggers beyond scheduled reviews ensure our plan remains current with significant changes. Major incidents revealing procedure gaps demand immediate updates to prevent similar issues. New regulations affecting our business require procedure additions for compliance. Technology changes including new tools, platforms, or cloud services necessitate procedure updates. Organizational changes through growth, restructuring, or key personnel transitions require role and contact updates. Audit findings or assessment recommendations provide external perspective on needed improvements. Industry incidents teaching new lessons get incorporated even if we haven't experienced them directly. These triggers ensure our plan evolves continuously rather than in annual jumps.

Updates follow our documentation change control process ensuring quality and traceability. Reviewers identify needed changes with clear justification. Draft updates use tracked changes enabling easy review. Technical review ensures accuracy of procedures and commands. Legal review validates compliance impacts of changes. Leadership approval confirms resource commitments and policy decisions. Communication of changes ensures all stakeholders understand updates. This process prevents well-meaning but problematic changes while enabling rapid updates when needed.

15.2 Version Control and Distribution

NIST Controls: CM-3, CM-9, SA-10

Effective version control ensures everyone uses current procedures during incidents while maintaining history for audit and improvement. Our approach balances accessibility with control, ensuring rapid access during incidents without losing track of versions.

Version numbering follows semantic versioning principles adapted for documentation. Major versions (1.0, 2.0) indicate significant structural changes affecting how teams use the plan. Minor versions (1.1, 1.2) capture procedural updates and additions that don't fundamentally change the plan structure. Patches (1.1.1) fix typos, update contact information, or make clarifications without changing procedures. The document header prominently displays version information including version number, effective date showing when this version takes effect, last review date indicating currency, next review due date setting expectations, and current status confirming this is the active version. This clear versioning prevents confusion about which version to follow during incidents.

Distribution controls ensure authorized personnel can access the plan rapidly while maintaining security. The master copy resides in SharePoint with automatic version history, access logging for audit trails, approval workflow for changes, and automated notifications when updates occur. Controlled copies exist in multiple formats for different use cases: wiki format for easy browsing during incidents, printed binders in incident response go-bags for infrastructure failures, offline copies on response team laptops for connectivity issues, and executive briefing versions with simplified procedures for leadership. Each copy clearly indicates its controlled status and where to verify currency.

We explicitly mark uncontrolled copies with "Uncontrolled when printed. Check SharePoint for current version." This warning appears on PDFs sent to auditors, printed copies for exercises, and any other distributions outside our control system. While we can't prevent outdated copies from existing, we can ensure users know to verify currency before depending on them during incidents.

15.3 Training on Updates

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

Plan updates require communication and training to be effective. Our approach ensures changes are understood and internalized before they're needed during high-stress incidents.

Communication methods vary based on update significance and urgency. Email announcements suffice for minor updates like contact information changes, providing the update directly in the message. Team meeting discussions address significant procedural changes, allowing questions and clarification. Tabletop exercises incorporate new procedures, building muscle memory through practice. Quick reference guide updates get posted in common areas and distributed electronically. Urgent changes use Slack channels for immediate awareness with follow-up training. This graduated approach ensures appropriate attention without overwhelming teams with minor changes.

Training requirements scale with update complexity and impact. Contact updates need only email notification as they're referenced rather than memorized. Procedure changes require walkthrough in team meetings ensuring understanding and identifying confusion. New playbooks demand tabletop exercises practicing the specific scenario. Major revisions trigger full training sessions covering all changes comprehensively. We track training completion for significant updates, ensuring all response team members understand changes before real incidents test them.

15.4 Integration with Other Documentation

NIST Controls: PL-2, SA-5, CM-7

The Incident Response Plan doesn't exist in isolation but forms part of our integrated security documentation architecture. Clear relationships with other documents ensure consistency while avoiding duplication that leads to maintenance problems.

