NEXUSAI TECHNOLOGIES, INC.

Global Information Security Policy & Operating Procedures

Version: 2025.1.0

Classification: Internal / Confidential

Status: Approved

Company Information

- **Company Name:** NexusAI Technologies, Inc.
- **Headquarters:** 500 Innovation Way, San Francisco, CA 94105 (Remote-First Operations)
- **Website:** https://www.nexusai.io
- **Industry:** Artificial Intelligence & Enterprise SaaS
- **Primary Contact:** security@nexusai.io

Document Control

- **Owner:** Chief Information Security Officer (CISO)
- **Approval Authority:** Board of Directors / Compliance Committee
- **Effective Date:** January 1, 2025
- **Last Review Date:** December 20, 2024
- **Next Review Date:** June 20, 2025

Legal Disclaimer

Table of Contents

SECTION 1: Identification, Authentication, and Access Management (IAAM)

1.1 Purpose and Scope

This section defines the requirements for ensuring that only authorized individuals, processes, and devices can access NexusAI resources. This policy applies to all employees, contractors, and third-party vendors accessing the NexusAI Production Environment, Corporate Network, and Cloud Service Providers (CSPs).

1.2 Password Complexity Standards (The "Technical Guardrail")

All system-level and user-level accounts must adhere to the following minimum complexity requirements. Systems that cannot technically enforce these must be documented as an exception and protected by compensating controls (e.g., IP whitelisting).

- **Minimum Length:** 16 characters for administrative accounts; 14 characters for standard user accounts.
- **Character Variety:** Must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character (e.g., !, @, #, $, %).
- **History:** Users cannot reuse any of their last 12 passwords.
- **Maximum Age:** Passwords must be rotated every 90 calendar days. Service accounts with "non-expiring" passwords must use SSH keys or secret management tools (e.g., AWS Secrets Manager).

1.3 Multi-Factor Authentication (MFA)

MFA is **mandatory** and non-negotiable for all NexusAI access points.

- **Primary Method:** Time-based One-Time Password (TOTP) via approved applications (e.g., Okta Verify, Google Authenticator) or Hardware Keys (e.g., YubiKey).
- **SMS Prohibitions:** Delivery of MFA codes via SMS or Voice is strictly prohibited due to SIM-swapping risks.
- **Conditional Access:** MFA must be re-challenged if the user’s IP address changes or if a "Sign-in Risk" is detected by the Identity Provider (IdP).

1.4 Account Lockout and Brute-Force Protection

To prevent automated credential stuffing and brute-force attacks:

- **Lockout Threshold:** Accounts will be automatically locked after five (5) consecutive failed login attempts.
- **Lockout Duration:** The account will remain locked for a minimum of 30 minutes or until manually reset by a Security Administrator.

- **Idle Timeout:** Sessions for web-based internal applications must expire after 60 minutes of inactivity.

1.5 Biometric and Mobile Device Authentication

NexusAI permits the use of biometric authentication (TouchID, FaceID) on company-managed mobile devices provided that:

- The biometric data is stored locally on the device's Secure Enclave and never transmitted to NexusAI servers.
- The device is enrolled in the NexusAI Mobile Device Management (MDM) solution.
- A secondary PIN/Passcode of at least 6 digits is required as a fallback.

1.6 Privileged Access Management (PAM)

- **Shared Accounts:** Use of shared or "group" accounts (e.g., `admin@nexusai.com`) is strictly prohibited. Every action must be attributable to a unique individual.
- **Just-In-Time (JIT) Access:** Access to production databases and "Level 4" confidential data must be granted on a JIT basis, expiring automatically after 4 hours.
- **Termination:** Upon employee termination (voluntary or involuntary), all access must be revoked within **two (2) hours**.

SECTION 2: Data Classification and Access Control Policy

2.1 Data Classification Framework

NexusAI categorizes all data into four distinct levels. Every file, database record, and communication must be treated according to its highest classification level.

