EXHIBIT B

DATA PRIVACY ADDENDUM

Modeled after Version 2.0 of the Student Data Privacy Consortium's Model Contract

[PARTNER SCHOOL NAME]

and

T.L.P. EDUCATION

This **DATA PRIVACY ADDENDUM** (this "Data Privacy Addendum") is entered into by and between **PARTNER SCHOOL** (as defined in the related Program Agreement) and **T.L.P. Education** ("Summit Learning"), a California nonprofit public benefit corporation located in Redwood City, California, on the Effective Date (defined in the related Program Agreement) (each of Summit Learning and Partner School, a "Party" and together the "Parties"). The Parties agree to the terms as stated herein.

1. PURPOSE AND SCOPE

1.1 Purpose of Data Privacy Addendum. The purpose of this Data Privacy Addendum is to describe the duties and responsibilities to protect Student Data transmitted to Summit Learning from the Partner School and its Users pursuant to the Agreement, including compliance with all applicable federal and state privacy statutes. This Data Privacy Addendum, together with the Summit Learning Platform Terms of Service ("Terms of Service") and the Summit Learning Program Agreement ("Program Agreement") is the "Agreement."

1.2 Nature of Services Provided. Pursuant to and as fully described in the Program Agreement, Summit Learning has agreed to provide the Summit Learning Program (the "Program") and the Summit Learning Platform ("Platform") and any other products and services that the Program may provide now or in the future (collectively, the "Services").

1.3 Student Data to Be Provided. In order to provide the Services, Partner School and its Users shall provide the categories of Student Data described in the Schedule of Data, attached hereto as Exhibit A.

1.4 Data Privacy Addendum Definitions. Capitalized terms used herein and not otherwise defined in the Program Agreement or Terms of Service shall have the meanings set forth in Exhibit B hereto.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of Partner School. All Student Data or any other Pupil Records transmitted to Summit Learning pursuant to the Program Agreement is and will continue to be the property of and under the control of the Partner School, or the party who provided such Student Data or Pupil Records (such as the student or parent). The Parties hereto agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Agreement shall remain the exclusive property of the Partner School or the party who provided such Student Data or Pupil Records (such as the student or parent). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Summit Learning from Partner School, Summit Learning shall be considered a School Official, under the control and direction of the Partner Schools as it pertains to the use of Education Records notwithstanding the above.

2.2 Parent Access. As set forth in applicable law, Partner School shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Pupil Records and correct erroneous information, consistent with the functionality of Services. Summit Learning shall respond in a reasonably timely manner to the Partner School's request for Personally Identifiable Information contained in a student's Pupil Records held by Summit Learning to view or correct as necessary. In the event that a parent/legal guardian of a student or other individual contacts Summit Learning to review any of the Pupil Records or Student Data accessed pursuant to the Services, Summit Learning shall refer the parent or individual to the Partner School. In such event, Partner School shall follow the necessary and proper procedures regarding the requested information.

2.3 Third Party Request. Should a Third Party, excluding a Service Provider, including law enforcement and government entities, contact Summit Learning with a request for Student Data held by Summit Learning pursuant to the Services, Summit Learning shall redirect the Third Party to request the Student Data directly from the Partner School. Summit Learning shall notify the Partner School in advance of a compelled disclosure to a Third Party unless legally prohibited.

2.4 No Unauthorized Use. Summit Learning shall not use Personally Identifiable Information from Student Data or in a Pupil Record for any purpose other than as explicitly specified in the Agreement.

2.5 Service Providers. Summit Learning shall enter into written agreements with all Service Providers performing functions pursuant to the Agreement, whereby the Service Providers agree to protect Student Data in a manner consistent with the terms of this Data Privacy Addendum.

3. DUTIES OF PARTNER SCHOOL

3.1 Provide Data In Compliance With FERPA. Partner School shall provide Student Data for the purposes of the Agreement in compliance with any applicable state or federal laws and regulations (including FERPA) pertaining to data privacy and security applicable to Partner School. If Partner School provides Education Records to Summit Learning, Partner School represents, warrants and covenants to Summit Learning, as applicable, that Partner School has:

a. complied with all applicable provisions of FERPA relating to disclosures to school officials with a legitimate educational interest, including, without limitation, informing parents in their annual notification of FERPA rights that the Partner School defines "school official" to include service providers and defines "legitimate educational interest" to include services such as the type provided by Summit Learning; or

b. obtained all necessary parental or eligible student written consent to share the Student Data with Summit Learning, in each case, solely to enable Summit Learning's operation of the Services.

