Resonant Education
Information and Data Security Policy

Last Updated November 3, 2025
Document Maintainer: Taylor Basilio, CTO, Resonant Education

People Security

Background Check

All Resonant Education personnel are required to complete a background check. An authorized member of Resonant Education must review each background check in accordance with local laws.

Confidentiality

Prior to accessing sensitive information, personnel are required to sign an industry-standard confidentiality agreement protecting Resonant Education confidential information.

Security Awareness Training

Resonant Education has a security awareness training program in place to promote the understanding of security policies and procedures. All personnel are required to undergo training following initial employment and annually thereafter. Completion of the training program is logged by Resonant Education.

Secure Coding

Resonant Education promotes the understanding of secure coding to its engineers in order to improve the security and robustness of Resonant Education products.

Remote Work

Any Resonant Education issued devices used to access company applications, systems, infrastructure, or data must be used only by the authorized employee or contractor of such device.

Employees or contractors accessing the Resonant Education network or other cloud-based networks or tools are required to use HTTPS/TLS 1.2+ at a minimum to protect data-in-transit.

If a public space, ensure sight lines are blocked and do not have customer conversations or other confidential conversations. If someone is close to you, assume they can see and hear everything. Connecting directly to a public wireless network that doesn't employ, at minimum, WPA-2 or an equivalent wireless protocol is prohibited

While working at home, employees and applicable contractors should be mindful when visitors (e.g. maintenance personnel) are at their residences, as visitors could become privy to sensitive information left up on computer screens.

Risk Management

Resonant Education requires a risk assessment to be performed at least annually. For risks identified during the process, Resonant Education must classify the risks and develop action plans to mitigate discovered risks.

Vendor Management

Resonant Education requires a vendor security assessment before third party products or services are used confirming the provider can maintain appropriate security and privacy controls. The review may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other security compliance evidence. Agreements will be updated and amended as necessary when business, laws, and regulatory requirements change.

Exceptions

Resonant Education business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Resonant Education policy. If an exception is needed, Resonant Education management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other Resonant Education policy or procedure may result in disciplinary action, up to and including termination of employment. Resonant Education reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Resonant Education does not consider conduct in violation of this policy to be within an employee’s or contractor’s course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Resonant Education as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Resonant Education reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

Information and Data Security Policy

Purpose

This document describes the minimal security policies to be implemented by employees and contractors in order to securely handle, transfer, store, and otherwise manage private information and data. In addition, it prescribes the steps to be taken should any of these policies be broken.

Resonant Education must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. It's primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

Scope

1. Any employee, contractor or individual with access to Resonant Education systems or data
2. Sensitive Data and Information includes files, data, spreadsheets, CSV, database exports, databases, emails, voice communication, videos, chats, SMS/MMS, training documents, servers or other sources of information pertaining to Resonant Education, their clients and customers, or any data that is processed, communicated, or discussed. This includes PII, financial data, health data, restricted/sensitive data, confidential data, or intellectual property.

All concerns or questions regarding this policy or data security in general should be directed to one of the following chief executive team members:

- Taylor Basilio - Chief Technology Officer - cto@resonanteducation.com
- Hardin Daniel - Chief Executive Officer - hdaniel@resonanteducation.com

Privacy and Confidentiality

Helping to protect the confidentiality, integrity, and availability of our customers' systems and data is of the utmost importance to Resonant Education, as is maintaining customer trust and confidence.

Data Classification Policy

Resonant Education enforces a Data Classification Policy to describe how data should further be classified and handled.

Family Education Rights and Privacy Act (FERPA)

FERPA is the primary federal legislation that governs the privacy of educational records. Resonant Education holds all PII obtained, learned or developed in confidence pursuant to applicable provisions of FERPA.

Disclosure and Data Confidence

Resonant Education holds client data in strict confidence and does not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.

Data Destruction

Any data housed in a Resonant Education system that is no longer useful for its primary or retention purposes is destroyed, making it unusable and unrecoverable. Data may also be removed at the behest of any client or customer.

Physical and Environmental Security

Resonant Education utilizes Google Cloud Platform (GCP) for physical and environmental infrastructure. GCP's data centers are state of the art, utilizing innovative architectural and engineering approaches. Google has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the GCP platform and infrastructure. GCP data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

GCP only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Google or Google Cloud. All physical access to data centers by GCP employees is logged and audited routinely. Additional information can be found here: https://cloud.google.com/security/

Third Parties and Contractors

Third parties and contractors that work with Resonant Education are subject to the same policies, requirements and security protocols as the internal Resonant Education team. In addition, access to source control, data, and documentation is strictly controlled to ensure vendors and contractors do not access information outside their scope of work.

