ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

STUDENT DATA PRIVACY AGREEMENT

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Edmentum, Inc. ("Service Provider" or "Vendor") on 09/23/2025 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for educational or digital services to the LEA;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed, or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms; and

WHEREAS, the provider and LEA agree that additional and modified sections are required to address the use of Artificial Intelligence ("AI") as part of the services or product provided;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Agree

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems, including file servers, routers, switches, NDS, and Internet services, is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software, is prohibited.

   Agree: Agree

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code, and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Agree

Provider Initial: JC
Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage, or use for demonstration purposes any Roseville City School District data without the prior written consent of Educational or Technology Services management.

   Agree: Agree

5. **TRANSPORT**: The Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Agree

6. **EXTERNAL SECURITY:** The Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Agree

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personnel (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protect unauthorized access to District data? How are backups performed, and who has access to and custody of the backup media? How long are backups maintained? What happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard-copy records?

   Agree: Agree

8. **DISTRICT ACCESS:** The Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Agree

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. The Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Agree

Provider Initial: JC
Date: 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. The Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Agree

2. The Vendor must attach a description of how student-created content can be exported and/or transferred to a personal account to this document.

   Agree: Agree

3. The Vendor is prohibited from allowing third parties access to student information beyond those purposes defined in the contract.

   Agree: Agree

4. The Vendor must attach a description of how parents, legal guardians, and students can review and correct their personally identifiable information to this document.

   Agree: Agree

5. The Vendor will attach to this document evidence of how student data is kept secure and confidential.

   Agree: Agree

6. The Vendor will attach to this document a description of the procedures for notifying affected parents, legal guardians, or eligible students when student records are unauthorizedly disclosed.

   Agree: Agree

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Agree

8. The Vendor will attach to this document a description of how they and any third-party affiliates comply with FERPA.

   Agree: Agree

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Agree

Provider Initial: JC
Date: 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Agree

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Agree

3. Vendors cannot sell student information.

   Agree: Agree

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Agree

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Agree

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Agree

7. Vendors must disclose student information when required by law, for legitimate research purposes, and for school purposes to educational agencies.

   Agree: Agree

Provider Initial: JC

Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section IV: Audit and Compliance Oversight

1. **Audit Rights.** The District reserves the right to audit the Vendor's privacy and security practices no more than once annually or at any time in response to a data incident, suspected noncompliance, or legal/regulatory inquiry. The Vendor shall provide reasonable access to systems, records, and personnel involved in the handling of District data.
2. **Confidentiality Agreement.** RCSD agrees to execute a reasonable non-disclosure agreement to protect Vendor trade secrets or proprietary information disclosed during the audit.

Section IV: Audit and Compliance Oversight (*Continued*)

3. **Framework Compliance.** Vendor agrees to implement and maintain security controls consistent with one or more of the following frameworks:
    a. NIST Cybersecurity Framework (NIST CSF)
    b. NIST SP 800-53 or 800-171
    c. ISO/IEC 27001
    d. CIS Critical Security Controls (Top 18)

    The Vendor shall indicate which framework is used and provide a summary upon request.

    Designated Security Framework(s):
    See attached document titled Section IV.3 Designated Security Frameworks

4. Security Program Documentation. Upon request, the Vendor shall furnish RCSD with the following:
    a. A summary of its data security policies and incident response procedures.
    b. Results from the most recent third-party security assessment or audit, redacted as necessary.
    c. Any certifications (e.g., SOC 2, ISO 27001).
5. **Remediation Obligations**. If a security deficiency or compliance failure is identified, the Vendor shall deliver a written remediation plan to RCSD within thirty (30) days. The District may suspend access to its data until the deficiency is addressed to the District's satisfaction.
6. **Subprocessor Oversight**. The Vendor is responsible for ensuring that all subprocessors or affiliates with access to District data comply with the terms of this agreement and are subject to equivalent audit and compliance obligations.

