STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, MISSOURI, NEW HAMPSHIRE, NEW YORK, OHIO, RHODE ISLAND, AND VERMONT

MA-ME-MO-NH-NY-OH-RI-VT-NDPA, Standard Version 1.0

School Administrative Unit 67

and

intelliVOL

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: School Administrative Unit 67, located at 55 Falcon Way, Bow NH 03304 USA (the "**Local Education Agency**" or "**LEA**") and intelliVOL, located at PO BOX 806, Comfort, TX 78013 (the "**Provider**").

WHEREAS, the Provider isproviding educational or digital servicesto 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 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 **<u>Exhibit "G"</u>** are hereby incorporated by reference into this DPA in their entirety.

   ☑ If Checked, the Provider, has signed **<u>Exhibit "E"</u>** 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 **<u>Exhibit "A"</u>** (the "**Services**").

6. **<u>Notices</u>**. 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: Michele Pitman Title: CEO

Address: 612 Lake Dr, Kerrville TX 78028

Phone: 214-669-2083

Email: mpitman@ intelliVOL.com

The designated representative for the LEA for this DPA is:

Roy Bailey, Director of IT
SAU67
55 Falcon Way, Bow NH 03304
rbailey@bownet.org 603.415.9633

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

School Administrative Unit 67

By: Roy Bailey Jr.

Date: 05/14/24

Printed Name: Roy D Bailey Jr

Title/Position: Director of IT

intelliVOL

By:

Date: May 13, 2024

Printed Name: Michele Pitman

Title/Position: CEO

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.

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

x2VOL, a tracking and reporting platform for managing and reporting student service hours. School administrators can manage activities, post opportunities, and quickly track and approve student volunteer hours and service learning projects.

x2VOL tracks and reports hours and experiences for students participating in community service, service learning, Work based learning (WBL), CTE, Clubs and internships.

x2VOL is also used by school and district leaders to centralize the data for reporting purposes. x2VOL allows school and districts to set up programs and manage them via x2VOL.com.

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	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	✓
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	✓
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	✓
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	✓
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	optional
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	School address
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	optional
	State ID number	
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	
Student Name	First and/or Last	✓
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	✓
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	optional
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify: service transcript	✓
Transportation	Student bus assignment	

Category of Data	Elements	Check if Used by Your System
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
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~~

_______________________________ ~~May 13, 2024~~

~~Authorized Representative of Company~~ Date

omit above
To be completed upon request to dispose of data. - MP

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

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)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

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"
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 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"
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"
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"
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. §§ 3319.32-3319.324, 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. 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: Ohio does not require data to be stored within the United States.

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~~) Comments + history	✓
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 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.

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 Contractor 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.

IntellVol_SAU67_8state

Final Audit Report 2024-05-14

Created:	2024-05-14
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA49ctz41GN7dN-S1myUGxKC0zMe0saGX5

"IntellVol_SAU67_8state" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-05-14 - 10:59:29 AM GMT

Document emailed to Roy Bailey (rbailey@bownet.org) for signature
2024-05-14 - 11:00:28 AM GMT

Email viewed by Roy Bailey (rbailey@bownet.org)
2024-05-14 - 11:03:03 AM GMT

Document e-signed by Roy Bailey (rbailey@bownet.org)
Signature Date: 2024-05-14 - 11:03:48 AM GMT - Time Source: server

✓ Agreement completed.
2024-05-14 - 11:03:48 AM GMT

Updated 12/7/23

Overview

Purpose

x2VOL is entrusted with the responsibility to provide services to clients who provide us with confidential information. Inherent in this responsibility is an obligation to provide strong protection against theft of data and all other forms of cyber threats.

The purpose of this policy is to establish standards for the base configuration, and acceptable use of equipment and any software running on it that is owned and/or operated by x2VOL or equipment that accesses x2VOL's internal systems.

Effective implementation of this policy will reduce the risk of unauthorized access to x2VOL proprietary information and technology and protect confidential client information.

