STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, ILLINOIS, IOWA, MISSOURI, NEBRASKA, NEW HAMPSHIRE, NEW JERSEY, NEW YORK, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA

MA-ME-IL-IA-MO-NE-NH-NJ-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Lancaster City School District

and

August Schools, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Lancaster City School District, located at 2780 Coonpath Road NE, Lancaster, OH 43130 USA (the "**Local Education Agency**" or "**LEA**") and August Schools, Inc., located at 337 W 37th St Suite 720 New York, NY 10018 USA (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.
NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   √ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Peter Russell Title: CEO

Address: 336 West 37th Street

Phone: 781-706-9945 Email: pete@augustschools.com

The designated representative for the LEA for this DPA is:

Sarah Daugherty, Supervisor Educational Technology
2780 Coonpath Road NE, Lancaster, OH 43130
740-687-7388 s_daugherty@lcsschools.net

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Lancaster City School District

By: Sarah A Daugherty
Sarah A Daugherty (May 9, 2025 09:21 EDT) Date: 05/09/2025

Printed Name: Sarah A Daugherty Title/Position: Supervisor Educational Technology

August Schools, Inc.

By: Date: 5/5/2025

Printed Name: Peter Russell Title/Position: CEO

STANDARD CLAUSES
Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

   (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

      i. The name and contact information of the reporting LEA subject to this section.
      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
      iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
      v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

   (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

   (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

   (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. Authority. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. Waiver. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT “A”
DESCRIPTION OF SERVICES

August, comprehensive health & wellness software for schools.

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	X
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify:	
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:	
Parent/Guardian Contact Information	Address	X
	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

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts/ health data	X
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/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 (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
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	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT “D”
DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[**Insert categories of data here**]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]

4. Signature

____ ___________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ ______________

Authorized Representative of Company Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
□	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
□	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
□	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☑	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
□	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
□	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT “G”
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep’t of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit “C” includes the name of the student’s family members, the student’s place of birth, the student’s mother’s maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit “C” includes information that:
    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider’s website, service or application for kindergarten to grade 12 school purposes;
    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider’s website, service or application for kindergarten to grade 12 school purposes; or
    c. Is gathered by the Provider through the operation of the Provider’s website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."

2. Replace Notices with: "Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid."

3. In Article II, Section 1, add: "Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest."

4. In Article II, Section 2, replace "forty-five (45)" with "five (5)". Add the following sentence: "In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA."

5. In Article II, Section 4, replace it with the following: "In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure."

6. In Article II, Section 5, add: "By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1)."

7. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

8. In Article IV, Section 6, replace the whole section with:

   The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

   If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

   Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

10. In Article IV, Section 7, add "renting," after "using."

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States.

12. In Article V, Section 4, add the following: "'Security Breach' does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure."

13. In Article V, Section 4(1) add the following:

    vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

    vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

14. In Article V, Section 4, add a section (6) which states:

    In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

    a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

    b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

    c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

    as a result of the security breach; and

    d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

15. Replace Article VII, Section 1 with: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."

16. In Exhibit C, add to the definition of Student Data, the following: "Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", “student temporary record” or “student permanent record” as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) “records” as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) “personal information” as defined in Section 530/5 of PIPA.”

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: “The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first.”

18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

20. **Student and Parent Access.** Access by students or parents/guardians to the Provider’s programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

22. The Provider will not collect social security numbers.

EXHIBIT "G"
Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Iowa;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

3. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.

4. In Exhibit "C" add to the definition of "Student Data" significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT "G"
Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
    a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
        i. Details of the incident, including when it occurred and when it was discovered;
        ii. The type of personal information that was obtained as a result of the breach; and
        iii. The contact person for Provider who has more information about the incident.
    b. "*Breach*" shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
    c. "*Personal information*" is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
        i. Social Security Number;
        ii. Driver's license number or other unique identification number created or collected by a government body;
        iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        v. Medical information; or
        vi. Health insurance information.

EXHIBIT "G"
Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Nebraska;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article II, Section 5, add, "Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices."
2. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
3. In Article IV, Section 4, replace: "Provider will not Sell Student Data to any third party" with "Provider will not Sell or rent Student Data to any third party.
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Jersey;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

EXHIBIT "G"
Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:

    a. Location-tracking features of a school-issued device;
    b. Audio or visual receiving, transmitting or recording features of a school-issued device;
    c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

    i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:

    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general

    ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

    iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq*., T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq*., T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq*.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
    a. Political affiliation;
    b. Religion;
    c. Voting history; and
    d. Firearms ownership

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." **"**Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…"
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

    (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

    (2) Limit unsuccessful logon attempts;

    (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

    (4) Authorize wireless access prior to allowing such connections;

    (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

    (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

    (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

    (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

    (9) Enforce a minimum password complexity and change of characters when new passwords are created;

    (10)Perform maintenance on organizational systems;

    (11)Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

    (12)Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

    (13)Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

    (14)Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

    (15)Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

    (16)Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17)Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18)Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19)Protect the confidentiality of Student Data and Teacher Data at rest;

(20)Identify, report, and correct system flaws in a timely manner;

(21)Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22)Monitor system security alerts and advisories and take action in response; and

(23)Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

    i. The estimated number of students and teachers affected by the breach, if any.

9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.

10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"
New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.

4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a)implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

    Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".**

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

    i. The name and contact information of the reporting LEA subject to this section.

    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

    iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

    iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

    v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

    vi. The number of records affected, if known; and

    vii. A description of the investigation undertaken so far; and

    viii. The name of a point of contact for Provider.

    (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

    (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

    (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.

    (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

    (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:
    - **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
    - **APPR Data**: Personally Identifiable Information from the records of an Educational Agency 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
    - **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
    - **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
    - **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
    - **Release:** Shall have the same meaning as Disclose
    - **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
    - **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

    -

Exhibit “J”

LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Exhibit "K"

Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at

See Attached
____

August Schools

Information Security Policy

Purpose and Scope

This Information Security Policy addresses the information security policy topics and requirements which maintain the security, confidentiality, integrity, and availability of August Schools applications, systems, infrastructure, and data. The topics and requirements called out in this policy should be continuously improved upon to maintain a secure information security posture. From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including compliance with applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all August Schools policies and plans upon starting and at least annually.

Information Security Communication

Please contact developers@augustschools.com if you have any questions about the August Schools information security program.

People Security

Background Check

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

Confidentiality

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

Security Awareness Training

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

Secure Coding

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

Physical Security

Clear Desk

August Schools personnel are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area when it is unattended. This requirement extends to both remote and in-office work.

August Schools personnel must remove hardcopies of sensitive information from desks and lock the information in a drawer when desks are unoccupied and at the end of the work day. Keys used to access sensitive information must not be left at an unattended desk.

Clear Screen

August Schools employees and contractors must be aware of their surroundings at all times and ensure that no unauthorized individuals have access to see or hear sensitive information. All mobile and desktop devices must be locked when unoccupied. Session time-outs and lockouts are enforced through technical controls for all systems containing covered information.

All devices containing sensitive information, including mobile devices, shall be configured to automatically lock after a period of inactivity (e.g. screen saver).

Remote Work

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

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

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

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

System Access Security

August Schools adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of privileges or changes to privileges and access permissions are documented and require approval by an authorized manager. System access is revoked immediately upon termination or resignation.

Account Audits

Audits of access and privileges to sensitive August Schools applications, infrastructure, systems, and data are performed regularly and reviewed by authorized personnel.

Password Security

Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with anyone. Where possible, all user and system accounts must invoke password complexity requirements specified in the Access Control and Termination Policy. All accounts must use unique passwords not shared with any other accounts.

