ROAR Data Privacy and Information Security Manual

Introduction

Purpose

This Data Privacy and Information Security Manual provides an overview of the policies and practices implemented by the ROAR team to ensure the security and privacy of data. The goal of this manual is to safeguard sensitive information, maintain regulatory compliance, and protect the confidentiality, integrity, and availability of data used in the ROAR application.

ROAR's information security policies align with the NIST Cybersecurity Framework (CSF) 2.0. For a detailed mapping of ROAR's policies to the NIST CSF, see Appendix A.

Scope

This manual applies to all ROAR employees, contractors, and third-party vendors who interact with the ROAR platform. It covers the collection, processing, storage, transmission, and destruction of data through the ROAR platform, including but not limited to data from students, teachers, caregivers, research participants, and partner administrators.

Data Privacy

Data privacy refers to the policies and practices that govern how ROAR collects, uses, shares, and retains personal information. This section outlines the measures ROAR takes to protect user privacy and comply with relevant data protection regulations. ROAR is committed to protecting the privacy of students, educators, and other stakeholders and to transparency in its data practices. This section covers how data is collected, how it is used for operational and research purposes, the rights of users regarding their data, the conditions under which data may be shared, and the policies for retaining and securely disposing of data when it is no longer needed.

Data Collection and Use

The data that ROAR collects from users can be broadly separated into two categories:

- **Personal Data**: ROAR receives student information such as student names for the purpose of sharing score reports with teachers. ROAR also collects grade level and date of birth (DOB) to generate standardized scores. For research purposes, ROAR also stores demographic information,

such as a student's IEP status, free and reduced lunch status, and home language. When this information is used in research, it is always de-identified before publication.

While the ROAR application does not directly store student IP addresses, these may be logged in Firebase audit logs for security purposes. These logs could be accessed during a security incident or breach investigation to aid in tracing unauthorized access or suspicious activity.

- **Assessment Data**: During student interactions with the app, ROAR collects data such as item responses, response times, start and end timestamps, and user actions like keyboard presses, mouse clicks, swipes, and taps. Additionally, the app collects browser and device information (e.g., whether the device is a laptop or tablet) to ensure optimal app performance.

Assessment data is stored separately from personal data. personally identifiable information (PII). The personal data is stored in the "admin" database, while the assessment data is stored in the "assessment" database.

While this data is stored separately, it is recombined when ROAR transmits back to the student's teacher, school administrator, or district administrator student name, grade level, scores, and support levels for the purpose of score reporting.

Data Flow Diagrams

ROAR maintains detailed data flow diagrams (DFDs) that describe how data moves through the system. The DFDs can be accessed using this link.

User Rights

Parents and guardians have the right to opt out of participation in ROAR and request that any existing data for their student be removed. These requests are made through each student's school. ROAR affirms adherence to the New York City Board of Education Parents' Bill of Rights for Data Privacy and Security and equivalent policies required by educational and governmental partners.

Data Sharing

ROAR only shares data with authorized individuals or entities, such as teachers or schools, and only when necessary to transmit score reports back to educational partners. Partner confidential information will not be disclosed to third parties without explicit written authorization.

Data Retention and Destruction

ROAR retains and destroys data in compliance with applicable privacy regulations, internal policies, and its obligations to both research and educational partners. To ensure clarity, data is categorized into two types: research data and partnership data. Each type is subject to specific retention and destruction policies to meet the needs of ongoing research as well as obligations to educational partners.

Data Categories

- Research Data:
  - Purpose: research data is used exclusively for academic purposes, such as peer-reviewed publications and ongoing research by ROAR team members.
  - Composition: this data comprises de-identified assessment data (as defined above) and a subset of personal data for participants that have consented to participant in ROAR research.
  - Retention: this data is retained for the duration of the ROAR project, as defined below, to ensure reproducibility of research and to facilitate further studies.
  - Destruction: Within one year of project conclusion, as defined below, all research data will be reviewed. Data that is no longer needed for reproducibility or archival research will be securely deleted. If continued retention is required for archival or legal purposes, the necessity for this retention will be documented, and the data will be de-identified to the fullest extent possible.
- Partnership Data:
  - Purpose: partnership data is collected and maintained to fulfill ROAR's obligations to educational partners, such as providing score reports, progress updates, and other services required by partner schools and districts.
  - Composition: this data comprises all assessment and personal data needed to fulfill obligations to partners.
  - Retention: this data is retained only as long as necessary to meet contractual and reporting obligations to our educational partners. That is, it is retained for the duration of the partner agreement, as explicitly stated in the partner's requirements, or until receipt of written direction from the partner. This may include providing student score reports, assessment data, and other partner-requested services.
  - Destruction: Once partnership data is no longer required to meet the contractual or operational obligations to educational partners, it will be securely deleted within 30 days. This applies to both data stored in production systems and backup environments.