Resonant Education does not disclose PII or any other data to any third parties without the express consent of the client.

Policy - General Employee Requirements

1. All employees and contractors of Resonant Education must complete security awareness training which includes but is not limited to following the policies set forth in this document and FERPA certification.
2. All employees must read and comply with company Terms and Conditions and Privacy Policy
3. Should an employee or contractor identify an unescorted or otherwise unauthorized individual in Resonant Education, they are to immediately notify the Chief Technology Officer or Chief Executive Officer of the company
4. Employees and staff are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by Resonant Education. For example, the use of external e-mail systems not hosted by Resonant Education to distribute data is not allowed.
5. Please keep a clean desk. To maintain information security you need to ensure that all printed in scope data is not left unattended at your workstation.
6. Visitors to Resonant Education must be escorted by an authorized employee at all times. If you are responsible for escorting visitors you must restrict them to appropriate areas.
7. Staff must use a secure password on all Resonant Education systems as per the password policy. These credentials must be unique and must not be used on other external systems or services. The use of an encrypted password manager is required. All passwords must be at least 16 characters long and changed twice per year.

8. Terminated employees will be required to return all records, in any format, containing personal information. This requirement should be part of the employee onboarding process with employees signing documentation to confirm they will do this.
9. You must immediately notify the CTO or CEO in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc).
10. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform the CTO or CEO so that they can take appropriate action.
11. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from the CTO or CEO if you are unsure as to your responsibilities.
12. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.
13. Data that must be moved within Resonant Education is to be transferred only via business provided secure transfer mechanisms (Google Drive, Slack, SFTP). Resonant Education will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with the CTO or CEO.
14. Any information being transferred on a portable device (e.g. laptop or phone) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from the CTO or CEO as appropriate.
15. The use of non-password protected and encrypted storage devices is not permitted. In general, the use of external storage devices like USB drives, especially those that can be easily lost and do not offer built-in encryption and password controls, are not permitted.
16. All workstations and approved devices that access Resonant Education data must be password-protected, encrypted, and enforce a 10-minute screen lock timeout where applicable.
17. Two-factor authentication must be used and enabled for all applicable systems.
18. Sensitive data must be securely destroyed and deleted when it is no longer required. In general, a 7-day limit is enforced unless specified otherwise.
19. Passwords to any company systems must be changed at minimum every 12 months.
20. Storage of sensitive Resonant Education data on cell phones is not permitted.
21. Systems using Microsoft Windows must have auto-run disabled. See https://support.microsoft.com/en-us/topic/how-to-disable-the-autorun-functionality-in-windows-8e5ff0da-c526-7624-c064-ff82aecfd145 for additional information under “How to disable or enable all Autorun features in Windows 7 and other operating systems” or contact the CTO for additional assistance.

22. Systems using Microsoft Windows and MacOS must install and configure BitDefender (https://www.bitdefender.com/solutions/free.html). Contact the CTO for additional assistance.
23. All new software dependencies, vendors, and subcontractors must be reviewed and approved by the CTO to assess security policies, risk, SLA agreements, data handling practices, access controls, and more.
24. Sensitive data should not be retained for more than 14 days on any personal device and when possible, the data should be deleted immediately after use.
25. All employee devices and systems must be updated with the latest security patches and operating system updates.
26. Sensitive data should never be sent directly in an email.

Policy - Technical and Development Team Requirements

1. All Resonant Education staff and contractors must follow these policies when implementing code, platform, server, database, or data processing mechanisms.
2. These policies are an addition to the General Employee Requirements policy
3. Where possible, servers and related platform services must not be directly accessible by the internet. This means connecting via VPN and other authentication methods is required.
4. Data must always be transferred using authenticated and secured protocols
5. Stored passwords must always be salted and encrypted
6. Data stored for long-term archival must always be encrypted using modern PGP methods
7. Access to all company resources, data, servers, or platform services must require secure authentication and data must be transferred securely via SSL or similar mechanism.
8. Mechanisms to easily purge or delete client data upon request must be implemented for all software systems
9. Web systems must actively protect against common known vulnerabilities which include but are not limited to XSS, SQL Injection, session hijacking, insecure direct object references, CSRF attacks, unvalidated redirects and forwards, and blatant security misconfiguration.
10. All code must be peer reviewed and all policies described here must be enforced.
11. All violations must be reported to the CTO or CEO, logged, fixed, and audited.
12. Automated security verification systems should be implemented where possible and approved.
13. Industry best practices should be applied to all systems, servers, services, and applications
14. On a yearly basis, review and study the OWASP Top 10: https://owasp.org/Top10/

15. On a yearly basis, review https://www.securecoding.com/blog/fixing-security-vulnerabilities-in-php-sites/
16. All new software dependencies, vendors, and subcontractors must be reviewed and approved by the CTO to assess security policies, risk, SLA agreements, data handling practices, access controls, and more.