Level	Label	Description	Storage/Handling Requirement
L1	**Public**	Marketing materials, public blogs, documentation.	No special requirements.
L2	**Internal**	Employee handbooks, internal memos, project roadmaps.	Access restricted to NexusAI employees only.
L3	**Confidential**	Source code, sales contracts, financial forecasts.	Encryption required at rest; access logged.
L4	**Restricted**	Customer PII (Names, Emails), Auth tokens, Encryption keys.	Full audit trails; JIT access only; hardware encryption.

2.2 Access Control Logic (Principle of Least Privilege)

Access to NexusAI systems is granted based on the **Principle of Least Privilege (PoLP)**. No user shall have more access than is required to perform their current job function.

- **Role-Based Access Control (RBAC):** Access is assigned to *Roles* (e.g., "DevOps Engineer," "Sales Rep"), not individuals.
- **Segregation of Duties:** Employees who write code (Engineering) cannot approve their own code for production deployment (Release Management).
- **Quarterly Access Reviews:** On the first Monday of every quarter, Department Heads must review and "re-attest" the access levels of every team member. Any access not explicitly re-approved is automatically revoked by the system.

2.3 Encryption Standards

To protect data against unauthorized physical access or intercept:

- **Data at Rest:** All L3 and L4 data stored in AWS (S3, RDS, EBS) must be encrypted using **AES-256**. Keys must be managed via AWS Key Management Service (KMS).
- **Data in Transit:** All data moving over public networks must be encrypted using **TLS 1.2 or 1.3**. Self-signed certificates are strictly prohibited in production.

- **Database Backups:** Backups must be encrypted using a separate master key and stored in a geographically distinct region for disaster recovery purposes.

2.4 Data Handling and Disposal

- **Production Data in Non-Prod:** The use of real L4 (Customer) data in Staging or Development environments is **strictly prohibited**. Developers must use "Sanitized" or "Synthetic" datasets for testing.
- **Physical Media:** Use of unencrypted USB drives or external hard drives for L3/L4 data is prohibited.
- **Secure Disposal:** When L4 data is no longer required (e.g., contract termination), it must be cryptographically erased. Physical hardware (SSD/HDD) containing L4 data must be physically shredded by a certified third-party vendor.

2.5 Data Residency and Sovereignty

- **Primary Region:** All customer production data is hosted in the **AWS us-east-1** (N. Virginia) region.
- **Data Localization:** For customers in the European Union (EU), NexusAI utilizes AWS regions in Frankfurt (eu-central-1) to ensure compliance with GDPR data residency requirements.
- **Cross-Border Transfers:** Any transfer of data outside of the original hosting region must be approved by the Legal & Compliance officer and documented in the Data Processing Agreement (DPA).

SECTION 3: Engineering and Software Development Security

3.1 Secure Software Development Life Cycle (S-SDLC)

NexusAI integrates security at every phase of the development lifecycle. Security is not a "final check"; it is a continuous requirement.

- **Design Phase:** All new features must undergo a **Threat Modeling** session using the STRIDE methodology to identify potential architectural flaws before a single line of code is written.
- **Development Phase:** Developers are required to follow **OWASP Top 10** coding standards to prevent common vulnerabilities such as SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- **Testing Phase:** Security testing is automated within the CI/CD pipeline. No code can be merged if it contains "Critical" or "High" severity vulnerabilities.

3.2 Automated Security Scanning (SAST & DAST)

NexusAI employs a multi-layered automated scanning strategy to catch vulnerabilities early.

- **Static Application Security Testing (SAST):** Every Pull Request (PR) is automatically scanned using tools (e.g., SonarQube or Snyk) to identify insecure code patterns in the source.
- **Dynamic Application Security Testing (DAST):** Weekly automated scans are performed on the Staging environment to identify runtime vulnerabilities, such as insecure headers or misconfigured SSL/TLS settings.
- **Secret Scanning:** Automated tools (e.g., GitGuardian) scan all repositories for accidentally committed "secrets" (API keys, hardcoded passwords, or private SSH keys). Any detected secret is immediately revoked and rotated.

