rinnalla
Vendor Privacy & Security Overview

Version 1.0 · Last Updated: June 8, 2026

About rinnalla

rinnalla is a parent-focused literacy platform designed to support families, educators, healthcare organizations, and community partners in promoting early literacy development through evidence-based coaching and learning experiences.

rinnalla's mission is to strengthen the relationship between adults and children through literacy-rich interactions while maintaining strong privacy protections and responsible data stewardship.

rinnalla is intentionally designed around a minimal-data architecture. We collect only the information necessary to provide our services, manage subscriptions, and support participating organizations.

Data Privacy Philosophy

rinnalla follows four guiding principles:

Data Minimization

We collect only the information necessary to operate the service.

Privacy by Design

Privacy considerations are incorporated into product design decisions and platform architecture.

Transparency

We clearly disclose what information is collected, how it is used, and how it is protected.

Educational Purpose

Information is used solely to provide and support educational and literacy-related services.

> **rinnalla** does not sell personal information and does not use personal information for targeted advertising.

Information We Collect

Parent Account Information

- Parent name
- Parent email address
- Account identifier

Purpose: Account creation, authentication, customer support, and subscription management.

Child Profile Information

- Child name
- Child age

- Child grade level
- Organization affiliation (when applicable)

Examples of organization affiliation include:

- School districts
- Healthcare organizations
- Literacy organizations
- Community partners

Purpose: Personalization of learning experiences and account administration.

Account Administration Information

- Subscription status
- License status
- Transaction identifiers
- Last login timestamp

Purpose: Subscription validation, licensing administration, customer support, and service operation.

Technical Information

- Device metadata
- Application metadata
- Crash reports
- Error diagnostics
- Authentication metadata

Purpose: System reliability, troubleshooting, security, and service improvement.

Information We Do Not Collect

rinnalla does not currently collect:

- State student identification numbers
- District student identification numbers
- Social Security numbers
- Home addresses
- Phone numbers
- Race or ethnicity information
- Disability information
- IEP or 504 information
- Medical information
- Attendance records
- Discipline records
- Free or reduced lunch status
- Standardized assessment scores
- Payment card information

Educational Performance Data

At this time, detailed literacy activity data, reading performance information, and educational progress information remain local to the user's device and are not stored within **rinnalla** cloud systems.

This architecture significantly reduces privacy risk and minimizes exposure of educational performance information.

Future platform features may introduce additional educational reporting capabilities. Any material changes to data collection practices will be reflected in updated privacy documentation.

Data Storage and Hosting

Primary Infrastructure Provider: Google Firebase

Storage Region: United States

Current production cloud data is stored within the United States.

Third-Party Service Providers

rinnalla utilizes a limited number of carefully selected service providers.

Firebase

Purpose: Authentication, hosting, and cloud data storage.

RevenueCat

Purpose: Subscription management and purchase restoration.

RevenueCat does not directly process payments.

Sentry

Purpose: Crash reporting and application diagnostics.

SiteDetour

Purpose: Dynamic QR code generation, routing, and experience delivery.

Security Controls

rinnalla maintains reasonable administrative, technical, and operational safeguards designed to protect information from unauthorized access, disclosure, alteration, or destruction.

Current safeguards include:

- HTTPS encrypted communications
- Firebase authentication services
- Password hashing and secure credential management
- Role-based access controls
- Restricted administrative access
- U.S.-based cloud hosting
- Vendor security review processes
- Incident response procedures

rinnalla maintains documented Security, Data Retention, and Data Breach Response policies.

Data Deletion and Retention

rinnalla supports verified account deletion requests.

Account records may be deactivated and removed from active use while deletion is processed in accordance with the **rinnalla** Data Retention Policy.

Information is retained only as long as necessary to support legitimate business, contractual, operational, or legal requirements.

Compliance Documentation

rinnalla maintains the following governance documents:

- Data Map
- NDPA Exhibit B
- Subprocessor Registry
- Application Privacy Policy
- Information Security Policy
- Data Breach Response Plan
- Data Retention Policy

These documents are available upon request and may be provided during procurement, contracting, or privacy review processes.