Data Security Policy: Data Leak Prevention - Data in Motion

Using this policy

This example policy is intended to act as a guideline for Resonant Education employees and contractors to implement DLP controls. Adapt this policy, particularly in line with requirements for usability or in accordance with the regulations or data you need to protect. This policy provides a framework for classes of data that may wish to be monitored. You should expand them to cover the sensitive assets in your business and subject to the types of you hold.

Background to this policy

Data leakage prevention is designed to make users aware of data they are transferring which may be sensitive or restricted in nature.

Purpose

Resonant Education must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of in scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical. It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. It's primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

Scope

1. Any Resonant Education device which handles customer data, sensitive data, personally identifiable information or company data. Any device which is regularly used for e-mail, web or other work related tasks and is not specifically exempt for legitimate business or technology reasons.

2. The Resonant Education information security policy will define requirements for handling of information and user behaviour requirements. This policy is to augment the information security policy with technology controls.
3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by the CTO or CEO.

Policy

1. Resonant Education does not currently employ dynamic or automatic data leak prevention measures to detect data leaks in motion. All data leak prevention measures are left to be implemented by specified systems or staff as directed by this policy
2. See the Data Security Policy for General Employee Requirements
3. Any concerns, inquiries, incidents, breaches of these policies should be immediately escalated to the CTO or CEO.

Application Development

The Resonant Education development and operations team employs a modern Agile methodology in application development. This allows the team to maintain high standards of software quality while simultaneously responding quickly to changing project requirements.

Resonant Education's development process follows secure software development best practices, which include formal design reviews, threat modeling, and completion of a risk assessment. We have a limited-but-growing number of automated testing tools for security and regression checks. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. We are committed to continually improving our security and quality assurance efforts.

Source Control

Resonant Education uses industry-standard git source control in application development. This affords the development advantages such as distributed development, compatibility with existing systems/protocols, efficient handling of large projects, and cryptographic authentication of history. Source code is hosted on GitLab. Additional information about GitLab's security processes can be found here: https://about.gitlab.com/security/

Access Control

All access to source control is granularly controlled on a per-user and per-project level. All access to source control employs two-factor authentication to ensure that compromised

credentials do not lead to intrusion and theft of source code. Access to source is also rigorously logged and routinely audited.

Code Review

During the development process, all code that is added or changed in a repository must go through a code review process. This ensures all code abides by existing company style conventions, testing coverage, security policies, and performance recommendations.

Before it is deployed, all code must be reviewed by at least one Resonant Education Senior Developer other than the author. Code reviews must happen over the dedicated system for code review. When a Maintainer deploys code, it must have been sufficiently reviewed that the Maintainer is confident in its correctness, and any outstanding objections must have been resolved.

Incident Management

All incidents such as bugs, hotfixes, and features are logged in a dedicated incident management system. Resonant Education uses Atlassian's Jira for this. This system allows bugs and other issues to be triaged in an orderly manner while ensuring that critical issues escalate and reach resolution quickly. Dedicated client support personnel are trained on escalation procedures, and utilize established protocols when recording an incident. The objectives of the incident management policy ensures:

- Incidents are properly logged
- Incidents are properly routed
- Incident status is accurately reported
- Queue of unresolved incidents is visible and reported
- Incidents are properly prioritized and handled in the appropriate sequence
- Resolution provided meets the requirements of the SLA for the customer

Reference the Security Incident Response Plan, Disaster Recovery Plan, and Business Continuity Plan for further information.

When in doubt, escalate the issue with the CTO or next senior-most company officer.

Testing

Resonant Education employs testing at every level of application development to prevent regression and maintain high application quality. Our current test suite is limited but growing. Examples of such tests include:

- Unit
- Functional

- Integration
- User Acceptance

Data Retention

The backup procedures of Resonant Education data stores enable point-in-time recovery for any database instance. This allows Resonant Education to restore a DB Instance to any second during the retention period, up to the last 5 minutes. In addition, full backups of logs are stored indefinitely. Full database snapshots are taken twice every day.