Provider Initial: JC
Date: 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

See attached document titled Section 1.6 & III.5 External Security_Edmentum Engagement Letter - S2Score Security Risk Assessment and Section 1.6 & III.5 External Security_Optiv Penetration Test Customer Summary

Section 1.7: Internal Security

See attached document titled Section 1.7 Internal Security

Section II.2: Exporting of Student-Created Content

Content that a student submits into a Lesson Activity can be printed by the teacher or the student, (therefore saved as PDF). Unit or Course activities can be saved by a teacher. Teacher Graded activities, including student submitted recordings, are automatically downloaded for teachers as they review.

Provider Initial: JC
Date: 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.4: Review and Correct Personally Identifiable Information (PII)

Parents and families can access and review personal information and student work securely through their student's login credentials.

Parents or students who are interested in accessing, modifying or deleting Personal Information from their education Institutional Services account should contact the Institutional Customer with the request. We will work with our educational Institutional Customers as needed to facilitate responding to those requests. See Product Privacy Policy | Edmentum: https://www.edmentum.com/product-privacy-policy/#how-you-access

Section II.5: Securing Student Data

See attached document titled Section II.5 Securing Student Data

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See attached document titled Section II.8 FERPA Compliance

Section III.5: How Student Data is Protected:

See attached document titled Section III.5, Section 1.6 & III.5 External Security_Edmentum Engagement Letter - S2Score Security Risk Assessment, and Section 1.6 & III.5 External Security_Optiv Penetration Test Customer Summary

Provider Initial: JC

Date: 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

1. AI Usage Limitations and Ownership

1.1. The Service Provider shall not use or reproduce Student Data for Artificial Intelligence (AI) training, model development, or content generation without the District's prior written consent. The Provider agrees to uphold the principles outlined in California Education Code §33328.5, ensuring that any AI systems used in connection with the Service align with values of equity, safety, transparency, and accountability in the interest of student welfare.

1.2. Sub-licensing Student Data for such purposes is strictly prohibited unless explicit written permission is obtained from the student's parent, legal guardian, or eligible student.

1.3. Ownership of all Student Data, including content generated with AI assistance, remains with the District or the student, as applicable.

2. Notification and Consent

2.1. If any feature of the Service is modified to include AI functionality, the Provider shall notify the District in writing prior to deployment.

2.2. The Provider must disclose the types of AI used, the purpose of such use, and how Student Data will be processed within these features.

2.3. No AI feature may be enabled until the District provides written consent and has reviewed any updated data-handling practices.

3. Algorithm Bias and Fairness

3.1. The Provider certifies that any AI technologies used in facilitating the Services are regularly audited for algorithmic bias and fairness.

3.2. Upon request by the District, the Provider shall furnish a summary of audit findings related to bias detection and mitigation strategies. These audits shall demonstrate the Provider's commitment to promoting equitable outcomes and addressing systemic bias, as emphasized in California Education Code §33328.5(d).

4. AI Hallucinations and Reliability

4.1. The Provider shall monitor the hallucination rate of any deployed generative AI models (e.g., large language models or chatbots) and employ industry-standard techniques to reduce the occurrence of inaccurate or misleading outputs.

4.2. The Provider shall maintain a mechanism for the District to report hallucinated or harmful responses and address such issues in a timely and accountable manner.

Provider Initial: JC
Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

5. Prohibited Uses of AI

5.1. The Provider shall not:

- Use AI to generate synthetic or inferred Student Data.
- Develop behavioral profiles for marketing or advertising.
- Engage in predictive analytics that may result in automated decision-making affecting students without human oversight.
- Deploy AI systems that are not designed to minimize harmful outcomes to minors, including but not limited to biased academic profiling or discriminatory content outputs.

These prohibitions align with California Education Code §33328.5(c), which calls for educational AI technologies to be designed to minimize harm and safeguard the well-being of students.

6. Student Content and AI-Generated Work

6.1. If students create content using AI tools embedded in the Service (e.g., essays, responses, or projects), the Provider shall:

- Ensure students can download or export that content.
- Retain no ownership or claim over AI-assisted student work.
- Maintain logs of AI interactions in accordance with FERPA.
- Support digital literacy and public awareness regarding the use of AI, in accordance with §33328.5(b), by enabling users to understand when they are interacting with an AI system.