Rotation Requirements

If a password is suspected to be compromised, the password should be rotated immediately and the security team should be immediately notified.

Storing Passwords

Passwords must only be stored using a August Schools approved password manager. August Schools does not hard code passwords or embed credentials in static code.

Asset Security

August Schools maintains a Configuration and Asset Management Policy designed to track and set configuration standards to protect August Schools devices, networks, systems, and data. In compliance with such policy, August Schools may provide team members laptops or other devices to perform their job duties effectively.

Data Management

August Schools stores and disposes of sensitive data, in a manner that; reasonably safeguards the confidentiality of the data; protects against the unauthorized use or disclosure of the data; and renders the data secure or appropriately destroyed. Data entered into August Schools applications must be validated where possible to ensure quality of information processed and to mitigate the impacts of web-based attacks on the systems.

Data Classification

August Schools defines the handling and classification of data in the Data Classification Policy.

Data Retention and Disposal Policy

The time periods for which August Schools must retain customer data depends on the purpose for which it is used. August Schools retains customer data as long as an account is active, as needed to provide services to the customer, or in accordance with the agreement(s) between August Schools and the customer. An exemption to this policy would include if August Schools is required by law to dispose of data earlier or keep data longer. August Schools may retain and use customer data to comply with its legal obligations, resolve disputes, and enforce agreements.

Except as otherwise set forth in the August Schools policies, August Schools also disposes of customer data when requested by customers.

August Schools maintains a sanitization process that is designed to prevent sensitive data from being exposed to unauthorized individuals. August Schools hosting and service providers are responsible for ensuring the removal of data from disks allocated to August Schools use before they are repurposed or destroyed.

Change and Development Management

To protect against unauthorized changes and the introduction of malicious code, August Schools maintains a Change Management Policy with change management procedures that address the types of changes, required documentation, required review and/or approvals, and emergency changes. Changes to August Schools production infrastructure, systems, and applications must be documented, tested, and approved before deployment.

Vulnerability and Patch Management

August Schools uses a proactive vulnerability and patch management process that prioritizes and implements patches based on classification. Such classification may include whether the severity is security-related or based on other additional factors. August Schools schedules third party penetration tests and/or performs internal assessments at least annually.

If you believe you have discovered a vulnerability, please email developers@augustschools.com and August Schools will aim to address the vulnerability, if confirmed, as soon as possible.

Environment Separation

As necessary, August Schools maintains requirements and controls for the separation of development and production environments.

Source Code

August Schools controlled directories or repositories containing source code are secured from unauthorized access.

Logging and Monitoring

August Schools collects & monitors audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services, as well as IAM user and admin activities. August Schools manages logging solution(s) and/or SIEM tool(s) to collect event information of the aforementioned systems and activities. August Schools implements filters, parameters, and alarms to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts.

Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. August Schools utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.

When events and alerts are generated from monitoring solutions and mechanisms, August Schools correlates those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy and Change Management Policy.

Additionally, August Schools utilizes threat detection solution(s) to actively monitor and alert on network and application-based threats.

Business Continuity and Disaster Recovery

August Schools maintains a plan for continuous business operations if facilities, infrastructure or systems fail. The plan is tested, reviewed and updated at least annually.

Backup Policy

Backups are performed according to appropriate backup schedules to ensure critical systems, records, and configurations can be recovered in the event of a disaster or media failure.

Security Incident Response

August Schools maintains a plan that defines responsibilities, detection, and corrective actions during a security incident. The plan will be executed following the discovery of an incident such as system compromise, or unintended/unauthorized acquisition, access, use or release of non-public information. The plan is tested, reviewed and updated at least annually.

August Schools utilizes various monitoring and surveillance tools to detect security threats and incidents. Early detection and response can mitigate damages and minimize further risk to August Schools.

A message should be sent to developers@augustschools.com if you believe there may be a security incident or threat.

Risk Management

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

Vendor Management

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

Privacy

Personal Data

August Schools personnel must treat personal data with appropriate security and handling and accommodate data subject requests, as required by applicable laws and regulations. No unauthorized personnel should have access to personal data.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Risk Assessment and Treatment Policy

Purpose and Scope

This Risk Assessment Policy guides August Schools in performing risk assessments to account for threats, vulnerabilities, likelihood, and impact to August Schools assets, team members, customers, vendors, suppliers, and partners based upon the August Schools services considering security, availability, integrity, and confidentiality needs.

From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all August Schools policies and plans.

Risk Assessment Framework

August Schools conducts assessments of risk, which includes the likelihood and impact of risk from the unauthorized access, use, disclosure, disruption, modification and/or destruction of August Schools systems, applications, infrastructure, and data pertaining to August Schools's environment.

The risk assessment process is coordinated by , which includes the identification and evaluation of assets, threats, and vulnerabilities. Assets should be identified by respective asset owners, and the assessment of threats as well as the likelihood and criticality of potential vulnerability exploitation, should be performed by respective risk owners.

A risk assessment may include a review of:

- internal controls including policies, procedures, business processes, and technical security safeguards
- human resource practices related to hiring, termination, and discipline procedures
- facility controls
- exposure to theft
- systems and applications used to collect, store, process or transmit confidential data

Risk Assessment Process

The risk assessment process should align with the following steps:

(1) Scoping Assets

In order to begin the risk assessment process, the assessor should determine the scope of what needs to be covered in the assessment. An effective assessment should be limited in its scope to the applicable assets.

Such scoping activities may include:

- Review inventory of critical system assets (hardware, software, facilities, etc.)
- Identification of data owners (electronic and non-electronic data)
- Identification of workforce members with access to stored data by hardware/software
- Mapping data flow through August Schools and vendor systems
- Conducting an inventory of data storage (including non-electronic data)
- System characterization (e.g. essential, non-essential)

(2) Identifying Threats and Vulnerabilities

Vulnerabilities and the related threats, both internal and external, to August Schools operations (including, but not limited to, its mission, functions, image, or reputation), assets, information, and individuals may be identified and documented as part of the August Schools risk assessment.

Threat

A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [SP 800-30 Rev.1]

Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [SP 800-30 Rev.1]

Vulnerabilities may be identified by the following:

- Vulnerability scanning and penetration tests
- Security control monitoring technologies
- Detected patterns, heuristics, or specific activities that indicate process gaps or technical weaknesses
- Internal and external audits
- External security vulnerabilities databases (e.g. CVE database) and reports

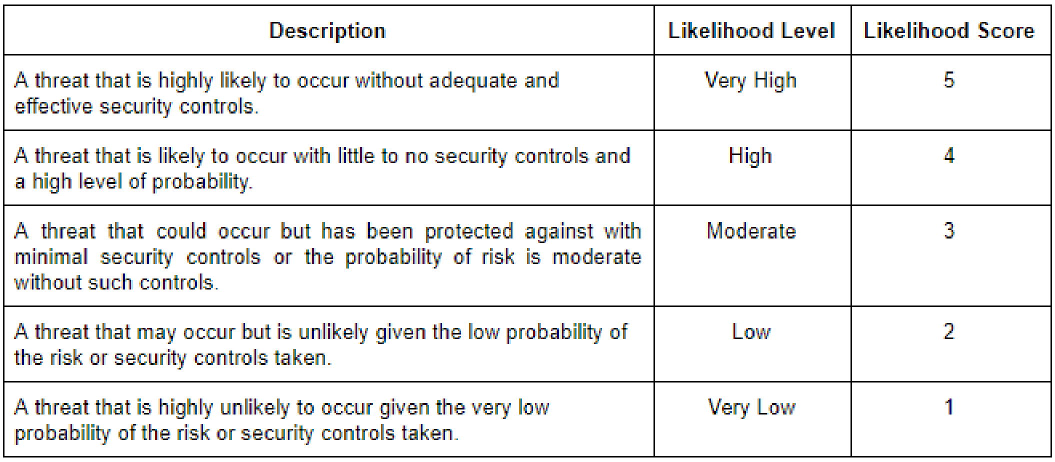
(3) Analyze Risks

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner. Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

Initial (or Inherent) Risk Likelihood Determination

How likely will an identified threat or vulnerability impact the organization given existing security controls?