Scope

This policy applies to equipment owned and/or operated by x2VOL, and to employees connecting to any x2VOL-owned network domain or cloud applications that are used as part of projects or assignments managed by x2VOL.

Network/Server Security

Server Configuration Guidelines

The most recent security patches must be installed on all systems as soon as it is feasible to do so, the only exception being when immediate application would interfere with business requirements.

Servers should be physically located in an access-controlled environment or a cloud infrastructure environment with an IT infrastructure provider that has achieved and maintains a high level of compliance with IT standards such as ISO-27001.

Servers are specifically prohibited from being operated from locations without appropriate physical access controls.

Security-Related Events

Security-related events will be reported to the IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

Evidence of port-scan or any other type of service scanning.

Evidence of unauthorized access to privileged or non-privileged accounts.

Service interruptions, error messages, or other anomalous occurrences such as that are not related to specific applications on the host.

Server Malware Protection

Anti-Virus - All servers MUST have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications if the server meets one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- Share access is open to this server from systems used by non-administrative users
- Any service access is open from the Internet
- The x2VOL IT department deems it necessary.

Mail Server Anti-Virus

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail and file attachments destined to and from the mail server.

All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified. If automatic updates are not being successfully applied, IT management must be notified immediately.

Notable Exceptions

Exceptions to above requirements may be deemed acceptable with proper documentation if one of the following notable conditions applies to this system:

- The system is a SQL server

- The system is used as a dedicated mail server
- The system is not a Windows based platform

All on premises servers, routers, and other network appliances MUST be directly powered by a UPS (battery backup) appliance that can adequately provide surge protection and alternative power in case of power interruption. All UPS appliances should be tested annually and verified to be able to provide at least 20 minutes of alternate power source.

Workstation Security

Authorized Users

Appropriate measures must be taken when using workstations to ensure that exposure of sensitive information is restricted to authorized users.

Safeguards

x2VOL will implement appropriate physical, administrative, and technical safeguards for all workstations that access data or information that is confidential or sensitive to restrict access to only authorized users.

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Configuring screen-locks to automatically lock the screen after 10 minutes of inactivity, and requiring personnel to manually enable screen-lock on workstations prior to leaving the area to prevent unauthorized access.
- Providing personnel with documentation for all password policies and procedures, and verifying personnel compliance said password policies and procedures as defined by IT management.
- Ensuring workstations are used for authorized business purposes only.
- Creating a documented list of authorized software applications for each classification of workstation determined by job requirements performed with that workstation, and providing personnel with this list that pertains to their role. Compliance should be verified by ensuring that no unauthorized software applications are installed on workstations.
- Storing all confidential or sensitive information on network servers or authorized cloud resources whenever possible.

- Applying full-disk encryption to all workstations and laptops that must store confidential or sensitive information as determined by IT management.
- Securing laptops that contain confidential or sensitive information by using cable locks or locking laptops up in drawers or cabinets when not in use.
- Anti-Virus - All workstations and laptops MUST have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications.
- All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified. If automatic updates are not being successfully applied, IT management must be notified immediately.
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to hinder public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access policy.

Software Installation

Employees may not install software on x2VOL's computing devices operated within the x2VOL internal network without explicit approval by IT management.

Installed software must be selected from an approved software list, maintained by the IT department, unless no selection on the list meets the requester’s need. The IT department will obtain and track the licenses, and test new software for conflict and compatibility before it is approved. This policy covers all computers, servers, and other computing devices operating within x2VOL's internal network.

Malware Protection

Anti-Virus - All x2VOL computers must have approved anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date.

Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into x2VOL's internal network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, and anyone caught in violation of this policy will be criminally prosecuted to the fullest extent of the law.

Password Security

Requirements

All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum. Technical controls should be used when possible to prevent the reuse of passwords. Technical controls should be used whenever possible to prevent the reuse of passwords, and enforce minimum password complexity.

All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. Technical controls should be used whenever possible to prevent the reuse of passwords, and enforce minimum password complexity.

All user-level and system-level passwords must conform to the standards described below in part b.