Database backups are stored for a maximum period of 2 years. Client data may be removed from operational databases upon request and/or at the end of contract.

Durable Secondary Storage

Long-term data backups are stored in Google Cloud Storage and designed to provide 99.999999999% durability of objects over a given year. Objects are redundantly stored across multiple regions. Additional information about Google Cloud's storage classes can be found here: https://cloud.google.com/storage/docs/storage-classes

Encryption of Data at Rest

Backups and data in storage are encrypted at rest by default using Google Cloud's default encryption mechanisms. Google uses the Advanced Encryption Standard (AES) algorithm to encrypt data at rest. All data at the storage level is encrypted with AES256 by default. Additional information can be found here: https://cloud.google.com/security/encryption/default-encryption.

Network Security

Resonant Education has implemented a world-class network infrastructure that is carefully monitored and managed. Security is an utmost priority and continually improved.

Resonant Education servers and cloud services are access controlled and monitored to ensure only authorized users may gain access. A combination of firewall rules, network ACLs, routing tables, and subnets ensure that applications are properly segregated and that only authorized employees have access to the appropriate networks. IP-restricted access is enforced for all systems. Two-factor authentication is also required where Single Sign On is used for granting certain privileges.

Transmission Protection

Clients connect to Resonant Education applications via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. Developers may only access servers using SSH keys; password logins are not permitted.

Account Security

Wherever possible, Resonant Education uses industry standards for identity and access management integration. Resonant Education has experience implementing systems that use external authentication and system-wide single sign-on (SSO) using both OAuth 2.0 and SAML 2.0 protocols. This includes integration with district student management systems for our online data and teacher management systems, parent and student portals. If implementing SSO using SAML 2.0, all guidelines and workflows detailed in Appendix L, Article VII will be followed. If implementing SSO using OAuth 2.0, the authorization flow as specified in section 1.2 of the official specification will be followed. (http://tools.ietf.org/html/rfc6749#section-1.2)

Logging

All Resonant Education systems extensively log user actions for security and threat analysis. A complete list of users with IP addresses, permission levels, system login dates, pages browsed, actions taken, and minutes spent logged in will be available for download for all users with the proper permission level.

Role Based Permissions

Resonant Education's implementation of a role based permission system allows for the assignment of roles and permissions based upon dynamic metadata about users that is derived from remote identity providers and external authentication systems. Resonant Education has developed systems whereby organizational groupings of schools, districts and regional networks can be developed. Standardized roles, with related access control permissions, can then be defined and applied to user accounts to allow only the minimum required number of users to access aggregated or disaggregated data on students that map to the grouping to which they are assigned which can be managed by district administrators.

Identity Management

The Resonant Education identity management policies provide robust security to ensure the protection of sensitive data like passwords and PII. These policies include:

- Production environments free of testing, development and non-production accounts.
- Enforcement of a strong password policy.
- Storing of all passwords using bcrypt, a key derivation function for passwords designed by Niels Provos and David Mazières, based on the Blowfish cipher. Besides

incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computational power.
- Logging of all successful and failed authentication attempts, including date, time, IP address, username.
- Secure resetting of passwords including a one-time-use password link that expires after a limited number of hours.
- Automatic de-provisioning of accounts for terminated employees.

Vulnerability and Threat Detection

Resonant Education employs two modes of threat and vulnerability detection with Google Security Command center and annual penetration testing by a third-party vendor. Google Security Command center is used for ongoing, automated rapid scanning of server and network infrastructure. This includes hundreds of vulnerability scans provided by Google and compliance checks including, but not limited to the following:

- CIS Google Cloud Platform Foundation 1.0
- CIS Google Cloud Platform Foundation 1.1
- CIS Google Cloud Platform Foundation 1.2
- PCI DSS 3.2.1
- NIST 800-53
- ISO 27001
- OWASP 2017
- OWASP 2021

Third-party penetration testing includes a combination of manual and automated testing of development and production environments. This audit includes hundreds of vulnerability checks.

Additional automated monitoring of the public-facing Resonant Education platform is performed by a third-party service provider. This includes scans of network security, DNS health, patching cadence, end-point security, IP reputation, application security, and hacker chatter.

Any threats or concerns discovered are immediately escalated with the Resonant Education CTO for resolution. Copies of these reports are available upon request.