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).

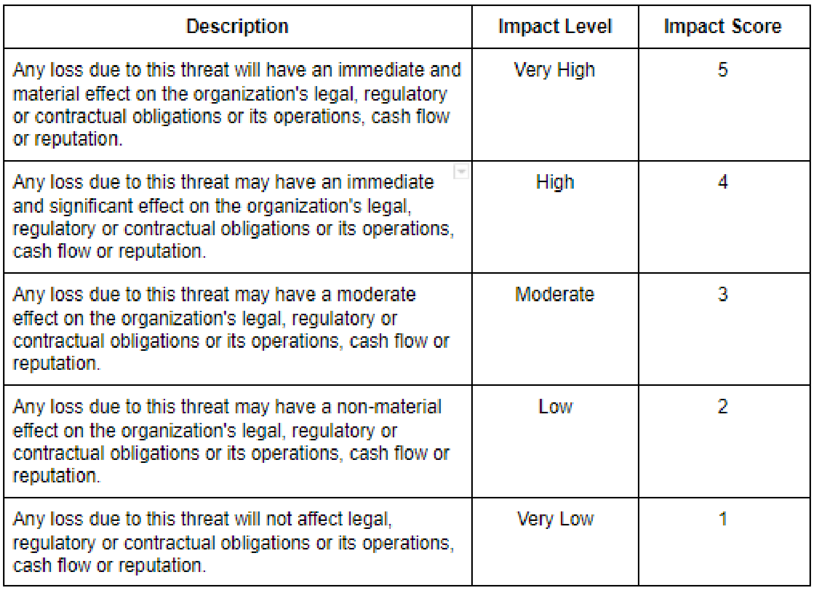


Description	Likelihood Level	Likelihood Score
A threat that is highly likely to occur without adequate and effective security controls.	Very High	5
A threat that is likely to occur with little to no security controls and a high level of probability.	High	4
A threat that could occur but has been protected against with minimal security controls or the probability of risk is moderate without such controls.	Moderate	3
A threat that may occur but is unlikely given the low probability of the risk or security controls taken.	Low	2
A threat that is highly unlikely to occur given the very low probability of the risk or security controls taken.	Very Low	1

Initial (or Inherent) Risk Impact Analysis

What is the cost if an identified threat or vulnerability impacts the organization given existing security controls?

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.



Description	Impact Level	Impact Score
Any loss due to this threat will have an immediate and material effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Very High	5
Any loss due to this threat may have an immediate and significant effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	High	4
Any loss due to this threat may have a moderate effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Moderate	3
Any loss due to this threat may have a non-material effect on the organization's legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Low	2
Any loss due to this threat will not affect legal, regulatory or contractual obligations or its operations, cash flow or reputation.	Very Low	1

Initial (or Inherent) Risk Score

After the likelihood and impact analysis, a risk determination should be made. Risk is a function of the likelihood of a threat event’s occurrence and potential adverse impact should the event occur. In order to determine risk score, August Schools multiplies impact * likelihood. The higher number equates to higher potential risk.

(4) Risk Treatment

For any critical or high risks identified during the risk assessment process, August Schools will immediately develop action plans to mitigate those risks which could include patching of vulnerable systems and/or applying other control activities. Risk responses shall consider obligations such as contractual agreements, laws, regulations and standards. The following items will have to be amended or defined based on discovered risk: IT policy and strategies, risk strategies, cost-effectiveness, type of protection, threats covered, risk levels, existing alternatives, and additional benefits derived from the treatment.

There are three possible responses to risk:

Risk Mitigation

Risk mitigation is the implementation of safeguards and countermeasures to reduce or eliminate vulnerabilities or threats.

Risk Transfer

Risk transfer is the placement of the cost of loss a risk represents onto another entity. This is accomplished by purchasing insurance and/or outsourcing.

Risk Acceptance

Acceptance of risk is the valuation by August Schools that the cost/benefit analysis of a possible safeguard and the determination that the cost of the countermeasure greatly outweighs the possible cost of loss due to a risk. Values under 3 are acceptable risks, while values 3+ are unacceptable risks. Unacceptable risks must be treated. On behalf of the risk owners, Senior Management will accept all residual risks.

(5) Calculate Residual Risks

Based on risk treatment decisions, plans, and net new compensating controls to be implemented, residual risks must be calculated, reassessing the respective initial risks' likelihoods and impacts.

(6) Reporting

or a designee is responsible for creating the risk assessment and treatment report and delivering results to senior management and other applicable personnel. This report shall include risk responses and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost. All risk assessment reports must be documented and retained for a minimum of three years.

Unacceptable risks should be appropriately remediated or mitigated in accordance with the Change Management Policy and Vulnerability Management Policy.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

or a designee is responsible for overseeing the successful completion of the risk assessment. Such risk assessments must be conducted at least annually or whenever there are significant changes to August Schools, its systems, or other conditions that may impact the security of August Schools such as the failure of a mission critical vendor or a security breach.

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

This document is maintained by .

August Schools

Vendor Management Policy

Purpose and Scope

This Vendor Management Policy guides August Schools in the execution, management, and termination of vendor and other third party agreements. From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets utilized by employees and contractors acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All employees and contractors are required to read, accept and follow all August Schools policies and plans.

Vendor Management Process

August Schools will maintain a profile of all August Schools vendors that includes the vendor, their executed agreements, and the appropriate reviews and documentation of such vendors in accordance with this policy. Such reviews will be based on the risk level of each vendor.

In order for August Schools to contract with a new vendor, the following steps should be taken in advance:

(1) Request for New Vendor

If an employee or contractor of August Schools wishes to use the free or paid services of a new vendor, a request for such use must be submitted to your manager. As part of the submission, the request may include a completed August Schools new vendor request form.

(2) Risk Assessment and Due Diligence

Before entering into a contract and granting access to August Schools systems, a risk assessment and appropriate due diligence should be performed to determine the possible risk and impact to August Schools. Vendors should be separated into three risk tiers: High, Medium and Low. Risk assessments must occur for all high risk vendors.

In particular, a vendor security assessment should include answers to at least the following:

- Is the vendor of a customer-facing nature?
- Would the vendor be involved in receiving and storing confidential data. Examples include: customer data, employee data, regulatory data, or financial data?
- If so, where does the vendor use, access, and store such data?
- What security controls and measures does the vendor have in place?
- Request copies of all relevant security policies.
- Has the vendor undergone third party audits (such as SOC2, HITRUST, ISO)?
- If so, a review of such reports should be performed and identified weaknesses should be documented
- Is there a risk of regulatory scrutiny and customer harm associated with the vendor?
- What is the operational reliance on this vendor?
- Does this vendor present supply chain risk?

(3) Contract Review

A confidentiality agreement or services agreement containing a confidentiality clause or equivalent must be reviewed and executed prior to any use of services and sharing of confidential data between August Schools and any third-party.

Vendor agreements should at a minimum require that third-parties maintain the privacy and security of the confidential information stored, used, or disclosed on behalf of August Schools.

(4) Monitoring of Vendors

or a designee is responsible for annual or more frequent vendor reviews of high-risk vendors as determined by this policy.