Standards

Password policy should be provided to all users at x2VOL in order to create awareness of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least one of each of the following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - “Special” characters (e.g. @!.',#$%^&*()_+|~-=\`{}[]:”;’<>/ etc)
- Have a minimum length of 12 characters
- A password manager must be used to generate a pseudo random password that conforms to the above characteristics of an arbitrary length between 12 and 30 characters. All personnel must use the

password manager to store passwords and make them available on all desktop, laptop, and mobile devices.

Protective Measures

- Do not share x2VOL passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential x2VOL information.
- Passwords should never be written down or stored anywhere online except in a password manager application that has been deemed acceptable by IT managers.
- Do not reveal a password in e-mail, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., “my family name”).
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT Department.
- Always decline the use of the “Remember Password” feature of native applications such as browsers, and web-applications.
- Multi-factor authentication (MFA) MUST be enabled on all accounts that provide such a feature, and MFA codes MUST be stored in an MFA authenticator mobile application that has been deemed acceptable by IT managers. MFA backup codes should also be stored in a password manager to ensure their security, and if MFA backup codes are provided via a downloaded file, that file must be deleted, and purged from the trash-bin of the device.

Passphrases

Access to the x2VOL internal network via remote access is to be controlled using either a one-time password (OTP) authentication or a public/private key system with a strong passphrase.

An acceptable passphrase is subject to the same requirements and limitations as account passwords which are stated above in Section IV items b and c.

Acceptable Use

General Use and Ownership

- The data created on the x2VOL corporate systems remains the property of x2VOL.
- Any information deemed to be confidential or sensitive by x2VOL management, team leaders, or IT management should be encrypted following the section VI Encryption or as otherwise provided instructions from management.
- For security and network maintenance purposes, authorized individuals within x2VOL may monitor equipment, systems and network traffic at any time.

Security and Proprietary Information

- The information contained on x2VOL's systems should be classified as either confidential, sensitive, or public, as defined by corporate confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to confidential and sensitive information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
- All desktops, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, and by logging-off when moving beyond direct visual contact with the device.
- All desktops, laptops and workstations used by the employee that are connected to the x2VOL internal network, whether owned by the employee or x2VOL, shall have approved virus-scanning software configured to scan all incoming files and complete a

complete device scan once per week with a current virus database unless overridden by departmental or group policy.

- Employees must use extreme caution and common sense when opening e-mail attachments received from unknown senders, which may contain various types of malware that can negatively impact x2VOL's devices or network.

Unacceptable Use

The following activities are prohibited. The lists below are not exhaustive, but attempt to exemplify activities which fall into the category of unacceptable use.

- Under no circumstances is an employee of x2VOL authorized to engage in any illegal activity as defined under local, state, federal or international law while utilizing x2VOL-owned resources.
- Violations of the rights of any person or corporation such as defamation, liable, trademark, copyright, patent or other intellectual property, trade secret, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by x2VOL.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which x2VOL or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, ransomware, or other malware, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using any x2VOL device or network connection to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any x2VOL account.
- Activity that leads to security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not authorized to access.
- Port scanning or security scanning is expressly prohibited unless prior permission is granted by IT management.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is approved by the IT management and deemed part of the employee's normal job/duty.
- Circumventing or altering the normal user authentication process or security of any host, network or account.
- Interfering with or denying service to any user including the employee's own host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with any local network hosts or services or any external hosts or services via the Internet ,whether or not they are owned and operated by x2VOL.

- Providing information about, or lists of, x2VOL employees, internal hosts, or network configuration to parties outside x2VOL.
- Otherwise altering host or network configuration, or broadcasting any network communication data other than what is considered part of the employee's job/duty.

Wireless Access

Device Requirements - All wireless devices that reside at a x2VOL site and connect to a x2VOL internal network must:

- Be installed, supported, and maintained by the IT department.
- Use x2VOL approved authentication protocols and infrastructure.
- Use x2VOL approved authentication protocols, which may include the installation and use of RSA private and public key certificates to enable WPA2-Enterprise authentication.
- Provide the device's manufacturer issued media access control hardware address (MAC address) to the IT department to whitelist the device for access to x2VOL wireless network.
- Maintain the original manufacturer issued media access control hardware address (MAC address) of the device.