Related documents each serve specific purposes while referencing the Incident Response Plan appropriately. Our Information Security Policy establishes the mandate and authority for incident response. The Business Continuity Plan defines coordination procedures when incidents affect business operations. The Disaster Recovery Plan provides technical recovery procedures we reference during recovery phases. The Risk Management Framework supplies risk ratings that drive our severity classifications. The Privacy Policy defines notification requirements we must meet. The Employee Handbook sets security responsibilities including incident reporting. These documents reference rather than duplicate incident response procedures, maintaining single sources of truth.

Cross-references ensure consistency across our documentation ecosystem. Common definitions get maintained in a glossary referenced by all documents. Contact information lives in one location referenced rather than copied. Classification schemes for data and incidents remain consistent across policies. Approval authorities align

across different procedures. Update cycles coordinate to review related documents together. This architectural approach prevents the divergence that naturally occurs when documents are maintained independently.

Our documentation hierarchy clarifies relationships while supporting navigation. The Information Security Policy serves as the parent document establishing overall security governance. Beneath it, the Incident Response Plan joins other operational policies like Access Control and Asset Management. The Business Continuity Plan exists as a peer, with the Disaster Recovery Plan as its child. This structure, documented and communicated, helps team members understand which document to reference for different needs while ensuring updates cascade appropriately.

Audit trail maintenance demonstrates due diligence to auditors while supporting continuous improvement. We maintain all document versions showing evolution over time, change justifications explaining why updates occurred, approval records demonstrating appropriate oversight, distribution logs proving communication, and training completion records ensuring effectiveness. These trails tell the story of our security program maturation while providing evidence for compliance requirements.

16. Document Control

NIST Controls: PM-4, SA-5

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

Review and Approval

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

Next Review Date: January 1, 2026

Distribution:

- Executive Team

- Incident Response Team
- Board of Directors (summary version)
- External Auditors (upon request)

17. Appendices

Appendix A: Incident Report Form

OversiteAI Incident Report

Incident ID: IR-[YYYY-MM-DD-###]

Report Date: _____

Reporter: _____

Incident Classification

- [ ] Severity 1 - Critical
- [ ] Severity 2 - High
- [ ] Severity 3 - Medium
- [ ] Severity 4 - Low

Incident Type

- [ ] Data Breach/Exposure
- [ ] Ransomware/Malware
- [ ] Account Compromise
- [ ] System Compromise
- [ ] Denial of Service
- [ ] Physical Security
- [ ] Other: _____

Initial Detection

- Detection Time: _____
- Detection Method: _____
- Detected By: _____
- Initial Indicators: _____

Impact Assessment

- Systems Affected: _____

- Data Potentially Exposed: _____
- Users Impacted: _____
- Business Operations Impact: _____

Response Actions

- Containment Actions: _____
- Eradication Steps: _____
- Recovery Actions: _____
- Evidence Collected: _____

Timeline of Events

[Detailed timeline with timestamps]

Root Cause Analysis

[5 Whys or similar analysis]

Lessons Learned

[Key takeaways and improvements]

Follow-up Actions

Appendix B: Evidence Chain of Custody Form

- Description: _____
- Type: [ ] Digital [ ] Physical [ ] Documentary
- Source System: _____
- Collection Date/Time: _____
- Collected By: _____
- Tool Used: _____
- Commands/Process: _____
- Original Location: _____
- Current Location: _____
- Hash Algorithm: SHA-256
- Hash Value: _____
- Verification Method: _____

Action	Owner	Due Date	Status

Date/Time	Action	Person	Purpose
	Collected		Initial collection
	Accessed		Analysis
	Transferred		Legal review

Notes: _____

Collector Signature: _____

Date: _____

Appendix C: Communication Templates

Customer Security Advisory Template

Subject: Security Advisory - [Brief Description] - [Date]

Dear [Customer Name],

We are writing to inform you of a security [incident/vulnerability] that [may affect/does not affect] your deployment of OversiteAI software.