Defining the end of the ROAR Project The end of the ROAR project for the purposes of Research Data retention will be determined by the absence of significant academic research activity. Specifically, the project will be considered concluded if no peer-reviewed academic publications authored by ROAR team members, based on ROAR data, have been submitted within the preceding three years.

Data Destruction Methods ROAR will employ secure data destruction methods that ensure the complete and irretrievable deletion of personal and research data, in compliance with NIST 800-88 standards for data sanitization and applicable data protection regulations. These methods may include:

- Cryptographic erasure for encrypted data.
- Secure overwriting or wiping for data on physical storage devices.
- Deletion of cloud-stored data through provider-managed processes to ensure it is permanently removed from all systems.
- Shredding of paper records.

Following data destruction, the ROAR information security officer will conduct a final audit to confirm that all required data has been securely deleted and that no residual data remains in any systems, backups, or storage devices.

Information Security

Information security encompasses the policies, procedures, and technologies that protect ROAR's information systems and data from unauthorized access, disclosure, alteration, or destruction. This section details the security controls ROAR implements to safeguard its infrastructure, protect sensitive information, and ensure compliance with industry standards, best practices, and Stanford's Minimum Security Standards for Applications (hereafter referred to as "minsec").

The section includes details on

- **Roles and responsibilities**
- **Access Control**
- **Data Storage and Encryption**
- **Audit logging and monitoring**
- **Security Continuous Monitoring**
- **Incident Response**
- **Testing and Review of Incident Response and Recovery Plans**

- **Recovery Communications Plan**
- **Vulnerability Scanning**
- **Penetration Testing**
- **Security certifications**
- **Supply Chain and Vendor Risk Management**
- **Employee Training**
- **Physical Security Controls**
- **Software Development Lifecycle Security Controls**

These security measures are designed to protect both ROAR's internal systems and user data from threats and vulnerabilities. The ultimate goal is to ensure that ROAR's information assets remain secure and resilient against both internal and external risks.

Roles and Responsibilities

- **Employees**:
  - Follow security best practices.
  - Review this manual quarterly.
  - Complete required security training.
  - Enroll all personal and Stanford-owned devices used for work with Stanford Device Registration. Enroll each device for use with high risk data. Ensure that this registration includes
    * enrollment in either BigFix or Jamf,
    * whole disk encryption using the operating system's native encryption facilities, and
    * malware scanning using Crowdstrike Endpoint Antivirus or a similar Stanford approved and managed anti-malware solution.
  - Back up your data. Employees appointed through the Graduate School of Education (GSE) can obtain CrashPlan through the GSE. Employees appointed through the School of Medicine (SoM) can obtain CrashPlan through the SoM.
  - Enable multi-factor authentication on all GitHub accounts used for ROAR development.
  - For the following following third-party vendors, enable multi-factor authentication and always use a Stanford email for authentication:
    * Google, GCP, and Firebase
    * Sentry
    * Cypress Cloud
    * Google Drive
    * Clever
    * ClassLink

    * Redivis / Stanford Data Farm
  - Use only your `@stanford.edu` email address to conduct ROAR business.

- **Developers, QA Team, and ROAR's Director of Technology and Innovation**
  - All employee responsibilities described above
  - Complete annual information security training from the Stanford Information Security Academy
  - Adhere to and enforce the ROAR software development lifecycle.

- **Information Security Officer**:
  - All employee responsibilities described above
  - Ensure that all employees and contractors complete required information security training and store completion certificates for each employee.
  - Oversee the security program
  - Conduct risk assessments
  - Ensure compliance with this manual
  - Ensure that third-party vendors comply with ROAR's security requirements and maintain necessary industry certifications.