3.3 Dependency and Supply Chain Management

NexusAI recognizes that 80% of modern software is built on third-party libraries.

- **Software Bill of Materials (SBOM):** NexusAI maintains an automated SBOM for every production release to track all open-source dependencies.
- **SCA (Software Composition Analysis):** We use automated tools to monitor third-party libraries for known **CVEs (Common Vulnerabilities and Exposures)**.
- **Vulnerability Patching:** * **Critical:** Must be patched within 48 hours.
    - **High:** Must be patched within 14 days.
    - **Medium/Low:** Must be addressed in the next scheduled sprint.

3.4 Code Review and Environment Segregation

- **Mandatory Peer Review:** No developer has "Merge to Main" permissions. Every change must be reviewed and approved by at least one other engineer who did not write the code.
- **Separation of Environments:** Development, Staging, and Production environments are logically and physically separated within the AWS organization.
    - Developers have **Zero Access** to the Production environment.
    - Deployment to Production is handled strictly via automated CI/CD runners (e.g., GitHub Actions or GitLab CI) with restricted IAM roles.
- **Immature Code:** Alpha or Beta features must be gated behind "Feature Flags" to ensure they do not impact the core security posture of the platform.

3.5 Vulnerability Disclosure and Penetration Testing

- **Annual Penetration Test:** NexusAI hires a certified third-party security firm to perform a "Grey Box" penetration test on our infrastructure and application at least once per year.
- **Vulnerability Disclosure Program (VDP):** We maintain a `security@nexusai.com` alias and a `security.txt` file for ethical hackers to report discovered vulnerabilities.
- **Bug Bounty:** (Optional/Planned) A private bug bounty program is maintained on platforms like HackerOne to incentivize continuous security testing.

SECTION 4: Remote Work and Mobile Device Security

4.1 The "Perimeter-less" Security Model

NexusAI operates under a **Zero Trust Architecture (ZTA)**. We do not assume that a device is secure just because it is connected to a known network. Every access request is fully authenticated, authorized, and encrypted based on device posture and user identity.

4.2 Mobile Device Management (MDM)

All devices (laptops, tablets, and smartphones) used for NexusAI business must be enrolled in the corporate **Mobile Device Management (MDM)** solution (e.g., Kandji, Jamf, or InTune).

- **Compulsory Features:**
  - **Full Disk Encryption:** FileVault (macOS) or BitLocker (Windows) must be enabled.
  - **Remote Wipe:** The Security Team must have the ability to remotely wipe company data if a device is reported lost or stolen.
  - **OS Patching:** Critical security updates must be installed within 72 hours of release. MDM will automatically enforce restarts if updates are ignored.
  - **Screen Lock:** A maximum 5-minute idle timeout with a mandatory password/biometric challenge to wake.

4.3 Secure Connectivity (VPN and ZTNA)

- **Corporate VPN:** Access to non-public internal resources (staging environments, internal wikis) requires a mandatory connection via the **NexusAI Secure VPN** with AES-256 encryption.
- **Public Wi-Fi Restrictions:** Employees are strictly prohibited from accessing internal systems or customer data over unsecured public Wi-Fi (e.g., cafes, airports) without the corporate VPN active.
- **Split Tunneling:** Prohibited for any traffic destined for the NexusAI cloud production environment to ensure all traffic is inspected for threats.

4.4 Bring Your Own Device (BYOD) Policy

NexusAI maintains a "Company-Issued First" policy.