What Happened:

[Clear, factual description without speculation or admitting liability]

When This Occurred:

[Timeline of discovery and relevant dates]

Impact Assessment:

[Specific impact to this customer, if any]

Actions We've Taken:

- [Specific remediation steps]
- [Additional security measures]
- [Monitoring or detection improvements]

What You Should Do:

- [Specific customer actions, if any]
- [How to check if affected]
- [Where to get updates/patches]

Additional Information:

[Links to patches, detailed technical information, etc.]

We take security seriously and apologize for any inconvenience. Our team is available to answer questions or provide assistance.

Contact Information:

- Email: security@oversiteai.io
- Phone: [Support number]
- Updates: [Status page URL]

Sincerely,

[Name]

CEO, OversiteAI

Breach Notification Letter Template

[Follow legal counsel guidance for specific jurisdiction]

Dear [Individual Name],

We are writing to notify you of a data security incident that may have involved your personal information.

What Happened:

On [date], we discovered [brief description]. Upon discovery, we immediately [containment actions].

Information Involved:

The following types of your information may have been accessed:

- [List specific data types]

What We Are Doing:

- Conducted thorough investigation

- Implemented additional security measures
- Notified law enforcement [if applicable]
- Engaged forensics experts

What You Can Do:

- Monitor your accounts for unusual activity
- Consider placing a fraud alert
- Review the enclosed reference guide
- [Other specific recommendations]

For More Information:

We have established a dedicated call center at [phone] available [hours]. You may also email [address].

We sincerely apologize and remain committed to protecting your information.

[Signature]

[Date]

Appendix D: Regulatory Requirements Matrix

Jurisdiction	Law	Timeline	Threshold	Our Exposure
EU	GDPR	72 hours	Risk to individuals	Employee data
California	CCPA/CPRA	Without unreasonable delay	CA residents	Employees/contacts
New York	SHIELD Act	Without unreasonable delay	NY residents	Employees/contacts
All US States	Various	30-90 days	Varies	Check each state

Key Definitions:

- **Personal Information**: Name + (SSN, DL#, financial account, health info)
- **Breach**: Unauthorized access where encryption keys not compromised
- **Risk of Harm**: Identity theft, financial loss, reputation damage

Notification Triggers:

1. Personal information accessed
2. Encryption not present or keys compromised
3. Risk of harm to individuals
4. Number exceeds statutory minimums

Appendix E: Technical Procedures

Azure AD Compromise Response

```
# Disable compromised account
Disable-AzureADUser -ObjectId [UserID]

# Revoke all sessions
Revoke-AzureADUserAllRefreshToken -ObjectId [UserID]

# Block sign-in
Set-AzureADUser -ObjectId [UserID] -AccountEnabled $false
```

1. **Immediate Containment**

```
# Get sign-in logs
Get-AzureADAuditSignInLogs -Filter "userPrincipalName eq '[email]'"

# Check recent changes
Get-AzureADAuditDirectoryLogs -Filter "initiatedBy/user/id eq '[UserID]'"
```

2. **Investigation**

```
# Force password reset
Set-AzureADUserPassword -ObjectId [UserID] -ForceChangePasswordNextLogin $true

# Remove app consents
Get-AzureADUserOAuth2PermissionGrant -ObjectId [UserID] | Remove-AzureADOAuth2PermissionGrant
```

3. **Remediation**

Ransomware Isolation

```
# Azure NSG emergency rule
az network nsg rule create \
  --resource-group [RG] \
  --nsg-name [NSG] \
  --name EmergencyBlock \
  --priority 100 \
  --direction Inbound \
  --access Deny \
  --protocol '*' \
  --source-address-prefix '*'
```

1. **Network Isolation**

```
# Check backup integrity
Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM

# Create recovery point
Backup-AzRecoveryServicesBackupItem -Item $backupItem
```

2. **Backup Validation**

Appendix F: Contact Lists

Contact Lists

[Current contact information maintained in secure password manager and incident response wiki]

