

STANDARD STUDENT DATA PRIVACY AGREEMENT

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

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

LOWELL PUBLIC SCHOOLS

and

TigerConnect, 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: Lowell Public Schools, located at 155 Merrimack Street, Lowell, MA 01852 USA (the “Local Education Agency” or “LEA”) and TigerConnect, Inc., located at 2110 Broadway, Santa Monica, California, 90404 (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 Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

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

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

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

The designated representative for the Provider for this DPA is:

Name: Jordan Leo Title: VP Controller

Address: 2054 Broadway; Santa Monica, CA 90404; Estados Unidos

Phone: (415) 755-8189

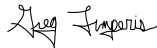
Email: legal@tigerconnect.com

The designated representative for the LEA for this DPA is:

Greg Limperis, Director of Technology
Lowell Public Schools
155 Merrimack Street, Lowell, MA 01852
glimperis@lowell.k12.ma.us
978-674-4320


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

LOWELL PUBLIC SCHOOLS

By: 
Date: 05/13/24

Printed Name: Greg Limperis
Title/Position: Director of Technology

TigerConnect, Inc.

DocuSigned by:
By: 
Date: April 2nd, 2024

Printed Name: Jordan Leo
Title/Position: VP Controller

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 these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

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

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

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

TigerConnect- a platform that can be used for clinical communication and also as a collaboration tool.

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.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
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	
	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	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	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.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
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

Authorized Representative of Company

Date

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"
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"
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 "1"**.
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.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"

New York

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

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

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

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 6 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:



Information Security Incident Management

Required Reading: Workforce members involved in information security incident response, mitigation and breach management Security

Original Date: 06/01/2020

Review Date: 02/13/2023

Revised: 02/15/2023

Disposition Instructions: Retain all previous versions of this policy for a minimum of 6 years from the date of creation or revision, whichever is later.

POLICY STATEMENT:

TigerConnect will support and maintain a viable information security incident management program.

PROCEDURE:

In accordance with the standards set forth under Federal and State statutory requirements (hereafter referred to as regulatory requirements), TigerConnect is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this policy/procedure is to define roles, responsibilities and processes for information security incident management.

Scope & Goals

The scope of this policy/procedure is to define the process for identification, response, reporting, assessment, analysis, and follow-up to information security incidents. This policy applies to the following types of security incidents (also refer to Appendix 1 – Examples of Security Incidents/Breaches):

- Technical security incidents (e.g., computer/network intrusions, denial of service to authorized users, unauthorized access, etc.)
- Non-technical security incidents (e.g., administrative and physical incidents including, but not limited to theft, lost devices, unlocked doors, unauthorized facility entry, unauthorized computer access, etc.)



Goals of this policy/procedure are, but not limited to the following:

- Define the relationship between a security incident and a reportable breach of ePHI/PHI.
- Describe activities associated with incident identification, containment, eradication, recovery and post-incident remediation.
- Define members of the Security Incident Response Team (SIRT).

Responsibilities

Information Security Officer (ISO)

The ISO is responsible for, but not limited to the following activities:

- Revisions, implementation, workforce education, interpretation and enforcement of this policy.
- Co-facilitate the Incident Response Team
- Coordinates efforts in respect to the vulnerability management program as applicable and needed to utilize network tools for IPS, IDS, forensics, vulnerability assessments and validation (refer to the Vulnerability Management Policy)
- Primary point of contact and investigation officer for all information security incidents. Will serve as an integral part of the organization's incident response capability and as needed offer advice and assistance to users of information systems for the handling and reporting of security incidents.
- Advisor to the organization's Crisis Management Team
- Assist Privacy Officer with breach management duties
- Facilitate semi-annual tabletop exercises with all members of the SIRT to ensure everyone understands their roles.
- Provide workforce members with a process and method to report security issues and/or breaches anonymously
- Maintain a list of third-party security contact information in the event an incident needs to be reported to an outside party
- Ensure workforce members that are part of the incident response and/or contingency management teams are provided the incident response and contingency plan immediately and training within ninety (90) days, when required by information system changes, and annually thereafter.
- Ensure members of the Incident Response Team are properly trained to handle incidents that involve or are caused by insider threat.
- Ensure a duress alarm is available for workforce members to use in the event of an emergency and that procedures are documented for how to respond to high-risk situations.