Contact Information

Privacy and Compliance Inquiries:
privacy@rinnallaliteracy.com

General Support:
support@rinnallaliteracy.com

Website:
www.rinnallaliteracy.com

7984 South 1300 East, Sandy, UT 84094
801-834-1798

rinnalla
Data Map

Version 1.1 · Effective Date: June 8, 2026

Purpose

This document serves as the official inventory of data collected, stored, processed, and transmitted by **rinnalla**. It provides the foundation for privacy policies, NDPA agreements, district compliance documentation, and internal development practices.

System Philosophy

rinnalla is intentionally designed around a minimal-data architecture.

The platform collects only the information necessary to:

- Create and maintain user accounts
- Associate a parent with a child
- Deliver personalized literacy coaching
- Manage subscriptions and licensing
- Support organizational partnerships

At this time, detailed literacy performance and activity data remain local to the user's device and are not transmitted to **rinnalla** cloud systems.

Parent Account Data

Purpose

Account creation, authentication, communication, and account management.

Collected Data

- Parent name
- Parent email address
- Account identifier

Storage

Firebase

Access

- Parent account holder
- Authorized **rinnalla** administrators

Child Profile Data

Purpose

Personalize user experiences and associate child profiles with licensed accounts.

Collected Data

- Child name
- Child age
- Child grade level
- Organization affiliation

Examples:

- School district
- Healthcare partner
- Literacy organization
- Community partner

Storage

Firebase

Access

- Parent account holder
- Authorized **rinnalla** administrators

Account Administration Data

Purpose

Subscription management, customer support, licensing administration, and account verification.

Collected Data

- Subscription status
- License status
- Transaction identifier
- Last login timestamp

Storage

Firebase and RevenueCat

Access

- Authorized **rinnalla** administrators

Technical Diagnostic Data

Purpose

Application stability, troubleshooting, and system maintenance.

Collected Data

- Crash reports
- Error diagnostics
- Device metadata
- Technical application logs

Storage

Sentry

Access

- Authorized **rinnalla** personnel

Data Not Currently Stored in Cloud Systems

The following information is not currently transmitted to or stored in **rinnalla** cloud infrastructure:

- Reading progress
- Literacy skill progression
- Activity completion records
- Reading assessment data
- Reading response data
- Student-generated educational content
- Coaching interaction history

Data Not Collected

rinnalla does not currently collect:

- State student identifiers
- District student identifiers
- Social Security numbers
- Student addresses
- Student phone numbers
- Race or ethnicity
- Disability information
- IEP or 504 information
- Medical information
- Attendance records
- Discipline records
- Free/reduced lunch status
- Standardized assessment scores

Hosting and Storage

Primary Hosting Platform: Firebase

Storage Region: United States

Third-Party Service Providers

- Firebase
- RevenueCat
- Sentry
- SiteDetour

Data Classification

Category A – Identifiable Data

- Parent name
- Parent email
- Child name
- Child age
- Child grade level
- Organization affiliation

Category B – Account Administration Data

- Subscription status
- License status
- Transaction identifiers
- Last login timestamp

Category C – Technical Data

- Crash reports
- Diagnostic logs
- Device metadata

rinnalla
Information Security Policy

Version 1.0 · Effective Date: June 8, 2026

1. Purpose

The purpose of this Information Security Policy is to establish the administrative, technical, and operational safeguards used by **rinnalla** to protect personal information, account information, and organizational data processed through the **rinnalla** platform.

rinnalla is committed to maintaining reasonable and appropriate security controls designed to protect information from unauthorized access, disclosure, alteration, destruction, or misuse.

This policy applies to all **rinnalla** personnel, contractors, systems, applications, and third-party service providers involved in delivering **rinnalla** products and services.

2. Security Philosophy

rinnalla follows a security-by-design approach based on the principles of:

- Data minimization
- Least privilege access
- Secure authentication
- Encryption in transit
- Vendor security review
- Continuous improvement

rinnalla intentionally limits the amount of personal and educational data collected in order to reduce privacy and security risks.

3. Governance and Responsibility

Leadership Responsibility

rinnalla leadership is responsible for:

- Maintaining security policies
- Reviewing security practices
- Coordinating incident response
- Managing vendor security oversight

Development Responsibility

rinnalla development personnel are responsible for:

- Secure system configuration
- Application security maintenance
- Vendor integration management
- Security updates and patches

4. Data Classification

rinnalla classifies information into three categories.