- **Laptops:** Only company-issued, MDM-managed laptops are permitted to access source code or production environments.
- **Personal Mobile Phones:** Permitted for communication (Slack, Email) only if a **Work Profile** is created via the MDM. This creates a logical "container" that separates personal apps/data from NexusAI corporate data.
- **Prohibitions:** "Jailbroken" or "Rooted" devices are strictly blocked from the NexusAI network via automated posture checks.

4.5 Physical Security for Remote Work

- **Screen Privacy:** Employees working in public or semi-public spaces (co-working spaces) are required to use privacy screens on their laptops.
- **Clean Desk Policy:** Sensitive documents (if any are printed) must be shredded. Laptops must be physically secured or stored in a locked room when not in use.
- **Travel to High-Risk Countries:** Employees must notify the Security Team before traveling to countries identified as "High Risk" for corporate espionage. A "Burner Laptop" may be issued for the duration of the trip.

4.6 Endpoint Detection and Response (EDR)

Every NexusAI-managed endpoint must run an active **EDR agent** (e.g., CrowdStrike or SentinelOne).

- **Real-time Monitoring:** The EDR must monitor for malicious processes, unauthorized registry changes, and lateral movement.
- **Isolation:** In the event of a detected infection, the Security Team has the authority to "Isolate" the device from the network instantly via the EDR console.

SECTION 5: Sales, Marketing, and Customer Acquisition Data Policy

5.1 Purpose and Scope

This policy governs the collection, storage, and processing of Lead and Prospect data. It ensures that NexusAI's growth activities remain compliant with global data protection regulations, including **GDPR (EU)**, **CCPA/CPRA (California)**, and **CAN-SPAM Act (USA)**.

5.2 Lead Generation and Lawful Basis for Processing

NexusAI only collects and processes marketing data where a valid lawful basis exists:

- **Consent:** Data collected via "Opt-in" forms on the NexusAI website or webinars.
- **Legitimate Interest:** B2B outreach to professionals whose job functions align with NexusAI's service offerings, provided a balancing test has been performed.
- **Contractual Necessity:** Data required to facilitate a trial or proof-of-concept (POC).

5.3 Data Storage and CRM Governance

- **The "Single Source of Truth":** All sales and marketing data must reside exclusively within the **Authorized CRM (e.g., Salesforce or HubSpot)**. Storage of lead lists in personal Excel files, Google Sheets, or local computer folders is **strictly prohibited**.
- **Access Control:** Access to the CRM is restricted via Role-Based Access Control (RBAC). A Sales Development Rep (SDR) can view their assigned leads, but only the Sales Operations Manager can export data.
- **Export Restrictions:** Bulk exporting of lead data requires a documented business justification and approval from the Data Protection Officer (DPO).

5.4 Consent Management and Communication

- **Double Opt-In:** NexusAI utilizes a double opt-in process for all newsletter and marketing subscriptions to ensure the validity of the email owner.
- **The "Unsubscribe" Mandate:** Every marketing email sent via NexusAI systems must contain a clear, functional "Unsubscribe" link.
- **Preference Centers:** Users must be able to manage the *frequency* and *type* of communication they receive (e.g., "Product Updates" vs. "Marketing Promotions").
- **Suppression Lists:** NexusAI maintains a "Global Do Not Contact" (DNC) list. If a lead unsubscribes, their email is moved to the suppression list within **24 hours** to prevent accidental future outreach.

5.5 Data Enrichment and Third-Party Providers

NexusAI may use third-party tools (e.g., ZoomInfo, Apollo, or LinkedIn Sales Navigator) to enrich lead data.

- **Vetting:** All third-party data providers must undergo a vendor security assessment to ensure they collect data ethically and legally.
- **Prohibition of Scraped Data:** The use of illegally scraped data or "gray market" email lists is strictly prohibited.