Access Control

Role-Based Access Control (RBAC) To protect sensitive data, access to ROAR systems is controlled based on user roles and responsibilities, consistent with the principle of least privilege. The ROAR team defines the following roles:

- **Super Administrators**: Full access to all data and systems. This is restricted to ROAR employees with a need for full access.
- **District Administrators**: Access to student data for a single district only.
- **School Administrators**: Access to student data for a single school only.
- **Educators**: Access to student data for assigned classes only.
- **Researchers**: Access to de-identified data for research purposes.
- **Caregivers**: Access to only their students' data for the purpose of viewing assessment scores.
- **Participants**: Access to only their own data for the purpose of completing assessments.

Access to data on Firestore is governed by Firestore security rules, which ensure that data is only accessible to authorized users. There are separate security rules for the admin database and the assessment database. All access rights are adjusted or removed immediately upon role changes or termination.

Authentication ROAR uses Firebase Authentication to manage user sign-ins and identity verification across its platform. Firebase Authentication is enhanced with the Google Identity Platform, providing an additional layer of security and flexibility. This integration allows ROAR to support multiple authentication methods, including email/password, OAuth providers (such as Google, Clever, and ClassLink), and anonymous authentication.

The only password requirement for participants, caregivers, educators, and school and district administrators is a minimum length of six characters. ROAR employees, either in their role as researchers or super administrators, are required to authenticate into the ROAR platform using Google SSO with their Stanford email addresses. This, in turn, uses Stanford's Duo Mobile for multi-factor authentication.

ROAR users can also authenticate using the Clever or ClassLink SSO providers. For these, ROAR uses the modern and secure OpenID Connect (OIDC) protocol, which is built on top of OAuth 2.0. OIDC is widely adopted for web and mobile applications and is considered a secure and streamlined protocol for identity management.

All privileged access to ROAR systems is granted only to ROAR employees under their `@stanford.edu` email accounts. They use only those accounts to conduct business. In accordance with minsec, all ROAR employees must use **Stanford Duo Mobile** for multi-factor authentication when accessing privileged accounts.

Onboarding and Offboarding User accounts are created for new employees based on their roles. Access is removed immediately upon termination of employment or change in role. The information security officer is responsible for maintaining both an onboarding checklist and an offboarding checklist to ensure access control. ROAR managers are responsible for completing these checklists when employees join or leave the team.

Data Storage and Encryption

ROAR enforces strict encryption policies to protect sensitive data. All data in transit, either between the ROAR application and users, or between different ROAR storage systems, is encrypted using **TLS/HTTPS** 1.2 or higher. When data is transmitted internally between ROAR employees, it is transmitted using secure mail or the Stanford managed, non-consumer Google Drive (described below), which is approved for high-risk data.

Data at rest is stored in multiple possible locations and encrypted using NIST-compliant algorithms (e.g., AES-256). Below, we describe each location along with it's associated encryption policy and key management policy:

- **Firebase Firestore** and other **Google Cloud Platform (GCP)** services

  - Encryption: This data is encrypted using the **AES-256** encryption standard.
  - Key management: The encryption keys themselves are encrypted and rotated regularly to ensure security. The management of encryption keys is handled by Google Cloud's internal processes, which follow strict security protocols.

- **Google Drive**

  - Description: Data shared between districts and ROAR researchers, especially via CSV file uploads, is often stored in secure, shared Google Drive folders. This data is manually imported by authorized staff into the ROAR platform when necessary, using encrypted communication channels.
  - Encryption: This data is encrypted using the **AES-256** encryption standard.
  - Key management: The encryption keys themselves are encrypted and rotated regularly to ensure security. The management of encryption keys is handled by Google Cloud's internal processes, which follow strict security protocols.

- Stanford-managed **encrypted devices**:

  - Description: ROAR employees may perform manual file handling with data that is downloaded to and processed on Stanford-managed encrypted devices. Whether this device is employee-owned or Stanford-owned, it's security is managed by Stanford through Stanford Device Registration. These devices are required to be registered with Stanford University and approved for use with high-risk data. ROAR partner data will not be processed or stored with personal accounts.
  - Encryption: Device registration includes enrollment in Jamf and BigFix and whole disk encryption using the operating system's native encryption facilities.
  - Key management: The use of Jamf and BigFix ensure that operating system patches and updates are deployed in a timely manner and that encryption is verified in an ongoing way that can be centrally audited. The encryption keys themselves are managed by each individual employee.