Category A – Identifiable Information

Examples:

- Parent name
- Parent email
- Child name
- Child age
- Grade level
- Organization affiliation

Protection Level: High

Category B – Account Administration Information

Examples:

- Subscription status
- License status
- Transaction identifiers
- Login metadata

Protection Level: Moderate

Category C – Technical Information

Examples:

- Error logs
- Crash reports
- Diagnostic information

Protection Level: Moderate

5. Access Control

Access to information is limited based on business need.

User Accounts

Users may access only information associated with their own account.

Administrative Accounts

Administrative access is limited to authorized personnel.

Administrative users may access:

- Parent account information
- Child profile information
- Subscription and license information
- Account administration data

Administrative users do not have access to locally stored literacy activity data or reading performance information.

6. Authentication

rinnalla utilizes Firebase Authentication services.

Security controls include:

- Secure password management
- Password hashing
- Authentication token management
- Session controls provided by Firebase

Passwords are not stored in plain text.

7. Encryption

Data in Transit

All communications between users and **rinnalla** services are protected using HTTPS encryption.

Data at Rest

Cloud-hosted information is stored within Firebase infrastructure utilizing industry-standard security controls.

8. Hosting Environment

Primary cloud infrastructure is provided through Firebase.

Current production data is hosted within the United States.

rinnalla relies on Firebase security controls, infrastructure protections, and platform monitoring capabilities.

9. Third-Party Service Providers

rinnalla utilizes carefully selected third-party providers.

Current providers include:

Firebase

Purpose: Authentication, hosting, and cloud data storage.

RevenueCat

Purpose: Subscription management and purchase restoration.

Sentry

Purpose: Application monitoring and crash diagnostics.

All providers must support reasonable security protections appropriate to their role in delivering services.

SiteDetour

Purpose: Dynamic QR code routing and experience delivery

10. Logging, Monitoring, Analytics

rinnalla maintains technical monitoring and operational visibility through platform and vendor-supported tools.

Monitoring may include:

- Authentication activity
- Login metadata
- Subscription and license status information
- Application errors
- Crash reports
- System diagnostics
- Operational service metrics
- QR routing and service delivery metrics

Logs and monitoring information may be used for:

- Troubleshooting
- Security review
- System maintenance
- Service reliability
- Operational support

rinnalla does not currently utilize cloud-based educational performance analytics or reading progress analytics as part of its monitoring processes.

11. Secure Development Practices

rinnalla seeks to incorporate security considerations into application development.

Practices include:

- Vendor-managed authentication
- Secure API communications
- Controlled administrative access
- Software updates and maintenance

Security improvements are reviewed periodically as the platform evolves.

12. Data Retention and Deletion

rinnalla supports deletion requests for user accounts and associated information.

Upon a verified deletion request, account records may be deactivated and removed from active use.

Deactivated records may be retained for up to six (6) months to support account recovery requests, customer support inquiries, audit activities, and operational continuity.

Following the retention period, records are reviewed and permanently deleted from production systems in accordance with the **rinnalla** Data Retention Policy.

Deletion activities may be performed through automated processes, manual administrative procedures, or a combination of both, depending on the systems involved and the capabilities of the platform at the time of deletion.

Additional retention requirements are documented in the **rinnalla** Data Retention Policy.

13. Incident Response

rinnalla maintains procedures for identifying, investigating, containing, and responding to suspected security incidents.

Incident response objectives include:

- Rapid identification
- Containment of unauthorized access
- Assessment of impacted information
- Notification when required by law or contract
- Documentation of corrective actions

Detailed procedures are maintained within the **rinnalla** Data Breach Response Plan.

14. Security Reviews

rinnalla periodically reviews:

- Security practices
- Vendor relationships
- Access permissions
- Data collection practices

Policies may be updated as the platform expands or security requirements evolve.

15. Future Enhancements

As **rinnalla** introduces:

- Teacher-facing products
- Organizational reporting
- Advanced analytics
- AI-supported recommendations

additional security controls may be implemented to address increased data sensitivity and organizational requirements.