5.6 Data Retention and the "Right to be Forgotten"

- **Stale Data Purge:** Marketing leads that have shown no activity (no email opens, no clicks, no logins) for **18 consecutive months** are automatically flagged for deletion.
- **Erasure Requests:** Under GDPR/CCPA, if a prospect requests to be "Forgotten," the Marketing Operations team must remove their record from the CRM, email automation tools, and any backup logs within **30 days**.
- **Audit Trail:** A record of the erasure request is kept in a "Hashed" format to ensure the individual is not accidentally re-imported later.

5.7 Marketing Security and Digital Assets

- **Website Tracking:** Use of cookies and tracking pixels (e.g., Meta Pixel, Google Analytics) must be disclosed in the NexusAI Privacy Policy. A "Cookie Consent Banner" must be active for all EU-based visitors.
- **Social Media Management:** Only authorized Marketing personnel are permitted to post on behalf of NexusAI. Multi-factor Authentication (MFA) must be enabled on all corporate social media accounts.

SECTION 6: Legal, Corporate Affairs, and Compliance

6.1 Purpose and Scope

This section outlines the legal framework and governance structures that protect NexusAI and its customers. It defines the company's approach to regulatory compliance, incident notification, insurance, and the management of legal risks associated with a global SaaS platform.

6.2 Regulatory Compliance Framework

NexusAI adheres to international security and privacy standards. Our compliance posture is validated annually through independent third-party audits.

- **SOC 2 Type II:** NexusAI maintains a SOC 2 Type II report covering the Trust Services Criteria of Security, Availability, and Confidentiality.
- **GDPR (General Data Protection Regulation):** NexusAI acts as a "Data Processor" for our customers and maintains a Standard Data Processing Agreement (DPA) including Standard Contractual Clauses (SCCs).
- **CCPA/CPRA:** Compliance is maintained for all California-based consumers, including the management of "Do Not Sell My Info" requests.
- **ISO 27001 (Planned):** NexusAI is currently aligning its internal controls with the ISO/IEC 27001:2022 framework for an anticipated certification in Q4.

6.3 Security Incident and Breach Notification

This is the most critical clause for legal liability. NexusAI maintains a strict **Incident Response Plan (IRP)**.

- **Definition of Breach:** Any unauthorized access to, or acquisition of, unencrypted customer data.
- **Notification Timeline:** In the event of a confirmed Data Breach, NexusAI will notify affected customers without undue delay and, where feasible, **no later than 48 hours** after discovery.
- **Notification Channel:** Primary notification will be sent via email to the "Security Contact" listed in the customer's contract, followed by an in-app notification.
- **Post-Mortem:** Within 15 business days of resolving an incident, NexusAI will provide a formal "Root Cause Analysis" (RCA) report to the affected parties.

6.4 Insurance and Liability

NexusAI maintains comprehensive Cyber Liability and Professional Insurance to mitigate financial risks.

- **Cyber Liability Insurance:** Coverage of at least **$5,000,000 USD** per occurrence, covering data restoration, legal fees, and notification costs.

- **Errors and Omissions (E&O):** Professional liability coverage of at least **$2,000,000 USD**.
- **General Liability:** Coverage of **$1,000,000 USD** per occurrence.
- **Evidence of Insurance:** A Certificate of Insurance (COI) is available to customers upon request under a Non-Disclosure Agreement (NDA).

6.5 Vendor Risk Management (Third-Party Risk)

NexusAI is responsible for the security of its sub-processors.

- **Due Diligence:** Every vendor with access to NexusAI data must undergo a **Security Risk Assessment** (SRA) and provide their own SOC 2 report or equivalent.
- **Contractual Flow-Down:** All security requirements in this policy (Encryption, MFA, Breach Notification) are "flowed down" into our contracts with third-party vendors.
- **Annual Review:** Critical vendors (like AWS or Snowflake) are reviewed annually for changes in their security posture.

