

# **STANDARD STUDENT DATA PRIVACY AGREEMENT**

**TX-NDPA v1r6**

**School District or LEA**

Goose Creek CISD

**and**

**Provider**

Zaner-Bloser, Inc.

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

[ Goose Creek CISD ], located at [ 4544 I-10 East, Baytown, TX 77521 ] (the "Local Education Agency" or "LEA")  
and

[ Zaner-Bloser, Inc. ], located at [ 1400 Goodale Blvd, Grandview Heights, OH 4312 ] (the "Provider").

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
  - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**
  - If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "Services").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Randal O'Brien Title: Superintendent

Address: 4544 Interstate 10 East, Baytown, TX 77521

Phone: \_\_\_\_\_ Email: randal.obrien@gccisd.net

The designated representative for the Provider for this DPA is:

Name: Laureen Reynolds Title: Director, RFP Services

Address: 1400 Goodale Blvd., Grandveiw Heights, OH 43212

Phone: 603-554-0697 Email: laureen.reynolds@zaner-bloser.com

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

LEA:

By: 

Date: 6.26.23

Printed Name: Randal O'Brien Title/Position: Superintendent

Provider:

By: 

Date: 5/20/23

Printed Name: Robert Heighton Title/Position: VP, Operations

**STANDARD CLAUSES**

Version 1.0

**ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the 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 to **Exhibit "H"**. 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



**Exhibit "H"**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

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

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

Access to activities and resources on MyZBPortal.com. Access is product-specific.

**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.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input checked="" type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input checked="" type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:	<input type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

**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**

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:

[ ]

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:

[ ]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

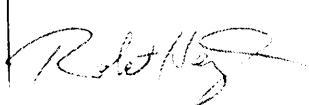
By [ ]

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

  
\_\_\_\_\_  
Authorized Representative of Provider

5/20/23  
Date

**EXHIBIT "E"**

**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [Goose Creek CISD ] ("Originating LEA") which is dated [ 5/20/23 ], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: laureen.reynolds@zaner-bloser.com

**[NAME OF PROVIDER]**

BY: Laureen Reynolds Date: 5/20/23

Printed Name: Laureen Reynolds Title/Position: Director, RFP Services

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **[Insert Name of Originating LEA]** and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA:**

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

DESIGNATED REPRESENTATIVE OF LEA:

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_ Email: \_\_\_\_\_

**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

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	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"****Supplemental SDPC State Terms for Texas**

Version 1.0

This **Exhibit "G"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [Goose Creek CISD ] (the "Local Education Agency" or "LEA") and [Zaner-Bloser, Inc. ] (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.
2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.
3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

~~**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.~~

**Consider Provider as School Official.** The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider's obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

5. **Modification to Article VII, Section 4 of the DPA.** Article VI, Section 4 of the DPA (Annual Notification of Rights.) is amended as follows:

**Entire Agreement.** This DPA and the ~~Service Agreement~~ constitutes 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.

6. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:
- a. Providing notification to the employees or parents of those students whose LEA Data was compromised and regulatory agencies or other entities as required by law or contract;
  - b. Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;
  - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
  - d. Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.
7. **No Exhibit E without unaltered DPA including Texas Addendum.** Any alterations are only allowed in **Exhibit "H"**. Any terms under **Exhibit "H"** do not apply to **Exhibit "E"** and render **Exhibit "E"** null and void.

**EXHIBIT "H"**

**Additional Terms or Modifications**

Version 1r6

LEA and Provider agree to the following additional terms and modifications:

Please see the attached Privacy Policy, Technology Safeguards, Data Breach Response Plan and NIST CSF table for a comprehensive overview of our policies and practices.

## **PRIVACY POLICY**

Zaner Bloser, Inc. ("Zaner-Bloser", "we", "us") respects your privacy and is committed to protecting it through our compliance with this policy.

This policy was last updated on June 29, 2020.

For your convenience, here is our contact information:

Our postal address is  
PO Box 16764  
Columbus, OH 43216-6764

Our address is  
1400 Goodale Boulevard, suite 200  
Grandview Heights, OH 43212

We can be reached via e-mail at [customerexperience@zaner-bloser.com](mailto:customerexperience@zaner-bloser.com) or you can reach us by telephone at [1-800-421-3018](tel:1-800-421-3018).

## **MYZBPORTAL.COM**

**Please be advised that there are important differences in how Zaner-Bloser handles data in connection with the MYZBPORTAL as compared to our public-facing consumer websites, specifically in connection with any data that may include Student PII (Personally Identifiable Information).**

### **School data and PII:**

MyZBPortal.com collects the following student PII:

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.



**Cookies:**

Superkids Portal (Teachers, Admins, Parents) and Superkids Online Fun app and desktop shortcut (Students)

The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the Superkids Portal is to track the user's session and visit. Zaner-Bloser, Inc.'s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

ZB Portal (Teachers, Admins, Students)

The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the MYZBPortal is to track the user's session and visit. Zaner-Bloser, Inc.'s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

**Data encryption:**

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

**Data retention:**

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

**Data access:**

Only authorized individuals are provided access to our systems. Passwords are never transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

**System hosting:**

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

**Perimeter security:**

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

**Vulnerabilities and patching:**

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

**Consent from Schools regarding Students' Personal Information:**

The Children's Online Privacy Protection Act ("COPPA") permits a school, acting in the role of "parent" to provide required consents regarding personal information of students who are under the age of 13. Where a school is the subscriber to our portal, we rely on this form of COPPA consent. We provide the school with this privacy policy, to ensure that the school, in providing its COPPA consent, has full information and assurance that our policies comply with COPPA.