Privacy Officer

The Privacy Officer is responsible for, but not limited to the following activities:

- Co-facilitate the Incident Response Team



- Advisor to the organization's Crisis Management Team
- Alternate investigation officer for all information security incidents
- Breach management

Security Incident Response Team (SIRT)

The SIRT is responsible for, but not limited to the following activities:

- Keeping the Crisis Management Team informed on all incident management activities.
- Ensuring that all incidents are fully documented from discovery to remediation and include all individuals involved and the actions that were taken.
- Providing oversight and management of incident response and reporting activities.
- Reviewing and approving the breach risk analysis.
- Specific duties outlined by the SIRT member roles and responsibilities in the Appendix 2.
- Ensuring that incidents are promptly reported to external entities when necessary.

Crisis Management Team

The Crisis Management Team is responsible for the process by which the organization deals with major events that threaten to harm the organization, its stakeholders/customers/clients, or the general public. The Crisis Management Team is responsible for keeping TigerConnect's leadership team apprised on incident/breach management activities.

Information Technology (IT)

The IT is responsible for, but not limited to the following activities:

- IT will be responsible for performing activities associated with the containment, eradication and recovery phases of this policy/procedure.
- Maintaining detailed internal procedures for performing containment, eradication and recovery activities.

Incident Discovery/Notification

Incident discovery/notification can come from, but not limited to the following:

- Workforce member
- Insider Threat
- Anonymous call/email
- Firewall, intrusion detection/prevention, anti-virus technology, etc.
- System audit log review
- Patient/client/customer
- Third party vendor/contractor/consultant
- Internal/external audit



- Business partner
- Third party security services (not associated with the organization)
- Third party threat notification services
- Media
- Duress alarm
- Physical security related incidents

Incident Response Process

The incident response process begins immediately upon discovery or notification. The date/time is very important to the breach notification process if the incident is determined to be a breach of ePHI/PHI (see [Breach Management policy/procedure](#)).

The following phases represent the entire information security incident management process. These phases often happen quickly and do not necessarily happen in the order listed in this policy/procedure. It is also common for activities within each phase to occur simultaneously.

Identification Phase

1. The ISO or Privacy Officer will determine if what is being reported is an event, precursor, or security incident.
2. If the issue is an event, the ISO/Privacy Officer will contact the appropriate internal resource for resolution.
3. If the issue is a precursor or security incident, the ISO/Privacy Officer will determine if it is technical or non-technical and at the same time activate the SIRT and Crisis Management Team and begin to document background information and any evidence found related to the incident on an Information Security Incident Response/Investigation Form. Among other factors being noted in this form, special attention will be given to listing all employees involved with the security incident. The SIRT will proceed as follows:
 - Non-Technical Security Incident: The SIRT completes the investigation, implements preventative measures, and resolves the security incident. Upon completion of the investigation, the SIRT will move to the Post-Incident Remediation Phase.
 - Technical Security Incident: Go immediately to the Containment Phase.
4. Other activities could include the following:
 - Contact law enforcement or other external parties (if appropriate), more on communication below.
 - Contact media outlets - If a security incident has already garnered media attention the Crisis Management Team may choose to initiate contact with media outlets. TigerConnect's media relations representative will serve as the sole point of contact for activities related to the news media.
 - Begin the breach risk analysis process if it is determined or suspected that ePHI/PHI may be involved.



- Contract with a third party to perform or internally begin forensic analysis (if necessary)
- Contact cyber-insurance representative (if the organization has cyber-insurance)

Containment Phase

During this Phase, TigerConnect's Information Technology (IT) department will attempt to contain the security incident. Depending on the type of incident, actions performed by IT will vary.

