DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the "Agreement") is made and entered into by and between Tobii Dynavox LLC (the "Vendor") and **Cuba-Rushford Central School** ("CRCS").

WHEREAS, CRCS and Vendor are parties to a contract or other written agreement (the "Contract") pursuant to which the Vendor will receive student data and/or teacher or principal data ("Protected Data") that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from CRCS for purposes of providing certain products or services to CRCS; and

WHEREAS, both CRCS and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

NOW THEREFORE, in consideration of the mutual promises and covenants contained in the Contract, as well as, this Agreement the parties hereto mutually agree as follows:

1. **Confidentiality**

   a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided for in the Agreement is deemed confidential information.

   b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with federal and state law and that any information obtained will not be revealed to any persons, firms or organizations.

2. **Data Protections and Internal Controls**

   a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by CRCS that directly relate to a student(s) (hereinafter referred to as "education record").

   b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:

      1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and

      2. Not use the education records for any other purpose than those explicitly authorized in the Contract and/or Agreement; and

3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

4. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

3. <u>Data Security and Privacy Plan</u>

a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from CRCS.

b. Vendor understands and agrees that it is responsible for submitting a Data Security and Privacy Plan to CRCS prior to the start of the term of the Agreement, and it shall:

1. Outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with CRCS's policy on data security and privacy, as adopted.

2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from CRCS under the Contract.

3. Outline the training requirement established by the Vendor for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

4. <u>Notice of Breach and Unauthorized Release</u>

a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:

1. Immediately notify CRCS in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or authorized release.

2. Advise CRCS as to the nature of the breach and steps Vendor has taken to minimize said breach.

b. In the case of required notification to a parent or eligible student, the Vendor shall:

1. Promptly reimburse CRCS for the full costs of such notification.

c. Vendor will cooperate with CRCS and provide as much information as possible directly to CRCS about the incident, including but not limited to:

1. The description of the incident;

2. The date of the incident;

3. The date Vendor discovered or was informed of the incident;

4. A description of the types of Protected Data involved;

5. An estimate of the number of records affected;

6. The schools within CRCS affected;

7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data; and

8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

d. The Vendor shall indemnify and hold CRCS harmless from any claims arising from its breach within the Data Sharing and Confidentiality Agreement confidentiality and data security and privacy standards provision.

e. Vendor acknowledges that upon initial notification from Vendor, CRCS, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by CRCS or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by CRCS, Vendor will promptly inform CRCS of the same.

5. <u>Vendor Information</u>

Vendor understands that as part of CRCS's obligations under New York Education Law Section 2-d, Vendor is responsible for providing CRCS with Vendor information (see Vendor Information for Data Privacy and Security) to include:

a. Exclusive purposes for which the student data will be used;

b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;

c. Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student;

d. Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

e. Vendor will provide a description of what will happen to the personally identifiable information upon expiration of the written agreement (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will be destroyed).

f. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and

g. Where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

6. <u>Termination or Expiration of Contract and/or Agreement</u>

a. Upon termination of the Agreement, Vendor shall return or destroy all confidential information obtained in connection with the services provided therein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement.

b. If requested by CRCS, Vendor will assist CRCS in exporting all Protected Data previously received back to CRCS for its own use, prior to deletion, in such formats as may be requested by CRCS.

c. In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with CRCS as necessary to transition Protected Data to the successor Vendor prior to deletion.

d. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide CRCS with a certification from an appropriate officer that these requirements have been satisfied in full.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

CRCS is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, CRCS informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to CRCS Data Privacy Officer, 5476 Route 305, Cuba, New York 14727. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first written above.

Authorized Vendor Signature	July 19, 2021 Date
Authorized CRCS Signature	July 19, 2021 Date

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: Tobii Dynavox LLC Product: Boardmaker 7

Collects: ☒ Student Data ☒ Teacher or Principal Data ☐ Does not collect either

Educational agencies including Cattaraugus-Allegany-Erie-Wyoming BOCES are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

Part 1: Exclusive Purposes for Data Use	**RESPONSE REQUIRED**
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:	

Part 2: Subcontractor Oversight Details	**RESPONSE REQUIRED**
☒ This contract has no subcontractors. ☐ This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law:	

Part 3: Contract Lifecycle Practices	**RESPONSE REQUIRED**
The contract expires on July 31, 2022 unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, the following will happen to the personally identifiable information (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will be destroyed):	

Part 4: Student Educational Records / Improper Disclosure
A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website. B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.

Part 5: Security Practices	**RESPONSE REQUIRED**
A. Protected data provided to the contractor will be stored: (include *where* and *how*) B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include:	

Part 6: Encryption Practices	**RESPONSE REQUIRED**
☒ By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).	

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.

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.

© 2020 Tobii Dynavox, LLC. All rights reserved.

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

© 2019 Tobii Dynavox, LLC. All rights reserved.

tobii dynavox

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.

©2020 Tobii Dynavox. All rights reserved. Boardmaker® is a registered trademark of Tobii Dynavox, in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.

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) Attachments

a) Attachment A – Information Privacy Policy
b) Attachment B – Incident Response Policy

2) Policy Enforcement

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) Employment and Human Resources

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) Internet Safety and Security

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) E-Mail Safety and Security

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) <u>End-User Device / Server Security</u>

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) **<u>Account and Password Security</u>**

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) <u>Data Retention and Disposal</u>

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) <u>Change Management</u>

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) <u>Detecting, Preventing, and Responding to Security Incidents and System Failures</u>

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) <u>Employee Training and Management</u>

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: 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.