6.6 Intellectual Property (IP) and Source Code Protection

- **Ownership:** NexusAI retains all rights, titles, and interests in its source code, algorithms, and proprietary datasets.
- **Escrow:** (Optional) NexusAI can enter into a Source Code Escrow agreement for Enterprise-tier customers to ensure business continuity.
- **Clean Room Development:** To prevent IP infringement, all development is conducted using original code or pre-approved Open Source libraries listed in the SBOM.

6.7 Records Retention and Litigation Hold

- **Retention Period:** Financial and contractual records are kept for **7 years**. System logs are kept for **365 days**.
- **Litigation Hold:** If NexusAI receives a subpoena or notice of pending litigation, the Legal Team will issue a "Litigation Hold." All automated deletion scripts for relevant data will be suspended immediately until the hold is lifted.

SECTION 7: Product & Engineering Handbook

7.1 Engineering Philosophy: The NexusAI Way

NexusAI follows a **"Security-by-Design"** and **"Privacy-by-Default"** philosophy. Engineering decisions are weighed against the "Nexus Triangle": Scalability, Security, and Maintainability.

- **YAGNI (You Ain't Gonna Need It):** We avoid over-engineering features that don't solve immediate customer needs, reducing the attack surface.
- **Continuous Improvement:** We dedicate 20% of every sprint to "Technical Hygiene," including refactoring, dependency updates, and security patching.

7.2 The Product Development Lifecycle (PDLC)

Our product roadmap is driven by customer feedback and security requirements.

1. **Discovery:** Product Managers (PMs) define the "Why" and "What."
2. **RFC (Request for Comments):** For significant changes, engineers write an RFC document detailing the technical approach. This must be approved by the Security Lead and Principal Architect.
3. **The Sprint:** We operate in 2-week Agile sprints. Every sprint begins with a "Security Grooming" session to identify potential risks in upcoming tickets.
4. **UAT (User Acceptance Testing):** New features are tested by the QA team in a dedicated environment that mimics production but uses zero real customer data.

7.3 Code Standards and Quality Assurance

- **Language Standards:** We primarily use type-safe languages (e.g., TypeScript, Rust, or Go) to minimize memory-safety vulnerabilities.
- **Linting and Formatting:** Every repository uses strict linting rules (e.g., ESLint, Prettier) enforced by CI/CD git-hooks.
- **Testing Pyramid:**
    - **Unit Tests:** Must cover >80% of business logic.
    - **Integration Tests:** Required for all API endpoints and database interactions.
    - **End-to-End (E2E) Tests:** Critical user paths (Login, Checkout, Data Export) are tested daily using automated browser testing (e.g., Playwright).

7.4 Branching Strategy and Deployment

NexusAI utilizes **Trunk-Based Development** with short-lived feature branches.

- **Pull Requests (PRs):** No PR can be merged without at least one "Approve" from a senior peer and a "Green" status from the automated security suite.
- **Continuous Deployment:** Merges to the `main` branch trigger an automated deployment to Staging. Deployment to Production requires a manual "Smoke Test" and a final sign-off from the On-call Engineer.

- **Rollback Protocol:** Every deployment must have an automated rollback path. If error rates exceed 1% post-deployment, the system automatically reverts to the last stable build.

7.5 Incident Response and On-Call (The "SRE" Layer)

- **On-Call Rotation:** A rotating "On-Call Engineer" is available 24/7/365 to respond to system outages or security alerts.
- **Severity Levels:**
  - **SEV-1 (Critical):** Service is down for all users. Response required within 15 minutes.
  - **SEV-2 (High):** Major feature is broken. Response required within 1 hour.
  - **SEV-3 (Medium/Low):** Minor bug or performance degradation. Addressed in the next business day.
- **Blameless Post-Mortems:** After every SEV-1 or SEV-2 incident, a formal post-mortem is conducted to identify "Process Failures" rather than "Human Errors." The resulting "Action Items" are prioritized at the top of the next sprint.

7.6 Infrastructure as Code (IaC)

NexusAI does not perform "Manual Configuration" in the AWS Console.