It is extremely important to take detailed notes and protect the chain of custody when information technology assets are involved in the incident. This information will be very helpful to digital forensic analysis and can be used during civil and criminal litigation and/or disciplinary/termination action.

Eradication Phase

This phase represents IT's activities to remove the cause, patch/repair security vulnerabilities that resulted in the security incident.

Recovery Phase

The Recovery Phase represents IT's effort to restore the affected environment back to normal operation after security vulnerabilities have been remediated.

Post-Incident Remediation

Once an incident has been recovered from, the SIRT team will ensure applicable audit trails and the related evidence are collected into a centralized location. The driving factors that determine the applicable information that is needed, and direction of this task is the following:

- Is the information essential for internal problem analysis?
- Could the information be used as forensic evidence in relation to a potential breach of contract or regulatory requirement, or in the event of civil or criminal proceedings?
- Could the information be used as leverage for negotiating for compensation from software and service suppliers.

If an answer to the above questions was YES, then that information will be collected and categorized.

Additionally, the post-incident remediation phase represents the review of the security incident by the SIRT to determine the following:

- What additional actions (if any) need to be taken.
- If breach notification is required (see [Breach Management policy/procedure](#)).
- Review incident and if applicable, breach related documentation to ensure that it is complete.



- Whether there are any recurring or high-impact incidents and any improvements to the existing incident response process that need to be implemented.
- Prepare formal communication or arrange a meeting with senior leadership to brief them on the outcome of the incident.
- Close the security incident.

After the final resolution of incidents, the SIRT team will ensure lessons learned are incorporated into the incident response policy and procedures, training, and testing exercises.

Security assessments will be used against all incidents or on a sample of incidents, to further validate the effectiveness (or expose weakness) of the established controls within the incident response program and the related risk assessment that led to them.

Incident Response Training & Evaluation

The SIRT will semi-annually review and evaluate the processes outlined in this policy/procedure. This activity will coincide with mandatory exercises to practice the effectiveness and maintain familiarity with the process by SIRT members. Reviews and analysis of prior incidents will be used in this training as well as simulations of possible incidents. The business continuity and disaster recovery teams (responsible for contingency planning activities for the organization) will also be part of these exercises. All lessons learned will be documented and incorporated into an updated incident response plan. The end goal of this training is to ensure that the SIRT and contingency teams understand the current threats and risks to the organization, as well as their responsibilities in supporting the incident response process. A formal test will not be necessary if the organization actively exercises its response capability because of real incidents.

Communications of incidents with external parties

When applicable, necessary, or required by law and regulations, communication of incidents to external parties will be made promptly. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting will be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The organization communicates with outside parties regarding the incident. External parties to be considered, but not limited to, would be the federal Computer Incident Response Center (FedCIRC) and the CERT Coordination Center (CERT/CC), law enforcement, and possibly fielding inquiries from the media.

Documentation Retention

Records related to security incidents, risk analysis and breach decisions will be retained for a period of no less than 6 years from the date of the documentation.

Exception Management



Exceptions to this policy/procedure will be evaluated in accordance with TigerConnect's Information Security Exception Management Policy

Applicability

All employees, volunteers, trainees, consultants, contractors and other persons (i.e. workforce) whose conduct, in the performance of work for TigerConnect, is under the direct control of TigerConnect, whether or not they are compensated by TigerConnect.

Compliance

Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with TigerConnect. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.

Jacob Scheid

06/08/23

Concurred By

Date Approved

Annual Review

Reviewed By	Review Date	Changes
TBJ	10/07/2021	No Changes
TBJ	10/21/2022	No Changes
EBK	02/15/2023	Formatting updates, no changes.



