STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

School District or LEA

Goose Creek CISD

and

Provider

Tobii Dynavox LLC

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

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

[Tobii Dynavox LLC   ], located at [2100 Wharton St., Suite 400, Pittsburgh, PA 15203] (the "**Provider**").

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

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

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

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

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

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

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

    ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

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

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: **Randal O'Brien**   Title: **Superintendent**

Address: **4544 Interstate 10 East, Baytown, TX 77521**

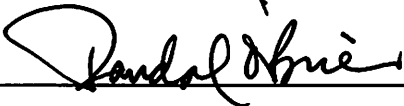Phone: _____ Email: **randal.obrien@gccisd.net**

The designated representative for the Provider for this DPA is:

Name: **Alicia Trax**   Title: **Healthcare Policy and Contracts Director**

Address: **2100 Wharton St., Suite 400, Pittsburgh, PA 15203**

Phone: **800-344-1778**   Email: **dataprivacy@tobiidynavox.com**

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

LEA:

By: _____   Date: **11/4/23**

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

Provider:

By: _____   Date: **10/27/2023**

Printed Name: **Tara Rudnicki**   Title/Position: **President of North America**

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

<u>**Exhibit "H"**</u>, the SDPC Standard Clauses, and/or the Supplemental State Terms, <u>**Exhibit "H"**</u> 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. <u>**Entire Agreement**</u>. 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. <u>**Severability**</u>. 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. <u>**Governing Law; Venue and Jurisdiction**</u>. 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. <u>**Successors Bound**</u>: 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. <u>**Authority**</u>. 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. **<u>Waiver</u>**. 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

Boardmaker 7

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☐
	Other application technology meta data-Please specify:	☐
Application Use Statistics	Meta data on user interaction with application	☑
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify: Please see attached docs.	☑
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)	☐

Category of Data	Elements	Check if Used by Your System
	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)	☐
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	☐

Category of Data	Elements	Check If Used by Your System
	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.	☐

Category of Data	Elements	Check if Used by Your System
	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	☐
	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

Provider to dispose of data obtained by Provider pursuant to the termsof 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 "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Goose Creek CISD   ] ("Originating LEA") which is dated [10/27/2023   ], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: dataprivacy@tobiidynavox.com

[NAME OF PROVIDER]

BY:_____Date: 10/27/2023_____

Printed Name: Tara Rudnicki_____Title/Position: President of North America

2. Subscribing LEA

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

Subscribing LEA:

BY:_____Date:_____

Printed Name:_____Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name:_____Title: _____

Address: _____

Telephone Number:_____Email:_____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

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

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☑	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization (ISO)	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)	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"

Supplemental SDPC State Terms for Texas
Version 1.0

This **Exhibit "G"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [Goose Creek CISD   ] (the "Local Education Agency" or "LEA") and [Tobii Dynavox LLC   ] (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:

None

Boardmaker® 7 Organization

Security White Paper

Boardmaker 7 Organization provides critical day-to-day education and therapy services to professionals and students within your district. Learn how Boardmaker has been built to deliver reliable and secure service within your district's existing network and security infrastructure.

Introduction

Boardmaker 7 Organization is a hybrid (web + installed) system that allows district staff to create and distribute accessible instructional materials to students across multiple platforms, including the iPad and Chromebooks. Please note that staff cannot create materials on iPad, they can only distribute. With built-in tracking tools and a huge library of included activities, an Organization account can meet a wide variety of needs across multiple educational programs (Special Education, Early Childhod, RTI, ELL) within your district.

Boardmaker 7 Organization functionality includes:

- Create and edit existing activities using the installed (web-connected) Boardmaker 7 Editor on Windows, Mac, and Chromebooks
- Online storage and management of activities
- Large included library of College and Career Readiness aligned activities
- Instructors can print any activity from any computer
- Instructors and students can play any activity on Window, Mac, Chromebook or iPad
- Instructors can assign activities to individual students
- Students will have six different ways to make the lesson accessible
- Instructors can track student performance against IEP goals and educational standards

Boardmaker 7 Organization is hosted entirely in Microsoft Azure Cloud Services. The service is composed of three main components:

- Boardmaker Portal: Each Organization customer is provided with a dedicated, unique URL of the form (<districtname>.boardmakeronline.com) for access to their account. An instructor or administrator simply visits the secure site, enters their account email/password to access their particular user account within their organization's account.
- Boardmaker 7 Student Center App: A free app is available for Windows, Mac, iPad, and Chromebooks that allow students access to their assigned activities. The difference is that the app downloads the student's activities at login so that the mobile device can still be used to operate the activities without internet access.

Boardmaker

Protecting the integrity and the privacy of data associated with students is a high priority. In addition, to ensure low total cost of implementation (TCI), online educational systems must integrate smoothly with a district's existing security infrastructure and require little IT support. Boardmaker 7 Organization was developed with both of these goals in mind. Secure from the ground up, Boardmaker 7 Organization uses an ASP model designed expressly to ensure robust and secure operation by communicating through secure internet protocols and standard ports.

Secure facility

Boardmaker 7 Organization software, communication and database servers are hosted in the Microsoft Azure Cloud, which is a highly secured Tier 1 data center. Physical access to servers is not allowed. Search services are currently provided by Elastic Search, which has similar facility security.

