RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Discovery Education, Inc. ("Service Provider") on 9/24/2019 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ◉ No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ◉ No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ◉ No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ◉ No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ◉ No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ◉ No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ◉ No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ◉ No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ◉ No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ◉ No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ◉ No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ◉ No ○

3. Vendors cannot sell student information.

   Agree: Yes ◉ No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ◉ No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ◉ No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ◉ No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ◉ No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Travis Barrs
Print Name

DocuSigned by:
78B6C33846AB459...
September 25, 2019
Signature, Date

Laura Assem, 9/27/2019
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section 1.6: External Security

Discovery Education has a comprehensive vulnerability management program that includes regular automated scans, and a suite of cybersecurity tools including endpoint protection and firewalls, with 24/7 monitoring provided by a Managed Security Services Provider (MSSP).

Section 1.7: Internal Security

Discovery Education has a comprehensive vulnerability management program that includes regular automated scans, and a suite of cybersecurity tools including endpoint protection and firewalls, with 24/7 monitoring provided by a Managed Security Services Provider (MSSP). Data from the district is uploaded via a secure FTP site. Only internal employees with appropriate access level approved by management will have access to district data. Data is encrypted at rest in the database. We perform daily onsite backup as well as offsite backup. Currently offsite backups are in 3-week rotation. 60 days after licenses expire, we anonymize district data.

Section II.2: Exporting of Student-Created Content

The service has an option for users to download their own content and move it to a desired location.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

We collect PII from school district. Parents, legal guardians and students should reach out to their district to correct their information. Once the information is corrected, district will use the same mechanism used during the onboarding process to update this information within our system. The mechanism offered include but not limited to a bulk upload process using a Secure FTP.

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Discovery Education has a comprehensive vulnerability management program that includes regular automated scans, and a suite of cybersecurity tools including endpoint protection and firewalls, with 24/7 monitoring provided by a Managed Security Services Provider (MSSP). Data from the district is uploaded via a secure FTP site. Only internal employees with appropriate access level approved by management will have access to district data. Data is encrypted at rest in the database. We perform daily onsite backup as well as offsite backup.

Section II.6: Disclosure Notification

Based on Discovery Education's security risk assessments and ongoing security monitoring, Discovery Education gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery Education uses this information to update and improve its risk assessment strategy and control processes.
In the event of an actual data breach, there is a comprehensive cybersecurity incident response plan in place that includes communication to relevant parties.
The Service Provider's Student Data Protection Addendum is attached hereto as Exhibit A.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Discovery Education shall use such student data provided in compliance with the COPPA, FERPA, CIPA and other applicable laws, regulations and statutes, and (b) the Student Data Transparency and Security Act in Colorado House Bill 16-1423 and (iii) Discovery's Data Security Policy.
The Service Provider's Student Data Protection Addendum is attached hereto as Exhibit A.

Section III.5: How Student Data is Protected:

Discovery Education has a comprehensive vulnerability management program that includes regular automated scans, and a suite of cybersecurity tools including endpoint protection and firewalls, with 24/7 monitoring provided by a Managed Security Services Provider (MSSP). Data from the district is uploaded via a secure FTP site. Only internal employees with appropriate access level approved by management will have access to district data. Data is encrypted at rest in the database. We perform daily onsite backup as well as offsite backup.
The Service Provider's Student Data Protection Addendum is attached hereto as Exhibit A.

Discovery EDUCATION

EXHIBIT A

DISCOVERY EDUCATION
STUDENT DATA PROTECTION ADDENDUM

This Discovery Education Student Data Protection Addendum ("**DPA**") describes Discovery's obligations to protect Student Data (defined below) during Discovery's provision of Subscriber the Services to Subscriber.

1. Student Data and Purpose of DPA. As between Subscriber and Discovery, Subscriber or the party who provided such data (such as the student or parent), is the exclusive owner of all right, title, and interest in and to any and all Student Data disclosed or transmitted to Discovery under the Agreement and this DPA. Discovery hereby waives any and all statutory and common law liens it may now or hereafter have with respect to Subscriber's Student Data. Nothing in the Agreement or this DPA will operate as an obstacle to Subscriber's right to retrieve any and all Student Data disclosed or transmitted to Discovery under the Agreement and this DPA. Notwithstanding the foregoing, Discovery may de-identify and aggregated Subscriber's Student Data with Discovery's other Subscribers' Student Data and use and exploit the de-identified and aggregated data for any lawful purpose. The parties agree to comply with the terms of this Addendum and Data Protection Laws as they relate to Student Data.

