DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements and forms part of the Standard Terms of Service and License ("**Standard Terms**") and Career Connect Terms of Use (collectively, the "**Agreement**") during Discovery Education's provision of the Services (defined below) to Subscriber in which the Parties collect and exchange Personal Information (defined below). Capitalized terms not otherwise defined in this DPA shall have the meanings ascribed to them in the Agreement.

1. Definitions

"**Account Information**" means the Personal Information of End Users described in **Exhibit B**.

"**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Subscriber's Personal Information transmitted, stored or otherwise Processed.

"**Data Protection Laws**" means, to the extent applicable, any federal, state, or municipal laws and regulations within the United States of America relating to the Processing, protection, or privacy of Subscriber Personal Information under the Agreement.

"**End User**" means an employee of an educator or corporate partner that has a Career Connect user account.

"**Personal Information**" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household and includes the terms "Personal Data" and "Personally Identifiable Information," as such terms are defined under Data Protection Laws.

"**Services**" means Discovery Education's delivery of Career Connect to Subscriber and Subscriber's End Users.

"**Subscriber Personal Information**" means Account Information or Usage Data, depending on the context.

"**Usage Data**" means the Personal Information of End Users described in **Exhibit A**.

The terms "**Business**", "**Controller**", "**Processing**", "**Processor**", "**Sell**", "**Share**", and "**Service Provider**" shall have the same meaning assigned to them under applicable Data Protection Laws. The term "Controller" is deemed to include "Business" and the term "Processor" is deemed to include "Service Provider."

2. Roles; Details of Processing

2.1 Discovery Education as a Service Provider. The Parties acknowledge and agree that regarding the Processing of Usage Data, Discovery Education is a Service Provider and Subscriber is a Business or Controller. The details of Discovery Education's Processing of Usage Data are set forth in **Exhibit A**.

2.2 The Parties acknowledge and agree that with regard to the Processing of Account Information, Discovery Education is a Third Party or Controller and Subscriber is a Business or Controller. The details of Discovery Education's Processing of Account Information are set forth in **Exhibit B**.

2.3 The Parties acknowledge and agree that Subscriber is sharing Usage Data and Account Information for the limited purposes outlined in **Exhibit A** and **Exhibit B**, respectively.

3. Business, Service Provider, and Third Party Obligations

3.1.1 Discovery Education will Process Usage Data and Account Information only for the limited and specified purposes outlined in this DPA and as set forth in **Exhibit A** and **Exhibit B**, respectively.

3.1.2 Each Party will comply with all obligations under applicable Data Protection Laws in connection with the Processing of Subscriber Personal Information under the Agreement and this DPA.

3.1.3 Discovery Education shall notify Subscriber if it determines that it is no longer able to comply with its obligations under applicable Data Protection Laws.

3.1.4 Throughout the Term (defined below) of this DPA, Subscriber may take reasonable and appropriate steps to ensure that Discovery Education uses the Personal Information in a manner consistent with Subscriber's obligations under applicable Data Protection Laws, including through manual reviews, automated scans, regular assessments, audits, technical and operational testing by Subscriber (or an auditor appointed by Subscriber) in relation to the Processing of Subscriber Personal Information by Discovery Education, subject to the provisions set forth in this Section 3.1.4. Subscriber cannot exercise this right more than once per any twelve (12) month period during the Term.

(a) Upon Subscriber's request to perform an inspection or audit, to the extent permitted by applicable Data Protection Laws, Subscriber may elect to retain a qualified and independent assessor to perform such inspection or audit, using an appropriate and accepted control standard or framework and assessment procedure for such assessments.

(b) The Parties agree that any such audit will be conducted: (i) upon thirty (30) calendar days' written notice to Discovery Education; and (ii) only during Discovery Education's normal business hours.

(c) Subscriber shall, without undue delay, notify Discovery Education of any non-compliance discovered during the audit.