Appendix 1 – Examples of Security Incidents/Breaches

Name	Description
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Disposal Mobile	Discovery of mobile devices not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud SE	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly, not stolen
Lost Drive	Lost data drive (unspecified if IDE, SCSI, thumb drive, etc.)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (e.g. disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc.
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Drive	Missing drive, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Other	Miscellaneous breach type arising primarily from data mishandling
Phishing	Masquerading as a trusted entity in an electronic communication to obtain data
Seizure	Forcible taking of property by a government law enforcement official
Skimming	Using electronic devices (such as a skimmer) to swipe victims' credit/debit card numbers
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Snooping	Exceeding intended privileges and accessing data for unauthorized purposes
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc.
Stolen Laptop	Stolen Laptop (generally specified as a laptop in media reports)
Stolen Media	Media generally reported or known to have been stolen by a third party
Stolen Mobile	Stolen mobile phone or device such as tablets, etc.
Stolen Tape	Stolen backup tapes
System Failure	System failure or loss of service
Unknown	Unknown or unreported breach type



Virus (Malware)	Exposure to personal information via virus or Trojan (possibly classified as hack)
Web	Web-based intrusion, data exposed to the public via search engines, public pages
Wireless Access Point	Installation / use of an unauthorized wireless access point

Appendix 2 – SIRT Members and Primary Responsibilities

SIRT Member	Role	Primary Responsibilities
Information Security Officer (ISO)	Team Leader and Security advisor	<ul style="list-style-type: none"> ● Convenes team and chairs SIRT meetings ● Oversees the information security incident response process. ● Assists the Privacy Officer with breach risk analysis activities. ● Submits progress and final reports to senior leadership. ● Submits final report and oversees debriefing. ● Tracks and reports on security related changes that could impact business operations, resulting from incident.
Privacy Officer	Alternate Team Leader and Privacy advisor	<ul style="list-style-type: none"> ● Provides information on privacy-related regulatory requirements. ● Oversees discovery and investigation from a privacy perspective. ● Recommends steps for privacy compliance and to mitigate the risk of penalties. ● Oversees breach management program and is responsible for breach risk analysis and notification processes. ● Advises team on privacy issues.
Legal	Legal advisor	<ul style="list-style-type: none"> ● Provides information on major contracts and other obligations that may be relevant to incident and breach management ● Oversees discovery and investigation from an evidentiary perspective, in the case of civil or criminal litigation. ● Provides advice on minimizing legal liability. ● Coordinates with internal and external legal teams as needed.



SIRT Member	Role	Primary Responsibilities
Information Technology (CTO)	IT advisor	<ul style="list-style-type: none"> ● Aids in determining the existence, cause and extent of an IT-related incident (e.g., reviews firewall/IPS/sys logs for correlating evidence of unauthorized access). ● Coordinates incident management activities assigned to IT. ● Coordinates with IT to identify victims in TigerConnect systems. ● Coordinates with IT organization to plan and implement actions to prevent similar future incidents.
Finance (CFO)	Financial advisor	<ul style="list-style-type: none"> ● Assists with evaluating financial liability. ● Provides financial assistance when needed. ● Assists with cost/benefit analysis when applying controls.
IT	Facilities and physical security advisor	<ul style="list-style-type: none"> ● Advises on matters related to physical, facility and environmental security. ● Coordinates activities between the organization and law enforcement. ● Remediates any physical facility changes.
Media Relations	Public relations advisor	<ul style="list-style-type: none"> ● Coordinates activities between the organization and public media. ● Prepares and issues press releases or statements, as needed.
Human Resources	Human Resource advisor	<ul style="list-style-type: none"> ● Advises on employment law issues. ● If employee personal data is compromised, handles internal communications ● If employee misconduct is a factor, works with appropriate business managers, legal representatives and others to take appropriate employment action (e.g., termination of employment).
SIRT Team Members		<p>https://tigertext.atlassian.net/wiki/spaces/SEC/pages/edit-v2/2748874927</p>





