

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

School District or LEA
Ector County ISD

and

Provider
eluma (speech teletherapy)

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:

[], located at [] (the “**Local Education Agency**” or “**LEA**”) and

[], located at [] (the “**Provider**”).

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

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Leslie Wilson Title: Exec Dir of Sp Services

Address: 804 Sam Houston

Phone: 432 456 8719 Email: leslie.wilson@ECTORCountyisd.org

The designated representative for the Provider for this DPA is:

Name: _____ Title: _____

Address: _____

Phone: _____ Email: _____

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

LEA:

By: Leslie Wilson Date: 11/30/22

Printed Name: Leslie Wilson Title/Position: Exec Dir of Sp. Serv

Provider:

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

The designated representative for the LEA for this DPA is:

Name: Leslie Wilson Title: Exec Dir of Sp Services
Address: 804 Sam Houston
Phone: 432.456.8719 Email: leslie.wilson@ECTORCountyisd.edu

The designated representative for the Provider for this DPA is:

Name: Chad Gundry Title: Senior Director
Address: 2801 N Thanksgiving Way, #170, Lehi, UT 84043
Phone: 801-719-4225 Email: cgundry@elumatherapy.com

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

LEA:

By: Leslie Wilson Date: 11/30/22

Printed Name: Leslie Wilson Title/Position: Exec Dir of Sp. S.

Provider:

By: eluma LLC / Chad G Date: 11-29-22

Printed Name: Chad Gundry Title/Position: Senior Director

The designated representative for the LEA for this DPA is:

Name: Leslie Wilson Title: Exec Dir of Sp Services
Address: 804 Sam Houston
Phone: 4324568719 Email: leslie.wilson@ECTORCountyisd.c

The designated representative for the Provider for this DPA is:

Name: Chad Gundry Title: Senior Director
Address: 2801 N Thanksgiving Way, #170, Cedar, UT 84043
Phone: 801-719-4225 Email: cgundry@eluma.com

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

LEA:

By: Leslie Wilson Date: 11/30/22

Printed Name: Leslie Wilson Title/Position: Exec Dir of Sp. S

Provider:

By: eluma LLC / Chad G Date: 11-29-22

Printed Name: Chad Gundry Title/Position: Senior Director

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

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

ARTICLE III: DUTIES OF LEA

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

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit “A”** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between

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

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

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

EXHIBIT "A"
DESCRIPTION OF SERVICES

EXHIBIT "B"
SCHEDULE OF DATA

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

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

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

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

EXHIBIT "C"**DEFINITIONS**

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

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

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

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

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

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

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

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

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

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

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

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

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[]

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

[]

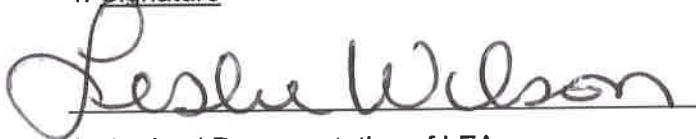
3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By []

4. Signature



Authorized Representative of LEA



Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[]

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

[]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By []

4. Signature

Leslie Wilson

Authorized Representative of LEA

11/29/22

Date

5. Verification of Disposition of Data

Chad Gandy

Authorized Representative of Provider

11-29-22

Date

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[]

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

[]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By []

4. Signature

Leslie Wilson

Authorized Representative of LEA

11/29/22

Date

5. Verification of Disposition of Data

Chad Gandy

Authorized Representative of Provider

11-29-22

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

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

[NAME OF PROVIDER]

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. Subscribing LEA

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

Subscribing LEA:

BY: Leslie Wilson Date: 11/29/22

Printed Name: Leslie Wilson Title/Position: Exec Dir of Sp. Services

SCHOOL DISTRICT NAME: Ector County ISD

DESIGNATED REPRESENTATIVE OF LEA:

Name: Leslie Wilson Title: Exec Dir of Sp Services

Address: 804 Sam Houston

Telephone Number: 432-456-8719 Email: Leslie.Wilson@ectorcountysd.org

EXHIBIT "E"**GENERAL OFFER OF PRIVACY TERMS****1. Offer of Terms**

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

[NAME OF PROVIDER]

