EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Vector Solutions (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the LINDENHURST UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Initial Here: Pursuant to the Plan Contractor will:

DS FS

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

DS FS

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

DS FS

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

Initial Here:

DS
FS

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

DS
FS

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

   a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

   b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

DS
FS

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

DS
FS

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

DS
FS

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Vector Solutions

SIGNED BY: DocuSigned by: Felicity Spicer DAC5E54D5A9A4CE... **DATED:** 6/23/2025

TITLE: Director of Sales, K-12

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR’S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Cybersecurity Policies and Information Handling Overview - Version 5.2

Revision Date 3/12/2025

4890 W. Kennedy Blvd., Suite 300 Tampa FL 33609

Contents

Overview

At Vector Solutions we know that information security and privacy is important to our customers, our colleagues, and our business partners. The purpose of this document is to provide an overview and a response to questions posed by customers and prospective customers to satisfy general concerns or compliance requirements. The information provided here offers responses primarily from a customer data perspective. In some cases, responses may represent Vector Solutions' Corporate IT or Information Security processes or controls. We are committed to maintaining Information Security through responsible management, appropriate use, and protection in accordance with legal and regulatory requirements and our agreements

While every effort is made to accurately reflect the current state of security operations at Vector Solutions, processes, the computing infrastructure, and the applications are all dynamic. Confirmation of specific information regarding critical requirements is advised. As of the published date provided at the end of this document, all information herein is provided in good faith and attested to be correct.

Information Security Program Overview

Information Security and the protection of our customers' data is the highest priority at Vector Solutions. The Information Security program is owned and managed by our VP of Information Security and governed by the Vector Solutions Board of Directors. Vector Solutions employs a team of trained information security, risk, and compliance subject matter experts to support our data security efforts.

Our Information Security Program aligns with the NIST Cybersecurity Framework (CSF). Security controls utilized are based on the CIS 18 Critical Security Controls, NIST 800-171, and NIST 800-53, depending on the specific product and regulatory requirements. Additionally, the Vector Solutions Information Security Program also includes best practices and requirements found in other recognized frameworks, laws, and standards, including the Cloud Security Alliance, SANS, PCI-DSS, COBIT, HIPAA, COPPA, EDUCAUSE, and other U.S. Federal, State, and international privacy laws.

Due to the dynamic nature of cybersecurity, our Information Security Program is continuously evolving to address the industry's best practices, regulatory compliance requirements, and guidelines that direct our customers' security programs.

Information Security Policies and Standards

The Vector Solutions Compliance and Risk team is responsible for managing and maintaining the Information Security Policies and Guidelines. Vector Solutions maintains written Information Security policies that define an employee's responsibilities and acceptable use of information system resources. The information security policies and guidelines include, but are not limited to:

- Acceptable Use
- Access Control
- Change Control
- Mobile Computing
- Password Policy
- Physical Security
- Privileged Access
- Encryption Guidelines
- Vendor Risk Management
- Vulnerability Assessment and Management
- Data Privacy & Protection
- Data Retention / Disposal
- Bring Your Own Device (BYOD)
- Incident Response Program
- Security Awareness Program

Vector Solutions receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the pertinent information security policies, the Company Code of Conduct, and Rules of Behavior before providing authorized access to Vector Solutions' information systems. These policies are routinely reviewed and updated, as necessary.
The Security policies and requirements apply to all employees and contractors working on behalf of Vector Solutions. They are communicated as part of the Security Awareness Program before receiving access to Vector Solutions systems upon hiring, and again annually as part of the security awareness training program.

In areas where Vector Solutions leverages the policies, processes, and controls of our Hosted Cloud Services Providers, AWS and Azure, information has been provided to us by them. Where possible, it is validated for completeness and appropriate usage in our environments as a part of Vector Solutions vendor risk management program and annual review.

Organizational Security

Information security roles and responsibilities are defined within the organization. The cybersecurity team focuses on data and information security, including global security auditing and compliance, as well as the identification of the security controls to protect Vector Solutions' infrastructure. The security team receives updated information system security notifications regularly from numerous sources including CISA. It distributes security alert and advisory information to the organization daily or as needed after assessing the risk and impact as appropriate.

Vector Solutions strives to follow industry best practices outlined by security frameworks such as the NIST Cybersecurity Framework to help identify, prevent, detect, and respond to security events and incidents. The VP of Information Security is responsible for tracking incidents, vulnerability assessments, overseeing penetration testing, threat mitigation, risk management, and maintaining a corporate-wide information security management program to ensure that information asset are adequately protected.