7. Transparency and Disclosure Requirements (SB 942)

7.1. The Provider shall maintain and make publicly available a free tool that enables users to verify whether content was generated by AI. This tool shall:

- Provide provenance data (excluding personal data).
- Support multiple content formats.
- Accept user feedback to support continuous improvement.

7.2. All AI-generated content must include permanent latent disclosures that identify:

- The Provider's name.
- Identification of the AI system used.
- The creation date and time.
- A unique identifier for the generated content.

7.3. The Provider shall also offer users the option to include visible disclosures indicating that the content was generated by AI. These disclosures must be conspicuous and designed to resist removal..

7.4. If the Provider licenses its AI technology to third parties, such license agreements shall require those third parties to uphold the same transparency and disclosure standards outlined herein.

Provider Initial: JC
Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

8. Definitions

8.1. **Artificial Intelligence (AI)**: Systems that analyze data and take actions, with some degree of autonomy, to achieve specific goals.

8.2. **Hallucination:** A response generated by an AI system that is incorrect, nonsensical, or misleading while appearing factually accurate.

8.3. **Algorithmic Bias:** Systematic and unfair discrimination in outcomes generated by an algorithm based on characteristics such as race, gender, or disability.

9. Compliance with State Advisory Guidelines

9.1. The Provider shall monitor and cooperate with any guidance or recommendations issued by the California Department of Education's Artificial Intelligence in Education Advisory Council, as established under Education Code §33328.5(a). This cooperation may include participation in feedback initiatives, alignment with recommended practices, or revisions to data governance protocols in response to evolving regulatory requirements.

Provider Initial: JC
Date: 09/23/2025

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

DATA INCIDENT NOTIFICATION ADDENDUM

This Exhibit outlines the Vendor's obligations in the event of a Data Incident involving Customer Data. These obligations are in addition to and do not limit any rights or remedies available to the Customer under the Agreement or applicable law.

1. Data Incident Notification

1.1. In the event Roseville City School District ("RCSD" or "District" or "Customer") Data is accessed, acquired, or reasonably believed to have been accessed or acquired by an unauthorized individual or third party ("Data Incident"), the Vendor shall notify the Customer in writing without undue delay, and in no case later than seventy-two (72) hours after confirming the occurrence of the Data Incident.

1.2. The Vendor shall comply with all reasonable instructions from the District in relation to the Data Incident and, in consultation with the District, take all appropriate and reasonable steps to investigate and mitigate any known or anticipated harmful effects resulting from such unauthorized access, use, or disclosure of Customer Data.

1.3. If the Data Incident involves Personally Identifiable Data (PII), including but not limited to Social Security numbers, government-issued identification numbers, financial account details, health records, or medical information protected under applicable privacy laws (e.g., HIPAA, FERPA, CCPA, SOPIPA, GDPR, CRPA, etc), the Vendor shall apply heightened protections in accordance with applicable state and federal law, including but not limited to breach notification, identity theft prevention, and mitigation requirements.

2. Notification to Affected Individuals and Authorities

The obligations in this Section apply in all cases where the Data Incident is caused, in whole or in part, by the actions or omissions of the Vendor, its subcontractors, or affiliates.

2.1. Following confirmation of a Data Incident, the vendor shall provide written notification to affected individuals whose data was compromised. This notification shall:

2.1.1. Be written in plain language;

2.1.2. Be delivered in compliance with applicable federal, state, or provincial laws;

2.1.3. Be issued without unreasonable delay following the District's approval and any required consultation with law enforcement

2.2. The notification to affected individuals shall include, at minimum:

2.2.1. A general description of the incident and the Vendor's response efforts.

2.2.2. The contact information of the Vendor's designated incident response representative.

2.2.3. The type(s) of Customer Data or PII involved (e.g., name, address, date of birth, Social Security number, student records, health/medical information, etc.);

2.2.4. The known or estimated date(s) of the Data Incident and the date of notification.

2.2.5. Whether law enforcement was involved and whether any delay in notification was due to a law enforcement investigation.