Secure platform

Boardmaker 7 Organization runs on hardened Windows servers with automatically updated security patches. The software is deployed to a secure scalable environment, with traffic SSL encrypted at 256 bits. The servers are configured with DDOS protection, automatic attack mitigation, continuous traffic monitoring, dedicated IP addresses, and with a dedicated security group defining database security.

Scalable and reliable infrastructure

The Boardmaker infrastructure is both robust and secure. The system is automatically load balanced across a scalable server architecture to ensure high availability. Automatic continuous backup systems are in place for the database, binary file storage, apps, and application assets allowing for fast, comprehensive recovery in the event of a failure.

Protecting customer privacy

Tobii Dynavox understands that school districts are concerned about privacy. We have a strong privacy policy (accessible here) that prohibits unauthorized disclosure of student or district information to any third party. In addition to Tobii's general Privacy Policy, the Tobii Dynavox (TD) business has adopted a Student Data Privacy Policy that outlines its adherence to FERPA, the U.S. Family Educational Rights and Privacy Act (20 U.S.C. §1232g, 34 CFR Part 99).

Protecting student data

There is a security option built into Boardmaker 7 Organization that will disallow the entry of student's last names or the uploading of profile photos. With this option enabled, even if the student data was accessed by an unauthorized individual, a student performance results or IEP goals could not be associated with a particular individual without access to the district's full student information database.

Teacher email addresses

Each instructor account must include a valid email address. Districts may want to ensure that instructors only use district provided email addresses. Instructors without admin privileges do not have the ability to change their own email address. If the Administrator configures all accounts to use district provided email addresses, they cannot be changed.

Disclosure of customer information

To deliver the Boardmaker Online service, Tobii Dynavox must collect certain user information, including first/last name, email address and account-level passwords. Unless expressly authorized, Tobii Dynavox will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. Tobii Dynavox may send service update messages to its users at the email addresses they provided when creating an account.

Even when Boardmaker 7 Organization is accessed from a public PC, no personal data is left behind that could pose a privacy threat. After a session ends, browser history indicates that Boardmaker 7 Organization was accessed – but information in the history cannot be used to access the account. The site also includes an auto logout timer so unattended accounts will logout automatically to enhance security.

Access to customer information

Tobii Dynavox staff are the only individuals with access to Tobii Dynavox servers – limited access is granted on a need-to-know basis for the express purpose of customer support and infrastructure maintenance.

Tobii Dynavox tracks domain names and browser types for traffic management. Stream analytics are stored for 60 days and used for error logging, troubleshooting, and general maintenance.

tobii dynavox

User privileges

Boardmaker 7 Organization allows an Organization to control which members of the organization can create and modify new user accounts and access district account settings. The chart below shows the three possible roles and functions that can be performed.

Role	Students	Instructors	Reporting & More
Instructor	Manage students assigned to me • Assign activities • Edit access settings • Manage IEP goals	• Nothing	• Run reports on students assigned to me
Instructor w/ Local Admin Privileges	Same as above plus: • Search for students and add them to your classroom • Edit student profile • Add new students	• Nothing	Same as above
Instructor w/ Admin Privileges	Same as above plus: • Pick which students are assigned to me • Assign students to other instructors • Edit student profile • Archive students • Add new students • Bulk import new students	• Edit instructor profile • Add new instructors • Delete instructors	Same as above
Instructor w/ Organization Admin Privileges	Same as above plus: • Bulk export of student account information	Same as above plus: • Set account privileges for Instructors • Bulk export of Instructor account information • Bulk import new instructors	Same as above plus: • Organization level reporting with filters • District account management • Standards management • Software download center access • District account settings • Site appearance • General settings • Hierarchy settings • Community Settings • Privacy settings • Instructional Level

tobiidynavox

Firewall compatibility

Boardmaker 7 Organization is firewall friendly. It generates only outgoing HTTP/TCP to ports 80, 443. Because most firewalls are already configured to permit outgoing Web traffic, you do not have to bypass or compromise your district or location firewall.

Protecting confidential data

Boardmaker 7 Organization uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the user's browser and the server is protected with end-to-end 256-bit RSA encryption. We use a Premium SSL wildcard certificate.

Advanced encryption

Boardmaker 7 Organization uses 256-bit RSA encryption. Through industry-standard encryption methods, Boardmaker 7 Organization can help an organization implement strong security policies and conform to district privacy mandates.

Password Protection

Any system that allows users to login can be compromised by using weak passwords that can easily be guessed, or by sharing passwords. Boardmaker Online enforces a minimum password length of 6 characters, and it does display password strength when users are creating or changing their passwords.

Password Recovery

If an instructor forgets their password, the login screen has a "Forgot Password" link that will ask for their email address. If the address matches the one we have in the system, an email will be sent with a link to allow the user to enter a new password.

If a student forgets their password, they should ask their instructor to reset their password.

Inactivity time-outs

Users walk away from laptop and desktop computers, and may switch away from the Student Center app without logging out. Boardmaker 7 Organization addresses this by applying inactivity time-outs. Users are automatically logged out of the website or app if their SSL connection is inactive for an extended period.

Conclusion

Tobii Dynavox's approach to security and privacy is simple: Start with a secure hosted service and operational practices that preserve customer privacy. Protect data connections with authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each district's existing network and security infrastructure. Provide flexible administrative controls for user management. The end result: Boardmaker 7 Organization is a robust, secure education management and delivery system with low total cost of implementation (TCI).