August Schools must periodically review all third-party agreements to reasonably ensure that vendors remain in compliance with state and federal law and appropriately address any legal risk to August Schools. Agreements will be updated and amended as necessary when business and regulatory requirements change.

Annual reviews of vendors will be documented and retained for audit purposes. The annual review may include the gathering of applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other evidence of security compliance including performing a review of in-place security controls.

Results of the reviews must be compared to in-place agreements and/or SLAs to ensure that services are being provided as intended. If vendors are found to be in violation of any executed agreement(s), action plans and processes may be initiated to remedy the issue(s) or access to August Schools systems may be removed immediately.

(5) Termination of Vendors

Upon termination of a vendor's services, all confidential information stored by the vendor should be deleted and/or provided back to August Schools within 60 days.

(6) Assignment of Vendor Relationship Owners and Contacts

Vendors should be assigned internal relationship owners, and key external vendor contacts should be identified. Vendor contacts should be actively maintained in case any issues with the vendor's product or service arise.

Vendor Security Controls

In order to protect August Schools, certain high-risk vendors may require additional controls such as:

- Not to use or further disclose confidential information other than as permitted or required by the agreement or as required by law
- Define the following service levels, where applicable:
- Service definitions,
- Delivery levels,
- Security controls,
- Aspects of service management, and
- Issues of liability, reliability of services, and response times
- Use appropriate safeguards to prevent use or disclosure of confidential information other than as provided for by the agreement
- Employ or implement appropriate administrative, physical, and technical security safeguards and privacy practices that meet the use and disclosure requirements of August Schools
- Require a prompt report of any inappropriate use, disclosure or breaches of confidential information
- Breach notification must include the following:
- names of breached individual(s) and contact information,
- date breach occurred and the date breach was discovered,
- information/data that was breached (e.g., social security number, name, address, etc.),
- mitigating activity undertaken to limit damages, and
- security controls that will be implemented to reasonably ensure a similar breach does not occur in the future
- Reasonably ensure that any agents, including subcontractors, who use and disclose confidential information will agree to the same restrictions and conditions that apply to August Schools and its team members.
- Require that third-parties coordinate, manage, and communicate changes to any services currently provided that could affect the security, availability, or integrity of covered data.
- Review warranties, indemnification and limitations of liability to determine maximum cost of risk.
- Upon termination of the agreement, if feasible, the service provider or vendor will return or destroy all confidential information, used or disclosed by the service provider on behalf of August Schools, in any form and will retain no copies of such information.
- If return or destruction is not feasible, the service provider may extend the agreement’s privacy and security protections to confidential information and limit further uses and disclosures to those purposes that make the return or destruction of confidential information infeasible.
- Authorize August Schools to terminate the agreement if August Schools determines the service provider or vendor has or is violating the executed agreement.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Internal Control Policy

Purpose and Scope

This Internal Control Policy guides August Schools regarding the maintenance of an internal control system in order to safeguard the August Schools's assets against loss, promote operational efficiency, and encourage adherence to prescribed managerial policies.

From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all August Schools policies and plans.

Internal Control

Control Environment

August Schools senior management recognizes that a proper control environment provides the discipline and structure to help August Schools achieve its objectives. August Schools manages and maintains its internal controls through the use of the Secureframe platform.

Responsibility

August Schools senior management is responsible for ensuring that an adequate and effective internal control system exists at August Schools and that dedicated personnel are necessary for monitoring the performance of the internal control system. Senior management must establish and define responsible parties with accountability for overseeing and maintaining internal control processes and procedures. These lines of accountability should be reviewed annually to ensure that performance measures are being met. Corrective measures or changes in responsibility should be implemented as needed.

Annual Review

Internal control processes and procedures should be reviewed by August Schools senior management annually. Senior management may choose to sample a number of controls for review per year. Any outdated or non-operating procedures should be updated or removed. New controls should be implemented where appropriate.

Identified Deficiencies

Identified control failures or deficiencies and proposed corrective action plans for newly identified issues must be addressed and communicated to management.

Evaluation of Internal Controls

- Internal control objectives are identified by relevance to the company, department, business line, or product
- As part of the evaluation process, a review of pertinent policies, procedures, and documentation will be completed to verify that applicable internal controls are operating effectively, and in line with business objectives
- A member of August Schools management or a designee will document the review of internal control policies and procedures and sign off on the review. Findings will be shared, as appropriate
- Identified issues are assessed to determine the impact to internal control. If necessary, corrective action plans are developed, tracked via documentation, and monitored until implementation

Changes to Internal Controls

- If a corrective action or change is required, August Schools management must assess the changes that could significantly impact the system of internal control including:
- External environment,
- Current business model,
- Leadership, and
- Business relationships (vendors, business partners, and other third-parties)
- All changes must be approved by management before implementation. If the change is related to security of network and IT resources, the change must be approved and documented in accordance with documented change management procedures
- Changes to internal control activities must be communicated to all affected users in a timely manner

Communication with External Third Parties

August Schools will communicate with external parties regarding the functioning of internal control (i.e. material changes to internal controls that affect nondisclosure agreement or contractual confidentiality and privacy provisions.).

August Schools will conduct an assessment to determine whether changes need to be communicated to and affirmed by the customer, partner, vendor, or other third parties. The manner in which the change is communicated must be in line with the significance of the change.

Communications with legal or regulatory implications must be reviewed and approved by management.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Change Management Policy

Purpose and Scope

This Change Management Policy defines how changes to applications, systems, services, and infrastructure are planned and implemented. The goal of change management is to increase awareness and understanding of proposed changes across August Schools and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers.

From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets and personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all August Schools policies and plans.

Change Management

All code change requests and critical infrastructure or network-related change requests must be documented end-to-end via August Schools's change management and ticketing tools.

Change management should be conducted according to the following procedure:

(1) Product Roadmap

The August Schools product management team evaluates which change requests and features will be implemented based on their alignment with the business plan and the overall level of effort required. All change requests should be prioritized in terms of benefits, urgency, effort required, security impacts, and other potential impacts on the organization’s operations.

A ticket should be created to track a change request at the onset. If the change is part of an existing ticket the original ticket may be used and modified appropriately.

(2) Planning and Evaluation

Planning and evaluation must include design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan. During planning, wire-frames, mockups, and functional requirements may be created and reviewed among the applicable team members. The team may set priority levels of the service and may determine any risk that the proposed change introduces to the system. It is during this phase that the scope and impact of the change will be determined.

(3) Build, Test, and Document

During building, August Schools sprints may be defined and the overall software design and development occurs.

UI/UX and other optimizations should be performed during this phase to enhance the performance and security of the change across all platforms.

The changes must be tested in a non-production environment before release to production. Test setups and scenarios are built for operational, performance, and security testing. Test scripts and suites should be developed, used, and updated as changes occur.

Documentation must be updated during this phase, such as release notes, help articles, and blog posts. Existing documentation is updated to ensure that team members and customers have the most up-to-date and accurate information related to the changes performed. Customer-facing documentation should be provided to August Schools customers as applicable.

(4) Code Review

August Schools uses code reviews to maintain the quality of August Schools code and products. Code reviewers should look at:

Design

Is the code well-designed and appropriate for your system?

Functionality

Does the code behave as intended by the plan? Is the way the code behaves good for its users?

Complexity

Could the code be made simpler? Would another developer be able to easily understand and use this code when they come across it in the future?

Tests

Does the code have correct and well-designed automated tests?

Security

Are there any security risks in the code as identified by the latest OWASP Top 10?

Naming

Are there clear names for variables, classes, methods, etc.?