- **Terraform/CloudFormation:** All infrastructure (VPCs, S3 Buckets, RDS Instances) is defined in code.
- **Immutable Infrastructure:** We do not patch live servers. We deploy new, patched images (AMIs/Containers) and decommission the old ones. This ensures that the state of production is always known and version-controlled.

7.7 Technical Debt and End-of-Life (EOL)

- **Deprecation Policy:** When a feature or API version is deprecated, customers are given a 6-month notice.
- **Legacy Code:** Any code older than 24 months that hasn't been touched is reviewed for potential removal to keep the system lean and secure.

SECTION 8: Disaster Recovery (DR) & Business Continuity Plan (BCP)

8.1 Strategy and Objectives

NexusAI's resilience strategy is built on the assumption that individual components, zones, and entire regions **will fail**. Our goal is to maintain "Always-On" availability through automated failover and geographic redundancy.

- **Recovery Time Objective (RTO):** 4 Hours. (The maximum allowable time to restore service after a disaster).
- **Recovery Point Objective (RPO):** 1 Hour. (The maximum allowable amount of data loss measured in time).

8.2 Architectural Resilience

NexusAI infrastructure is hosted on AWS and utilizes a **Multi-Availability Zone (Multi-AZ)** and **Cross-Region** architecture.

- **Redundancy:** All critical microservices are deployed across at least three (3) physically separate Availability Zones (AZs) within a single region.
- **Load Balancing:** AWS Application Load Balancers (ALBs) perform continuous health checks. If an instance or an entire AZ fails, traffic is automatically rerouted to healthy nodes.
- **Database High Availability:** We utilize Amazon RDS Multi-AZ deployments with synchronous replication to a standby instance.

8.3 Data Backup and Restoration Policy

- **Automated Backups:** Full database snapshots are taken every 24 hours. Incremental transaction logs are backed up every 5 minutes (Point-in-Time Recovery).
- **Off-site Storage:** Backups are replicated to a secondary AWS Region (e.g., from `us-east-1` to `us-west-2`) to protect against a total regional failure.
- **Encryption:** All backup data is encrypted at rest using AES-256 with keys managed in AWS KMS.
- **Restoration Testing:** The SRE team performs a "Full Restore" drill into a sandbox environment every six (6) months to verify data integrity and ensure the RTO/RPO targets are achievable.

8.4 Business Continuity Plan (BCP)

The BCP ensures that NexusAI can continue operations even if our primary physical or digital infrastructure is compromised.

- **Crisis Management Team (CMT):** Led by the CTO and CEO, the CMT is responsible for declaring a "Disaster" and activating the recovery protocols.

- **Communication Plan:** In the event of a service-wide outage, NexusAI will update its public status page (`status.nexusai.com`) every 30 minutes until resolution. Primary customer contacts will be notified via email for any incident lasting longer than 1 hour.
- **Remote Workforce Continuity:** Since NexusAI is a "Remote-First" company, the loss of any single physical office location does not constitute a Business Continuity event. Employees are distributed across multiple time zones to ensure support coverage remains active.

8.5 Disaster Recovery Tiers (Failover Procedures)

1. **Tier 1: Component Failure:** (e.g., a single server dies). Handled automatically by Auto-Scaling Groups. No human intervention required.
2. **Tier 2: Zone Failure:** (e.g., a data center fire). Load balancers reroute traffic to other AZs. Minimal performance degradation.
3. **Tier 3: Regional Failure:** (e.g., total AWS North Virginia outage). The CMT activates the "Regional Failover" script. DNS is updated to point to the secondary region (`us-west-2`). Standby databases are promoted to Primary.

8.6 Disaster Recovery Drills (Simulation)

NexusAI conducts an annual **"Game Day"** exercise.