Tobii Dynavox

Product information: **get.boardmakeronline.com**

Sales inquiries: **1-800-588-4548**

For more information on Tobii Dynavox please visit **www.goboardmaker.com** or **www.tobiidynavox.com**

About Tobii Dynavox

Tobii Dynavox, is the leading provider of speech-generating devices and symbol-adapted special education software used to assist individuals in overcoming their speech, language and learning challenges. These solutions are designed to help individuals who have complex communication and learning needs participate in the home, classroom and community. Our mission is to enable our customers to realize their full communication and education potential by developing industry-leading devices, software and content, and by providing the services to support them. We assist individuals, families and professionals with an extensive field support organization, as well as centralized technical and reimbursement support. For more information, visit www.tobiidynavox.com.

Tobii Dynavox: Information Security Policy and Procedures (ISPP)

This policy and the specified attachments is intended for use by all personnel, contractors, and other third parties assisting in the direct implementation of information security measures of Tobii Dynavox, Inc. Executive management reserves the right to change or supplement this policy at any time. Information security is the ultimate responsibility of the Executive Management team of Tobii Dynavox. Operational responsibility of this policy is executed and enforced by the entire Executive Management team. The Director of Enterprise Systems is responsible for the overall ownership of this document, as well as, communicating this policy to all employees on a regular basis and serves as the Chief Information Security Officer ("**CISO**") for purposes of this policy. This policy is reviewed on a annual basis for appropriateness and effectiveness as it relates to Tobii Dynavox and generally accepted information technology standards. It is reviewed by the CISO and reported to the Executive Management team should approval for alteration be necessary.

1) <u>Attachments</u>
   a) Attachment A – Information Privacy Policy
   b) Attachment B – Incident Response Policy

2) <u>Policy Enforcement</u>
   a) Violations of this policy may result in suspension or loss of network use and privileges, and/or disciplinary action up to and including termination of employment. At the sole discretion of Tobii Dynavox, additional civil or criminal remedies may be pursued. All violations or exceptions to this policy must be reported to the CISO and brought before the Executive Management team for appropriate action.

3) <u>Employment and Human Resources</u>
   a) Background Checks
      i) All Tobii Dynavox employees are subject to a background check prior to gaining employment, and therefore prior to accessing any systems or data. This check alerts Tobii Dynavox to all Federal, County, or multi-jurisdictional findings. This includes a 9-panel drug screening, as well as additional offender and predator watch-lists.
      ii) The driver's license information for all employees required to operate a vehicle while working is sent annually to our Insurance broker to ensure driving records are adequate to commute as necessary to client sites.

4) <u>Internet Safety and Security</u>
   a) Users will practice safe browsing behavior to ensure no additional risk of malware, viruses, etc. contaminate the network.
   b) Business and client information should be protected always while browsing, and care should be given to when any information is provided to any online presence.
   c) Users shall not provide any personally identifiable information unless authorized explicitly by a client. Credit card or other sensitive information should never be transmitted on behalf of clients unless authorized explicitly, and then only in an approved, encrypted manner.
   d) Browsing behavior will be monitored, and content filtered, as seen fit by Tobii Dynavox. Filtering will be applied to restrict sites with possible malware or other malicious content.
   e) Users may not disable, alter, or block the filtering system in any way. Appropriate measures are in place to prevent this, and any action to circumvent them is strictly prohibited.
   f) Login information should never be supplied to any website not using modern, approved, SSL encryption standards.

5) <u>E-Mail Safety and Security</u>
   a) All Tobii Dynavox business should be conducted only through your TobiiDynavox business email account. Any 3rd party email accounts should be considered insecure and should not be used for business purposes at any time.
   b) Users shall never open attachments that appear to be related to spam messages. If phishing messages are received, users should alert the CISO, and warnings should be conveyed to employees as appropriate.
   c) Private or sensitive information including, but not limited to the following, should never be sent via e-mail without using an approved encrypted e-mail system. Certain information may trigger automatic encryption of the e-mail, though manual methods should always be taken to ensure the information is transmitted securely:
      i) Account and Login/Password Information
      ii) Social Security Numbers (or other personally identifiable ID information)

      iii)   Driver's License Numbers
      iv)   Credit Card Information
      v)   Bank Account Information
      vi)   Trademark or Client information
      vii) All information deemed private by Tobii Dynavox during a specific communication

d) In the event the above information is received non-encrypted from a client via e-mail, the individual recipient should notify their direct manager or the CISO and contain/dispose the e-mail appropriately. The sending client should be notified of the occurrence and the information should be changed or safe-guarded as necessary.

e) Tobii employs a third-party e-mail filtering and security service that scans inbound and outbound e-mail for spam, viruses and other malware, and possible phishing scenarios.

6) End-User Device / Server Security

a) Users shall never store personally identifiable information, credit card or other financial information, or any other information associated with clients that could be considered sensitive or private, including logins and passwords, unless explicitly approved by the Executive Management team.

b) Users will log off or lock their workstation or end-point device when leaving it unattended for any period.

c) End-point security software (Anti-Virus, Anti-Malware, etc.) is installed on all server and desktop resources at the discretion of Tobii Dynavox.

d) The end-point security software receives updated definitions for all security packages on a regular basis as soon as they become available from the manufacturer. The software is centrally managed to ensure compliancy of all devices with updates and security policies.

e) The end-point security software features on-access and on-demand scanning to ensure clean systems always. New systems, or systems with possibly dangerous files found, are scanned fully before reintroduction to the network.

f) Users may not disable, alter, or block the end-point security system in any way and any action to circumvent them is strictly prohibited.