16. Policy Review

This policy shall be reviewed at least annually or whenever significant changes are made to:

- Platform architecture
- Data collection practices
- Vendor infrastructure

- Security requirements

rinnalla
Application Privacy Policy

Last Updated: June 8, 2026

Our Commitment to Privacy

rinnalla is designed to support families and organizations in promoting early literacy and learning through parent coaching and educational guidance.

We believe that children deserve strong privacy protections. For that reason, **rinnalla** is intentionally designed to collect only the information necessary to operate the service and support families.

> We do not sell personal information, we do not use student information for advertising, and we do not build marketing profiles based on children's information.

This Application Privacy Policy explains what information **rinnalla** collects, how it is used, how it is protected, and the choices available to users.

1. Scope

This Privacy Policy applies to the **rinnalla** mobile applications, websites, and related services (collectively, the "Services").

This policy applies to information collected through the use of **rinnalla**'s educational products and services.

2. Information We Collect

Parent or Account Holder Information

To create and manage an account, **rinnalla** may collect:

- Parent or account holder name
- Email address
- Account identifier

This information is used for:

- Account creation
- Authentication
- Customer support
- Subscription management
- Service communications

Child Profile Information

To personalize learning experiences, **rinnalla** may collect:

- Child name

- Child age
- Child grade level
- Organization affiliation, if applicable

Examples of organization affiliation include:

- School districts
- Healthcare organizations
- Literacy organizations
- Community partners

This information is used solely to support the educational services provided through **rinnalla**.

Subscription and Licensing Information

To manage subscriptions and licensing, **rinnalla** may collect:

- Subscription status
- License status
- Transaction identifiers
- Account activity related to subscription management

rinnalla does not collect or store payment card information.

Payment transactions are processed through third-party providers such as Apple App Store, Google Play Store, or other authorized payment providers.

Technical Information

rinnalla may automatically collect technical information necessary to operate and improve the service, including:

- Device information
- Application version information
- Crash reports
- Error logs
- Login metadata
- Authentication metadata

This information is used for system reliability, troubleshooting, and security.

3. Information We Do Not Collect

rinnalla does not currently collect:

- Social Security numbers
- State student identification numbers
- School district student identification numbers
- Home addresses
- Phone numbers
- Race or ethnicity information
- Disability information

- IEP or 504 information
- Medical information
- Attendance records
- Discipline records
- Free or reduced lunch status

4. Educational Progress Information

At this time, detailed literacy activity data, reading performance data, and educational progress information remain local to the user's device and are not transmitted to or stored in **rinnalla** cloud systems.

Future versions of **rinnalla** may introduce additional educational reporting features. If those features require the collection or storage of additional educational data, this Privacy Policy will be updated accordingly.

5. How We Use Information

rinnalla uses information only for purposes related to providing and improving the Services.

Examples include:

- Creating and managing accounts
- Delivering educational content
- Supporting subscriptions and licensing
- Providing customer support
- Maintaining system security
- Troubleshooting technical issues
- Improving product functionality

We do not use personal information for targeted advertising.

We do not sell personal information.

6. Children's Privacy

rinnalla is designed for use by parents, guardians, educational organizations, and authorized adults supporting children.

Children do not create independent accounts within the Service. Information associated with a child profile is managed through a parent, guardian, or authorized organizational account.

When **rinnalla** is provided through a school district, healthcare organization, literacy organization, or other educational partner, that organization may act as the authorized administrator of the service relationship.

7. Information Sharing

rinnalla does not sell personal information.

rinnalla does not share personal information with third parties for advertising purposes.

Information may be shared only:

- With service providers necessary to operate the Services
- When required by law
- To protect the security of the Services
- As directed or authorized by the account holder or contracting organization

8. Service Providers

rinnalla utilizes trusted third-party service providers to support operation of the Services.

Current providers include:

- Firebase (authentication, hosting, cloud storage)
- RevenueCat (subscription management)
- Sentry (crash reporting and diagnostics)
- SiteDetour (dynamic QR code routing and experience delivery)

These providers are contractually obligated to use information only for the services they provide.

9. Security

rinnalla implements reasonable administrative, technical, and physical safeguards designed to protect information against unauthorized access, disclosure, alteration, or destruction.

Current safeguards include:

- Encrypted HTTPS communications
- Secure authentication systems
- Password hashing through Firebase authentication services
- Access controls limiting administrative access
- U.S.-based cloud hosting

While no system can guarantee absolute security, **rinnalla** is committed to maintaining appropriate security measures consistent with industry practices.