- Stanford Data Farm (Redivis) Description: The Stanford Data Farm is a data storage and analytics platform. It integrates with other ROAR data storage through manual or automated data export from the ROAR assessment Firestore database. It contains assessment results with de-identified data only (i.e., it excludes PII). Access is restricted to authorized ROAR researchers.

Audit Logging and Monitoring

User activities within the ROAR system are logged to ensure transparency and traceability. **Login events**, **data access**, and **data modifications** are logged in Firebase audit logs. IP addresses and

device information may be logged for security purposes. Firebase audit logs are retained for 400 days. These logs are monitored as described in the incident response plan section.

Security Continuous Monitoring

ROAR employs continuous monitoring to detect security events and anomalous activity:

- **Firebase Audit Logs**: All access and actions are logged and reviewed regularly.
- **Google Cloud Monitoring**: Automated tools monitor infrastructure for suspicious activity, unauthorized access, and system health.
- **Dependabot & CodeQL**: Automated dependency and code security scanning for vulnerabilities.
- **Qualys Web Application Scanning**: Regular scans for web application vulnerabilities.
- **Log Review**: Logs are reviewed at least monthly and after any security incident.

These monitoring activities ensure timely detection and response to threats.

Incident Response

In the event of a data breach or security incident, ROAR follows a detailed incident response process to contain the breach, mitigate damage, and notify affected parties. As ROAR relies on Google Cloud Platform (GCP) and Firebase for its infrastructure, the breach response procedures are aligned with Google's established protocols for handling security incidents. Additionally, ROAR follows Stanford's minimum security (minsec) requirements, which further specify steps for breach management. Here's an overview of the procedures and response timings:

1. Detection and Reporting of a Breach
    - Monitoring and Detection: Google Cloud and Firebase utilize automated systems for constant monitoring and logging of all access and activity across their platforms. Any abnormal behavior or access patterns are flagged for immediate review by Google's security teams. Further details on Google's intrusion detection measures are available in Appendix 2, section 1(b) of the Firebase data processing terms.
    - Incident Reporting: If ROAR detects or suspects a breach (internally or through Google's detection systems), it is required to notify relevant stakeholders, including school districts and partners, per their data use agreements.
    - Timing: Immediate detection and notification systems are in place. For suspected breaches, Stanford's internal policies require that suspected breaches are reported immediately to the University's Information Security Office.
2. Initial Notification, Response, and Containment

- Initial Assessment: Once a breach is suspected or confirmed, the vendor (Google Cloud, in this case) initiates an immediate investigation to assess the scope and impact of the incident. At the same time, ROAR's internal team would begin containment procedures, including suspending access and isolating affected systems.
- Suspected information security incidents are reported immediately to the Stanford University Privacy Office and Information Security Office. Following those reports, Stanford follows its information security incident response.
- Containment Measures: GCP's infrastructure provides automated tools to block further unauthorized access, including halting affected services, rotating encryption keys, or revoking compromised credentials.

3. Investigation and Root Cause Analysis

    - Forensic Analysis: Google's security team works on identifying the root cause of the breach using forensic tools to trace the source and scope of the compromise. They examine logs, system changes, and any unauthorized access points.
    - ROAR Team's Role: The ROAR team collaborates with Google to provide context for the incident and ensure Stanford's data is safeguarded. ROAR's internal team, governed by Stanford's security policies, plays a key role in determining what data, if any, has been compromised.

4. Notification of Affected Parties

    - Stakeholder Notification: In the event that personally identifiable information (PII) or sensitive information is compromised, ROAR, following Stanford's minsec requirements and any data usage agreements that ROAR has signed with affected parties, would notify affected school districts and individuals. The notification includes the type of data affected, the estimated scope, and steps taken to mitigate further risk.

5. Remediation and Recovery

    - Remediation Plan: Once the breach is contained, the vendor (e.g., Google Cloud) and ROAR initiate a remediation process, which may involve restoring systems from secure backups, reconfiguring security settings, or enhancing system defenses to prevent future occurrences.
    - Data Restoration: Any lost or corrupted data is restored from encrypted backups maintained on Google Cloud's infrastructure, and system integrity is verified before returning services to normal operation.
    - Remediative modifications to the ROAR platform are not deployed until after Stanford's Information Security Office has completed its investigation and authorizes such activity.