(d) Subscriber is responsible and fully liable for the actions and omissions of its personnel and authorized representatives while on Discovery Education's premises and/or inspecting Discovery Education's systems and facilities. Subscriber will bear the costs for any audit initiated by Subscriber.

3.1.5 Each Party providing Personal Information is responsible for the accuracy, quality, and legality of the Personal Information provided to the other Party under the Agreement or this DPA. For the avoidance of doubt, Subscriber represents and warrants to Discovery Education that its End Users are authorized to provide their Account Information to Discovery Education for the purposes set forth in Exhibit B.

3.1.6 Notwithstanding the foregoing or anything to the contrary in this DPA, Discovery Education acknowledges and agrees that to the extent Discovery Education collects on behalf of Subscriber, or receives from Subscriber deidentified data or pseudonymized data (as those terms are defined under applicable Data Protection Laws) (collectively, "Deidentified Data") or to extent the Agreement permits Discovery Education to render Personal Information into Deidentified Data, Discovery Education will implement such de-identification in accordance with applicable Data Protection Laws. In addition, for Deidentified Data, Discovery Education will: (i) take reasonable measures to ensure that the information cannot be, linked, attributed, or otherwise associated with a consumer, household, or device (including without limitation: (a) implementing and maintaining technical and administrative safeguards that prohibit re-identification of the Deidentified Data; (b) implementing and maintaining business processes that specifically prohibit re-identification of the Deidentified Data and prevent inadvertent release of the Deidentified Data; (c) periodically reassessing technical safeguards and processes to ensure that they are still adequate to prevent reidentification of and prohibit inadvertent release of the Deidentified Data); (ii) publicly commit to maintain and use the Deidentified Data in deidentified form and not to attempt to reidentify the information; and (iii) contractually obligate any recipients of the Deidentified Data to comply with all provisions of this Section 3.1.6.

4. Obligations of Discovery Education as a Service Provider

4.1 Discovery Education will not Sell (as defined by applicable Data Protection Laws), Share (as defined by applicable Data Protection Laws), retain, use or disclose the Usage Data: (i) for any purpose other than the specific business purpose necessary to perform the Services as described in **Exhibit A** or as otherwise permitted by applicable Data Protection Laws; (ii) for any commercial purpose other than the business purposes specified in **Exhibit A**, including in the servicing of a different business, unless expressly permitted by applicable Data Protection Laws; or (iii) outside of the direct relationship with Subscriber, including to build or improve the quality of the Services provided to Subscriber, unless expressly permitted by

applicable Data Protection Laws. Discovery Education may not combine Usage Data with Personal Information that Discovery Education receives from, or on behalf of, another person or collects from its own interaction with consumers. Notwithstanding the foregoing, Discovery Education may aggregate and use such data for benchmarking and internal analytics purposes.

4.2 Following termination or expiration of the Agreement, Discovery Education will, within a commercially reasonable time period, delete all relevant Usage Data, except to the extent Discovery Education is required to retain such information by law or where such information is necessary for defense of legal claims, in which case the confidentiality obligations and use restrictions in this DPA will continue to apply to such information and/or copies so retained.

4.3 Upon Subscriber's written request to Discovery Education, Discovery Education will make available to Subscriber all information reasonably necessary to demonstrate compliance with this DPA and applicable Data Protection Laws.

4.4 To the extent an End User is not able to access, amend or delete their information through the features available to it through the Services, Discovery Education will fulfill the individual's request within the time periods set forth under applicable Data Protection Laws. Discovery Education will provide reasonable assistance to Subscriber with: (i) complying with Subscriber's obligations in relation to the security of Processing Subscriber's Personal Information and notification of a Data Breach, (ii) any data protection assessments, and (iii) any investigations by competent data privacy authorities, in each case solely in relation to Processing of Subscriber's Personal Information by and taking into account the nature of the Processing and information available to Discovery Education. Discovery Education will provide to Subscriber all information reasonably necessary to demonstrate compliance with applicable Data Protection Laws. Upon notification of unauthorized use of Subscriber Personal Information, Subscriber shall have the right to take reasonable and appropriate steps to remediate the unauthorized use; provided, however, Subscriber and Discovery Education will make reasonable efforts to mutually agree on steps to remediate and ensure Subscriber Personal Information is used appropriately. Discovery Education hereby certifies that it understands its obligations under this Section 4 and shall comply with them.