Partner School represents, warrants, and covenants to Summit Learning that it shall not provide information to Summit Learning from any student or parent/legal guardian that has opted out of the disclosure of Directory Information. Summit Learning depends on Partner School to ensure that the Partner School is complying with the FERPA provisions regarding the disclosure of any student information that will be shared with Summit Learning.

3.2 Reasonable Precautions. Partner School shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted data in accordance with the Agreement and applicable law.

3.3 Unauthorized Access Notification. Partner School shall notify Summit Learning immediately of any known or suspected unauthorized use or access of the Platform or Student Data. Partner School will assist Summit Learning in any efforts by Summit Learning to investigate and respond to any unauthorized use or access.

3.4 Partner School Representative. The Principal Contact Person designated in the Program Agreement shall serve as the representative of the Partner School for the coordination and fulfillment of the duties of this Data Privacy Addendum.

4. DUTIES OF SUMMIT LEARNING

4.1 Privacy Compliance. Summit Learning shall comply with all applicable state laws of the jurisdiction in which Partner School is located and federal laws and regulations pertaining to data privacy and security, applicable to Summit Learning in providing the Services to Partner School.

4.2 Authorized Use. The Student Data shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Agreement and/or as otherwise legally permissible. The foregoing limitation does not apply to any De-Identified Data.

4.3 Employee Obligation. Summit Learning shall require all employees and agents who have access to Student Data to comply with all applicable laws with respect to the Student Data shared under the Service Agreement. Summit Learning agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure. Summit Learning shall not disclose any Student Data obtained under the Agreement in a manner that directly identifies an individual student to any other entity except as authorized by the Agreement. Summit Learning will not Sell Student Data. Additionally, Summit Learning will not trade or transfer Student Data to any third parties, except with the prior written consent of the Partner School. The prohibition on disclosing, trading, or transferring Student Data does not apply to the access to or disclosure of Student Data to (a) Partner School, (b) to authorized Licensed Users, including parents or legal guardians, (c) as permitted by law or (d) to Service Providers, in connection with operating or improving the Services. The list of Summit Learning's current Service Providers can be accessed through the Privacy Policy (which may be updated from time to time).

4.5 De-Identified Data. De-Identified Data may be used for any lawful purpose including, but not limited to, operating and improving the Services. Summit Learning's use of such De-Identified Data shall survive termination of this Data Privacy Addendum or any request by Partner School to return or destroy Student Data. Summit Learning agrees not to attempt or have any third party attempt to re-identify De-Identified Data.

4.6 Disposition of Student Data. Summit Learning shall, at Partner School's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If a written request is received from a Partner School, Summit Learning shall transfer said Personally Identifiable Information contained in Student Data to Partner School or Partner School's designee within sixty (60) days of the date of such written request by Partner School, or as required by law, and according to a schedule and procedure as Summit Learning and the Partner School may reasonably agree. If no written request is received, Summit Learning shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or de-identified. Summit Learning shall provide written notification to the

Partner School when the Personally Identifiable Information contained in the Student Data has been disposed. The duty to dispose of Student Data shall not extend to De-Identified Data.

4.7 Advertising Prohibition. Summit Learning shall not use Personally Identifiable Information contained in Student Data to (a) serve Behaviorally Targeted Advertising to students or families/guardians; or (b) develop a profile of a student for any commercial purpose other than providing the Services to Partner School or as set forth in the Service Agreement. Summit Learning shall not use or disclose Personally Identifiable Information contained in Student Data for Third-Party Advertising.

5. DATA PROVISIONS

5.1 Data Security. Summit Learning agrees to employ administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, and use or acquisition by an unauthorized person, including when transmitting and storing such information. The general security duties of Summit Learning are set forth below. Additional detail regarding Summit Learning's security programs and measures are listed in Exhibit C hereto. These measures shall include, but are not limited to:

- **Passwords and Employee Access**. Summit Learning shall use commercially reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Summit Learning shall only provide access to Student Data to employees, contractors or Service Providers that are performing the Services. Summit Learning shall conduct criminal background checks of employees prior to providing access to Student Data and prohibit access to Student Data by any person with criminal or other relevant unsatisfactory information that presents an unreasonable risk to Partner School or its Users.