7) Account and Password Security

a) All users authenticating to Tobii Dynavox resources, including any network access method, and application, shall have their own unique username and password combination.

b) User access to networks, systems, and applications, will be granted in the most restrictive basis, meaning a user is granted the least amount of privileges to successfully accommodate their job functions. Access will be granted explicitly and only after approval by the CISO to any application or data deemed sensitive, private, or personally identifiable.

c) Any attempts to forge authentication or access permission levels outside of your explicitly assigned level is strictly prohibited and in direct violation of this policy.

d) Administrative access (domain administrator, root, etc.) is restricted to a limited number of personnel and will be granted only upon approval from the CISO or Executive Management team. Additional agreements are required for such access to systems.

e) Where possible, two-factor authentication will be employed to protect access to critical or sensitive systems.

f) All password information is encrypted and unreadable during transmission and storage.

g) Password resets or account unlocking will be performed only after confirming a user's identity. Individuals can e-mail the Tobii Dynavox Help Desk to create a ticket based on their work e-mail address.

h) You will be assigned a temporary password upon account creation, and will be required to change it upon first login.

i) Users shall select passwords that are strong in nature and that have the following characteristics:
    i)   Is at least ten (10) characters long
    ii)   Does not contain your username, any part of your real name, or the company name
    iii) Does not contain a complete dictionary word
    iv) Does not repeat your previous four (5) passwords
    v)   Is significantly different from previous password and not simply an iteration
    vi) Contains at least one character from each of the following categories:
        (1) Uppercase characters (A-Z)
        (2) Lowercase characters (a-z)
        (3) Digits (0-9)
        (4) Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

j) Passwords will expire and must be changed every thirty (90) days.

k) User's account will become locked out after ten (10) invalid password attempts within thirty (30) minutes, and will remain locked out for at least 30 minutes, or until an administrator unlocks the account.

l) All end-user devices will automatically lock and require the password after fifteen (15) minutes of inactivity.

m) Accounts are disabled immediately upon end of employment via a HR Termination Notice. This ticket includes the steps necessary for each department to complete and secure the environment.

n) Passwords will be unique to each named user, regardless of vendor or employee affiliation. Shared accounts or passwords will not be permitted under any circumstances.

8) Infrastructure Configuration and Maintenance

a) Internal Workstation and Server Patching
   i) Operating system patches/upgrades are evaluated biannually.
   ii) Operating system patches/upgrades are installed based on their criticality.
   iii) Operating system patches/upgrades are reviewed via a test environment whenever possible/practical.
   iv) Operating system patches/upgrades are installed during off-peak hours to minimize the disruption to business.
   v) The IT department reviews all servers regularly to ensure that they remain up to date and are properly patched.

b) Internal Infrastructure Patching
   i) Infrastructure (routers, switches, virtual hosts, etc.) patches/upgrades are evaluated as they come available from vendors.
   ii) Infrastructure patches/upgrades are installed based on their criticality. Security critical patches/upgrades are installed with IT approval.
   iii) Infrastructure patches/upgrades are reviewed via a test environment whenever possible/practical.
   iv) Infrastructure patches/upgrades are installed during off-peak hours to minimize the disruption to business.
   v) Networking hardware/software updates follow the regular change management procedures.

c) Infrastructure Support Documentation
   i) The infrastructure topology is maintained by Tobii Dynavox IT Partners and is available upon request. A network diagram is available to all appropriate service personnel as needed and approved by the CISO.
   ii) The infrastructure topology is never shared with outside personnel unless properly sanitized of all IP addresses and any other sensitive information.
   iii) Configuration standards for the setup of all infrastructure devices are in place and are formally documented as necessary.
   iv) Configuration standards include a standard list of security hardening principles.
   v) Access to the network and communication devices is available as needed with approval by the CISO.

9) Infrastructure Security

a) Device Best Practices and Hardening
   i) Hardening and best practice guides will be employed to ensure all device installation is properly guarded from vulnerabilities and unauthorized attempts to access the systems at the discretion of Tobii, Inc or Tobii Dynavox.
   ii) Vendor supplied defaults, including usernames, passwords, and any other common settings that that may result in unauthorized attempts to access to the systems, will be changed in accordance with hardening guides.
   iii) Local passwords, when required, will be randomly generated and securely stored in the approved password vaulting system.
   iv) Two-factor authentication should be used whenever available/supported on the device platform.

b) Service Account and Password Security
   i) Services requiring access shall always be created with named accounts, unshared between service, and given the most restrictive access required to still perform their function.

10) Security Assessment and Vulnerability Management

a) Manufacturer and Industry security bulletins
   i) As security bulletins and new software releases are made available, we review for any critical security patches and apply on an expedited scheduled to any public facing, affected, devices or piece of infrastructure.

b) Vulnerability Management and Monitoring
   i) All systems and infrastructure are Firewall protected.
   ii) All system and application software are monitored so that all security vulnerabilities that may exist can be managed in a timely manner.

    iii) A process exists to identify and risk rank security vulnerabilities. This process may leverage the use of outside resources to identify security vulnerabilities in systems.

    iv) A process exists to scan for and detect unauthorized access points that may be connected to the network.

    v) Internal and external vulnerability scans are performed and vulnerabilities are prioritized and remediated in a timely fashion.

    vi) Internal and external vulnerability scans are performed after any significant network changes. Vulnerabilities are prioritized and remediated in a timely fashion.

    vii) External and internal penetration testing is performed at least once a year and after any significant infrastructure of application upgrades or network modifications.

    viii) Intrusion detection/prevention systems are in place at critical access points on the network that restrict access to areas with sensitive data. Critical points within the sensitive environment are also monitored on an as needed basis.

    ix) Intrusion detection/prevention systems are configured to automatically alert IT personnel if an alarm is triggered.

    x) Auditing files for security-related systems are centrally stored and kept for more than one (1) year.