Privacy

Vector Solutions protects personal data using appropriate physical, technical, and organizational security measures. All Vector Solutions staff are required to take privacy protection training at least annually as part of the Security Awareness Program.

Vector Solutions only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized under our privacy policy published on our website. We take all reasonable steps to protect the information we receive from our users from loss, misuse, or unauthorized access, disclosure, alteration, or destruction.

The Privacy Policy and related standards define requirements for establishing and managing a program to protect the personal information of employees, customers, and stakeholders. Along the same lines as security, Vector Solutions maintains and fosters a strong privacy awareness culture and considers training and awareness a critical component of a holistic privacy program. A significant consideration is given to federal, state, and international laws and regulations pertaining to privacy including GDPR, PIPEDA, CCPA, and other emergent state-level privacy laws.

Vector Solutions recommends that unnecessary pieces of sensitive or personally identifiable information (PII) not be stored in the application(s), and alternate unique identifiers be used when possible.

- https://www.vectorsolutions.com/privacy-policy/
- https://www.vectorsolutions.com/ccpa-privacy-policy/
- https://www.vectorsolutions.com/dpa

Risk Management

As a part of the Company's vendor risk management program, critical vendors are subject to vendor security reviews annually. Regularly scheduled security assessments (e.g., Risk Assessment, Vulnerability Assessment, penetration test, web application security test, etc.) are conducted to identify any vulnerabilities or risks to the environment. After each assessment, all findings are reviewed to determine their validity and the level of risk. Mitigation may come in the form of a vendor patch (if one exists), code changes, or other available security control mitigations.

Incident Response

The Vector Solutions Incident Response Program and related standards establish requirements for discovering and managing potential threats to the Vector Solutions environment. As part of our Incident Response Program, the following provisions are in place:

- Comprehensive Incident Response Plan is documented and reviewed regularly.
- Creation and implementation of a multi-disciplinary Computer Emergency Response Team (CERT) to be called upon to contribute to the management of incidents, as necessary.
- Regular testing of the Incident Response Plan includes training and exercises such as threat simulations and plan walkthroughs.
- Validated high-risk vulnerabilities with known exploits are deemed threats and managed via the Incident Management Process until the threat is mitigated.
- Potential threats are continuously monitored and evaluated. Confirmed threats are addressed based on risk and potential impact.

The Incident Management Standard defines requirements for addressing incidents within the Vector Solutions environment and is the basis for the Incident Management Process. Incident Management at Vector Solutions includes the following provisions:

- Incidents and potential incidents are documented in the incident tracking system, where they are risk-ranked based on various factors.
- Incidents are managed through its resolution by the CERT via a documented process that is based on the NIST 800-61 Computer Security Incident Handling Guide and include the following stages:
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery

- Post-incident activity

The CERT team is defined in the Incident Response Plan and is composed of appropriate individuals with specific roles and responsibilities based on their areas of expertise. The team at times consists of members from:

- IT Infrastructure
- Application Development
- Finance (if applicable)
- Legal
- Communications
- Customer Services (if customer data is affected)
- Human Resources
- The affected unit or department that uses or manages the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data types involved
- Additional individuals as deemed necessary by the VP of Information Security, CTO, or Senior Management

Incidents are addressed based on Severity and Risk. Depending on the solution's complexity and/or permanence, incidents may spawn an equivalent event in the Problem Management Process.

The Incident Management Process is utilized/exercised regularly and is reviewed and validated at least annually.

Root cause analysis and blameless postmortem exercises are also conducted where possible to ensure that our incident response capabilities are always evolving.

Data Breach Response

Vector Solutions maintains a Data Breach Response (DBR) process as part of our Incident Response Program. The DBR applies to all who collect, access, support, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information located within Vector Solutions' cyber assets.

As soon as a theft, data breach or exposure of Protected or Sensitive data of Vector Solutions is identified, the process of removing all access to that resource will begin, and forensics teams will be deployed to determine the impact of the lost data.

Customer Data Breach Notification

When restricted data, including Personally Identifiable Information, has been exposed, Vector Solutions shall consult with General Counsel to determine the extent to which breach notification is required under legislative or regulatory obligations. In jurisdictions or circumstances where no laws or regulations dictating data breach notifications exist, Vector Solutions shall notify affected parties within 48 business hours after Vector Solutions has verified the scope and impact of the data breach. Notwithstanding the foregoing, in the event Vector Solutions reasonably determines that suspected data network activity is more than likely to result in the unauthorized exposure of restricted data, it will promptly notify Client of such reasonable suspicion so that Client may take actions it deems appropriate under the circumstances to mitigate the risk of such exposure.