Comments

Are the comments clear and useful?

Style

Does the code follow August Schools style guides?

Documentation

Was the relevant documentation updated or created?

How to do a code review?Google Engineering Practices Documentation provided under the CC 3.0 License.

Secure Coding

Secure coding practices are incorporated into the development lifecycle and security architecture of August Schools. Engineers at August Schools are responsible for defining security requirements initially and throughout all phases of the software development life cycle and then evaluating for compliance with those requirements.

All engineers at August Schools are responsible for reviewing theOWASP Top 10 Web Application Security Risks.

(5) Approval and Implementation

Once the new release is ready for deployment and the appropriate documentation is in place, the new release must be approved and reviewed by the appropriate product owner prior to being pushed to the production environment.

The ability to push changes to production at August Schools must be restricted to a limited set of authorized team members, and the engineer responsible for coding the change should not also be responsible for pushing the change to production, unless there is prior approval of the exception by management.

(6) Communication

Implemented changes should be communicated to all applicable team members and externally as appropriate.

(7) Post-Change Review

August Schools continuously measures the success of new releases and identifies areas that can be enhanced further in the future.

The appropriate team must conduct a post-implementation review to determine how the change is impacting August Schools and August Schools's customers, either positively or negatively. Discuss and document any lessons learned with product management and other appropriate team members.

August Schools must utilize version control tools that allow for efficient rollbacks of commits from production if any issues arise during the post-change review.

Hotfixes / Critical Issues / Emergencies

The following are potential emergencies that may require a hotfix:

- A customer is completely out of service
- There is severe degradation of service needing immediate action
- A system/application/component is inoperable and the failure causes a significant negative impact
- A response to a natural disaster

- A response to an emergency business need
- A critical vulnerability or security issue is identified

If a hotfix is required, the applicable manager should be immediately notified.

The notification should include at a minimum the following information:

- Will the change cause an interruption in service?
- What additional customers will be affected (in the event a change is needed to fix an outage) and who needs to be notified?
- What is the possible workaround until the problem is resolved?
- What is the approximate length of the outage?
- Notification of resolution
- Submission of a ticket to accurately describe the outage

Emergencies after normal business hours, on the weekend, or on holidays, must follow an appropriate communication and resolution process. A ticket must be generated and team members may need to notify affected customers, as determined by management. Emergency changes must be revisited to ensure no additional security issues were introduced into the product, service, or supporting infrastructure. A completed ticket should be submitted through the regular reporting process promptly following when the change was made.

Management must review all emergency submissions to ensure the change met the criteria for an “emergency change” and to prevent the process from becoming normal practice to circumvent the Change Management Policy. Any questions will be directed to the individual(s) who approved the change.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Secure Development Policy

Purpose and Scope

The purpose of this document is to define basic rules for secure development of software and systems.

This document is applied to the development and maintenance of all services, architecture, software and systems that make up August Schools's product/service.

Users of this document are all employees and applicable contractors who are involved with the development and maintenance of applications and systems at August Schools.

Secure Development and Maintenance

Securing the Development Environment

Access to the development environment is restricted only to authorized employees via logical access control. Development and production environments are logically separated.

Secure Engineering Principles

August Schools developers follow secure information system engineering practices for the development of new systems and for the maintenance of the existing systems. Minimum-security standards must be maintained and complied with when implementing new systems.

The same secure engineering principles are applied to outsourced development.

All developed code should be reviewed, utilizing the following peer review best practices:https://google.github.io/eng-practices/review/reviewer/.

Security Requirements Related to Public Networks

is responsible for defining security controls related to information in application services passing over public networks:

- the description of authentication systems to be used
- the description of how confidentiality and integrity of information is to be ensured
- the description of how non-repudiation of actions will be ensured

is responsible for defining controls for online transactions, which must include the following:

- how misrouting will be prevented
- how incomplete data transmission will be prevented
- how unauthorized message alteration will be prevented
- how unauthorized message duplication will be prevented
- how unauthorized data disclosure will be prevented

Repository and Version Control

August Schools utilizes code version control management tools to track and manage code development, testing, and merges with production. Changes in the development and during the maintenance of the systems must be done according to the Change Management Policy.

Protection of Test Data

Confidential and restricted data, as well as data that can be related to individual persons should not be used as test data, except as required for customer debugging, where approved by customers or where approved by management. On a similar note, test data should be restricted from entering the production environment.

Required Security Training

All engineers must periodically review the OWASP Top 10 as defined in the Change Management Policy.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Configuration and Asset Management Policy

Purpose and Scope

This Configuration and Asset Management Policy provides procedures supporting effective organizational asset management, specifically focused on electronic devices within the organization and baseline configurations for August Schools assets and systems.

From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all August Schools policies and plans.

Configuration Standards

Production systems handling confidential data must have documented baseline configurations, when available. August Schools management is responsible for following documented standard configurations for all applicable assets including third-party cloud products and employee devices. Configuration standards should be available for reference by applicable personnel.

August Schools must continuously harden its systems via Secureframe compliance and security checks as well as Center for Internet Security (CIS) benchmarks and best practices. The compliance checks monitor system security parameters and safeguards.

August Schools must regularly patch and keep all applicable systems up to date.

All vendor supplied default configurations, including but not limited to passwords, user accounts, and administrative accounts, should be changed before any systems or devices are implemented.

Each applicable asset and system in the August Schools environment should be hardened to the minimum standards defined by August Schools management.

Hardening standards should be in line with industry standards and provide sufficient logical and physical security for the asset(s) being configured.

Minimum Device Configuration Settings

August Schools devices should be configured to these settings where possible:

- **Encryption:** User endpoint storage is encrypted at rest (e.g. FileVault for MacOS or Bitlocker for Windows)
- **Security Updates**: OS security updates are enforced and monitored
- **Malware Protection**: Malware protection is enabled (e.g XProtect for MacOS, Defender for Windows, or ClamAV for Linux)
- **Screensaver / Lockscreen**: Screensavers / lockscreens are configured to activate after a maximum of 15 minutes
- **Logging**: Logs are captured and stored to assist with security investigations
- **Password Policy**: Required passwords must align with August Schools's Access Control and Termination Policy
- **Firewall**: Local firewall is enabled to provide layered host protection unless it interferes with development activities
- **Remote Wipe** (*Optional*):In the event of employee departure or theft, the mobile devices can be remotely wiped

Non-Standard Configuration

If an asset must use a non-standardized configuration, approval of the use must be provided by August Schools management and such approval and request must be documented.

Asset Management

August Schools inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information. The asset inventory will include all systems connected to the network and network devices themselves. Examples of items to be inventoried are servers, datastores, network devices, applications, and workstations.

Lost Asset

If an asset is known to be lost or stolen, please report it immediately to developers@augustschools.com.

Acquisition of New Assets

Business considerations must be reviewed, documented, and addressed prior to the acquisition of any new assets. August Schools management must approve any new assets that may be used to access August Schools data, systems, network, or applications. Reference the Data Classification Policy for more information.

Data as an Asset

Sensitive data is also considered an asset and should be tracked accordingly. Sensitive data must be stored in accordance with all security policies and the location of all covered data regardless of classification or encryption status must be maintained.

Asset Management Procedures

- August Schools must maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information.
- All assets should be mapped to the device’s serial number or another identifier.
- Any asset no longer in use or deemed no longer usable will be removed from the inventory.
- August Schools must perform periodic asset management system checks for various classes of asset records.
- Any August Schools devices issued to personnel must be returned upon termination or resignation

Asset Inventory Audit

or a designee will be held accountable for the accuracy of the inventory and must perform a documented review of the asset list at least annually.