Home Wireless Device Requirements

- Wireless devices used at the employee's home such as WiFi routers, that are used in the process of accessing the x2VOL internal corporate network, must conform to the security protocols as detailed in sections IV Password Security and VIII Remote Access.

Encryption

Standards

Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Encryption algorithms that are considered weak by IT security industry standards should not be used, and disabled in all applications.

- Key bit strength must be at least a minimum of 2048-bit keys for RSA public / private keypairs.
- Symmetric encryption for data-in-transit and data-at-rest must use AES 256-bit keys unless otherwise specified by IT management.
- x2VOL's allowed encryption algorithms and key length requirements will be reviewed annually and upgraded as technology allows.

Mobile Device Encryption

- Scope - All mobile devices containing stored confidential or sensitive data owned by x2VOL must use an approved method of encryption to protect data at rest such as full-disk encryption or application specific encryption as described below. Mobile devices are defined to include laptops, tablets, and smartphones.
  - *Laptops* - Laptops must employ full disk encryption with an encryption package approved by IT management. No x2VOL data may exist on a laptop in cleartext.
  - *Tablet and smartphones* - Any x2VOL data stored on a smartphone or tablet must be saved to an encrypted file system using an encryption package approved by IT management. All x2VOL tablets and smartphones shall also employ remote wipe technology to remotely disable and

delete stored data in case of emergency such as a lost or stolen device.

- Keys - All keys used for encryption and decryption must meet complexity requirements described in x2VOL’s Password Security policy.

E-mail

Prohibited Use

x2VOL e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any x2VOL employee must report the matter to their supervisor immediately.

The following activities are strictly prohibited for e-mail, telephone, or any other messaging service or application:

- Sending unsolicited messages, including the sending of “junk mail”, "spam", or other advertising material.
- Any form of harassment, whether through language, frequency, or size of messages.
- Fraud, identity misrepresentation, or forging of e-mail protocol header information.
- Using non-x2VOL e-mail accounts (i.e., Gmail, Hotmail, Yahoo), or other external resources to conduct x2VOL business.

E-mail Retention

- Administrative Correspondence - x2VOL Administrative Correspondence includes, though is not limited to clarification of established policy, including holidays, time card information, dress code, workplace behavior and any legal issues such as intellectual property violations. All e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. x2VOL Administration is responsible for e-mail retention of Administrative Correspondence.

- Fiscal Correspondence - x2VOL Fiscal Correspondence is all information related to revenue and expense for x2VOL. x2VOL's finance department is responsible for all fiscal correspondence.
- General Correspondence - x2VOL General Correspondence covers information that relates to customer interaction and the operational decisions of the business. x2VOL is responsible for e-mail retention of General Correspondence.
- Ephemeral Correspondence - x2VOL Ephemeral Correspondence is by far the largest category and includes requests for recommendations or review, e-mail related to product development, updates and status reports.
- Recovering Deleted e-mail via backup Media - x2VOL maintains backups from the e-mail server and once a quarter a set of backups is moved to an offsite location for long-term storage. No effort will be made to remove e-mail from the offsite backups.
- Opening any e-mail that has been labeled as "spam" and placed into the "spam" is strictly prohibited. If a legitimate business related e-mail is found to be in the spam folder, it must not be opened, and the incident must be reported to the IT department for review.

Monitoring

x2VOL employees shall have no expectation of privacy in anything they store, send or receive on the x2VOL’s e-mail system. x2VOL may monitor messages without prior notice. x2VOL is not obliged to monitor e-mail messages.

Remote Access

Persons Affected

All x2VOL employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the x2VOL.