5. Obligations of Discovery Education as Third Party

5.1 Discovery Education will not Sell or Share Account Information with any third party without providing notice and procuring the opt out/consent as required by applicable Data Protection Laws. In connection with the Account Information Discovery Education will: (i) provide all required notices under applicable Data Protection Laws; (ii) procure all required consents or offer required opt outs under applicable Data Protection Laws. Discovery Education shall not retain such information longer than necessary for the purposes for which it Processes it.

6. **Recipients and Subprocessors.** Discovery Education will ensure that its Subprocessors comply with all applicable Data Protection Laws and obligations under this DPA. Subscriber hereby approves of the Subprocessors which Discovery Education currently engages, as listed on **Exhibit C**. Discovery Education may engage new Subprocessors in accordance with this Section 6 only after notice to Subscriber and providing Subscriber an opportunity to object to such Subprocessors within thirty (30) days of receipt of such notice. If, within thirty (30) calendar days after receiving such notice, Subscriber objects to the new Subprocessor, Discovery Education will make commercially reasonable efforts to: (i) find another Subprocessor that will be acceptable; (ii) (if applicable) change the Services at issue so that the Services of the new Subprocessor are no longer necessary; or (iii) have Subprocessor adequately remediate Subscriber's objections in a timely manner to Subscriber's reasonable satisfaction. If Discovery Education cannot reasonably accommodate Subscriber's objection, Discovery Education shall notify Subscriber within thirty (30) days from receipt of the notice of objection. Subscriber may, upon written notice to Discovery Education, with immediate effect, terminate this DPA and/or the Agreement to the extent it relates to the Services that require the use of such objected-to Subprocessor. Discovery Education will enter into written contracts with its Subprocesors which: (i) includes terms substantially equivalent to those set out in this DPA; and (ii) meet the requirements of applicable Data Protection Laws. These written contracts will also require Subprocessors to enter into the same agreements with subsequent Subprocessors. Discovery Education will notify Subscriber upon its request by email or otherwise about the name, address and role of each Subprocessor being used by Discovery Education to Process Personal Information.

7. **Discovery Education Personnel.** Discovery Education will ensure that its personnel engaged in the Processing of Subscriber's Personal Information are informed of the confidential nature of such information and are subject to a duty of confidentiality with respect to such information.

8. **Information Security.** Discovery Education will provide at least the same level of privacy protection as required by applicable Data Protection Laws. Discovery Education represents and warrants that it has implemented and maintains appropriate technical and organizational measures to ensure a level of security commensurate to the risk to Subscriber Personal Information. Such measures include taking appropriate administrative, physical, organizational, and technical safeguards to prevent and guard against the unauthorized or accidental access, disclosure, destruction, loss, processing, damage, or alteration of Subscriber Personal Information. Subscriber represents and warrants that it has evaluated the security measures implemented by Discovery Education set forth on **Exhibit D** as providing an appropriate level of protection for the Subscriber Personal Information, taking into account the risk associated with the Processing of such information.