- **Destruction of Student Data**. Summit Learning shall destroy or delete all Personally Identifiable Information contained in Student Data obtained under the Agreement as set forth in Section 4.6 hereof.

- **Security Protocols**. Both Parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data as described in Exhibit C, including ensuring that Student Data may only be viewed or accessed by individuals or entities legally allowed to do so. The foregoing does not limit the ability of Summit Learning to allow any necessary Service Providers to view or access data as set forth in Section 4.4 hereof. Summit Learning shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computing environment and shall not copy, reproduce, or transmit data obtained pursuant to the Agreement, except as necessary to fulfill the purpose of data requests by Partner School or as otherwise set forth in the Agreement.

- **Employee Training**. Summit Learning shall provide periodic security training to those of its employees who operate or have access to the Platform.

- **Security Technology**. When the Services are accessed using a supported web browser, Summit Learning will ensure that Secure Socket Layer ("SSL"), or equivalent technology that protects information, using both server authentication and data encryption is used to help ensure that Student Data is transmitted in a safe and secure manner. Summit Learning shall host data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards.

- **Security Coordinator**. Summit Learning shall provide the name and contact information of Summit Learning's security coordinator for the Student Data received pursuant to the Agreement that Partner School may contact if there are any security questions or concerns ("Security Coordinator"). Summit Learning's Security Coordinator shall be as set forth in Exhibit C.

- **Service Provider Bound**. Summit Learning shall enter into written agreements whereby Service Providers agree to secure and protect Student Data in a manner consistent with the terms of this Section 5. Summit Learning shall periodically conduct or review compliance monitoring and assessments of Service Providers to determine their compliance with this Section 5.

5.2 Data Breach.

a. In the event that Summit Learning becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to Student Data (a "Security Incident"), Summit Learning shall provide notice to the Partner School as required by the applicable state law (each, a "Security Incident Notification").

b. Unless otherwise required by the applicable law, the Security Incident Notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

c. The Security Incident Notification described above in Section 5.2(a) shall include such information required by the applicable state law and the following information:

(i) The name and contact information of the reporting Partner School subject to this section.

(ii) A list of the types of Personally Identifiable Information that were or are reasonably believed to have been the subject of the Security Incident.

(iii) If the information is known at the time the Security Incident Notification is provided, then either (1) the date of the Security Incident, (2) the estimated date of the Security Incident, or (3) the date range within which the Security Incident occurred. The Security Incident Notification shall also include the date of the notice.

(iv) Whether, to the knowledge of Summit Learning at the time notice is provided, the notification was delayed as a result of a law enforcement investigation or request.

(v) A general description of the Security Incident, if that information is possible to determine at the time the notice is provided.

d. At Summit Learning's discretion, the Security Incident Notification may also include any of the following:

(i) Information about what Summit Learning has done to protect individuals whose Personally Identifiable Information has been breached by the Security Incident.

(ii) Advice on steps that the person whose Personally Identifiable Information has been breached may take to protect himself or herself.

e. To the extent required by the applicable state law, Summit Learning shall notify the affected parent, legal guardian or eligible pupil of the Security Incident, which shall include as applicable the information listed in subsections (c) and (d), above.

5. MISCELLANEOUS

5.1 Term. Except as otherwise stated herein, Summit Learning shall be bound by this Data Privacy Addendum for the duration of the Program Agreement or as required by law.

5.2 Termination. In the event that either Party seeks to terminate this Data Privacy Addendum, they may do so by terminating the Program Agreement as set forth therein.

5.3 Effect of Termination Survival. If the Agreement is terminated, Summit Learning shall dispose of all of Partner School's Personally Identifiable Information contained in Student Data pursuant to Section 4.6.

5.4 Priority of Agreements. This Data Privacy Addendum shall govern the treatment of Student Data. With respect to the treatment of Student Data, in the event there is conflict between the terms of this Data Privacy Addendum and the Program Agreement, the Terms of Service, or any other agreement between the Partner School and Summit Learning, the terms of this Data Privacy Addendum shall apply and take precedence. Except as described in this paragraph, all other provisions of the Program Agreement shall remain in effect.