2.2.6. Steps the individual can take to protect themselves.

Provider Initial: JC

Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

2.3. The Vendor agrees to adhere to all applicable federal, state, and provincial laws concerning the protection of Customer Data, including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA), where applicable

In the event of a Data Incident involving Personally Identifiable Information (PII) of a minor, the Vendor acknowledges that PII includes both direct and indirect identifiers that could reasonably identify an individual student. Under FERPA, PII includes, but is not limited to:

- Student's full name
- Student identification number or state/local student identifier
- Date and/or place of birth
- Grade level or classroom assignment
- School name or teacher name
- Mailing address or contact information
- Parent/guardian names and contact information
- Any combination of the above elements that would reasonably allow identification of the student with reasonable certainty

2.4. If such PII is involved in a Data Incident, the Vendor shall:

2.4.1. The Vendor shall fully fund and coordinate identity monitoring and/or credit monitoring services for a minimum of twelve (12) months, including, at a minimum, dark web monitoring, identity theft insurance, and access to fraud resolution agents, without cost to the affected individual or the District.

2.4.2. As described in Section 2.2, notify all affected individuals (or their legal guardians, as applicable).

2.4.3. If five hundred (500) or more individuals are affected, the Vendor shall notify the appropriate State Attorney General or supervisory authority in accordance with relevant state data breach laws and ensure that the notification complies with all timing, format, and content requirements set forth under the relevant state's breach notification statute. A copy of the regulatory notification shall be provided to the Customer.

2.4.4. Maintain a record of the Data Incident, including the nature of the breach, categories of data affected, notification steps taken, and services provided. Upon request, the customer will have access to these records.

2.4.5. The Vendor shall ensure that all breach response and notification processes are consistent with applicable FERPA guidance and any other relevant federal, state, or provincial privacy regulations. No PII shall be re-disclosed or shared with any third party—including subcontractors or affiliated entities—without prior written consent from the District or as explicitly required by law. The Vendor shall document and maintain detailed records of all data disclosures made in relation to the incident and shall make such records available to the District upon request.

Provider Initial: JC
Date: 09/23/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

3. **Legal Compliance and Risk Management**

The Vendor agrees to comply with all applicable local, state, provincial, and federal data privacy and security laws, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- State-specific data breach notification statutes

3.1. The Vendor shall maintain a written incident response and breach notification policy that complies with industry standards and applicable law. The Vendor shall, upon request, make a summary of its policy available to the District.

3.1.1. The Vendor shall ensure that any subcontractor, service provider, or third party with access to Customer Data is contractually bound by equivalent or stronger data protection, confidentiality, and incident response obligations as outlined in this Agreement. The Vendor shall remain fully responsible for any acts or omissions of such third parties in connection with the handling of Customer Data.

3.2. At the District's request, and where such assistance is not unduly burdensome, the Vendor shall provide reasonable cooperation and support for any investigation, regulatory inquiry, or litigation arising out of or relating to the Data Incident, including support in notifying affected individuals and interfacing with regulatory authorities.

3.3. The Vendor shall not disclose the existence or details of a Data Incident to any third party, including media, regulators, or other customers, without the District's prior written approval, except as strictly required by law.

3.4. In no event shall the District be held financially liable for any costs, damages, regulatory penalties, or legal expenses arising from a breach of Customer Data caused, in whole or in part, by the Vendor, its subcontractors, or affiliates. The Vendor shall be solely responsible for all costs associated with investigation, response, notification, remediation, credit or identity monitoring, and any regulatory or legal actions stemming from such a breach.

The Vendor shall fully indemnify, defend, and hold harmless the District from and against any and all claims, damages, liabilities, penalties, costs, and expenses (including reasonable attorneys' fees) arising from or related to a Data Incident caused, in whole or in part, by the Vendor, its subcontractors, or agents. This includes, but is not limited to, costs associated with breach notification, regulatory inquiries, litigation, and third-party claims.

Provider Initial: JC

Date 09/23/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

This Agreement constitutes the entire understanding among the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral. No amendment or modification of this Agreement shall be valid unless in writing and signed by authorized representatives of both Parties.

As an authorized representative of my organization, I accept the conditions listed in this document.