10. Data Storage

rinnalla stores production cloud data within the United States.

11. Access, Correction, and Deletion

Account holders may request access to, correction of, or deletion of information associated with their account.

Requests may be submitted through **rinnalla** customer support.

Where required by applicable law or contractual obligations, **rinnalla** will work with schools, organizations, and account holders to fulfill requests related to personal information.

12. Changes to This Policy

rinnalla may update this Privacy Policy periodically to reflect product improvements, legal requirements, or operational changes.

When material changes are made, **rinnalla** will provide notice through the Services or by other reasonable means.

13. Contact Information

Questions regarding this Privacy Policy may be directed to:

rinnalla – Chasing Impact, LLC
privacy@rinnallaliteracy.com
7984 South 1300 East, Sandy, UT 84094
801-834-1798

rinnalla
Subprocessor Registry

Version 1.1 · Effective Date: June 8, 2026

Purpose

This registry identifies third-party service providers that may process, transmit, store, or otherwise access data necessary to operate the **rinnalla** platform.

Firebase

Purpose:

- Authentication
- User account management
- Cloud data storage
- Application hosting

Data Potentially Processed:

- Parent account data
- Child profile data
- Subscription and licensing data
- Login metadata

Storage Region: United States

RevenueCat

Purpose:

- Subscription validation
- Purchase restoration
- Subscription status management

Data Processed:

- Subscription status
- Transaction identifiers
- Purchase metadata from Apple App Store
- Purchase metadata from Google Play Store

Not Processed:

- Credit card information
- Bank account information
- Payment processing information

Notes: RevenueCat does not directly process payments. Payment transactions occur through Apple App Store, Google Play Store, and potentially future payment providers such as Stripe.

Sentry

Purpose:

- Crash monitoring
- Error diagnostics
- Application stability monitoring

Data Processed:

- Technical diagnostics
- Device metadata
- Error logs

Not Intended to Process:

- Educational performance data
- Reading progress data

SiteDetour

Purpose:

- Dynamic QR code generation
- QR code management
- Link routing
- Experience delivery

Data Processed:

- QR code destination information
- Routing metadata
- Link interaction metadata

Not Intended to Process:

- Reading progress data
- Educational performance data
- Assessment data
- Payment information

Notes: SiteDetour is used to route users to the appropriate **rinnalla** experience when accessing the platform through QR codes or dynamic links.

Future Subprocessors

Any future subprocessor added to the **rinnalla** platform shall:

- Undergo privacy and security review.
- Be documented in this registry.

- Be disclosed to contracting organizations when required by law or contract.

Examples may include:

- Stripe
- Learning analytics providers
- Teacher dashboard infrastructure
- Organizational reporting systems

rinnalla
Data Retention Policy

Version 1.0 · Effective Date: June 8, 2026

1. Purpose

The purpose of this Data Retention Policy is to establish guidelines for the retention, archival, and deletion of information processed by **rinnalla**.

rinnalla is committed to collecting and retaining only the information necessary to:

- Provide services
- Support customers
- Maintain subscriptions and licensing
- Meet contractual obligations
- Comply with applicable legal requirements

This policy supports **rinnalla**'s commitment to data minimization and privacy-by-design principles.

2. Scope

This policy applies to:

- Parent account information
- Child profile information
- Subscription and licensing information
- Technical diagnostic information
- Administrative records
- Vendor-managed data associated with **rinnalla** services

This policy applies to information stored within:

- Firebase
- RevenueCat
- Sentry
- Internal administrative systems
- SiteDetour

3. Retention Principles

rinnalla follows the following principles:

Data Minimization

Information shall not be retained longer than necessary for business, contractual, or legal purposes.

Purpose Limitation

Information shall only be retained while it continues to support a legitimate business or operational purpose.

Secure Disposal

When information is no longer required, it shall be securely deleted or anonymized when reasonably practicable.