5.5 Notice. All notices or other communication required or permitted to be given hereunder must be sent to Partner School or Summit Learning, as applicable, as provided in the Program Agreement.

EXHIBIT A

SCHEDULE OF DATA

Category of Data	**Elements**	**"X" Indicates Category is Used by Summit Learning**
Application Technology Meta Data	IP addresses of users, use of cookies etc.	
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test data (NWEA MAP, SBAC, AP, IB, etc)	X
	Observation data	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
	Other attendance: ● Suspensions/expulsions	
Communications	Online communications that are captured (emails, blog entries)	

Conduct	Conduct or behavioral data	
Demographics	Date of birth	X
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify: ● Socioeconomic status	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify: ● Clever ID# ● SIS ID#	X
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X

Parent/Guardian Name	First and/or last	X
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts	
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/app assigned student ID number	X
	Student app username	
	Student app passwords	
Student Name	First and/or last	X
Student In App Performance	Program/application performance (reading program-student reads below grade level)	X

Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Anonymous student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	X
	Other student work data -Please specify:	
Student Outcome Information	Student outcome information (grade level promotion and matriculation, AP and IB test information, college admission test scores, college eligibility and acceptance, and employment)	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please specify:	

Other	Please list each additional data element used, stored or collected by your application: ● teacher feedback on coursework ● teacher curricula and notes and feedback to or about students ● Teacher and parent answers to surveys about the Services or curricula; and feedback, suggestions, questions, and ideas submitted to Summit Learning from parents/legal guardians, teachers or school administrators or officials ● mentor observations	X

EXHIBIT B

DEFINITIONS

"Agreement" means, collectively, the Terms of Service and the Program Agreement.

"Behaviorally Targeted Advertising" means presenting an advertisement to a User where the selection of the advertisement is based on Student Data or Pupil Generated Content or inferred over time from the usage of Summit Learning's website, online service or mobile application by such student or the retention of such student's online activities or requests over time and across non-affiliate website for the purpose of targeting subsequent advertising.

"De-Identified Data" is information that has all direct and indirect personal identifiers removed such that the data cannot reasonably be used to identify or contact a student. This includes, but is not limited to, persistent unique identifiers, name, ID numbers, date of birth, and school ID.

"Directory Information" shall have the meaning therefor under FERPA cited as 20 U.S.C. 1232g(a)(5)(A).

"Education Records" shall have the meaning therefor under FERPA cited as 20 U.S.C. 1232g(a)(4).

"Indirect Identifiers" means any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. When anonymous or non-personal information is directly or indirectly linked with personal information, this anonymous or non-personal information is also treated as personal information. Persistent identifier that are not anonymized, de-identified or aggregated are personal information.

"Licensed User" means a teacher, employee, official, agent of a Partner School or the parent or legal guardian of a Student User.

"Personally Identifiable Information" or ***"PII***" means data that can be used to identify or contact a particular individual, such as the individual's name, email address or billing information, or other data which can be reasonably linked to that data or to that individual's specific computer or device. PII includes, without limitation, at least the following: first and last name, home address, telephone number, email address, discipline records, test results, special education data, juvenile dependency records grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, and videos.

"Pupil Generated Content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

"Pupil Records" means both of the following: (1) any information that directly relates to a pupil that is maintained by Partner School and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other employee of the Partner School.

"School Official" means, for the purposes of this Data Privacy Addendum and pursuant to CFR 99.31 (B), a contractor that: (1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use and maintenance of Education Records; and (3) is subject to CFR 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

"***Sell***" consistent with the Student Online Privacy Protection Act (SOPIPA) and the Student Privacy Pledge, does not include or apply to the purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the personal information in a manner consistent with the Education Privacy Principles with respect to the previously acquired personal information.

"Service Provider", means, for the purposes of the Data Privacy Addendum, a party other than Partner School or Summit Learning or Users, who Summit Learning uses for data collection, analytics, storage, or other service to operate and/or improve the Platform, and who has access to PII.