11) Risk Assessment

a) The CISO shall conduct a risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of client information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise, and assess the sufficiency of any safeguards in place to control these risks.

b) The risk assessment shall cover all relevant areas of the organization's operations, as determined by the CISO. At a minimum, the risk assessment shall cover the following:

    i) Employee training and management

    ii) Infrastructure systems and design, as well as information processing, storage, transmission and disposal

    iii) Detecting, preventing and responding to attacks, intrusions or other systems failures.

c) Once the CISO has identified the reasonably foreseeable risks to the organization's client information, the CISO will determine whether the organization's current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the CISO shall design new policies and procedures that meet the objectives of the infrastructure.

d) The CISO shall regularly test or audit the effectiveness of the organization's safeguards' key controls, systems, and procedures, to ensure that all safeguards implemented because of the risk assessment are effective to control the risks identified in the risk assessment. The risk assessment matrix shall be reviewed with the CISO annually and revised as necessary to ensure safeguards and/or implement new safeguards as necessary to ensure the continued viability of the infrastructure.

12) Encryption

a) Non-console administrative access to systems, including the administration panel of websites is encrypted via technologies such as SSH, VPN, SSL.

b) Wherever sensitive information is stored, it is rendered unreadable using strong cryptography, with associated key-management processes and procedures.

c) Only strong cryptographic algorithms are used (AES, RSA public key cryptography, and SHA-256) or higher.

d) Whole disk encryption may be utilized on sensitive laptops, workstations, and removable storage devices (including mobile devices as applicable) when they are required to hold sensitive client data. Storing this information on devices is discouraged in almost all cases as access methods are done through virtual methods.

e) Whenever cryptographic keys are stored, they are stored securely with strong access controls and are always stored in encrypted format and are only accessible to the fewest number of authorized personnel as absolutely necessary.

f) All random numbers, random file names, random GUIDs, and random strings are generated in a cryptographically strong fashion and never by hand.

g) Keys are changed periodically and whenever they may be compromised.

h) Transmission of sensitive information is encrypted when transmitted via the internet or any other public networks.

i) Sensitive information is never transmitted via email, or instant messenger without appropriate encryption.

13) Physical Access Security and Availability

a) Administrative Locations

    i) Physical access to all locations are restricted to appropriate authorized employees, vendors, and escorted guests only.

    ii) All guests must sign in with reception and be escorted while in controlled areas.

    iii) Physical access throughout all locations are restricted via a badge access system that is controlled by the CISO and is requested and approved via employee on-boarding, off-boarding, and position-change tickets.

b) Datacenter Locations

    i) Physical access to the data center is restricted to only authorized IT personnel and trusted IT vendors.

    ii) Physical access to other portions of the network infrastructure is restricted to authorized personnel only.

    iii) Physical access to publicly accessible network jacks is restricted. Publicly accessible network jacks are disabled and are not connected to the network when not needed.

    iv) Physical access is reviewed quarterly for appropriateness and adjusted as needed.

    v) Vendors must be accompanied by Tobii Dynavox personnel when performing work in any sensitive areas.

    vi) Portions of infrastructure are maintained at third party data centers. Tobii Dynavox receives and reviews reports on controls (SOC 2 Type II and SOC 1 Type II (if available)) of any third-party data centers or critical outsourced processes.

14) Data Retention and Disposal

a) Retention

    i) Private and sensitive information is not stored longer than needed. Additional consideration may be given to data meeting the following qualifying conditions:

        (1) HIPAA and Medicare data will follow CMS retention policies

        (2) FERPA will follow DOE retention policies

        (3) Data subject to GDPR will follow GDPR Data retention policies

        (4) Non-client-specific data will be disposed of securely when no longer needed for legal, regulatory, or other business reasons.

    ii) All information required to be returned to a client will be done so following the appropriately secure method for the transport (secure FTP, encrypted media, etc.).

    iii) Traffic and device logs are stored for ninety (90) days. Summarized traffic and device logs, syslog information, and auditing information, is saved for one (1) year where possible.

b) Physical Disposal

    i) Paper content, or other non-electronic physical media, that contains sensitive information, including private or sensitive data, is disposed of in a proper fashion (shredded with cross-cut) when it is no longer required for business or service purposes.

c) Electronic Disposal

    i) Electronic media containing sensitive or private data and information, is disposed of in the proper fashion. Depending on the media, and whether it will be reused, it will be deleted/wiped, or destroyed following NIST guidelines.

    ii) If a third-party vendor is used to securely destroy media, the destruction will be validated by a member of management, or the appropriate certification will be acquired.

    iii) When technology assets have reached the end of their useful life, or transitioned to secondary production use, they will be wiped (have data deleted) following appropriate NIST guidelines, then deposed of if not being repurposed.