BY: Chad Gundry Date: 11-29-22

Printed Name: Chad Gundry Title/Position: Senior Director

2. Subscribing LEA

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

Subscribing LEA:

BY: Leslie Wilson Date: 11/29/22

Printed Name: Leslie Wilson Title/Position: Exec Dir of Sp. Services

SCHOOL DISTRICT NAME: Ector County ISD

DESIGNATED REPRESENTATIVE OF LEA:

Name: Leslie Wilson Title: Exec Dir of Sp Services

Address: 804 Sam Houston

Telephone Number: 432-456-8719 Email: Leslie.Wilson@ectorcountysd.org

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

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

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

EXHIBIT "G"**Supplemental SDPC State Terms for Texas**

Version 1.0

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

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

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

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

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

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

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

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

EXHIBIT "H"**Additional Terms or Modifications**

Version

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

The wording in the first sentence of Article V.3 is changed from " The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. " to " The Provider agrees to utilize reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. "

eLuma uses NIST Cybersecurity Framework v1.1. We have included a self-assessment in each of the following areas of the framework - Identify, Protect, Detect, Recover, and Respond.

eLuma is in the process of enhancing and hardening our Insight Application and company practices and policies regarding data security. We have an independent risk assessment and penetration testing scheduled for December 2022/January 2023 to further enhance our security technology and practices. We plan to update our NIST self assessment following the completion of the risk assessment.

EXHIBIT “H” cont.

NIST - Identify

Identify: Functional Area summary			
Category	Name	As Is	To Be
Asset Management (ID.AM) Average	Asset Mgmt	1.83	4
Business Environment (ID.BE) Average	Bus. Environment	2	4
Governance (ID.GV) Average	Governance	1	4
Risk Assessment (ID.RA) Average	Risk Assessment	1.33	4
Risk Management Strategy (ID.RM) Average	Risk Mgmt. Strategy	1	4
Supply Chain Risk Management (ID.SC) Average	Supply Chain RM	0.2	4
Identify: Self-scoring worksheet			
Asset Management		As Is	To Be
ID.AM-1: Physical devices and systems within the organization are inventoried	ID.AM-1	2	4
ID.AM-2: Software platforms and applications within the organization are inventoried	ID.AM-2	3	4
ID.AM-3: Organizational communication and data flows are mapped	ID.AM-3	1	4
ID.AM-4: External information systems are catalogued	ID.AM-4	1	4
ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	ID.AM-5	3	4
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	ID.AM-6	1	4
Business Environment		As Is	To Be
ID.BE-1: The organization’s role in the supply chain is identified and	ID.BE-1	2	4

EXHIBIT “H” cont.

communicated			
ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	ID.BE-2	2	4
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	ID.BE-3	2	4
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ID.BE-4	2	4
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	ID.BE-5	2	4
Governance		As Is	To Be
ID.GV-1: Organizational information security policy is established	ID.GV-1	1	4
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	ID.GV-2	1	4
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ID.GV-3	1	4
ID.GV-4: Governance and risk management processes address cybersecurity risks	ID.GV-4	1	4
Risk Assessment		As Is	To Be
ID.RA-1: Asset vulnerabilities are identified and documented	ID.RA-1	1	4
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	ID.RA-2	1	4
ID.RA-3: Threats, both internal and external, are identified and documented	ID.RA-3	1	4
ID.RA-4: Potential business impacts and likelihoods are identified	ID.RA-4	3	4
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ID.RA-5	1	4
ID.RA-6: Risk responses are identified and prioritized	ID.RA-6	1	4
Risk Management Strategy		As Is	To Be
ID.RM-1: Risk management processes are established, managed, and agreed	ID.RM-1	1	4

EXHIBIT “H” cont.

to by organizational stakeholders			
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	ID.RM-2	1	4
ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	ID.RM-3	1	4
Supply Chain Management		As Is	To Be
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	ID.SC-1	1	4
ID.SC-2: Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process	ID.SC-2	0	4
ID.SC-3: Suppliers and 3rd-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan	ID.SC-3	0	4
ID.SC-4: Suppliers and 3rd-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted	ID-SC.4	0	4
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	ID-SC.5	0	4

NIST - Protect

Protect: Functional Area summary			
Category	Name	As Is	To Be
Identity Management, Authentication and Access Control (PR.AC) - Average	Identity Mgt	3	4
Awareness and Training (PR.AT) - Average	Awareness and Training	2	4

EXHIBIT “H” cont.