6. Post-Incident Review and Reporting

- Post-Mortem Analysis: After the issue is fully resolved, ROAR, in concert with Stanford's Information Security Incident Response Team and Google Cloud, perform a post-mortem analysis to identify lessons learned and implement additional security measures where needed. This analysis is shared with relevant parties if necessary.
- Reporting: ROAR provides a detailed report to stakeholders (e.g., school districts) on the nature of the breach, the steps taken to mitigate it, and the corrective actions to prevent future incidents.

Testing and Review of Incident Response and Recovery Plans

ROAR's incident response and disaster recovery plans are tested and reviewed at least annually. Testing may include tabletop exercises, simulated incidents, and recovery drills. After each test or real incident, a post-mortem review is conducted to identify lessons learned and update plans as needed. Updates and improvements are tracked to completion.

Recovery Communications Plan

In the event of a major incident or disaster recovery event, ROAR will:

- Designate a communications lead (typically the Information Security Officer or Director of Technology and Innovation).
- Provide timely updates to affected stakeholders (e.g., partner districts, school administrators, users) about the status of recovery efforts, expected timelines, and any actions required of them.
- Issue a final summary report after recovery is complete, detailing the incident, recovery actions, and steps taken to prevent recurrence.
- Maintain records of all communications for audit and compliance purposes.

Vulnerability Scanning

Continuous vulnerability scanning ensures that the ROAR platform remains secure, up-to-date, and free from critical vulnerabilities. ROAR employs a multi-layered approach to vulnerability scanning:

1. GitHub CodeQL Scanning
    - **Purpose**: CodeQL is used to perform automated code analysis and identify potential security vulnerabilities in ROAR's codebase.
    - **Integration**: CodeQL scanning is enabled for all pull requests and code changes submitted via GitHub. Each pull request triggers an automated scan that checks for common vulnerabilities such as SQL injection, XSS, and insecure code patterns.

- **Process**:
  - Every time a new pull request is created or a code change is pushed, CodeQL scans the repository and flags any potential security issues in the code.
  - Developers are notified of vulnerabilities directly in the pull request so they can address them before merging the changes into the main branch.
  - Any high or critical vulnerabilities must be resolved before the code can proceed through the SDLC process.

2. GitHub Dependabot Scanning

   - **Purpose**: Dependabot automatically detects and manages outdated or vulnerable dependencies in ROAR's software.
   - **Integration**: Dependabot continuously monitors ROAR's project dependencies (e.g., third-party libraries) for known vulnerabilities. When a vulnerability is discovered, Dependabot automatically raises a pull request to update the affected dependency to a secure version.
   - **Process**:
     - Dependabot performs regular scans of the dependencies listed in package.json, requirements.txt, and other dependency management files.
     - If a vulnerability is found in one of the dependencies, Dependabot opens a pull request with a recommended update.
     - This pull request follows the same SDLC steps and applies the same security controls as any other ROAR pull request.

3. Qualys Web Application Scanning

   - **Purpose**: Qualys Web Application Scanning (WAS) is used for continuous web application discovery and detection of vulnerabilities in ROAR's live web applications.
   - **Integration**: Qualys WAS is scheduled to run periodically to scan ROAR's production environment for potential web application security issues, including common web vulnerabilities like cross-site scripting (XSS), SQL injection, and other OWASP Top 10 vulnerabilities.
   - **Process**:
     - Regular scans are performed to detect vulnerabilities in the web application layer.
     - The Qualys Web Application Scanning tool automatically scans ROAR's web applications for any newly introduced vulnerabilities.
     - Security issues identified by Qualys are documented and prioritized for remediation based on severity. High and critical vulnerabilities are escalated and addressed immediately.

4. Malware protection and update management

- ROAR's Google cloud backend and its associated encryption keys are managed by Google cloud. Firestore is updated regularly (see the Firestore release notes) to apply patches and manage updates.
- For employee hardware, updates are managed using Stanford's BigFix software. BigFix is a centralized operating system patch management service. This service enables both local and central technical support staff to deploy critical security patches to Stanford registered devices as soon as they're made available by Microsoft or Apple and tested at Stanford. Through BigFix, ROAR employee hardware is also scanned for malware using Crowdstrike Endpoint Antivirus or a similar Stanford recommended anti-malware solution.