15) Change Management

a) The change management process is applicable to changes in all infrastructure and server devices that are involved in handling or storing sensitive information such as sensitive data, or can adversely impact security and availability.

b) All changes of the nature as described are reviewed by the CISO and approved after all information has been obtained and scenarios have been reviewed.

c) All other changes such as content changes, non-transactional changes, client-originated changes, etc. have an email trail to document the origination of the change at a minimum. The severity of the change is subject to the discretion of the CISO.

d) All changes of the nature as described are entered, tracked, and centrally managed by the internal ticketing/help-desk system. The following items are recorded and updated during the lifecycle of the change:
   i) Ticket ID
   ii) Status (Open, Closed, Awaiting Approval, etc.)
   iii) Ticket Creator
   iv) Change Summary
   v) Impact Analysis
   vi) Implementation Plan
   vii) Test Plan
   viii) Back Out Plan
   ix) Approval Comments
   x) Review Notes and Follow-Up
e) Evidence of testing documentation is maintained and attached to the change/help-desk ticket as applicable.
f) Any changes affecting Security or Privacy related systems will also possibly affect Job Descriptions and roles/responsibilities. These will be addressed during the Review period of the change management process.

16) Detecting, Preventing, and Responding to Security Incidents and System Failures

a) The CISO shall ensure the organization has adequate procedures to address any breaches of the organization's information safeguards that would materially impact the confidentiality and security of client information.
b) The policy and accompanying procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.
c) The CISO and their team shall utilize and maintain a working knowledge of widely available technology for the protection of client information.
d) The CISO and their team shall communicate with the organization's vendors from time to time to ensure that the organization has installed the most recent patches that resolve software vulnerabilities.
e) The organization shall utilize end-point security systems that update automatically and regularly per this policy.
f) The organization shall maintain up-to-date firewalls and review them per this policy.
g) The CISO shall establish procedures to preserve the security, confidentiality and integrity of client information in the event of an infrastructure or other technological failure.
h) The CISO shall ensure that access to client information is granted only to legitimate and valid users.
i) The CISO shall ensure a prompt notification to clients if their client information is subject to loss, damage or unauthorized access.
j) Please refer to the official Incident Response Plan (IRP) for more detailed information.

17) Employee Training and Management

a) All employees and third party contractors/agents are responsible for complying with this policy.
b) The organization will take appropriate steps to encourage awareness of, and compliance with this policy.
c) All new employees and third party contractors/agents who perform services in the organization, that have access to client information shall sign and acknowledge his or her agreement to abide by the policy. Reaffirming their acknowledgement will recur at least once each year, or as required changes are made to the policy.
d) All employees and third party contractors/agents will be permitted to access client information on a "need-to-know" basis as determined by organization management.
e) Personnel shall not be permitted to access, use or reproduce client information, whether electronic or non-electronic, for their own use or for any use not authorized by the organization.
f) All persons who fail to comply with the policy shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for third party contractors/agents that perform services with the organization. This remedy shall be expressly provided for in organization's agreements with such third-party contractors/agents.

Tobii Dynavox	SOP-0123-B	Title: Tobii Dynavox: Information Security Policy and Procedures (ISPP)

Tobii Dynavox: Information Privacy Policy (IPP) – Attachment A

This policy is intended for use by all personnel, contractors, and other third parties who may come into contact with infrastructure, systems, or information relating to Health Insurance Portability and Accountability Act ("HIPAA") protected information, Family Educational Rights and Privacy Act ("FERPA"), the EU General Data Protection Regulation ("GDPR"), Protected Health Information ("PHI") or other private and confidential client information of Tobii Dynavox (the company) and its Clients. This policy on the use and protection of this information consists of policy descriptions as well as procedures that describe how our organization will interact and comply with this policy. Executive management reserves the right to change or supplement this policy at any time.

1) **Overview**
   a) This policy, its associated procedures and related concepts apply to all company and Client Confidential Information. Confidential Information, in general, is information whose unauthorized disclosure, compromise, or destruction could directly, or indirectly, have an adverse impact on the company, its clients, or its employees.
   b) This policy is designed to complement the Information Security Policy and Procedures ("ISPP") document. Personnel, contractors, and other third parties are responsible for familiarizing themselves with this policy and acknowledging their understanding and compliance.

2) **Definitions**
   a) **Protected Health Information ("PHI")** is the combination of any health-related information and patient demographic information that can be used to reasonably identify the individual. The following items are considered elements of PHI that identifies an individual:
      i) An individual's name with any of the following:
         (1) All geographic subdivisions smaller than a state (street address, city, county, zip code)
         (2) All dates directly relating to the individual (birth date, admission date, discharge date, date of death)
         (3) Telephone numbers, fax numbers, e-mail addresses
      ii) Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers
      iii) License numbers, vehicle identification numbers, license plate numbers
      iv) Biometric identifies, including finger printers, voice prints, facial recognition data
      v) Any other unique identifying number or characteristic code
   b) **Personally Identifiable Information ("PII")** is any data or other information that could readily be used to identify a specific person and make personal information about them known. PII includes, but is not limited to:
      i) An individual's name with any of the following: address, phone number, email address
      ii) Social Security Number, driver's license or passport number
      iii) Credit card information, bank account, or other financial account information
      iv) Medical conditions, medical records
      v) Any combination of data that could be used to identify an individual such as birth date, zip code, mother's maiden name, and gender
   c) **Other Private and Confidential Information** includes any information whose unauthorized disclosure, compromise, or destruction could directly or indirectly have an adverse impact on the company, its clients, or employees. This information may include, but is not limited to:
      i) Propriety, copyrighted, trademarked, or patented Intellectual Property ("IP") if not public
      ii) Company Trade Secrets and other's Trade Secrets which have been entrusted to the company
      iii) Any non-public data that has been entrusted to the company by its clients
      iv) Research and development plans, projects, data, and reports
      v) Computer materials such as programs, source and object code, and reports
      vi) Passwords to company owned or operated systems
      vii) Strategies, forecasts, and other marketing techniques
      viii) Business plans, whether executed or not
      ix) Budgeting information and financial planning data, including pricing strategy and cost data
      x) Contracts, agreements, and licenses that the company agrees to keep confidential