Data Security (PR.DS) - Average	Data Security	2.5	4
Information Protection Processes and Procedures (PR.IP) - Average	Info Protection	2.41	4
Maintenance (PR.MA) - Average	Maintenance	3	4
Protective Technology (PR.PT) - Average	Protective Tech	2.8	4

Protect: Self-scoring worksheet

Identity Management		As Is	To Be
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	PR.AC-1	3	4
PR.AC-2: Physical access to assets is managed and protected	PR.AC-2	3	4
PR.AC-3: Remote access is managed	PR.AC-3	3	4
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	PR.AC-4	3	4
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	PR.AC-5	3	4
PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	PR.AC-6	3	4
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)	PR.AC-7	3	4
Awareness and Training		As Is	To Be
PR.AT-1: All users are informed and trained	PR.AT-1	1	4
PR.AT-2: Privileged users understand roles and responsibilities	PR.AT-2	3	4
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	PR.AT-3	1	4

EXHIBIT "H" cont.

PR.AT-4: Senior executives understand roles and responsibilities	PR.AT-4	2	4
PR.AT-5: Physical and information security personnel understand roles and responsibilities	PR.AT-5	3	4
Data Security		As Is	To Be
PR.DS-1: Data-at-rest is protected	PR.DS.1	3	4
PR.DS-2: Data-in-transit is protected	PR.DS.2	3	4
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	PR.DS.3	2	4
PR.DS-4: Adequate capacity to ensure availability is maintained	PR.DS.4	2	4
PR.DS-5: Protections against data leaks are implemented	PR.DS.5	2	4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	PR.DS.6	2	4
PR.DS-7: The development and testing environment(s) are separate from the production environment	PR.DS.7	4	4
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	PR.DS.8	2	4
Info Protection		As Is	To Be
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)	PR.IP-1	2	4
PR.IP-2: A System Development Life Cycle to manage systems is implemented	PR.IP-2	4	4
PR.IP-3: Configuration change control processes are in place	PR.IP-3	4	4
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	PR.IP-4	4	4
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	PR.IP-5	4	4
PR.IP-6: Data is destroyed according to policy	PR.IP-6	3	4
PR.IP-7: Protection processes are continuously improved	PR.IP-7	3	4

EXHIBIT “H” cont.

PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	PR.IP-8	1	4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	PR.IP-9	0	4
PR.IP-10: Response and recovery plans are tested	PR.IP-10	0	4
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PR.IP-11	4	4
PR.IP-12: A vulnerability management plan is developed and implemented	PR.IP-12	0	4
Maintenance		As Is	To Be
PR.MA-1: Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools	PR.MA-1	3	4
PR.MA-2: Remote maintenance of organizational assets are approved, logged, and performed in a manner that prevents unauthorized access	PR.MA-2	3	4
Protective Tech		As Is	To Be
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PR.PT-1	2	4
PR.PT-2: Removable media is protected and its use restricted according to policy	PR.PT-2	3	4
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	PR.PT-3	3	4
PR.PT-4: Communications and control networks are protected	PR.PT-4	3	4
PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations)	PR.PT-5	3	4

NIST - Detect

Detect: Functional Area summary			
--	--	--	--

EXHIBIT "H" cont.