For all types of vulnerability scanning (CodeQL, Dependabot, and Qualys WAS), ROAR developers and security personnel are notified when a vulnerability is detected. These vulnerabilities are converted to tickets in the ROAR SDLC and classified based on severity (low, medium, high, critical) to prioritize their resolution. High and critical vulnerabilities are addressed as a top priority and must be resolved before code is deployed to production. Low and medium vulnerabilities are tracked and addressed during the regular development cycle.

Penetration Testing

ROAR will engage with third-party independent security firms to conduct penetration testing at least annually. These penetration tests will provide an external evaluation of the platform's security posture, identifying vulnerabilities that may not be detectable through automated scanning or internal reviews.

Penetration testing will assess:

- Web Application Security: Testing for common web vulnerabilities such as cross-site scripting (XSS), SQL injection, and other threats listed in the OWASP Top 10.
- Infrastructure Security: Evaluating the security of ROAR's underlying cloud and deployment infrastructure.
- Authentication and Access Control: Verifying that the platform's authentication and access control mechanisms are secure and properly implemented.
- API Security: Assessing the security of APIs exposed by the ROAR platform to ensure that they are properly secured against unauthorized access and data leaks.
- Data Handling and Encryption: Ensuring that sensitive data, including PII, is handled and encrypted in accordance with security best practices.

The third-party penetration testers will provide a detailed report on the findings, including any vulnerabilities identified and their associated risk levels (e.g., low, medium, high, critical). ROAR will prioritize

remediation of identified vulnerabilities based on severity, with high and critical issues addressed immediately. A post-test review will be conducted to verify that all issues have been adequately resolved before any affected systems are brought back online.

Security Certifications

ROAR operates on Google Cloud Platform (GCP) and Firebase, which are certified under various security standards including FedRAMP Moderate, SOC 2 Type II, and ISO/IEC 27001. These platforms provide the secure infrastructure that underpins ROAR's operations, ensuring that data is stored and processed in a compliant, secure environment. We provide details below on GCP and Firebase compliance with those standards.

- FedRAMP Certification:
  - FedRAMP Level: Google Cloud Platform and Firebase are FedRAMP Moderate certified.
  - Environment: ROAR is hosted in Google Cloud Platform's nam5 multi-region, which complies with FedRAMP requirements for government data protection.
  - Security Controls: The certification includes compliance with over 325 security controls based on NIST SP 800-53, which covers areas such as access control, incident response, data encryption, and continuous monitoring.
  - Why This Matters: FedRAMP Moderate certification ensures that GCP meets strict U.S. federal security requirements, including those related to confidentiality, integrity, and availability of cloud services.
- SOC 1/2/3 Reports:
  - SOC 2 Type II Certification: Google Cloud services, including Firebase, undergo independent audits and are certified under SOC 2 Type II standards.
  - Security Controls: This certification ensures that Google Cloud implements and enforces strict controls related to security, availability, processing integrity, confidentiality, and privacy. These include regular security audits, encryption, access control, and threat detection.
  - Why This Matters: SOC 2 Type II certification ensures that Google Cloud consistently maintains high standards for data security and privacy, making it suitable for applications like ROAR, which handle sensitive student data.
- ISO/IEC 27001:
  - Certification: Google Cloud has been certified under ISO/IEC 27001, a globally recognized standard for managing information security.

  - Security Controls: This certification covers risk management, access control, data encryption, incident management, and compliance with data protection laws.
  - Why This Matters: ISO/IEC 27001 certification demonstrates that the infrastructure used by ROAR follows international standards for managing data securely and effectively.

However, it is important to note that ROAR itself does not hold these security certifications independently. Instead, ROAR aligns its security practices with Stanford minsec. These minsec requirements ensure that ROAR adheres to best practices in data security, including encryption, access control, and regular audits, while relying on GCP and Firebase to meet industry standards for infrastructure security.