3) **Privacy Structure**

a) The privacy structure enables the delegation of roles and responsibilities across the organization, from management and implementation, to enforcement and monitoring. It further enables the effective implementation and ongoing maintenance of the privacy policies.

b) The Chief Information Security Officer ("CISO") is the main privacy contact regarding this policy, and is enabled by the Executive Management Team to enforce and monitor said policies. Individual department managers are also enable to engage their teams to enforce, monitor, and assure understanding of security policies.

4) Questions, Complaints, and Incidents

a) Questions, complaints, and incidents regarding the protection of and privacy of Confidential Information will have a defined communication structure.

b) Employees should contact their direct manager with any questions regarding the procedures contained in this policy.

c) Complaints and incidents should be reported directly to the CISO with additional information being provided by their manager. Any incident including the unauthorized disclosure of Confidential Information will trigger the incident response policy as well as the potential engagement of Executive Management.

d) External users and clients may report such questions, complaints, or incidents as well, by using the privacy@tobiidynavox.com e-mail address

5) Minimum Access

a) The concept or minimum access is reasonably applied to all situations regarding Confidential Information. The company will take reasonable measures to protect the privacy of Confidential Information by limiting the amount of information disclosed to the minimum amount of necessary to perform a job of complete a function.

b) This concept will also include limiting any access to Confidential Information to the minimum number of individuals as possible or practical.

6) Computer Information Security Summary

a) Additional and complete requirements on the following procedures are detailed in the ISPP.

b) All users must log off or lock their computers when leaving them unattended.

c) Users must protect their passwords, not share them, and keep their logins secure. Login information may never be written down, left in drawers or cabinets (locked or unlocked), or attached to any workstation, keyboard, monitor, etc.

d) All unused equipment, whether from employee attrition or extended absence, that contains or has direct access to Confidential Information will be removed from the work area and stored in a secure location. Laptop computers that contain Confidential Information should not be left unattended in unsecure locations or work areas.

7) Review and Acknowledgement

a) All users will receive mandatory review sessions of the appropriate security policies pertaining to their position and job function, as well as their level of access to confidential information. This review should occur no longer than thirty (30) days from their start of employment or newly gained access to Confidential Information.

b) If there are new policies or significant changes to existing policies or procedures, the relevant employees will receive reviews on those changes and adjustments. At a minimum the security and privacy policies will be acknowledged through our Human Resources system on an annual basis.

c) As a condition of continued employment, employees must diligently protect all company and client Confidential Information as specified in this policy from unauthorized disclosure or misuse.

8) Electronic Transmission of Confidential Information

a) Due to the sensitive and critical nature of all Confidential Information, the company will implement appropriate encryption with modern algorithms sent via any electronic means. Additional details specified in the ISPP.

9) Confidential Information Outside of Company Controlled Facilities

a) Users will take reasonable measures to ensure that all Confidential Information leaving a company has physical safeguards and controls. This includes, but is not limited to, certified mail, signature requirements on mail, as well as secure couriers where necessary.

b) These provisions apply to any Confidential Information for which the company has assumed responsibility, regardless of whether inbound to or outbound from a company facility, including any client-requested transport of data.

c) The same encryption and security practices apply to any equipment or information transported between facilities.

10) Media Management

    a) The company will secure and maintain all Confidential Information during its storage, delivery, removal, and transportation. Additional details specified in the ISPP.

11) Data Retention and Destruction
    a) Confidential Information as defined in this policy, will be stored per modern encryption requirement and security protocols as described in the ISPP.
    b) Confidential Information will be purged from the system in a secure and clean fashion in accordance with NIST security protocols (more details in the ISPP).
    c) Confidential Information may be removed from company software when all contracts with a client are terminated or expired that require such access to that information to perform our services.
    d) Clients may request that this information be retained for longer than said contract length to cover any service provider overlap or transition period outside of the contract agreement term.
    e) Any hardware or equipment will be cleaned and destroyed in a secure manner, depending on the contents of the device or hardware. Third-party wiping and destruction may be implemented if available. More details available in the ISPP.

12) Physical Access
    a) Tobii Dynavox takes reasonable measures to ensure Confidential Information is safeguarded from any unauthorized persons in areas under their physical control. Administrative offices have enforced visitor procedures to prevent unauthorized access.
    b) Visitors are required to sign in and out, and must be escorted through any secure areas of the facility.
    c) When required, visitors may receive limited card access to secure areas of the facility.