Service Provider		**Roseville City School District**	
Jamie Candee		Laura Assem	
Authorized Representative Signature		*Authorized Representative Signature*	
Date:	09/23/2025	**Date:**	09/23/2025
Name:	Jamie Candee	**Name:**	Laura Assem
Title:	President / CEO	**Title:**	Executive Director, Technology
Email:	agreements@edmentum.com	**Email:**	lassem@rcsdk8.org

Edmentum, Inc

Application Security Assessment – Customer Summary

Apex, CTN, Study Island, and ELF

Opportunity Number: OP-4243933

Version Number: 1.1

Date: March 28, 2025

OPTIV

Table of Contents

Customer Summary

Risk reduction through security assessments is one area where Optiv Security Inc. (Optiv) helps our customers better their overall security posture. As part of their ongoing commitment to ensuring the security and integrity of their application, Edmentum, Inc (Edmentum) engaged Optiv to perform a security assessment of the organization's Apex, CTN, Study Island, and ELF applications and supporting application environments and infrastructure. The objective was to assess the current security posture and the effectiveness of the controls in place within the application environment, compare the results of the assessment with industry best practices, and identify vulnerabilities that could negatively affect the application or business.

Scope and Methodology

Optiv follows a phased assessment approach that includes thorough application profiling, threat analysis, and dynamic and manual testing. Security consultants utilize automated security tools, custom scripts, and manual testing and validation techniques to scan for, enumerate, and uncover vulnerabilities. This methodology identifies an organization's tactical and strategic security challenges, examines its current security posture, and analyzes the policy and procedures that will affect that posture for the long term. In this manner, our approach ensures that gaps in the current level of security are identified, and steps needed to close those gaps can be recommended.

The assessment included direct interaction with the application as authenticated and unauthenticated users. An in-depth analysis of session security, authentication, authorization, and parameter manipulation was performed. Optiv examined the web server environment and supporting infrastructure. Optiv assessed risks based on security industry consensus of the most critical web application security flaws, the Open Worldwide Application Security Project (OWASP) Top 10, and performed custom test cases specifically designed for Edmentum's application. Within 90 days of completion of testing, Optiv conducted a retest to verify the extent of success regarding fixes to the application.

Conclusions

Initial testing in December 2024 identified 2 high risk findings, 14 medium risk findings, 19 low risk findings and 2 informational risk findings. At the conclusion of retesting in March 2025, Optiv observed that 1 high severity finding was properly remediated, and 1 high severity finding was downgraded to a medium. Overall, the Apex, CTN, Study Island, and ELF applications can be classified as being at a moderate level of exposure. Edmentum's customers can be assured that Edmentum performed proper due diligence utilizing a trusted third party to independently evaluate the Apex, CTN, Study Island, and ELF applications from an information security standpoint.

Optiv understands the importance Edmentum places on data security and sincerely appreciates the opportunity to have worked on this engagement. Should you have any questions regarding these findings or the contents of this report, please feel free to contact us.

General

Copyright

Version Control

Application Security Assessment – Customer Summary	
Client Name	Edmentum
Client Contact	Dan Hess
Document Revision Number	1.1
Author(s)	Tejashwini G
Peer Reviewer	Rushyendra Reddy Induri
QA Reviewer	Kim Folse
Project Manager	Roshan Vincent
Delivery Date	March 28, 2025
Data Classification	Client Confidential

6/10/25

To Whom It May Concern:

In April 2025 Edmentum retained FRSecure LLC, an Information Security company, to provide information security services. Part of this engagement involves performing a full information security assessment, theS2SCORE® Risk Assessment, of Edmentum to determine the overall risk of unauthorized disclosure, modification, and/or destruction of sensitive data

TheS2SCORE® assessment leverages and references current security frameworks and standards such as ISO/IEC 27001:2013 and the NIST Cybersecurity Framework (CSF) and is calculated in a range from 300 to 850. The lower the score, the higher the risk and vice versa. The ranges are Very Poor (300-500), Poor (500-600), Fair (600-660), Good (660-780), and Excellent (780-850). In our opinion, aS2SCORE® of 660 or better is an "acceptable" score.