General Standards

It is the responsibility of x2VOL employees, contractors, vendors and agents with remote access privileges to x2VOL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password or public/private keys with strong pass-phrases and will always be supplemented when possible with multi-factor authentication (MFA) that supplies a one-time-password to an mobile MFA authenticator application that has been approved by the IT management. For information on creating a strong pass-phrase see the section IV Password Security policy.
- At no time should any x2VOL employee provide their login or e-mail password to anyone, inside or outside the organization. In the case that IT support needs to access an employee's account directly, the IT support shall change the user's password using admin privileges, and after finished, will provide the user with a temporary password, which will be required to be changed when the user accesses their account.
- Remote access to the x2VOL internal network is only allowed by connecting directly via an employee's home internet connection provided by an authorized ISP. Under no circumstances may an

employee connect to the x2VOL internal network by connecting via a tethered connection to another device, or from any public WiFi connections such as a restaurant or coffee shop, a library, hotel, or other publicly available WiFi networks unless explicit permission has been provided by IT management.

- When traveling for business, x2VOL employee's may be provided authorization to connect to x2VOL internal network connections from a list of approved WiFi connections such as hotel WiFi. Alternatively, an employee may be provided with a mobile device or SIM card with mobile internet access, and instructions on how they may tether their laptop, such that they can connect to the x2VOL internal network securely.
- Home routers used to access to the x2VOL internal network must meet the minimum configuration requirements described below:
    - Admin and user authentication passwords used to connect to the WiFi services on the router must meet the requirements as specified in section IV Password Security.
    - The router must be configured to use WPA-2 or WPA-3 for authentication to WiFi services. WPA (1) and WEP WiFi authentication protocols must not be used.
- Reconfiguration of a home user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Non-standard hardware configurations must be approved by the IT department, and x2VOL must approve security configurations for access to hardware.
- All desktop computers, laptops and workstations that are connected to x2VOL internal network via remote access technologies must have approved and fully updated anti-virus software installed and configured to immediately scan all incoming files and configured to conduct a complete scan of all files on the device at least once per week.

- Personal equipment that is used to connect to x2VOL's internal network must meet the requirements of x2VOL-owned equipment for remote access as defined by IT management. All employees will be provided with these policies when they are provisioned credentials and other information required for a remote access connection.
- Individuals who wish to implement non-standard Remote Access solutions to the x2VOL production network must obtain prior approval from the IT department.

Virtual Private Network (VPN)

Persons Affected - this policy applies to all x2VOL employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the x2VOL internal network.

Connectivity - Approved x2VOL employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Requirements

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to x2VOL internal network by protecting any devices used to connect to the x2VOL internal network using all policies described in section III Workstation Security.
- VPN authentication is to be controlled using either a multi-factor authentication (MFA) one-time password provided by an approved

authenticator app or another physical token based MFA device, or a public/private key authentication with a strong passphrase. The method of authentication will be approved by IT management and provided to the employee when they are provisioned credentials and other information about the VPN connection.

- When actively connected to the corporate network, VPNs will force all traffic to and from the client device over the VPN tunnel (known as a full-tunnel): all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by x2VOL's IT department.
- All computers connected to the x2VOL internal network via VPN or any other technology must use the most up-to-date anti-virus software that has been approved by IT management; this includes personal computers.
- VPN users will be automatically disconnected from x2VOL's internal network after thirty minutes of inactivity. The user must then login again to reconnect to the network. Pings or other artificial network processes MUST NOT be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not x2VOL-owned equipment must configure the equipment to comply with x2VOL's VPN and Network policies.
- Only x2VOL-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of x2VOL's internal network, and as such are subject to the same rules and regulations that apply to x2VOL-owned equipment, i.e., their

machines must be configured to comply with x2VOL’s Security Policies.

Data Retention

Reasons for Retention

x2VOL retains only that data that is necessary to effectively conduct its business operations and activities, and to remain compliant with applicable laws and regulations.