13) Working Remotely
    a) When working remotely, users may only access the internal network via a virtual private network (VPN).
    b) Traffic to this network is encrypted and done through VPN clients to ensure no Confidential Information is transmitted to unauthorized users. No other external direct access will be provided, whether the device is owned by the company or through a Bring Your Own Device ("BYOD") program.

14) Business Associates
    a) Tobii Dynavox must ensure that any third party that performs a function involving the use or disclosure of Confidential Information ("Business Associate") is adequately protecting and safeguarding all Confidential Information.
    b) Tobii Dynavox will only disclose Confidential Information to Business Associates that they have executed a Business Associate Agreement ("BAA") with. This agreement will be consistent with the HIPAA Privacy Rule's recommended BAA contract language.
    c) Specific changes and adjustments to the BAA requested by a Business Associate must be approved and ratified by both the Executive Management Team and appropriate legal consultants.

15) Disclosures
    a) A disclosure is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." Tobii Dynavox will response to all appropriate requests for Confidential Information that are required by law.

16) Incident and Breach Response
    a) Any incident that contains a reasonable likelihood that Confidential Information has been disclosed inappropriately or through unauthorized means, will be handled in accordance with our Incident Response Policy ("IRP").
    b) Appropriate law enforcement and regulatory organizations will be contacted per said policy, if necessary.
    c) A full Root Cause Analysis ("RCA") will be available for client access should they request it. This will contain root cause for the breach or incident, as well as steps to prevent it in the future, along with any other post-mortem reviews and risk assessment adjustments, as necessary.

Tobii Dynavox: Incident Response Plan (IRP) – Attachment B

Tobii Dynavox (the "company") has implemented all precautions and safeguards deemed necessary by its risk assessment procedures to safeguard client data and information. This Information Security Policies and Procedures ("ISPP") document governs its efforts in this area. Despite safeguards and due diligence, incidents related to Infrastructure and Security Systems, including those that contain/process client information, are possible. As such, the Incident Response Plan ("IRP") outlines the required response to security incidents. This plan will be approved by the Executive Management Team, and will be distributed to members of the organization that will be involved in the incident response process.

1) **Incident Response Team Duties**
   a) An Incident Response Team has been established to provide a quick, effective and orderly response to information security related incidents such as infections, hacking attempts, improper disclosure of confidential information to others, service interruptions, breach of personal information, and other events with serious information security implications. This team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving infrastructure, systems, networks or data.
   b) b. This team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve any information security related incident. This team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to the CISO and the appropriate authorities as necessary.
   c) c. The Tobii Dynavox Incident Response Team shall include the following members:
      i) CEO
      ii) Vice President of Global Operations
      iii) Director of Enterprise Systems and Applications (CISO)
      iv) Manager of Global IT, Tobii AB (Sweden)
      v) Enterprise Systems and Applications Department Personnel
      vi) Privacy Officer/Compliance Manager

2) **Incident Response Policy**
   a) **Any and all information security incidents must be reported to the CISO.** A preliminary analysis of the incident will take place and that will determine whether Incident Response Team activation is appropriate. This determination is based in part on the volume and sensitivity ("the scope") of the data involved in the incident. Furthermore, incidents will be classified and remediated as necessary per the incident classification. (Security related, Availability related, or Privacy related). These incidents include, but are not limited to:
      i) Breach of Private Information (Intentional or Unintentional)
      ii) Suspicious Phone Calls and Inquiries
      iii) Denial of Service Attacks
      iv) Excessive Port Scans
      v) Firewall Breach
      vi) Virus/Malware Outbreak

   b) The Incident Response team will first take any actions necessary to contain the threat and prevent any further damage. The team will then appropriately document all incidents in the ticketing system using the appropriate template. An incident notification will be initiated from the Cloud Portal and sent to the documented contacts supplied by the organization. These notifications will be updated every hour, or when additional information is available. The notifications will include:
      i) The incident summary and details
      ii) The incident category and classification information
      iii) Affected locations and services
      iv) Corresponding change management ticket information

   c) After documenting the incident, the team will review the details of the incident, and determine whether they believe that client information has been obtained by an unauthorized party and will be misused. The following incidents (but

not limited to) may require notification to individuals under contractual commitments or applicable laws and regulations:
  i)   A user (employee or third-party contractor/agent) has obtained unauthorized access to private information maintained in either paper or electronic form.
  ii) Technology equipment such as a workstation, laptop, or other electronic media containing private information on an individual has been lost or stolen.
  iii) A department or individual has not properly disposed of records containing private information.

d) If client notification is delayed due to legal or regulatory investigations, the company will request in writing documentation showing that the notification of clients was delayed according to law enforcement/regulatory instruction. The company will develop a written client notification that describes clearly the incident that has occurred, as well as the impact on the client's private information. Employees that receive client inquiries relating to the incident should direct them to a member of the Incident Response Team.

e) The CISO is responsible for ensuring that the company performs a prompt investigation of circumstances surrounding potential unauthorized access to sensitive client information to determine the likelihood that the information has been or will be misused. The CISO is responsible for ensuring that notification of customers is carried out if the investigation determines that misuse of its information about a client has occurred or is reasonably possible. Any disclosure of information security incidents, including reports to regulators and notifications to clients, must also be approved in advance by the CEO and CISO.

f) After any necessary remediation, a Root Cause Analysis ("RCA") should be documented by the Incident Response Team and presented to the Executive Management for further discussion. As applicable, a Risk Assessment and the Change Management process, including any related preventative controls, should be updated.