4. Data Retention Schedule

Parent Account Information

Examples:

- Parent name
- Parent email
- Account identifiers

Retention Period:

- While account remains active
- Up to 6 months following account deletion request

Purpose:

- Account recovery
- Customer support
- Error correction
- Deletion verification

Deletion Method:

- Permanent deletion from production systems when retention period expires

Child Profile Information

Examples:

- Child name
- Child age
- Grade level
- Organization affiliation

Retention Period:

- While associated account remains active
- Up to 6 months following account deletion request

Purpose:

- Account recovery
- Customer support
- Deletion verification

Deletion Method:

- Permanent deletion from production systems when retention period expires

Subscription and Licensing Information

Examples:

- Subscription status
- License status
- Transaction identifiers

Retention Period:

- Active subscription period
- Seven (7) years after subscription termination

Purpose:

- Financial recordkeeping
- Audit support
- Customer support
- Contract administration

Deletion Method:

- Secure deletion after expiration of retention period unless otherwise required by law

Login and Authentication Metadata

Examples:

- Last login date
- Authentication logs
- Session metadata

Retention Period:

- Twenty-four (24) months

Purpose:

- Security investigations
- Account support
- Fraud prevention

Deletion Method:

- Automatic deletion or rotation where technically feasible

Technical Diagnostic Information

Examples:

- Crash reports
- Error logs
- Device diagnostics

Retention Period:

- Twenty-four (24) months

Purpose:

- Product stability
- Technical troubleshooting
- Security investigations

Deletion Method:

- Automatic deletion through vendor retention controls where available

Incident Records

Examples:

- Security incident investigations
- Breach documentation
- Corrective action records

Retention Period:

- Seven (7) years

Purpose:

- Legal compliance
- Security review
- Risk management

Deletion Method:

- Secure deletion after expiration of retention period

5. Account Deletion Requests

rinnalla supports account deletion requests.

Upon verified request:

- Account access may be disabled immediately.
- Information will be scheduled for deletion.
- Information may remain in backup systems for a limited period consistent with normal backup cycles.

Deletion requests will be processed within a reasonable timeframe and in accordance with applicable contractual and legal requirements.

6. Organizational and District Requests

When services are provided through an organization, school district, healthcare partner, or other contracting entity:

- Data deletion requests may be coordinated through the contracting organization.
- Contractual obligations may affect retention timelines.
- NDPA and applicable agreements shall govern where applicable.

7. Legal Holds

If **rinnalla** is required to preserve information due to:

- Litigation
- Government investigation
- Legal process
- Contractual dispute

Relevant information may be retained beyond normal retention periods until the matter is resolved.

8. Vendor Retention

Third-party providers may maintain information according to their own documented retention schedules.

Current providers include:

- Firebase
- RevenueCat
- Sentry
- SiteDetour

rinnalla will make reasonable efforts to ensure vendor retention practices remain consistent with business and contractual requirements.

9. Policy Review

This policy shall be reviewed:

- At least annually
- Following significant product changes
- Following major vendor changes
- Following changes in applicable legal requirements

rinnalla
Data Breach Response Plan

Version 1.0 · Effective Date: June 8, 2026

1. Purpose

The purpose of this Data Breach Response Plan is to establish procedures for identifying, investigating, containing, documenting, and responding to actual or suspected security incidents involving **rinnalla** systems, services, or data.

This plan is intended to:

- Protect users and organizations
- Minimize potential harm
- Support legal and contractual obligations
- Maintain business continuity
- Provide clear internal response procedures

2. Scope

This plan applies to:

- **rinnalla** applications
- Firebase-hosted systems
- RevenueCat integrations
- Sentry monitoring systems
- Company devices used to administer **rinnalla** services
- Authorized personnel with access to **rinnalla** systems

3. Definitions

Security Incident

Any event that may compromise the confidentiality, integrity, or availability of **rinnalla** systems or data.

Examples:

- Unauthorized account access
- Compromised administrator credentials
- Suspicious login activity
- Malware infection
- Unauthorized system changes
- Third-party vendor security incidents

Data Breach

A security incident resulting in unauthorized access to, disclosure of, acquisition of, destruction of, or loss of protected information.

Examples:

- Exposure of parent account information
- Unauthorized access to child profile information
- Public exposure of cloud data
- Accidental disclosure of protected information

4. Incident Response Team

The following individuals are responsible for breach response activities.