Appendix G: NIST Control Mapping

This Incident Response Plan implements the following NIST SP 800-53 controls:

Incident Response Family (IR)

- IR-1: Incident Response Policy and Procedures - Sections 1, 12, 17
- IR-2: Incident Response Training - Sections 2, 8, 11
- IR-3: Incident Response Testing - Sections 2, 8, 12, 13
- IR-4: Incident Handling - Sections 1-7, 9, 10, 12, 13, 14
- IR-5: Incident Monitoring - Sections 3, 4, 10
- IR-6: Incident Reporting - Sections 3-5, 15
- IR-7: Incident Response Assistance - Sections 2, 11, 14
- IR-8: Incident Response Plan - Sections 1, 3, 5, 10

Audit and Accountability Family (AU)

- AU-2: Audit Events - Section 15
- AU-6: Audit Review, Analysis, and Reporting - Section 10
- AU-9: Protection of Audit Information - Sections 7, 15
- AU-10: Non-repudiation - Section 15
- AU-11: Audit Record Retention - Sections 7, 11
- AU-16: Cross-Organizational Auditing - Section 15

Contingency Planning Family (CP)

- CP-2: Contingency Plan - Section 9
- CP-4: Contingency Plan Testing - Section 9
- CP-10: Information System Recovery - Sections 4, 9

Access Control Family (AC)

- AC-2: Account Management - Section 6
- AC-7: Unsuccessful Logon Attempts - Section 6

System and Communications Protection Family (SC)

- SC-5: Denial of Service Protection - Section 6
- SC-36: Distributed Processing and Storage - Section 16

System and Information Integrity Family (SI)

- SI-2: Flaw Remediation - Section 14
- SI-3: Malicious Code Protection - Section 6
- SI-4: Information System Monitoring - Section 4
- SI-7: Software, Firmware, and Information Integrity - Section 15

Configuration Management Family (CM)

- CM-3: Configuration Change Control - Section 17
- CM-7: Least Functionality - Sections 16, 17
- CM-9: Configuration Management Plan - Section 17
- CM-10: Software Usage Restrictions - Section 15
- CM-14: Signed Components - Section 16

Personnel Security Family (PS)

- PS-4: Personnel Termination - Section 6
- PS-7: Third-Party Personnel Security - Section 16

Security Assessment Family (CA)

- CA-2: Security Assessments - Section 8
- CA-3: System Interconnections - Section 14
- CA-5: Plan of Action and Milestones - Section 12
- CA-7: Continuous Monitoring - Sections 10, 12, 14

System and Services Acquisition Family (SA)

- SA-2: Allocation of Resources - Sections 11, 16
- SA-5: Information System Documentation - Section 17
- SA-9: External Information System Services - Sections 2, 14, 15, 16
- SA-10: Developer Configuration Management - Section 17
- SA-12: Supply Chain Protection - Section 14

Risk Assessment Family (RA)

- RA-2: Security Categorization - Section 15

Planning Family (PL)

- PL-2: System Security Plan - Section 17

Program Management Family (PM)

- PM-1: Information Security Program Plan - Section 9
- PM-2: Senior Information Security Officer - Section 16
- PM-3: Information Security Resources - Sections 11, 16
- PM-4: Plan of Action and Milestones Process - Sections 12, 17
- PM-6: Information Security Measures of Performance - Section 10
- PM-8: Critical Infrastructure Plan - Section 9
- PM-11: Mission/Business Process Definition - Section 16
- PM-12: Insider Threat Program - Section 14
- PM-13: Information Security Workforce - Section 15
- PM-14: Testing, Training, and Monitoring - Section 10
- PM-16: Threat Awareness Program - Section 15

Physical and Environmental Protection Family (PE)

- PE-17: Alternate Work Site - Section 14

This comprehensive control mapping demonstrates our commitment to federal standards while maintaining practical implementation appropriate for our size and cloud-native architecture.