Physical Media Transfer

Any media or device containing sensitive data must be shipped by a tracked carrier with a recipient signature required. For encrypted data, the encryption key should only be released after the package has arrived and been signed for. Media containing data will be protected against unauthorized access, misuse or corruption during transportation.

Legal advice should be sought to ensure compliance before media containing encrypted information or cryptographic controls are moved across jurisdictional borders.

Asset Disposal

When disposing of any asset, sensitive data must be removed prior to disposal. Any physical media storing confidential or personally identifiable information that is not being repurposed must be destroyed prior to disposal. Sanitization should occur in accordance with the NIST Guidelines for Media Sanitization (NIST S.P. 800-88 Rev. 1).

August Schools's third-party providers are responsible for physical protections and disposal of all assets under their control such as databases and servers.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Data Retention and Disposal Policy

Purpose and Scope

This Data Retention and Disposal Policy addresses how a customer's data is retained and disposed of and to ensure this is carried out in a consistent manner. From time to time, August Schools may update this policy. This policy is guided by security requirements specific to August Schools including compliance with applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all August Schools policies and plans.

Data Retention

The time period for which August Schools must retain customer data depends on the purpose for which it is used. August Schools must retain customer data for as long as an account is active or in accordance with the agreement(s) between August Schools and the customer, unless August Schools is required by law or regulation to dispose of data earlier or retain data longer.

Data Disposal

August Schools must dispose of customer data within 30 days of a request by a current or former customer or in accordance with the Customer’s agreement(s) with August Schools. August Schools may retain and use data necessary for the contract such as proof of contract in order to comply with its legal obligations, resolve disputes, and enforce agreements. August Schools hosting and service providers are responsible for ensuring the removal of data from disks allocated to August Schools use before they are repurposed and the destruction of decommissioned hardware.

Only a limited number of August Schools employees should have access to delete customer data.

Upon employee or contractor termination, company-owned devices will be collected and sanitized prior to device re-issuance in accordance with NIST Guidelines for Media Sanitization (NIST S.P. 800-88 Rev. 1).

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

August Schools reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually.

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Business Continuity and Disaster Recovery Plan

Purpose and Scope

This Business Continuity and Disaster Recovery Plan guides August Schools in the event of a significant business disaster or other disruption to normal service. August Schools must respond to business disasters and disruption by safeguarding employees' lives and company assets, making a financial and operational assessment, securing data, and quickly recovering operations.

This plan applies to all August Schools assets utilized by employees and contractors acting on behalf of August Schools or accessing its applications, infrastructure, systems, or data. All employees and contractors are required to read, accept, and follow all August Schools policies and plans.

Scope for Mission Critical Services

Mission critical services and systems are those required for the functioning of the August Schools product(s). Mission Critical services and systems include critical production systems required for immediate recovery, services affecting the engineering team's ability to support production operations and product development, and the ability to support August Schools customers.

All essential data is typically stored remotely using commercial cloud providers with proper backup and redundancy processes in place. This approach is subject to change and designed to minimize any disruption from physical incidents or disasters.

System Outages

Planned Outage

From time to time, August Schools may distribute a service update to all affected users prior to planned downtime.

Unplanned Outage

All unplanned outages should be treated as an incident; developers@augustschools.com and the executive team should be immediately emailed and notified of any unplanned outage.

Expectations

Alternate Physical Location(s) of Employees

In the event of an internal disaster that affects a August Schools office location, all team members will be moved from such affected offices to each member's respective home or an alternate location to work remotely.

Reliance on Third-Party Services

August Schools utilizes and relies on mission critical third-party cloud services. In the event of a significant business disaster, August Schools will quickly work to establish alternative arrangements if a mission critical vendor can no longer provide the needed services or goods.

Mission critical third-party vendors include:

This plan depends on the likelihood that:

1. Remote work can continue to take place in the event of a disaster; and
2. Mission critical vendor services, and essential August Schools services, systems, and data can still be made available or alternative solutions can be implemented (including backups and services provided by such third-party vendors)

Priorities

In the event of a disaster affecting August Schools essential systems or its team members, will oversee and respond in accordance with this Plan and will initiate specific actions for recovery.

The priorities during a business disaster are to:

1. Secure the safety of team members and visitors;
2. Mitigate threats or limit the damage that threats can cause to August Schools, its team, and its customers; and
3. Ensure that essential business functions can continue or determine what is required to restart essential business functions

Backup and Retention

All vital data that would be affected by disruption are maintained and controlled by the data's applicable teams.

In the event of a facility disruption, critical records located in such a facility may be destroyed or inaccessible. The number of critical records, which would have to be reconstructed, will depend on when the last transfer of critical records to the cloud storage location occurred.

Backup Requirements

1. Database backups must be performed
2. Backups must be retained for at least
3. The maximum allowable retention period for a database backup should be determined base on regulatory and contractual requirements
4. Backups are periodically tested to ensure that backups are sufficient and reliable in accordance with this plan
5. Backup systems and media protect the availability of stored data

Alternate Communication

The organization may communicate using telephone, video conferencing tools, messaging tools, email, physical mail, and in person.

In the event of a significant business disaster, an assessment will be conducted to determine which means of communication are still available. These means of communication will then be utilized to communicate with personnel, customers, partners and other third-parties.

Testing

Testing the plan is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by and any designee. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods noted in the subsections below.

Walkthroughs

Team members must walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with all relevant stakeholders and familiarize them with procedures, equipment, offsite facilities, and recovery efforts in preparation of a business disaster or disruption.

Table Top Exercises

Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test.

Personnel involved with business continuity must utilize validated checklists to provide a reasonable level of assurance for many disaster scenarios. These personnel must analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Business Continuity and Disaster Recovery Stages

This Plan divides recovery into three stages: Disaster, Response, and Recovery.

Declaring a disaster is the responsibility of senior management. Since it is almost impossible to predict when and how a disaster might occur, August Schools and its team members must be prepared to monitor and signal a disaster to management from:

- First hand observation
- Security applications
- Network monitoring and logging tools
- Environmental and security alarms
- Team members
- Customers
- Partners
- Vendors
- Media

Disaster Stage

If a disaster has been declared, this Plan and any related responses would go into effect.

The disaster stage may include the following processes:

1. Senior management declares the disaster, and
2. Notifies management and appropriate team members to create the appropriate Disaster Recovery Team (DRT),
3. DRT initiates internal and external communication lines, and communicate to the following parties as appropriate:
4. General Counsel
5. Authorities
6. Personnel
7. Customers
8. Vendors, third-parties, and other applicable stakeholders
9. DRT determines appropriate emergency response measures

Response Stage

In this phase, the team determines what team members, facilities and customer deployments are affected by the disaster scenario and in what way they are affected by performing an impact assessment.

This stage continues until an alternate facility location and/or essential business and production functions are established and services restored. If non-essential functions are affected, essential functions may be prioritized during a disaster event.

The response stage may include the following processes:

1. Execution of a business impact assessment,
2. Relocation to an alternative facility or establish work from home requirements,
3. Verification and/or backing up of affected data and systems, and
4. Restoration of essential August Schools services

Recovery Stage

Recovery begins with the activities necessary to return to business as usual including re-establishing the primary facility. For engineering, this stage begins with the restoration of August Schools services in an available commercial cloud provider's region. Recovery time objectives (RTOs) and recovery point objectives (RPOs) are to be defined when relevant for applicable systems.

Key Learning Stage

As soon as possible, August Schools senior management must meet with the DRT and other stakeholders for a post-mortem review to better understand the disaster event that took place and how it and others may be prevented in the future.