The Family Educational Rights and Privacy Act ("FERPA") permits a school to provide educational records (including those that contain students' personal information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of "school official" by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this personal information except for the purposes of providing this portal to the school. We comply with FERPA by relying on this form of consent.

**Your Rights:**

As a user of the portal, you have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of and erase your personal information. If you are a student at an educational institution using the Portal, you should direct any requests to exercise your data rights to the appropriate representative at your educational institution. If you are an educator or an administrator, you may reach out to us directly via e-mail at [customerexperience@zaner-bloser.com](mailto:customerexperience@zaner-bloser.com) or you can reach us by telephone at 1-800-421-3018.

### School data and PII:

MyZBPortal.com collects the following student PII (personally identifiable information):

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.

### Data encryption:

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

### Data retention:

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

### Data access:

Only authorized individuals are provided access to our systems. A username and password must be input and authenticated prior to gaining access to any information. Passwords use one-way salted hashes and technical support does not have access to a user's password. Passwords are **never** transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

### System hosting:

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

Perimeter security:

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

Vulnerabilities and patching:

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

## Zaner-Bloser, Inc. Security Incident Response Process

The following denotes the high-level steps to be followed when a potential security issue is suspected, reported, or detected. In case of an actual *security incident*, detailed procedures for each of the steps will be carried out based upon the type and/or nature of the incident.

### Assessment

- Assess the potential security issue and all pertinent information to determine if the event is an actual security incident.

**Note:** This process will stop here if it is determined that the reported issue was not an actual security incident and no breach occurred

- Determine if any *Cardholder Data* is involved
- Create a Security Incident Report Form and document the preliminary findings
- Notify (via email) SIRT at: SIRT@highlights.com and the Information Security Steering committee (ISSC) at: ISSC@Highlights.com that an actual security incident has occurred
- If necessary, notify the user(s) of the affected device, system or network that a problem has occurred and access and/or usage must be limited and/or halted until the problem is resolved
- Document ongoing analysis as appropriate on the Security Incident Response Form

### Containment

- If *Cardholder Data* (CHD) is involved:
  - Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials). The compromised system(s) must be taken offline immediately and not be used to process payments or interface with payment processing systems.
  - Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging the network cable(s) or through other means.
  - Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
  - Await further instruction from the ISSC or the V.P., Government Relations, Information Security and Privacy before proceeding with this process
- If *Cardholder Data* (CHD) is not involved:
  - Determine if it is necessary to disconnect the device from the Internet and/or the network
  - Determine if it is necessary to shut down the affected device, system, or network

- Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
- Document and track all actions taken to contain the *security incident* on the Security Incident Response Form

#### **Eradication**

- Eradicate the problem that is affecting the device, system or network
- Determine whether disk drives should be cleaned/reformatted
- Ensure that previous device, system, and/or network file backups are not infected and take appropriate action
- Document and track all actions taken to eradicate all issues related to the security incident on the Security Incident Response Form

#### **Restoration**

- Decide whether the device, system and/or network needs to be restored from previous uninfected file backups
- Perform recovery procedures/processes as required
- Document and track all actions taken to restore workstation, network, system, etc. to its normal state on the Security Incident Response Form

#### **Communication and Notification**

- Communicate the appropriate information to the appropriate senior management personnel regarding the occurrence of the security incident (if a breach occurred)
- As warranted, notify the appropriate external entities (law enforcement, federal agency, state agency, Office of the Privacy Commissioner of Canada, payment card brands, payment card acquirers, customers, etc.) regarding the occurrence of the security incident (if a breach occurred involving credit card information or other personally identifiable information)
- If a user's workstation has to be reimaged due to a security incident, the user's manager will be notified and a copy of the Security Incident Response Form sent to the manager

#### **Closure**

- Ensure that the incident response process and the Cardholder Data Security Breach Response Process is updated with all lessons-learned and all appropriate industry developments regarding security incident or security breach response
- Ensure that all documentation, data, and/or information related to the security incident has been captured and is securely stored
- Ensure that all appropriate internal and external communication has been conducted as required

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor’s Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	Policies, processes, and procedures around asset management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	<b>Business Environment (ID.BE):</b> The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	<b>Risk Management Strategy (ID.RM):</b> The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working

Function	Category	Contractor Response
		towards the implementation of a high-level risk strategy in upcoming years.
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	The organization reviews and mitigates supply chain risks on a regular basis.
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Active Directory and Multi-factor authentication is used to access backend end system. Web user access is controlled using local authentication. Industry best practices are used for password strength.
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Security training and acknowledgement of our corporate information security policy is required for all staff and contractors annually and immediately upon hire.
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	All connections are transmitted over secure channels using strong encryption (TLS 1.2). persistent data stored (at rest) is encrypted within our Microsoft Azure Cloud services. Systems and data are managed in a way that is consistent with our corporate information security policy.
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.  For instance, access is granted using a least-privilege model based on need. Where resources permit, access is granted based on defined roles and separation of duties.
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Automated Backups are conducted regularly. Maintenance and repairs of the physical components are managed by Microsoft within the Azure Cloud.
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Technical tools used are consistent with our policies, procedures, and agreements. For instance, tools such Web vulnerability scanners are deployed to identify potential risks and guide remediation efforts.



Function	Category	Contractor Response
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incidents are managed in a way that is consistent with our corporate information security policy and incident response process.
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Our incident response procedures call for this type of communications.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Our incident response procedures call for this type of activity.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our incident response procedures call for this type of activity.
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We continually assess and enhance our processes to address the evolving threat environment as time and resources permit.
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Restoration of application and database assets are done using routinely taken backups in accordance with our incident response procedures.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Our incident response procedures call for this type of activity. Additionally, retrospectives are routinely conducted to discussion process improvements.
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Our incident response procedures call for this type of activity. Internal and external communication is done on a case-by-case basis.