- **Simulation:** A production environment component (or an entire zone) is intentionally taken offline without prior notice to the engineering team.
- **Evaluation:** The response is timed and measured against the RTO/RPO.
- **CAP (Corrective Action Plan):** Any gaps identified during the drill (e.g., a script that failed to run) are assigned a "Critical" ticket and must be resolved before the next sprint.

SECTION 9: Employee Code of Conduct and Ethics

9.1 Core Ethical Principles

NexusAI operates on a foundation of integrity, transparency, and accountability. Every employee, regardless of rank or department, is expected to act as a guardian of company and customer data.

- **Integrity:** We do not misrepresent our product capabilities to customers.
- **Confidentiality:** Every employee signs a comprehensive **Non-Disclosure Agreement (NDA)** upon hire, which remains in effect even after termination of employment.
- **Conflict of Interest:** Employees must disclose any outside business activities that could conflict with their duties at NexusAI (e.g., consulting for a competitor).

9.2 Background Checks and Personnel Vetting

To mitigate the risk of "Insider Threats," NexusAI performs rigorous vetting of all personnel before granting access to internal systems.

- **Standard Background Check:** Includes criminal history, employment verification, and educational degree verification.
- **Role-Specific Vetting:** Employees with access to "Level 4 - Restricted" data (SREs, Finance, Legal) undergo deeper financial and background re-investigations every two (2) years.
- **Right to Work:** Continuous verification of legal authorization to work in the respective jurisdiction.

9.3 Acceptable Use Policy (AUP)

All employees must adhere to the AUP regarding company-issued hardware and software.

- **Prohibited Activities:** Using company resources for illegal activities, cryptocurrency mining, harassment, or storing personal adult content is strictly prohibited.
- **Software Installation:** Employees are prohibited from installing unauthorized third-party software ("Shadow IT") on company laptops. All software must be sourced from the pre-approved **Self-Service App Portal**.
- **Personal Use:** Incidental personal use of company laptops (e.g., checking personal email) is permitted, provided it does not interfere with productivity or compromise security.

9.4 Security Awareness Training

Security is a continuous learning process, not a one-time event.

- **Onboarding Training:** All new hires must complete a 2-hour Security & Privacy training module (covering Phishing, Social Engineering, and GDPR) within their first 5 days.
- **Annual Refresher:** Mandatory annual security training for all staff. Failure to complete training results in automated revocation of system access.
- **Phishing Simulations:** The Security Team conducts unannounced monthly phishing simulations. Employees who "click" the simulated malicious link are required to attend immediate remedial training.

9.5 Reporting Malpractice (Whistleblower Policy)

NexusAI encourages a "Speak Up" culture.

- **Anonymous Reporting:** We maintain a 24/7 anonymous "Ethics Hotline" and a digital reporting portal managed by a third party.
- **Non-Retaliation:** NexusAI strictly prohibits any form of retaliation against employees who report suspected security breaches, ethical violations, or illegal activities in good faith.
- **Duty to Report:** Employees have a mandatory obligation to report any lost/stolen devices or suspected unauthorized access to `security@nexusai.com` immediately.

9.6 Disciplinary Action

Violations of the Code of Conduct or Security Policies are taken seriously.

- **The "Three Strikes" Rule:** Minor policy infractions result in a written warning and mandatory retraining.
- **Zero Tolerance:** Severe violations (e.g., intentional data exfiltration, sharing passwords, or harassment) are grounds for **immediate termination for cause** and potential legal action.
- **Offboarding:** Upon termination, the "Involuntary Termination Protocol" is triggered, ensuring all digital and physical access is revoked within 60 minutes.

9.7 Insider Threat Monitoring

NexusAI utilizes User and Entity Behavior Analytics (UEBA) to identify anomalous activity.

- **Monitored Activities:** Unusual bulk downloads from the CRM, access attempts at odd hours, or unauthorized use of USB ports.
- **Privacy Balance:** Monitoring is limited to company-issued devices and corporate accounts. Personal privacy is respected in accordance with local labor laws.