Category	Name	As Is	To Be
Anomalies and Events (DE.AE) - Average	Anomalies and Events	1	4
Security Continuous Monitoring (DE.CM) - Average	Continuous Monitoring	1.75	4
Detection Processes (DE.DP) - Average	Detection Processes	1	4
Detect: Self-scoring worksheet			
Anomalies and Events		As Is	To Be
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	DE.AE-1	1	4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	DE.AE-2	1	4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	DE.AE-3	1	4
DE.AE-4: Impact of events is determined	DE.AE-4	1	4
DE.AE-5: Incident alert thresholds are established	DE.AE-5	1	4
Continous Monitoring		As Is	To Be
DE.CM-1: The network is monitored to detect potential cybersecurity events	DE.CM-1	1	4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	DE.CM-2	1	4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	DE.CM-3	1	4
DE.CM-4: Malicious code is detected	DE.CM-4	2	4
DE.CM-5: Unauthorized mobile code is detected	DE.CM-5	2	4
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	DE.CM-6	2	4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	DE.CM-7	2	4

EXHIBIT "H" cont.

DE.CM-8: Vulnerability scans are performed	DE.CM-8	3	4
Detection Process		As Is	To Be
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	DE.DP-1	1	4
DE.DP-2: Detection activities comply with all applicable requirements	DE.DP-2	1	4
DE.DP-3: Detection processes are tested	DE.DP-3	1	4
DE.DP-4: Event detection information is communicated to appropriate parties	DE.DP-4	1	4
DE.DP-5: Detection processes are continuously improved	DE.DP-5	1	4

NIST - Recover

Recover: Functional Area summary			
Category	Name	As Is	To Be
Recovery Planning (RC.RP) - Average	Recovery Planning	1	4
Improvements (RC.IM) - Average	Improvements	1	4
Communications (RC.CO) - Average	Communications	1	4
Recover: Self-scoring worksheet			
Recovery Planning		As Is	To Be
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	RC.RP-1	1	4
Improvements		As Is	To Be
RC.IM-1: Recovery plans incorporate lessons learned	RC.IM-1	1	4
RC.IM-2: Recovery strategies are updated	RC.IM-2	1	4
Communications		As Is	To Be
RC.CO-1: Public relations are managed	RC.CO-1	1	4

EXHIBIT "H" cont.

RC.CO-2: Reputation after an event is repaired	RC.CO-2	1	4
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	RC.CO-3	1	4

NIST - Respond

Respond: Functional Area summary			
Category	Name	As Is	To Be
Response Planning (RS.RP) - Average	Response Planning	1	4
Communications (RS.CO) - Average	Communications	1.2	4
Analysis (RS.AN) - Average	Analysis	1	4
Mitigation (RS.MI) - Average	Mitigation	1	4
Improvements (RS.IM) - Average	Improvements	1	4
Respond: Self-scoring worksheet			
Response Planning		As Is	To Be
RS.RP-1: Response plan is executed during or after an incident	RS.RP-1	1	4
Communications		As Is	To Be
RS.CO-1: Personnel know their roles and order of operations when a response is needed	RS.CO-1	2	4
RS.CO-2: Incidents are reported consistent with established criteria	RS.CO-2	1	4
RS.CO-3: Information is shared consistent with response plans	RS.CO-3	1	4

EXHIBIT “H” cont.

RS.CO-4: Coordination with stakeholders occurs consistent with response plans	RS.CO-4	1	4
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	RS.CO-5	1	4
Analysis		As Is	To Be
RS.AN-1: Notifications from detection systems are investigated	RS.AN-1	1	4
RS.AN-2: The impact of the incident is understood	RS.AN-2	1	4
RS.AN-3: Forensics are performed	RS.AN-3	1	4
RS.AN-4: Incidents are categorized consistent with response plans	RS.AN-4	1	4
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	RS.AN-5	1	4
Mitigation		As Is	To Be
RS.MI-1: Incidents are contained	RS.MI-1	1	4
RS.MI-2: Incidents are mitigated	RS.MI-2	1	4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	RS.MI-3	1	4
Improvements		As Is	To Be
RS.IM-1: Response plans incorporate lessons learned	RS.IM-1	1	4
RS.IM-2: Response strategies are updated	RS.IM-2	1	4