CONTROL REFERENCE

- **1502.02f1Organizational.4:** A list of employees involved in security incidents is maintained with the resulting outcome from the investigation. (#1)
- **1523.11c3Organizational.24:** Incidents are promptly reported to the appropriate authorities and outside parties (e.g., FedCIRC, CERT/CC). (#2)
- **1506.11a1Organizational.2:** There is a point of contact for reporting information security events who is made known throughout the organization, always available, and able to provide adequate and timely response. The organization maintains a list of third-party contact information, which can be used to report a security incident. (#3)
- **1516.11c1Organizational.12:** The security incident response program accounts for and prepares the organization for a variety of incidents. (#4)
- **1517.11c1Organizational.3:** There is a point of contact who is responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process. (#5)
- **1311.12c2Organizational.3:** The organization's employees are provided with crisis management awareness and training. (#6)
- **1508.11a2Organizational.1:** The organization provides a process/mechanism to anonymously report security issues. (#7)
- **1522.11c3Organizational.13:** An incident response support resource, who is an integral part of the organization's incident response capability, is available to offer advice and assistance to users of information systems for the handling and reporting of security incidents in a timely manner. (#8)
- **1515.11a3Organizational.3:** Incidents (or a sample of incidents) are reviewed to identify necessary improvement to the security controls. (#9)
- **1521.11c2Organizational.56:** Testing exercises are planned, coordinated, executed, and documented periodically, at least annually, using reviews, analyses, and simulations to determine incident response effectiveness. Testing includes personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team. (#10)
- **1313.02e1Organizational.3:** The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities within ninety (90) days of assuming an incident response role or responsibility; when required by information system changes; and within every three hundred sixty-five (365) days thereafter. (#11)
- **1507.11a1Organizational.4:** The organization has implemented an insider threat program that includes a cross-discipline insider threat incident handling team. (#12)



- **1560.11d1Organizational.1:** The information gained from the evaluation of information security incidents is used to identify recurring or high impact incidents and update the incident response and recovery strategy. (#13)
- **1589.11c1Organizational.5:** The organization tests and/or exercises its incident response capability regularly. (#14)
- **1510.11a2Organizational.47:** Reports and communications are made without unreasonable delay and no later than sixty (60) days after the discovery of an incident, unless otherwise stated by law enforcement orally or in writing and include the necessary elements. (#15)
- **1511.11a2Organizational.5:** All employees, contractors and third-party users receive mandatory incident response training to ensure they are aware of their responsibilities to report information security events as quickly as possible, the procedure for reporting information security events, and the point(s) of contact, including the incident response team, and the contact information is published and made readily available. (#16)
- **1512.11a2Organizational.8:** Intrusion detection/information protection system (IDS/IPS) alerts are utilized for reporting information security events. (#17)
- **1520.11c2Organizational.4:** The incident response plan is communicated to the appropriate individuals throughout the organization. (#18)
- **1539.11c2Organizational.7-** Incident response is formally managed and include specific elements. (#19)
- **1562.11d2Organizational.2:** The organization coordinates incident handling activities with contingency planning activities. (#20)
- **1563.11d2Organizational.3:** The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, training and testing exercises, and implements the resulting changes accordingly. (#21)
- **1587.11c2Organizational.10:** The incident management plan is reviewed and updated annually. (#22)
- **1514.11a3Organizational.12:** A duress alarm is provided whereby a person under duress can indicate such problems and responded to accordingly by the organization. (#23)
- **1505.11a1Organizational.13:** A formal security incident response program has been established to respond, report (without fear of repercussion), escalate and treat breaches and reported security events or incidents. Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that is included in the incident notification. This reporting includes notifying internal and external stakeholders, the appropriate community Computer Emergency Response Team, and law enforcement agencies in accordance with all legal or regulatory requirements for involving such organizations in computer incidents. (#24, for reporting requirements, rest of policy for everything else)
- **1259.09ab2System.9:** The organization responds to physical security incidents and coordinates results of reviews and investigations with the organization's incident response capability. (#25 for specific policy statement, and the rest for incident response process)
- **1509.11a2Organizational.236:** The incident management program formally defines information security incidents and the phases of incident response; roles and responsibilities; incident handling, reporting and communication processes; third-party relationships and the handling of



third-party breaches; and the supporting forensics program. The organization formally assigns job titles and duties for handling computer and network security incidents to specific individuals and identifies management personnel who will support the incident handling process by acting in key decision-making roles. **(#26, for statements and the rest for incident response program overview)**