2. Schedule A (Discovery's Security Policy). Schedule A attached hereto and incorporated herein sets forth Discovery's policies regarding: (i) what steps Discovery takes to protect personally identifiable information ("**PII**") that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII. For purposes of this DPA, PII includes Student Data.

3. Consents and Notifications for Disclosures of Student Data. Subscriber affirms, represents, and warrants that it has obtained, and is solely responsible for obtaining, all consents as may be required by the Data Protection Laws, as well as making all required disclosures to the parents, legal guardians, and students as may be required by the Data Protection Laws, to disclose or transmit Student Data to Discovery. Subscriber will provide proof of the required consent within 5 business days of Discovery's written request.

4. Discovery's Personnel and Subcontractors. Discovery will ensure that its personnel and subcontractors that access the Student Data are informed of the confidential nature of the Student Data and are bound by appropriate obligations of confidentiality or are under an appropriate statutory obligation of confidentiality. Discovery will take all reasonable steps and to ensure the reliability of Discovery personnel and subcontractors that access Student Data.

5. Student Data Requests. Discovery will, without undue delay, notify, then record, and then refer to Subscriber full details of all Student Data Requests. To the extent Subscriber is unable to respond to a Student Data Request with information available through Discovery's products or services, Discovery will provide reasonable assistance to Subscriber in responding to a Student Data Request. Discovery will not respond to a Student Data Request without Subscriber's explicit instruction.

6. Deletion or Return Of Student Data. Upon termination or expiration of the Agreement, Discovery will promptly, but without undue delay, destroy Student Data upon Subscriber's written request. Discovery may retain Student Data to the extent required by the laws, rules, and regulations to which Discovery is subject, or if Student Data resides in Discovery's backup archives, Discovery will continue to protect the security and confidentiality of such retained Student Data in accordance with the Agreement and this DPA. Discovery has implemented retention rules so that Student Data in backup archives is retained for as short a time as necessary.

7. Audits. Subscriber may request once per calendar year to audit Discovery's Security Policy and related systems that are used to store Student Data in order to verify compliance with this DPA and the Data Protection Laws. If Subscriber wishes to conduct an audit using a third party auditor, Discovery may object to Subscriber's choice of third party auditor on reasonable grounds and in such event, Subscriber will select a different auditor. Subscriber will reimburse Discovery for any time expended in relation to such audit at Discovery's then-current hourly professional services rate. Subscriber and Discovery will mutually agree upon the scope and timing of an audit prior to any such audit. An audit performed pursuant to this DPA will not exceed one business day and will not unreasonably interfere with the normal conduct of Discovery's business. Subscriber (or Subscriber's third-party auditor) will at all times comply with the use, security, and access policies at such location. Any audit performed pursuant to this Section DPA will be conducted under a confidentiality agreement and any information or report derived from such audit will be deemed Discovery's confidential information.

8. Student Data Breach.

8.1. **Student Data Breach Notification.** In the event of any Student Data Breach, upon Discovery becoming aware of such Student Data Breach, without undue delay Discovery will:

8.1.1. notify Subscriber of the Student Data Breach; and

8.1.2. provide Subscriber with details that are available to Discovery at the time of notice regarding:

(a) the nature of the Student Data Breach, including the categories and approximate numbers of students and Student Data records concerned;

(b) any investigations into such Student Data Breach; and

(c) any measures taken to address the Student Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of the Student Data Breach.

8.2. **Notification Sharing.** Subscriber may share any notification and details provided by Discovery under this Section 11 with the appropriate government agency or law enforcement authority if required to do so under the Data Protection Laws.

9. Suspension. Subscriber may suspend the transfer of Student Data to Discovery, or terminate the affected Agreement without penalty to Subscriber if: (i) Discovery is in material breach of its obligations under this DPA and does not cure such breach within thirty (30) days of Subscriber's notification to Discovery of such breach; or (ii) Discovery notifies Subscriber that it cannot comply with the obligations set forth in this DPA or the Data Protection Laws.

10. Student Data Disclosures. To the extent legally permissible, Discovery will promptly notify Subscriber of any legally binding request for disclosure or seizure of Student Data by a government agency or law enforcement authority.

11. Term. The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement; or (ii) when all Student Data is deleted from Discovery's systems.