9. **Data Breach.** Discovery Education will notify Subscriber without undue delay after Discovery Education having become aware of a Data Breach affecting Subscriber Personal Information. In its notification, Discovery Education shall provide Subscriber with

reasonably sufficient information and documentation to allow Subscriber to meet any notification obligations to regulators or inform impacted individuals of the Data Breach. To the extent Discovery Education has or learns of information relevant to a Data Breach, such notification shall include: (i) the types of Subscriber Personal Information that were or are reasonably believed to be the subject of the Data Breach; (ii) the date or estimated date of the Data Breach; (iii) a general description of the Data Breach; and (iv) the steps Discovery Education has taken to remediate the Data Breach. If acting as a Service Provider, Discovery Education will not make any notification in connection with a Data Breach unless instructed to do so by Subscriber in writing. Discovery Education will continuously supplement the information provided to Subscriber as additional information becomes available to it. To the extent Discovery Education is acting as a Third Party and has an independent notification obligation under applicable law, Discovery Education will inform Subscriber of its independent obligation prior to any such notification and will provide Subscriber with a copy of the proposed notification for review. Subscriber and Discovery Education will work in good faith to address any concerns or proposed revisions presented by Subscriber with respect to the notification as it relates to Subscriber Personal Information. Discovery Education will make all reasonable efforts, in accordance with its security incident management policies and procedures, to identify the cause of any Data Breach, to remediate it, and to put in place any measures designed to prevent subsequent breaches.

10. **Indemnification.** Indemnification under this DPA is subject to the indemnification section of the Agreement.

11. **Severability.** If any provision of this DPA be deemed invalid, illegal, or unenforceable by any court of competent jurisdiction, then the remaining provisions of this DPA shall remain in full force and effect.

13. **Governing Law and Jurisdiction.** The Parties hereby submit to the choice of law and jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity, or termination or the consequences of its nullity.

14. **Nondisclosure.** The Parties agree that the details of this DPA constitute each Party's confidential information. Notwithstanding the foregoing, this Section 14 will not prohibit the Parties from disclosing this DPA to regulatory authorities, if required to comply with applicable Data Protection Laws.

15. **Term.** The term of this DPA will end simultaneously and automatically at the later of: (i) the termination of the Agreement; or (ii) when Subscriber Personal Information is deleted from Discovery Education's systems.

16. **Survival.** The obligations set forth herein will survive termination of the Agreement for as long as the Parties are Processing Personal Information.

17. **No Amendment; Order of Precedence.** Nothing in this DPA reduces the Parties' obligations under the Agreement in relation to the protection of Personal Information or permits the Parties to Process (or permit the Processing of) Personal Information in a manner which is prohibited by the Agreement. For clarity, the obligations under this DPA are in addition to the obligations under the Agreement and are intended to be additive and provide additional protections for Personal Information. In the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail.

18. All Exhibits to this DPA are hereby incorporated by reference into, and made a part of, this DPA.

19. **Changes in Data Protection Laws**. If any change is required to this DPA as a result of a change in applicable Data Protection Laws, then either Party may provide written notice to the other Party of that change in law and the Parties will, in good faith, execute modifications to this DPA to comply with such change in applicable Data Protection Laws.

Exhibit A

Processing Details: Discovery Education as a Service Provider

Categories of individuals whose Personal Information is Processed: Subscriber's End Users (i.e. employees).

Categories of Personal Information Processed:

- Usage data of the Services: time spent in the Services; number of sessions; pending, accepted, and completed requests; volunteer hours (if the End User is an employee of a corporate partner); aggregate number of students reached; device ID; operating system; and IP address (collectively, "**Usage Data**").

The frequency of the Processing: Continuous for as long as Subscriber uses the Services.

Nature of the Processing: Discovery Education will collect, aggregate, store, retain, analyze, transmit, and delete the Usage Data.

Purpose(s) of the Processing: The purpose of the Processing is to: (i) facilitate Discovery Education's provision of the Services to Subscriber; (ii) generate and share with Subscriber aggregated reports of Subscriber's End Users' Usage Data; and (iii) aggregate data to produce reports for analytics and benchmarking purposes.

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period: Discovery Education will Process Usage Data for as long as required to provide the Services.

Exhibit B

Processing Details: Discovery Education as a Third Party

Categories of individuals whose Personal Information is Processed: Subscriber's End Users (i.e. employees).