- **1561.11d2Organizational.14:** The organization has implemented an incident handling capability for security incidents that addresses (i) policy (setting corporate direction) and procedures defining roles and responsibilities; (ii) incident handling procedures (business and technical); (iii) communication; (iv) reporting and retention; and (v) references to a vulnerability management program. **(#27 for specific policy, entire document for “ii” from illustrative procedures)**
- **1518.11c2Organizational.13:** The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its incident management program. **(#28)**
- **1513.11a2Organizational.9:** The organization adheres to the HITECH Act requirements for responding to a data breach (of covered information) and reporting the breach to affected individuals, media, and federal agencies. **(#29)**
- **1713.03c1Organizational.3:** The organization mitigates any harmful effect that is known to the organization of a use or disclosure of covered information (e.g., PII) by the organization or its business partners, vendors, contractors or similar third party in violation of its policies and procedures.

Incident Response Process & Security Incident Response Team (SIRT)

Summary

In accordance with the standards set forth under Federal and State statutory requirements (hereafter referred to as regulatory requirements), TigerConnect is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities and processes for information security incident management.

SIRT Members

Name	Title	Email	Phone
Jacob Scheid	Sr. DevOps Security Engineer	jscheid@tigerconnect.com	513-490-2743
Tyler Jones	DevOps Security Engineer	tjones@tigerconnect.com	937-269-8172
Ebony Kassama	DevOps Security Engineer	ekassama@tigerconnect.com	443-900-5758
Brett Potter	Security Engineer	bpotter@tigerconnect.com	206-992-3213
Scott Fretheim	Sr. Director, IT	sfretheim@tigerconnect.com	425-419-9372
Brandon Neal	Director, DevOps	bneal@tigerconnect.com	310-310-9439
Mike Olson	Sr. Manager, Web Software Engineering	molson@tigerconnect.com	818-288-1462

Cary Dobeck	Lead Android Engineer	cdobeck@tigerconnect.com	310-341-8375
Sourabh Gupta	Sr. iOS Software Engineer	sgupta@tigerconnect.com	+64-21-296-3649
Patrick Southall	Director, QA	psouthall@tigerconnect.com	805-231-0847
Darren Zhu	VP, Engineering	dzhu@tigerconnect.com	404-509-1387
Anders Wei	Director, Engineering	anders@tigerconnect.com	+8615618819906
Grant Olson	Team Lead, Engineering	golson@tigerconnect.com	619-997-8918

SIRT Functions/Services

Reactive - Respond to active incident handling, including but not limited to:

- Incident analysis
- Incident response support and coordination
- Incident response resolution

Proactive - Improve the infrastructure and security processes of TigerConnect before any incident occurs or is detected. The main goals are to avoid incidents and to reduce the impact and scope when they do occur.

- Cyber Threat Analysis of vulnerability warnings and security advisories
- Monitor Adversaries' activities and related trends to help identify future threats
- Configuration and maintenance of security tools, applications, and infrastructure
- Annual incident response tabletop exercises to test current controls, processes, and overall security posture

Administrative - Services design to assist with requests from TigerConnect's Legal and HR Departments.

Engaging the SIRT

To directly contact the SIRT send a message to the ***IT Security Incidents/Support*** Forum in TC Messenger.