Personnel Security

Vector Solutions employees are required to conduct themselves according to the Company's Code of Conduct and integrity guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees must sign non-disclosure confidentiality agreements and acknowledge the Vector Solutions Code of Conduct Policy. The policy outlines the Company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the Company's users, partners, and competitors.

- Processes and procedures are in place to address employees who are on-boarded and off-boarded from the Company.
- Preemployment background checks including criminal search and global watchlist search are performed on all new employees.

Data Centers: Physical & Environmental Security

Our information systems and infrastructure are hosted in world-class data centers, including hosted cloud systems that are regionally dispersed in North America to provide high availability, redundancy, and quick failover should an issue arise. At the time of this edit we utilize predominately AWS, as well as Azure hosted services with data centers in the USA and Canada.

The standard physical security controls implemented at each data center include electronic card access control systems, fire alarm and suppression systems, interior and exterior cameras, and security guards. Physical access is centrally managed and strictly controlled by data center personnel. All visitors and contractors are required to present identification, are required to log in, and be escorted by authorized staff through the data center. Access to areas where systems or system components are installed or stored is segregated from unrelated systems. The cameras and alarms for each of these areas are centrally monitored 24x7 for suspicious activity, and security guards routinely patrol the facilities. Servers have redundant internal and external power supplies. Data centers have backup power supplies and can draw power from diesel generators and backup batteries. These data centers are certified under the Service Organization Controls (SOC) 2 program. Verification of this certification is conducted at least annually through a review of the SOC 2 and/or SOC 3 reports.

Additional information on the data center security controls may be found online:
AWS - https://aws.amazon.com/compliance/data-center/controls/
Microsoft Azure - https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Auditing and Logging

We maintain audit logs on infrastructure and systems. Access to our auditing and logging tool is limited to authorized individuals only. Security events are logged, monitored, and addressed by trained security team members.

Vector Solutions employs a 24/7 monitored Security Operations Center. All alerting is triaged by the SOC staff and is escalated as needed to multiple levels of security staff that respond to these alerts in an ongoing manner. Network monitoring tools are in place to manage and control complications that may compromise the organization's business operations. The IT team uses an enterprise monitoring system to provide real-time information on system failures and outages. The monitoring system is further configured to generate alert notifications when network performance exceeds predefined thresholds. These alerts are configured to be sent to appropriate Vector personnel.

Endpoint Systems Protection

An endpoint protection system is used to monitor traffic within the internal network for malware and unwarranted network access. The endpoint system is configured to detect and quarantine the transmission of data or files that contain malicious code and automatically updates current virus signatures in real-time as they are released by the vendor. The system is also configured to detect non-signature-based issues where possible. All systems are centrally managed and monitored for malicious activity via host-based firewalls, intrusion prevention systems, antivirus, and malicious code protection. Our Security Operations Center monitors all endpoint logs. Endpoint Detection and Response is deployed on all user systems to ensure that Vector Solutions can respond to any emerging threat in a swift manner.

Data Protection & Encryption

Vector Solutions continually develops products that support the latest recommended secure cipher suites and protocols to encrypt traffic while in transit. We monitor the changing cryptographic landscape closely and work to upgrade our products to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. The policy for acceptable encryption is reviewed and updated on an ongoing basis as needed.

Sensitive customer data is encrypted while at rest, including when stored in local or offsite backups within secure data centers. Backups are performed to disk only (no removable storage is used) and no media leaves the protected environment. Transactional data between the Customer and the application is encrypted via TLS, which are applicable across the internet, except where customers request exceptions. Internal management/Operations utilize SSH or protocols tunneled over SSH or other VPN technologies when possible.

End users do not have direct access to the platform or to the database. Vector Solutions deploys security controls to prevent unauthorized access or modification of customer data. New or existing security controls are continually evaluated for effectiveness and implementation.

Data Loss Protection (DLP) is deployed to workstations, servers, email, and cloud file storage for Vector Solutions corporate systems.

Data Retention and Disposal

Data retention and destruction policies and procedures have been defined by management to ensure necessary records and documents of Vector are adequately protected and maintained, and to ensure that records that are no longer needed by Vector or are of no value are discarded securely at the proper time.