Supply Chain and Vendor Risk Management

ROAR evaluates and manages risks from third-party vendors and service providers as follows:

- Maintain a list of all vendors with access to ROAR data or systems.
- Require vendors to provide evidence of relevant security certifications (e.g., SOC 2 Type II, ISO 27001, FedRAMP).
- Conduct vendor risk assessments at onboarding and at least annually thereafter.
- Review vendor security practices, incident history, and compliance with contractual requirements.
- Require vendors to notify ROAR of any security incidents that may impact ROAR data or services.
- Terminate vendor access promptly upon contract expiration or termination.

The **Information Security Officer is responsible** for ensuring that all ROAR third-party vendors, such as Google Cloud Platform, Clever, and ClassLink, maintain **SOC 2 Type II** or **ISO 27001** certifications. For each vendor, the Information Security Officer shall generate a third-party vendor assessment report that assesses the security practices of the vendor and verifies compliance with the above privacy and security standards. The Information Security Officer shall review these vendor assessments quarterly.

Employee Training

ROAR requires all employees and contractors to complete regular training on data privacy and information security best practices. All ROAR employees that access participant data must complete the following required training:

- **CITI Biomedical Responsible Conduct of Research**: Ethical research practices and data handling
- **HIPAA Training**: Protecting Personal Health Information and PII

- **FERPA Training**: Understanding the Family Educational Rights and Privacy Act requirements for handling student education records

Additionally, all ROAR developers complete annual information security training from the Stanford Information Security Academy, covering the importance of PII protection, the specifics of our data privacy policies, and their roles in maintaining these standards.

Due to ROAR's work with educational institutions, special emphasis is placed on FERPA compliance training, which covers:

- Proper handling of student education records
- Parental rights to inspect and review education records
- Requirements for consent before disclosing personally identifiable information
- Exceptions to consent requirements
- Proper response to data breaches involving education records

The Information Security Officer shall ensure that all employees and contractors complete these training requirements and store completion certificates for each employee. Training must be renewed annually, and special training sessions are conducted whenever significant updates to FERPA regulations occur.

Physical Security Controls

ROAR does not operate its own physical servers or data centers. Instead, all infrastructure is hosted on Google Cloud Platform (GCP) and Firebase, which are part of Google's secure, globally distributed infrastructure. As such, ROAR inherits robust physical security controls from Google, and enforces device-level and endpoint security through Stanford University's IT governance policies.

1. Cloud Infrastructure Security (Google Cloud Platform)

All ROAR data is stored and processed in GCP's nam5 multi-region, which consists exclusively of U.S.-based data centers. GCP's physical infrastructure security is regularly audited and certified under SOC 2 Type II, ISO 27001, and FedRAMP Moderate. GCP data centers employ industry-leading physical protections, including:

- 24/7 on-site security staff
- Biometric scanners, key card access, and multi-layered authentication systems
- Man-trap entry points to control physical access
- Video surveillance and centralized access logging
- Redundant power, cooling, and fire suppression systems

More information is available through the Google Cloud Security and Compliance documentation.

1. ROAR Workstation Security

ROAR team members access systems from remote locations using institutionally managed or compliant personal devices. These devices are governed by Stanford University's Minimum Security Standards (MinSec), which ensure:

- Full disk encryption on all endpoints
- Multi-factor authentication (2FA) for all administrative systems
- Timeout and auto-lock policies to prevent unauthorized physical access
- Device management and remote wipe capabilities for Stanford-issued devices
- Security awareness training for all ROAR staff with access to institutional data

These controls ensure that even in a distributed work environment, ROAR maintains a high level of physical security for all systems accessing sensitive institutional data.

Software Development Lifecycle Security Controls

ROAR enforces secure Software Development Lifecycle (SDLC) policies that govern how software changes are managed, implemented, and deployed. The SDLC process ensures that changes to the system are tracked, reviewed, tested, and implemented in a manner that prioritizes security, confidentiality, and compliance with industry best practices. All ROAR software developers, including ROAR assessment developers, are responsible for complying with the ROAR SDLC.

Operational Security and Resilience

Operational security and resilience refers to the measures and processes in place to ensure that ROAR can maintain business continuity, recover from unexpected disruptions, and protect the integrity and availability of its data. This section focuses on how ROAR safeguards critical data and infrastructure, ensures swift recovery in the event of failures or disasters, and maintains operational continuity under various circumstances.