Incident Response Process

Identification Phase

1. The ISO or Privacy Officer will determine if what is being reported is an event, precursor, or security incident.
2. If the issue is an event, the ISO/Privacy Officer will contact the appropriate internal resource for resolution.
3. If the issue is a precursor or security incident, the ISO/Privacy Officer will determine if it is technical or non-technical and at the same time activate the SIRT and Crisis Management Team and begin to document background information and any evidence found related to the incident on an Information Security Incident Response/Investigation Form. Among other factors being noted in this form, special attention will be given to listing any and all employees involved with the security incident. The SIRT will proceed as follows:
 - a. Non-Technical Security Incident: The SIRT completes the investigation, implements preventative measures, and resolves the security incident. Upon completion of the investigation, the SIRT will move to the Post-Incident Remediation Phase.
 - b. Technical Security Incident: Go immediately to the Containment Phase.
4. Other activities could include the following:
 - c. Contact law enforcement or other external parties (if appropriate), more on communication below.
 - d. Contact media outlets - If a security incident has already garnered media attention the Crisis Management Team may choose to initiate contact with media outlets. TigerConnect's media relations representative will serve as the sole point of contact for activities related to the news media.
 - e. Begin the breach risk analysis process if it is determined or suspected that ePHI/PHI may be involved.
 - f. Contract with a third party to perform or internally begin forensic analysis (if necessary)

- g. Contact cyber-insurance representative (if the organization has cyber-insurance)

Containment Phase

During this Phase, TigerConnect's Information Technology (IT) department will attempt to contain the security incident. Depending on the type of incident, actions performed by IT will vary.

It is extremely important to take detailed notes and protect the chain of custody when information technology assets are involved in the incident. This information will be very helpful to digital forensic analysis and can be used during civil and criminal litigation and/or disciplinary/termination action.

Eradication Phase

This phase represents IT's activities to remove the cause, patch/repair security vulnerabilities that resulted in the security incident.

Recovery Phase

The Recovery Phase represents IT's effort to restore the affected environment back to normal operation after security vulnerabilities have been remediated.

Post-Incident Remediation

Once an incident has been recovered from the SIRT team will ensure applicable audit trails and the related evidence are collected into a centralized location. The driving factors that determine

the applicable information that is needed, and direction of this task is the following:

5. Is the information essential for internal problem analysis?
6. Could the information be used as forensic evidence in relation to a potential breach of contract or regulatory requirement, or in the event of civil or criminal proceedings?
7. Could the information be used as leverage for negotiating for compensation from software and service suppliers.

If an answer the above questions was YES, then that information will be collected and categorized.

Additionally, the post-incident remediation phase represents the review of the security incident by the SIRT to determine the following:

8. What additional actions (if any) need to be taken.
9. If breach notification is required (see Breach Management policy/procedure).
10. Review incident and if applicable, breach related documentation to ensure that it is complete.
11. Whether there are any recurring or high-impact incidents and any improvements to the existing incident response process that need to be implemented.
12. Prepare formal communication or arrange a meeting with senior leadership to brief them on the outcome of the incident.
13. Close the security incident.

After the final resolution of incidents, the SIRT team will ensure lessons learned are incorporated into the incident response policy and procedures, training, and testing exercises. Security assessments will be used against all incidents or on a sample of incidents, to further validate the effectiveness (or expose weakness) of the established controls within the incident response program and the related risk assessment that lead to them.






TigerConnect_Lowell_VendorSigned

Final Audit Report

2024-05-13

Created:	2024-05-13
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA_XGwyavCMvr5pCW4dFByei6yB-MM5-e0

"TigerConnect_Lowell_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-05-13 - 11:19:09 AM GMT
-  Document emailed to Gregory Limperis (glimperis@lowell.k12.ma.us) for signature
2024-05-13 - 11:19:17 AM GMT
-  Email viewed by Gregory Limperis (glimperis@lowell.k12.ma.us)
2024-05-13 - 12:15:00 PM GMT
-  Document e-signed by Gregory Limperis (glimperis@lowell.k12.ma.us)
Signature Date: 2024-05-13 - 12:17:13 PM GMT - Time Source: server
-  Agreement completed.
2024-05-13 - 12:17:13 PM GMT