The retrospective must be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Lessons learned during the disaster must be captured within the post-mortem review and incorporated as updates into existing documentation.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

This Business Continuity and Disaster Recovery Plan is reviewed and tested at least annually. Ensuring that the plan reflects ongoing changes to resources is crucial. This task includes updating the plan, testing the updates with walkthroughs, tabletop exercises, and training necessary personnel. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

August Schools reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually.

August Schools

Physical Security Policy

Purpose and Scope

The Physical Security Policy specifies the requirements for physically protecting assets and their data via physical controls and safeguards. Physical security is the first line of defense in information security, and without physical protections, virtual protections offer minimal security for assets and data. August Schools maintains reasonable steps to ensure that its facilities, information systems, and data are accessed only by authorized personnel or authorized third party visitors to prevent unauthorized access, damage, theft, and interference. All physical security requirements are applicable to both remote and in-office work. Key aspects of physical security include: perimeter and border security, entry controls, visitor management, restricted areas, equipment protection and maintenance, awareness and training, and risk management.

Perimeter and Border Security

August Schools facilities should be secured via external locked doors. August Schools facilities should be monitored via personnel, security cameras, and/or other mechanisms to detect potential security threats and respond to alerts.

Entry Controls

August Schools requires employees and applicable contractors to utilize access cards/keys to unlock external doors throughout all business hours. For facilities that have a security desk at the point of initial external access, external doors can be left unlocked as long as 1) employees and/or contractors authenticate prior to internal access via key/badge and 2) visitors are required to sign-in at the security desk prior to internal admittance.

Visitor Management

All visitors must sign-in with security prior to being allowed in internal office areas. Upon sign-in, the following visitor-specific information should be collected:

- Visitor name
- Visitor organization name (if applicable)
- Government-issued identification card information

Upon exit, the badge/nametag and should be collected and the hr/min/sec timestamp for visitor exit should be captured. Visitor logs should be stored for at least 90 days via securely stored paper or digital records. Visitors that are unescorted should not have the ability to logically access restricted areas unless pre-authorization has been given by the approving manager. Visitors should receive a temporary badge or nametag - badge/nametag should be marked in a way that identifies them as a visitor. Any non-escorted or unauthorized visitors should be reported to the security team immediately.

Restricted Areas

Only authorized personnel shall be allowed entry into restricted areas. Restricted areas may include:

- Personal, confined offices
- Network closets
- Power & utilities closets
- Server rooms (as applicable)

Restricted areas must be secured via access badges/keys or security personnel.

Equipment

The following types of protection and monitoring equipment should be maintained at all times:

- Power utilities (e.g. generators, UPS)
- HVAC systems, including environmental sensors (thermometers and humidity sensors)
- Fire suppression systems
- Network, power, and telecommunications cabling
- On-premise servers and desktops (as applicable)
- Physical data backups

August Schools must securely store/protect the aforementioned equipment/assets from physical threats via proper access controls.

August Schools should maintain awareness of necessary maintenance schedules for the aforementioned equipment/assets. Maintenance should occur accordingly to prevent the failure of any of the aforementioned assets. Any third party/maintenance company that has access to a August Schools facility (e.g. night cleaning company) must receive security clearance from management and must follow all applicable parts of the security policies. Maintenance to and external movement of physical security components should be documented and tracked accordingly.

Risk Management

August Schools includes physical security within annual risk assessment scope.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Network Security Policy

Purpose and Scope

The purpose of this document is to define basic rules and requirements for network security and ensure the protection of information within and across networks and supporting information processing facilities.

This document applies to the security of all services, architecture, software and systems that make up August Schools's product/service.

Users of this document are all employees and applicable contractors who work on network engineering, security, and maintenance at August Schools.

Network Controls

August Schools manages, controls, and secures its networks, the connected systems, applications, and data-in-transit to safeguard against internal and external threats.

Firewalls & Threat Defense

August Schools must utilize network firewalls, web application firewalls, and/or equivalent mechanisms to safeguard applicable internet connections, internal network zones, and applications from threats. August Schools configures appropriate firewall alerts and alarms for timely response and investigation. This also applies to applicable wireless networks.

August Schools ensures networking ports and protocols are restricted based on the principle of least functionality. Ports and network routes should only be open when there is proper business justification. Firewall configurations and rulesets are maintained. Firewall rules are implemented to minimize exposure to external threats. Significant changes to network services and configurations should be tracked in accordance with the Change Management Policy.

As an additional layer of defense, August Schools utilizes monitoring solutions to detect and alert on network-based intrusions and/or threats.

Network Diagramming

maintains network and data flow diagrams. Diagrams are reviewed and updated when significant network infrastructure changes occur.

Network Access Control

In addition to the Network Security Policy, August Schools establishes, documents, and reviews the Access Control and Termination Policy based on business and security requirements. This policy also encompasses network access control.

August Schools segregates networks based on the required groups of information services, users, and systems.

August Schools utilizes firewall configurations to restrict connections between untrusted networks and trusted networks.

Additionally, August Schools may utilize security groups and network access control lists (NACLs) to improve network security for individual virtual machines.

Network Engineering

August Schools implements security functions in a layered approach, minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

August Schools utilizes a defense-in-depth (DiD) architecture to protect the confidentiality, integrity, and availability of information systems and data, i.e. placing information systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.

August Schools synchronizes clocks of all applicable information systems to the same time protocol to enforce consistent and accurate timestamping.

Network Service Level Agreements (SLAs)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Vulnerability and Patch Management Policy

Purpose and Scope

This Vulnerability Management Policy defines an approach for vulnerability management to reduce system risks and integrate with patch management. From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to August Schools including applicable laws and regulations.

This policy applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept, and follow all August Schools policies and plans.

Vulnerability and Patch Management Program

August Schools maintains a vulnerability management process that is integrated into the Change Management Process.

August Schools may periodically test the security posture of its applications and systems through third-party testing as well as vulnerability scanning.

August Schools also monitors multiple security alert lists such as theCVE Database and US-CERT to get up to date information on the latest vulnerabilities and threats.

Third-Party Penetration and Vulnerability Tests

August Schools schedules third party security assessments, penetration tests, and/or dynamic analysis tests at least annually.

August Schools periodically performs vulnerability scans.

Identifying Vulnerabilities

August Schools reviews third-party penetration test reports and vulnerability scan results to verify vulnerabilities and determine impact.

Scoring Vulnerabilities

Vulnerabilities are derived from the Common Vulnerabilities and Exposures (CVE) Database and are documented and scored based upon the Common Vulnerability Scoring System (CVSS) standard.

Mitigating Vulnerabilities

If remediation is required, the appropriate team member at August Schools will be notified of the requirements to remediate or mitigate the vulnerability and the time frame of such requirement will depend on the severity and risk of the vulnerability. Such tracking of vulnerabilities must be done through the company's change management tool and in accordance with the Change Management Process.

The information obtained from the vulnerability scanning process will be shared with appropriate personnel throughout the organization on a “need to know” basis to help eliminate similar vulnerabilities in other information systems.

Patching

All system components, software and production environments shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

System and Non-Company Application Patching

Patching includes updates to all operating systems and third party applications as provided by the appropriate vendor.

August Schools Application Patching

August Schools applications are patched in accordance with the Change Management Policy. Patches deemed to be of a high or critical nature may be rolled out in a compressed schedule as set forth in such policy.

Patching Exceptions

Patching production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigating alternative should be determined through a documented risk analysis.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

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

This document is maintained by .

This document was last updated on 05/03/2023.