Executive Lead

Responsible for:

- Executive decision-making
- External communications approval
- Contractual and organizational notifications

Assigned To: CEO or designated executive

Technical Lead

Responsible for:

- Technical investigation
- System containment
- Log review
- Remediation activities

Assigned To: Lead Developer or designated technical representative

Operations Lead

Responsible for:

- Documentation
- Communication tracking
- Vendor coordination
- Incident records

Assigned To: COO or designated operations representative

5. Incident Severity Levels

Level 1 – High Severity

Examples:

- Confirmed unauthorized access
- Data exposure

- Compromised administrative account
- Vendor-reported breach affecting **rinnalla** data

Impact:

- Actual or suspected exposure of protected information

Response:

- Immediate containment
- Executive notification
- Vendor engagement
- Formal incident investigation
- Notification review

Level 2 – Moderate Severity

Examples:

- Suspicious account activity
- Credential compromise
- Unauthorized access attempts

Impact:

- Potential risk to protected information
- Limited scope

Response:

- Immediate investigation
- Password resets if necessary
- Access review
- Incident documentation

Level 3 – Low Severity

Examples:

- Minor application errors
- Failed login attempts
- Isolated user account issues

Impact:

- No evidence of unauthorized access
- No protected data exposure

Response:

- Document issue
- Correct problem
- Monitor for recurrence

6. Detection and Reporting

Potential incidents may be identified through:

- User reports
- Internal staff reports
- Firebase alerts
- Sentry monitoring
- Vendor notifications
- Security reviews

All personnel are expected to report suspected incidents immediately.

7. Initial Response Procedures

Upon discovery of a suspected incident:

Step 1

Document:

- Date and time discovered
- Reporter
- Systems involved
- Initial observations

Step 2

Notify:

- Executive Lead
- Technical Lead
- Operations Lead

Step 3

Determine:

- Whether protected information may be involved
- Whether active compromise is occurring
- Whether immediate containment is required

8. Containment Procedures

When appropriate:

- Disable compromised accounts
- Revoke credentials
- Restrict administrative access
- Suspend affected integrations
- Preserve system logs
- Preserve evidence

The goal is to stop further exposure while maintaining information necessary for investigation.

9. Investigation Procedures

The Technical Lead shall investigate:

- What happened
- When it occurred
- What systems were affected
- What information may have been involved
- Whether exposure can be confirmed

Investigation findings shall be documented.

10. Notification Procedures

If a breach involving protected information is confirmed, **rinnalla** will evaluate notification requirements under:

- Applicable laws
- Contractual obligations
- NDPA agreements
- Customer agreements

Notifications may include:

- Contracting organizations
- School districts
- Organizational partners
- Affected users

Where required by contract or law, notifications will be provided as soon as reasonably practicable following confirmation of the incident.

11. Vendor Coordination

If an incident involves a third-party provider, **rinnalla** will coordinate with the vendor.

Current vendors include:

- Firebase
- RevenueCat
- Sentry
- SiteDetour

Vendor-provided incident reports may be incorporated into the investigation.

12. Recovery Procedures

Following containment and investigation:

- Restore normal operations
- Verify system integrity
- Implement corrective actions necessary to resolve identified issues
- Identify preventive measures to reduce the likelihood of similar incidents

- Review access permissions
- Review security controls

Recovery activities shall be documented.

13. Post-Incident Review

For all significant incidents, **rinnalla** shall conduct a post-incident review to evaluate the effectiveness of the response and identify opportunities for improvement.

The review shall document:

- Root cause of the incident
- Timeline of events
- Information or systems impacted
- Effectiveness of the response
- Corrective actions implemented to resolve the issue
- Preventive measures implemented to reduce the likelihood of recurrence
- Needed process improvements
- Required policy, security, or operational updates
- Lessons learned

The Incident Response Team shall review findings and assign responsibility for any corrective or preventive actions resulting from the review.

Lessons learned and follow-up actions shall be documented and retained in accordance with the Data Retention Policy.

14. Incident Records

The Operations Lead shall maintain records including:

- Incident description
- Timeline
- Investigation findings
- Communications
- Corrective actions

Incident documentation shall be retained in accordance with the Data Retention Policy.

15. Plan Review

This Data Breach Response Plan shall be reviewed:

- At least annually
- Following any significant incident
- Following major platform changes
- Following major vendor changes