Categories of Personal Information Processed: The below shall be collectively referred to as "**Account Information.**"

- If the End User is an employee of an educator:
  - Personal identifiers: (name and email address)
  - Professional or employment-related information: (school or school district, job title, and grade level)

- If the End User is an employee of a corporate partner:
  - Personal identifiers: (name, email address, city/state, pronouns (if provided))
  - Professional or employment-related information: (employer, position/title, industry, employment level, tenure with employer, volunteer status, professional biography)
  - Visual information: (Career Connect account photo)
  - Protected classifications: (gender (if provided))
  - Sensitive protected classifications (race or ethnicity (if provided))

Purpose(s) of the Processing: The purpose of the Processing is to:

- create and manage End Users' Career Connect account;
- authenticate access to End Users' Career Connect account;
- personalize End Users' experience within the Services (such as providing content relevant to the applicable End User's requests);
- communicate with End Users within the Services and via email for scheduling classroom sessions;
- request End Users' feedback on the Services;
- request End Users' feedback on their volunteer experience (if the End User is an employee of a corporate partner);
- send promotional, marketing, or operational communications
- deliver video conferencing invitations;
- improve the Services;
- develop new features and functionalities within the Services;
- prevent fraudulent use of the Services and detect unlawful activity; and
- diagnose and repair errors occurring within the Services.

Exhibit C

List of Approved Subprocessors

- Pendo
- Zoom SDK
- Iterable
- Auth0

Exhibit D

DISCOVERY EDUCATION DATA SECURITY POLICY

This Security Policy ("Policy") describes, in general, (i) what steps Discovery Education, Inc. ("Discovery") takes to protect Personal Information that is provided to Discovery; (ii) how Personal Information may be used; (iii) with whom Discovery may share Personal Information, and (iv) the steps Discovery takes to protect the Personal Information. All capitalized terms not defined herein shall have the meaning set forth in the DPA.

No Personal Information is required for the use of any of the basic Discovery Education services, however, in the event End Users elect to use any of the functionality within the Discovery Education services which provide personalized pages, individual accounts, other user-specific customization, or otherwise submit or upload information (all such data is generally limited to the following: school name, first name, last name, grade level, and Discovery generated username/password), all such Personal Information provided to Discovery will be protected in accordance with this Policy.

No school employee Personal Information is required for Professional Development Services other than first name and last name for the purposes of attendance logs.

I. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

"Authorized Disclosee" means the following: (1) third parties to whom the Subscriber has given Discovery written approval to disclose Personal Information; (2) third parties to whom disclosure is required by law; and (3) if applicable, third party vendors working on Discovery's behalf or performing duties in connection with Discovery's services (e.g. hosting companies) and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized User" means a Discovery employee authorized by the Subscriber to access Personal Information in order to perform the Services under the Agreement.

"Destroy" means: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying Personal Information in paper, electronic, or other means so as to make it unreadable, unreconstructible, and indecipherable.

II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

Basic Privacy Protections

1. Compliance with Law and Policy. All Personal Information is handled, processed, stored, transmitted and protected by Discovery in accordance with all applicable federal data privacy and security laws (including FERPA) and with this Policy.

2. Training. Employees (including temporary and contract employees) of Discovery are educated and trained on the proper uses and disclosures of Personal Information and the importance of information privacy and security.