August Schools

Security Incident Response Plan

Purpose and Scope

The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) (defined below) that affect any of August Schools's information technology systems, network, or data, including August Schools data held or services provided by third-party vendors or other service providers. From time to time, August Schools may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations.

This plan applies to all August Schools assets utilized by personnel acting on behalf of August Schools or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all August Schools policies and plans.

August Schools intends for this plan to:

- Define the August Schools security incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assist August Schools and any applicable third parties (including vendors and partners) in quickly and efficiently responding to and recovering from different levels of information security incidents.
- Mitigate or minimize the effects of any information security incident on August Schools, its customers, employees, and others.
- Help August Schools consistently document the actions it takes in response to information security incidents.

“Information Security Incident” means an actual or reasonably suspected unauthorized use, disclosure, acquisition of, access to, corruption of, deletion, or other unauthorized processing of sensitive information that reasonably may compromise the privacy, confidentiality, integrity, or availability of that information.

Management

August Schools has a Security Response Team (SRT) consisting of predetermined employees from key departments at August Schools to manage security incidents. The SRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to the August Schools systems, network, and data; (b) minimize economic, reputational, or other harms to August Schools and its customers, employees, contractors and partners; and (c) manage litigation, enforcement, and other risks.

The SRT also oversees and coordinates the development, maintenance and testing of the plan, its distribution, and on-going updates of the plan. The Security Incident Response Plan is activated or enabled when a security incident occurs, and the SRT is responsible for evaluating the situation and responding accordingly. Depending on the severity of an incident the SRT may request engagement from various support teams to assist with the mitigation of the incident. The SRT meets on a periodic basis for training, education, and review of the documented plan.

The SRT consists of a core team with representatives from key August Schools groups and stakeholders.

The current SRT roster may be contacted at developers@augustschools.com.

Incident Response Process

The process outlined below should be followed by the appropriate Staff at August Schools in the event of an Information Security Incident. August Schools shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. August Schools shall document each identified Information Security Incident.

Detection and Reporting

Automated Detection

August Schools may utilize automated detection means and other technical safeguards to automatically alert August Schools of incidents or potential incidents.

Report from August Schools Personnel

All August Schools personnel must report potential security incidents as follows:

1. If you believe an incident occurred or may occur or may have identified a threat, vulnerability, or other security weakness, please report it to the following email immediately: developers@augustschools.com;
2. Provide all available information and data regarding the potential incident; and
3. Once an incident has been submitted, please stop using the affected system, or any other potentially affected device until being given the okay from the SRT

Report from External Source

External sources, including August Schools's customers, who claim to have information regarding an actual or alleged information security incident should be directed to developers@augustschools.com.

Employees who receive emails or other communications from external sources regarding information security incidents that may affect August Schools or others, security vulnerabilities, or related issues should immediately report those communications to developers@augustschools.com and should not interact with the source unless authorized.

Response Procedures

Overview

Responding to a data breach involves the following stages:

1. Verification
2. Assessment
3. Containment and mitigation
4. Post-breach response

All of the steps must be documented in an incident log and/or corrective action plan.

The data breach response is not purely linear, as these stages and the activities associated with these stages frequently overlap. August Schools must keep a record of any actions the organization takes in responding to the incident and preserve any evidence that may be relevant to any potential regulatory investigation or litigation including through use of an incident log, corrective action plan or other applicable documentation.

(1) Verification

The SRT will work with August Schools employees and contractors to identify the affected systems or hardware (such as a lost laptop or USB drive) and determine the nature of the data maintained in those systems or on the hardware.

The SRT will determine the threshold at which events are declared a security incident and officially initiate the incident response process.

(2) Assessment

Following verification of an Information Security Incident, the SRT will determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to August Schools and its customers, employees, or others.

The incident assessment must include what employees or contractors were affected, what customers were affected, and what data was potentially exfiltrated, modified, deleted or compromised.

The SRT will work together to assess a priority with respect to the incident based on factors such as whether:

1. the incident exposed or is reasonably likely to have exposed data; or
2. personally identifiable information was affected and the data elements possibly at risk, such as name or date of birth.

In addition, the SRT will consider whether the disclosure was:

1. internal or external;
2. caused by a company insider or outside actor; and/or
3. the result of a malicious attack or an accident.

Lastly, if an information security breach has occurred, federal/country-wide law enforcement and local law enforcement should be contacted and informed of the breach. Law enforcement should be contacted in alignment with applicable breach notification laws. Internal and/or external general counsel should lead law enforcement communication efforts (in collaboration with SRT). If general counsel is not available, SRT should lead law enforcement communication efforts.

(3) Containment and Mitigation

As soon as August Schools has verified and assessed the breach, the SRT must take all necessary steps to contain the incident and return the August Schools systems back to their original state and limit further data loss or intrusion.

Such steps may include:

1. Acting to stop the source or entity responsible, for example by:
2. taking affected machines offline;
3. segregating affected systems; or
4. immediately securing the area if the breach involves a physical security breach.
5. Determining whether other systems are under threat of immediate or future danger.
6. Determining whether to implement additional technical measures to contain the data breach, such as changing locks, passwords, administrative rights, access codes, or passwords.

(4) Post-Breach Response

Any post-breach response including external and internal communications, notifications, and further inquiries will depend on the assessment and priority of the data breach.

August Schools will respond to confirmed disclosures affecting data subjects in accordance with breach notice periods defined in applicable laws and regulations. In the event of a data breach, if such affected data pertains to an EU citizen, August Schools must notify the data subject and necessary authorities within 72 hours.

As part of the final response based on the results of the breach, August Schools will review applicable access controls, policies and procedures and determine whether to take any actions to strengthen the organization’s information security program.

Key Learnings

As soon as the incident has been resolved, August Schools senior management should meet with the SRT and other relevant team members of the August Schools for a post-mortem to better understand the incident that took place, and determine how similar incidents may be prevented in the future.

The retrospective should be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Testing

Testing the plan annually is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by August Schools management. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods:

Walkthroughs

Team members walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with a larger subset of people, allowing the team to draw upon an increased pool of knowledge and experiences. Team members should be familiar with procedures, equipment, and offsite facilities.

Table Top Exercises

An incident is simulated so normal operations will not be interrupted. Scenarios of various security incidents are used and this plan is put into action to determine its use and effectiveness.

Validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

Exceptions

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

Enforcement

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

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

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

Responsibility, Review, and Audit

This plan will be reviewed and tested on an annual basis. Ensuring that the plan reflects ongoing changes to resources is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updates; and training personnel. Test results will be documented and signed off by August Schools management. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is tested, maintained and enforced by .

This document was last updated on 05/03/2023.

August_LancasterCity_OH_14State_OHG_VendorSigned1

Final Audit Report 2025-05-09

Created:	2025-05-08
By:	Michael Klisiwecz (mklisiwecz@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAckaK2ne1wwrYrIyJVgUW7sAkzK3LhpJ4

"August_LancasterCity_OH_14State_OHG_VendorSigned1" History

Document created by Michael Klisiwecz (mklisiwecz@tec-coop.org)
2025-05-08 - 6:55:03 PM GMT

Document emailed to s_daugherty@lcsschools.net for signature
2025-05-08 - 6:55:10 PM GMT

Email viewed by s_daugherty@lcsschools.net
2025-05-09 - 1:20:04 PM GMT

Signer s_daugherty@lcsschools.net entered name at signing as Sarah A Daugherty
2025-05-09 - 1:21:35 PM GMT

Document e-signed by Sarah A Daugherty (s_daugherty@lcsschools.net)
Signature Date: 2025-05-09 - 1:21:37 PM GMT - Time Source: server

✓ Agreement completed.
2025-05-09 - 1:21:37 PM GMT