During the assessment, we review and assign risk ratings to thousands of controls that Edmentum uses to secure their administrative, technical, and physical environment. Just as in the overall risk rating, individual control ratings of a "660" or better are generally considered to be "acceptable" in our opinion.

Controls that are rated at or below a "660" should be reviewed by Edmentum, but do not necessarily require any remediation. Many of these controls can be accepted as-is. It is our recommendation that organizations conduct aS2SCORE® annually to ensure they are maintaining their Information Security program as new risks evolve.

The engagement also includes a roadmap.

Please contact FRSecure for any further guidance or questions regarding the content and meaning of the report, and we will be glad to assist.

Sincerely,

Melissa Kjendle

Consulting Team Manager

Consulting | FRSecure

CvCISO | CISSP | SEC+ | NET+

mkjendle@frsecure.com

frsecure.com

6550 York Ave S #500 Edina, MN 55435

If you are experiencing a potential incident, please email CSIRT@frsecure.com

Section 1.7: Internal Security

Edmentum follows industry security best practices. We implement and maintain administrative, technical, and physical safeguards designed to help protect the confidentiality, integrity, and availability of Personal Information, including restrictions against unauthorized access to Personal Information by Edmentum employees or contractors and authorizing access to Personal Information by Edmentum employees or contractors only as necessary to fulfill their official duties.

Safeguards include:

- Edmentum provides rule- and role-based data access where only personnel who require access to personally identifiable information in order to provide services to [clientabbreviation] are permitted access to such data
- Edmentum employees are required to implement passwords consistent with current NIST guidance and utilize multifactor authentication when accessing systems storing customer data
- Edmentum utilizes AWS data centers with robust, mature security controls
- All customer data are encrypted in transit and at rest using up-to-date, industry-standard encryption methods
- Software is patched and updated with patch releases
- Privacy and security assessments are conducted on third parties requiring personally identifiable information to provide contracted services, and all such third parties are contractually obligated to comply with all applicable data protection and security requirements
- Customer data are backed up regularly, and redundant backups are encrypted in transit and at rest
- All Edmentum employees must pass background checks consistent with Edmentum requirements as a condition of hire
-
- All Edmentum employees receive annual data protection training, inclusive of FERPA, COPPA, data security and [state] student data privacy law. Training may take the form of online learning modules, in-person training, written guidelines, and ongoing advice and counsel from internal and external advisors.

Please see the Security Measures and Data Retention section of our Product Privacy Policy at edmentum.com/product-privacy-policy. Our additional documentation, including our COPPA and FERPA statements, are thorough and should address any concerns. Our documents are public and reside on our website (links provided below).

- Edmentum's Standard Terms - edmentum.com/standardterms
- Edmentum's COPPA Customer Notice - edmentum.com/coppa
- Edmentum's FERPA Statement - edmentum.com/ferpa

Section II.5: Securing Student Data

Edmentum adheres to industry security best practices and implements comprehensive administrative, operational, and technical safeguards to protect the confidentiality, integrity, and availability of personal information. These measures include:

Administrative Safeguards

Role-Based Data Access: Only personnel who require access to personally identifiable information to provide services to [clientabbreviation] are permitted access

Privacy and Security Assessments: Conducted on third parties requiring personally identifiable information, with contractual obligations to comply with all applicable data protection and security requirements

Background Checks: All employees must pass background checks consistent with Edmentum requirements as a condition of hire

Annual Data Protection Training: Employees receive training on FERPA, COPPA, data security, and state student data privacy laws through various formats, including online modules, in-person training, and written guidelines

Operational Safeguards

AWS Data Centers: Uses AWS data centers with robust, mature security controls

Regular Backups: Customer data are backed up regularly, with redundant backups encrypted in transit and at rest

Software Patching: Software is patched and updated with the latest releases to ensure security

Technical Safeguards

Password and Authentication: Employees implement passwords consistent with current NIST guidance and use multifactor authentication when accessing systems storing customer data

Data Encryption: All customer data is encrypted in transit and at rest using up-to-date, industry-standard encryption methods

For more details, please refer to the Security Measures and Data Retention section of our Product Privacy Policy at edmentum.com/product-privacy-policy.