Reasons for data retention include:

- Providing ongoing services to registered users, customer, and clients
- Compliance with applicable laws and regulations associated with financial reporting by x2VOL to its funding agencies and other donors
- Compliance with applicable labor, tax and immigration laws
- Other regulatory requirements
- Compliance with industry standards certification
- Investigation of a security incident
- Restoration of data from a security incident
- Intellectual property preservation
- Defense against potential litigation

Data Retained

x2VOL has set the following specifications for types of data that shall be retained:

- Website registered and non-registered guest's data will be retained as long as necessary to provide the service requested/initiated through the x2VOL website, unless in the case that any registered or non-registered user requests that their any collected personally identifiable information (PII) be deleted. In such a case, any PII data associated with the requesting party will be deleted as soon as feasibly possible.

- Financial information used to process payment transactions will not be retained longer than is necessary to process a single transaction. Any IDs or tokens provided by the payment gateway provider to identify a user or process recurring payments will be stored in a database field encrypted with AES-CBC with a 256-bit key and 128 bit initialization vector (IV).
- Collected data of subcontractors and vendors will be kept for the duration of the contract or agreement and then for 2 more years.
- Employee data will be held for the duration of employment and then 1 year after the last day of employment.
- Financial data associated with employee wages, leave and pension shall be held for the period of employment plus 1 year.
- Recruitment data, including interview notes of unsuccessful applicants, will be held for 1 year after the closing of the position recruitment process.
- Consultant data will be held for the duration of the consulting contract plus 1 year after the end of the consultancy.
- Board member data will be held for the duration of service on the Board plus for 1 year after the end of the member's term.
- Data associated with tax payments (including payroll, corporate and VAT) will be held for 5 years.
- Operational data related to project activities, project proposals, reporting and project management will be held for the period required by x2VOL.

Data Backup

Daily Backups

Backup software shall be scheduled to run nightly to capture all incremental backup data from the previous day.

- Backup logs are to be reviewed to verify that the backup was successfully completed.

Monthly Backups

One full copy of "off-site" backup data shall be properly labeled and stored in a secure location other than x2VOL's premises at the end of each month. In case of a disaster, these off-site backups should be available for retrieval. This off-site location shall be specified by IT management.

Physical Backups

Data on hard drives will be backed up daily, and mobile devices shall be brought in to be backed up on a weekly basis or as soon as practical if on an extended travel arrangement.

Documentation

Written documentation shall be maintained and updated that are relevant to each specific personnel role in the backup procedure. These instructions shall be provided to each personnel as a reference to their role and responsibilities as they pertain to backups.

Backup Configuration

Backup services shall be enabled on any cloud infrastructure / VPS infrastructure used by x2VOL. The minimum backup configuration is as follows:

- Cloud-server backup snapshots shall be configured to maintain one full backup of each server separately at least once per week. These weekly backups shall be maintained for at least 2 months.
- Each month, one full backup snapshot will be maintained as a long-term backup. Each long-term backup shall be maintained for at least one year.
- Backup restoration process shall be tested regularly.

Mobile Device Data

Items Covered

Mobile computing and storage devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives (also known as a "thumb-drive"), smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or x2VOL owned, that may connect to or access the information systems at the x2VOL.

Risks

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the x2VOL. These risks must be mitigated to acceptable levels as described below:

- Under no circumstances should confidential or sensitive information be copied to a USB flash drive or other unencrypted device. Files that must be transferred between devices may be transferred via a direct e-mail or by an approved cloud-storage service via a protected URL link to the resource that requires authentication.
- If files are stored on a removable hard-disk or network attached storage (NAS) device, the device must be a self-encrypting device (SED) that is capable of encrypting all stored data with an AES algorithm that uses 256-bit key strength unless otherwise approved by IT management.

Encryption

Portable computing devices and portable electronic storage media that contain confidential, or sensitive x2VOL information must use encryption to protect the data while it is being stored.

Database

Databases or portions thereof, which reside on the network at the x2VOL, shall not be downloaded to mobile computing or storage devices.

Minimum Requirements:

- Report lost or stolen mobile computing and storage devices to the IT department.
- Non-departmental owned devices that may connect to the x2VOL internal network must first be approved by the IT department.
- Compliance with the Remote Access policy is mandatory.