SaaS Offerings Customer Owned Data

Customers are the Data Controllers of all data they create and maintain into any of the Vector Solutions SaaS services they subscribe to.

Upon Termination of services the customer has the right to:

- Request an export or copy of their data.
- Request that their data be disposed of properly.

All customer data that is to be disposed of must follow all requirements for that deletion as dictated by regulatory compliance or contractual obligations. Data may also be anonymized to ensure that it cannot be used to reference a customer or individual person.

Vector Solutions Information Security Department has delineated policy related to appropriate disposal methods. The means of disposal will depend on the type of system and technically feasible means of data sanitization.

If the customer has not submitted a written request for data disposal, their data will be retained after the date of termination, but still cared for via the appropriate controls and surviving contract clauses.

Vector Solutions Operational Data

Data that Vector Solutions collects, creates, and maintains as part of our business operations is retained as needed in accordance with applicable federal, regulatory, and state laws. Due diligence is taken to protect the information that we hold against wrongful use, or disclosure.

Access Controls

Role-Based Access

Role-based access controls are implemented for access to information systems. Employee termination processes and procedures are in place to ensure that access is secured upon employee separation. Access controls to sensitive data in our databases, systems, and environments are established on a need-to-know basis following the principles of least privilege. All personnel with access to sensitive or confidential data have a background check performed against them before allowing access to the data. In addition, privacy and data handling training are required for all Vector Solutions employees and contractors. Annual security training and policy attestation is required for all employees.

Authentication and Authorization

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases and requires the use of complex passwords, which are deployed to protect against unauthorized use of passwords. Use of an identity access management system has been deployed internally to further strengthen user access controls.

Vector Solutions employees are granted a limited set of default permissions to access company resources, such as their email and the corporate intranet. Vector Solutions requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on the employee's job responsibilities, job duty requirements necessary to perform authorized tasks, and a need-to-know basis. Requests for further access follow a formal process that requires approval from a data or system owner, manager, or other executives, as defined by our security guidelines. The granting or modification of access rights must also be in accordance with the internal Access Control and Account Management Policy.

Business Continuity and Disaster Recovery

We implement a disaster recovery program within our software services to minimize service interruption due to hardware failure, natural disaster, or other catastrophes. This program includes multiple components to reduce the risk of any single point of failure. For business-critical applications, application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup data centers that are geographically dispersed to provide adequate redundancy and high availability. The hosted cloud service providers we use are required to have high-speed connections between data centers to support fast failover.

System Backups

Vector Solutions has backup standards and guidelines and associated procedures for performing backup and restoring data in a scheduled and timely manner. Incremental daily and full weekly backups are done on productions systems. Controls are established to help safeguard backed-up data (onsite and offsite). Periodic tests and exercises are conducted to determine whether data can be recovered from backup in a timely manner.

More Information

For more information regarding Vector Solutions Information Security policies or processes, please contact your primary point of contact at Vector Solutions.

Policy Version History

Version	Date	Description	Approved By
1.0	8/19/2019	Initial Draft	Greg Surla
2.0	11/6/2019	Updated numerous sections and document style	Greg Surla
2.1	8/3/2020	Updated sections to match current controls and processes in place	Greg Surla
3.0	3/12/2021	Updated sections to match current controls and processes in place. Format change.	Greg Surla
3.1	3/23/2021	Added Data Disposal section	Greg Surla
3.2	7/8/2021	Addition of Data Retention to the data disposal. Minor edits to provide additional information related to applicable policies. Added DLP statement Fixed version history to reflect proper date for Initial draft	Greg Surla
3.3	1/18/2022	Updated Data Breach section to match policy Added information regarding Data Center Security	Greg Surla
4.0	04/22/2022	Breach Notification sections updated. In jurisdictions or circumstances where no laws or regulations dictating data breach notifications exist, Vector Solutions shall notify affected parties within 24-hours after the company has verified the scope and impact of the data breach.	Greg Surla
5.0	11/15/2022	Some sections moved to align more naturally by topic. Risk Management section relocated. Updates added to provide additional information and clarity. Endpoint systems protection statement revised to be more complete. Purpose changed to Overview- Auditing and Logging further defined. Authentication and Authorization further defined. Systems backups further defined. Privacy Policy Links and DPA added. Data Retention and destruction further defined. Data Centers information added to Physical & Environmental Security.	David Smart
5.1	3/5/2024	Adjusting high-level statements to match changes that have been made to individual internal policies.	Scott Beauregard
5.2	3/12/2025	Annual review, no significant changes	Scott Beauregard