Section II.6: Notification

In the event that Edmentum discovers or is notified of a security incident, Edmentum will promptly investigate the matter, take steps to mitigate the potential impact on its customers, and promptly notify all affected customers. Edmentum will comply with all applicable laws in these efforts.

Section II.8: FERPA Compliance

Edmentum acknowledges and appreciates the importance of protecting student privacy and complying with all applicable data privacy laws, including FERPA. With respect to Edmentum's access to student education records in order to fulfill its responsibilities under a resulting contract, we understand that the District will designate Edmentum as a "school official" with a legitimate educational interest, as defined by FERPA with respect to those records.

We agree to operate under the direct control of the District regarding the use and maintenance of education records. We will use information contained within such records solely for the purpose of delivering the services. Edmentum maintains commercially reasonable administrative, technical, and physical safeguards to protect the confidentiality and security of student information, in accordance with applicable federal and state requirements.

Our FERPA statement can also be found at edmentum.com/ferpa.

For additional information, please review Edmentum's Product Privacy Policy at edmentum.com/product-privacy-policy.

Section III.5: Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices

Edmentum follows industry security best practices. We implement and maintain administrative, technical, and physical safeguards designed to help protect the confidentiality, integrity, and availability of Personal Information, including restrictions against unauthorized access to Personal Information by Edmentum employees or contractors and authorizing access to Personal Information by Edmentum employees or contractors only as necessary to fulfill their official duties.

Safeguards include:

Edmentum provides rule- and role-based data access where only personnel who require access to personally identifiable information in order to provide services to [clientabbreviation] are permitted access to such data

Edmentum employees are required to implement passwords consistent with current NIST guidance and utilize multifactor authentication when accessing systems storing customer data

Edmentum utilizes AWS data centers with robust, mature security controls

All customer data are encrypted in transit and at rest using up-to-date, industry-standard encryption methods

Software is patched and updated with patch releases

Privacy and security assessments are conducted on third parties requiring personally identifiable information to provide contracted services, and all such third parties are contractually obligated to comply with all applicable data protection and security requirements

Customer data are backed up regularly, and redundant backups are encrypted in transit and at rest

All Edmentum employees must pass background checks consistent with Edmentum requirements as a condition of hire

All Edmentum employees receive annual data protection training, inclusive of FERPA, COPPA, data security and [state] student data privacy law. Training may take the form of online learning modules, in-person training, written guidelines, and ongoing advice and counsel from internal and external advisors.

Please see the Security Measures and Data Retention section of our Product Privacy Policy at edmentum.com/product-privacy-policy. Our additional documentation, including our COPPA and FERPA statements, are thorough and should address any concerns. Our documents are public and reside on our website (links provided below).

Edmentum's Standard Terms - edmentum.com/standardterms

Edmentum's COPPA Customer Notice - edmentum.com/coppa

Edmentum's FERPA Statement - edmentum.com/ferpa

All Edmentum security policies are aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is reviewed at least annually. A third party has assessed our compliance with our existing set of security policies.

Our cloud hosting vendor (AWS) continuously maintains and certifies a variety of third-party compliance programs, including SOC 2 Type II and CSA STAR. Current reports can be made available upon request.

In addition to the NIST CSF, Edmentum's security policies use the following security frameworks for additional guidance:

ISO 27002 – Code of Practice for Information Security Management

Section 9 – Physical and Environmental Security

Section 8 – Human Resources Security

NIST Special Publication 800 Series Guidance

SP 800-53: Security Controls & Assessment Procedures

SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

SP 800-123: Guide to General Server Security

SP 800-88: Guidelines for Media Sanitization

SP 800-34: Contingency Planning Guide (Disaster Recovery)

Our last third-party penetration test of our products was conducted in December 2024 with follow-up retesting completed in March 2025. Our last external security assessment was completed in June 2025. See attached documentation. We would be happy to discuss further security reporting details in a closed session.

Section III.5: Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices

Edmentum has created a set of security policies that are based on the National Institute of Standards and Technology (NIST) Special Publication 800-53 control families and aligned to informative references prescribed in the identified subcategories of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (also referred to as NIST SP 800-53 and NIST CSF respectively).