12. Indemnification. Each of the parties ("**Indemnifying Party**") agrees to indemnify and hold harmless the other party and its officers, employees, directors, and agents ("**Indemnified Party**") from, and at the Indemnifying Party's option defend against, any and all third party claims, losses, liabilities, damages, costs, and expenses (including attorneys' fees, consultants' fees, and court costs) (collectively, "**Claims**") arising out of the Indemnifying Party's (i) violation of a Data Protection Law; or (ii) breach of any provision of this DPA.

13. Definitions and Interpretation.

13.1. **Definitions.**

"**Data Protection Law**" means:

(a) the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR part 99) ("**FERPA**");

(b) the Children's Online Privacy and Protection Act (15 U.S.C. §§ 6501–6506) ("**COPPA**");

(c) the Colorado Student Data Transparency and Security Act (C.R.S. 22-16-101 et.al.);

(d) the Connecticut Public Act 16-189;

(e) the California Student Online Student Information Protection Act (**SB-1177**) ("**SOPIPA**"); and

(f) all other federal and state data protection and breach notification laws applicable to Student Data;

in each case, as in force and applicable, and as may be amended, supplemented, or replaced from time to time.

"**Student Data**" means any personally identifiable information of a student that through the course of Subscriber's use of the Services is: (i) provided by a student, or the student's parent or legal guardian, to Discovery in the course of the student's, parent's, or legal guardian's use of Discovery's website, service, or application that is designed and marketed for K–12 school

purposes; (ii) created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to Discovery; or (iii) gathered by Discovery through the operation of Discovery's website, service, or application that is designed and marketed for K–12 school purposes and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

"**Student Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Student Data; and

"**Student Data Request**" means a request made by Subscriber, a parent or legal guardian, or student to exercise any rights granted by the Data Protection Laws.

Discovery EDUCATION

Schedule 1

DISCOVERY EDUCATION, INC. DATA SECURITY POLICY

This Policy describes, in general, (i) what steps Discovery takes to protect personally identifiable information ("PII") that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII.

No student PII is required for the use of any of the basic Discovery Education services, however, in the event 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 PII provided to Discovery will be protected in accordance with this Policy.

No school employee PII 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/Customer/Distributor has given Discovery written approval to disclose PII; (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 Use" means a Discovery employee authorized by the Subscriber/Customer/Distributor to access PII in order to perform services under an Agreement.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S Department of Education,and are available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA.

II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

Basic Privacy Protections

1. Compliance with Law and Policy. All PII provided to Discovery 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 PII 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 PII. Discovery, and its respective personnel do not access PII 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 with Subscriber/Customer/Distributor. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:

   a. Limit internal access to PII to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the PII to carry out the services provided under the Agreement.
   b. Disclose PII only to Authorized Disclosees
   c. Access PII only by Authorized Users.
   d. When PII is no longer needed, delete access to PII.

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 PII remain in the United States.
g. Prohibit the unencrypted transmission of information, or any other source of PII, wirelessly or across a public network to any third party.
h. Upon expiration or termination of Agreement, Discovery shall Destroy all PII previously received from Subscriber/Customer/Distributor no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber/Customer/Distributor to Discovery to hold such PII. Each electronic file containing PII provided by Subscriber/Customer/Distributor to Discovery will be securely Destroyed. This provision shall apply to PII 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 PII maintained by Discovery; Discovery reports such risks as promptly as possible to Subscribers/Customers/Distributors; 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 Contractor 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 PII 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 PII.
   e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to PII.
   f. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

2. Physical Safeguards
   a. Access to PII: Procedures that grant access to PII 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 PII 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 the PII.
   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 PII is stored.
   g. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.

3. Technical Safeguards
   a. Data Transmissions: Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.
   b. Data Integrity: Procedures that protect PII 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/Customer's/Distributor's right to audit any PII collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to 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 PII 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 should occur.

If a Subscriber/Customer/Distributor 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 breach of confidentiality laws.

Discovery reports as promptly as possible to Subscribers/Customers/Distributors (or their designees) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. 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 employed in Discovery's business, whether or not owned by Discovery or operated by its employees or agents in performing work for Discovery.

Personnel Security Policy Overview

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new personnel, in particular those who have access to PII.
2. Obtaining agreements from internal users covering confidentiality, nondisclosure and authorized use of PII.
3. Providing training to support awareness and policy compliance for new hires and annually for personnel.

DS SH