"Student Data" means any data, whether gathered by Summit Learning or provided by Partner School or its users, students, or students' parents/guardians, that is directly related to a Partner School student including, but not limited to, information in the student's Educational Record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Data Privacy Addendum. Student Data as specified in Exhibit A is confirmed to be collected or processed by Summit Learning pursuant to the Services. Student Data shall not constitute that information that has been anonymized, De-Identified Data, or anonymous usage data regarding a student's use of the Services.

"Student User" means a student enrolled at the Partner School with an account on the Platform.

"***Summit Learning Website***" means the website for the Program presently located at www.summitlearning.org, which URL is subject to change from time to time.

"***Terms of Service"*** means the Summit Learning Platform Terms of Service between each Partner School and Summit Learning, located at [cdn.summitlearning.org/marketing/privacy_center/partner_terms_of_service.pdf].

"Third Party" means, for purposes of this Data Privacy Addendum, any person other than Summit Learning, Partner School, a User, or a Service Provider.

"Third-Party Advertising" means direct advertising of third-parties and their products or services on our Services (e.g., such as when an advertiser would bid to place an advertisement directly on a platform). Summit Learning does not allow third parties to advertise directly on its Services in user logged in areas of the Services, nor does Summit Learning sell advertising space in logged in areas on the Platform. Summit Learning also does not use third-party ad servers (such as Google AdWords or AdSense) in user logged in areas of the Platform.

"Users" means, collectively, Student Users and Licensed Users.

EXHIBIT C

DATA SECURITY REQUIREMENTS

Definitions

Event is any observable occurrence in a system or network

Site Event (SEV) is an event impacting platform functionality and/or availability requiring remediation and/or investigation.

Sensitive Data is defined to include:

- Personally Identifiable Information contained in Student Data as previously defined in Exhibit B
- Personally Identifiable Information (as defined in Exhibit B) of teachers, parents, administrative staff or site admin of the Services
- Any login credentials, passwords, user authentication tokens or security devices used for Platform or infrastructure access

Security Coordinator – [TBD]

Security Incident is an incident where Summit Learning becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to Sensitive Data.

On-Call means the Summit Learning personnel tasked with monitoring system alerts and responding to incidents. Summit Learning will use reasonable efforts to have an engineer on-call at any given moment.

Platform is as defined in this Data Privacy Addendum.

System Alert means an automated notification triggered by specified Platform system conditions.

Security

Security Controls: Summit Learning shall be responsible for the implementation and maintenance of controls that align with the Center for Internet Security Critical Security Controls as well as other industry best practices for education technology security. This includes appropriate administrative, physical, and technical safeguards to protect Sensitive Data from unauthorized access, disclosure, and use. Specifically, Summit Learning shall:

- Implement effective identification and authentication methods using multi-factor authentication (MFA) with strong password complexity and a mobile security application based on two-factor authentication (2FA).

- Employ strong encryption technologies to securely transmit and store all sensitive data. These procedures will include; data-in-transit secured with encrypted transportation protocols (HTTPS, SSL/TLS). When at rest sensitive data will be encrypted using one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256) to protect sensitive data.

- Create a highly effective data backup and recovery capability that ensures a timely and accurate restoration of all Sensitive Data. The capability will minimize the amount of Sensitive Data loss in the event of some form of catastrophic failure. For further protection, those backups will be encrypted and are stored in a different region.

- Adopt and maintain a secure software development lifecycle (Secure SDLC) with industry recognized security practices to establish secure application(s), network, and infrastructure architectures. The Secure SDLC will also incorporate security assurance activities such as penetration testing, code reviews and architecture analysis as essential functions of the development effort.

Security Incident and Event Monitoring:

- Maintain platform availability through event monitoring and response procedures for all Site Events, automated Site Event notifications, handling and reporting by On-Call personnel.

- Guard against Security Incidents and maintain incident response policies, plans and procedures focused on timely and effective incident response. These procedures shall be made to Partner School upon request.

- Employ industry leading intrusion detection measures focused on monitoring and identifying deviations in normal network, user, and platform behaviors. Employ trained incident handling professionals with experience in Security Incident and Event Monitoring (SIEM), Configuration Auditing and Threat Intelligence.

Security Governance:

- Develop and conduct security risk assessments focused on the identification and remediation of risks collected through a well defined assessment process.

- Employ oversight and accountability procedures for risk management and remediation.