Backup and Restoration

ROAR uses comprehensive backup and restoration processes to ensure the continuity of critical data and services in the event of a system failure, data corruption, or other disruption. All backups are encrypted to maintain data confidentiality and protect sensitive information. ROAR's **Recovery time objective (RTO)** is to restore services within 72 hours of an outage.

Firestore Database Backup All Firestore backups are encrypted at rest using industry-standard encryption protocols to ensure that sensitive data remains protected during the retention period. ROAR backs up its production databases into Google Cloud's geographically redundant storage according to two schedules:

- Daily Backups: ROAR's production databases are automatically backed up on a daily basis. These daily backups are encrypted to ensure that sensitive information remains secure. Daily backups are retained for one week before they are overwritten.
- Weekly Backups: In addition to daily backups, ROAR performs weekly backups of the database. These weekly backups are retained for 14 weeks, providing an extended archive in case of longer-term recovery needs.

If the Firestore database becomes unavailable or data is corrupted, the most recent uncorrupted backup is restored following Firebase's restoration protocols. Restoration can be performed from either the daily or weekly backups, depending on the specific recovery needs and the time elapsed since the incident.

Codebase Backup and Restoration The ROAR codebase, including all application components and infrastructure-as-code scripts, is stored and maintained in GitHub repositories. GitHub acts as the primary system for version control and code storage, providing built-in redundancy and security features.

- GitHub Version Control: All code changes are tracked using GitHub's version control system, ensuring that code can be restored to any previous state. Each commit serves as a snapshot, and branches are protected to ensure only authorized changes are merged into production.
- Disaster Recovery: In the event of code corruption or accidental deletion, ROAR's GitHub repositories allow for quick restoration by reverting to a previous commit or tag. The decentralized nature of GitHub ensures that the codebase is backed up across multiple locations and systems. This restoration process follows the same security controls described in ROAR's SDLC.

Employee device backup and restoration ROAR employees are required to backup their stanford-managed devices. Stanford provides a centrally managed, automatic data backup solution through CrashPlan.

Business Continuity and Disaster Recovery

ROAR maintains a disaster recovery plan to ensure the availability of services in case of system outages or disasters. Further details are in the ROAR Business Continuity and Disaster Recovery Plan.

Appendix A: NIST Cybersecurity Framework 2.0 Compliance Matrix

The following matrix maps the policies and controls described in this manual to the NIST Cybersecurity Framework (CSF) 2.0, showing which sections address each category.

Function	Category	Reference in Manual
GOVERN	Organizational Context (GV.OC)	Introduction
		Scope
		Data Privacy
	Risk Management (GV.RM)	Vendor Risk Management
		Incident Response
	Roles & Responsibilities (GV.RR)	Roles & Responsibilities section
	Policy (GV.PO)	Information Security policies
		Quarterly review requirements
	Oversight (GV.OV)	InfoSec Officer responsibilities
		Review processes
	Supply Chain Risk (GV.SC)	Vendor Risk Management section
IDENTIFY	Asset Management (ID.AM)	Device Registration
		Asset Inventory
	Risk Assessment (ID.RA)	InfoSec Officer risk assessments
		Vendor Risk Assessment
	Improvement (ID.IM)	Software Development Lifecycle
		Post-Incident Review processes
PROTECT	Authentication & Access (PR.AA)	Role-Based Access Control
		Authentication section
	Training (PR.AT)	Employee Training section
		CITI Training
		HIPAA Training
	Data Security (PR.DS)	Data Storage and Encryption
		Data Retention and Destruction

Function	Category	Reference in Manual
	Platform Security (PR.PS)	GCP security
		Firebase security
		SDLC controls
	Infrastructure (PR.IR)	GCP infrastructure
		Redundancy and backup systems
DETECT	Monitoring (DE.CM)	Firebase Audit Logs
		Google Cloud Monitoring
	Event Analysis (DE.AE)	Audit Logging and Monitoring
		Incident Response procedures
RESPOND	Incident Management (RS.MA)	Incident Response section
		Detection and Reporting
	Incident Analysis (RS.AN)	Root Cause Analysis section
	Communication (RS.CO)	Initial Notification and Response
		Recovery Communications Plan
	Mitigation (RS.MI)	Containment Measures
		Remediation steps
RECOVER	Recovery Execution (RC.RP)	Remediation and Recovery
		Backup and Recovery sections
	Communication (RC.CO)	Recovery Communications Plan