3. Personnel Guidelines. All Discovery employees are required to be aware of and work to protect the confidentiality, privacy, and security of Personal Information. Discovery, and its respective personnel do not access Personal Information except to comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the Agreement. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:

a. Limit internal access to Personal Information to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the Personal Information to carry out the Services provided under the Agreement.
b. Disclose Personal Information only to Authorized Disclosees.
c. Access Personal Information only by Authorized Users.
d. When Personal Information is no longer needed, delete access to Personal Information.
e. Permit employees to store or download information onto a local or encrypted portable devices or storage only when necessary, and to create a written record for retention verifying that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).
f. Any downloaded materials consisting of Personal Information remain in the United States.
g. Prohibit the unencrypted transmission of information, or any other source of Personal Information, wirelessly or across a public network to any third party.
h. Upon expiration or termination of the Agreement, Discovery will Destroy all Personal Information previously received from Subscriber no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber to Discovery to hold such information Personal Information. Each electronic file containing Personal Information provided by Subscriber to Discovery will be securely Destroyed. This provision shall apply

to Personal Information that is in the possession of Discovery, Discovery employees/personnel and/or Authorized Disclosees.

Information Security Risk Assessment

Discovery periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing Personal Information maintained by Discovery; Discovery reports such risks as promptly as possible to Subscribers; and Discovery implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented by Discovery based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

1. Administrative Safeguards
    a. Sanctions: Appropriate sanctions against Subcontractor personnel who fail to comply with Discovery's security policies and procedures.
    b. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
    c. Security Oversight: Assignment of one or more appropriate management level employees of Discovery to be responsible for developing, implementing, and monitoring of safeguards and security issues.
    d. Appropriate Access: Procedures to determine that the access of Discovery personnel to Personal Information is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Discovery personnel who have access to Personal Information.
    e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to Personal Information.
    f. Access Termination: Procedures for terminating access to Personal Information when employment ends, or when an individual no longer has a legitimate need for access.

2. Physical Safeguards
    a. Access to Personal Information: Procedures that grant access to Personal Information by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
    b. Awareness Training: On-going security awareness through training or other means that provide Discovery personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.

c. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.

d. Physical Access: Procedures to limit physical access to Personal Information and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.

e. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to Personal Information.

f. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where Personal Information is stored.

g. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain Personal Information into and out of a facility.

3. Technical Safeguards

a. Data Transmissions: Technical safeguards, including encryption, to ensure Personal Information transmitted over an electronic communications network is not accessed by unauthorized persons or groups.

b. Data Integrity: Procedures that protect Personal Information maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.

c. Logging off Inactive Users: Inactive electronic sessions are designed to terminate automatically after a specified period of time.

Security Controls Implementation

Discovery has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

Security Monitoring

In combination with periodic security risk assessments, Discovery uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Discovery also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.

Security Process Improvement

Based on Discovery's security risk assessments and ongoing security monitoring, Discovery gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery uses this information to update and improve its risk assessment strategy and control processes.

Audit

Discovery acknowledges Subscriber's right to audit any Personal Information collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to Discovery, at Discovery's principal place of business, during normal business hours, and no more than once per year. Discovery shall maintain records and documentation directly and specifically related to the Services performed under the Agreement for a period of three (3) years, unless otherwise stated in Section II(3)(h) of this Policy.

Breach Remediation

Discovery keeps Personal Information provided to Discovery secure and uses reasonable administrative, technical, and physical safeguards to do so. Discovery maintains and updates incident response plans that establish procedures in the event a breach occurs. Discovery also identifies individuals responsible for implementing incident response plans should a breach occur.

If Subscriber or Discovery determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Discovery provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all applicable breach of confidentiality laws.

Discovery reports as promptly as possible to Subscriber (or its designees) any incident involving unauthorized access to or acquisition of Personal Information of which they become aware that results from any breach or hacking of Discovery's Electronic Data System. Such incidents include any breach or hacking of Discovery's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "**Electronic Data System**" means all information processing and communications hardware and software owned or controlled by Discovery and used by Discovery in connection with providing the Services.

Personnel Security Policy Overview

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new Discovery personnel, in particular those who have access to Personal Information.

2. Obtaining agreements from internal users covering confidentiality, nondisclosure, and authorized use of Personal Information.
3. Providing training to support awareness and policy compliance for Discovery's new hires and annually for Discovery personnel.