

CONTRACTOR ACCESS TO REED COLLEGE
ELECTRONIC DATA AND/OR COMPUTER RESOURCES

This data access agreement (this “Data Access Agreement”) is between the Reed Institute, an Oregon nonprofit corporation doing business as Reed College (“Reed”), and _____, a _____ (“Contractor”).

Contractor is performing certain services for Reed under separate agreement relating to the educational interests of Reed (“Services”) and may, in the performance of such Services, require access to confidential information and information that identifies particular individuals, including Students. Reed desires Contractor to perform such Services in compliance with all applicable laws and regulations, as well as the policies and procedures of Reed. In consideration of access to confidential information and Protected Information, Contractor and Reed agree as follows:

1. **DEFINITIONS.** When used in this Data Access Agreement, the following terms will have the meanings below:

1.1. “Data” means the observations and information collected or accessed during the performance of Services. Data includes Protected Information.

1.2. “Education Records” has the meaning set forth in the Family Educational Rights and Privacy Act (“FERPA,” codified at 20 U.S.C. § 1232g, with regulations set forth at 34 C.F.R. § 99, *et seq.*).

1.3. “Reed Network” means the group of interconnected computers administered by Reed (directly or through third parties), including the servers, routers, other hardware, and software necessary to maintain the connections, regardless of the method of connection, functional relationship, or topology of the connections.

1.4. “Personally Identifiable Information” has the meaning set forth in FERPA.

1.5. “Protected Information” means information provided by or at the direction of Reed, or to which access was provided in the course of Contractor’s performance of Services, that (i) is an Education Record or Personally Identifiable Information; (ii) identifies any individual (by name, signature, address, telephone number, email address, or other unique identifier) (iii) can be used to authenticate any individual (including without limitation any employee identification number, Social Security number, driver’s license number or other government-issued identification number, passwords or PINs, biometric or health Data, answers to security questions, or other personal identifiers); or (iv) includes credit card, debit card, or other financial information. Reed business contact information is not by itself Protected Information.

1.6. “Security Breach” means any actual, probable, or reasonably suspected misuse, compromise, or unauthorized access of Protected Information, including but not limited to (i) physical trespass on a secure facility; (ii) electronic systems intrusion or hacking; (iii) loss or theft of a notebook, desktop, or other electronic or mobile device, hard drive, or information storage device; (iv) loss or theft of printed materials; (v) receipt of a complaint in relation to the

privacy practices of Contractor; or (vi) a breach or alleged breach of the privacy or Data protection policies of Contractor that involves Protected Information.

1.7. "Student" has the meaning set forth in FERPA. References to individuals include Students.

2. CONFIDENTIALITY.

2.1. Contractor acknowledges that in the course of its engagement by Reed, Contractor may receive or have access to Protected Information. In recognition of the foregoing, Contractor covenants and agrees that:

(a) It will use and disclose Protected Information solely and exclusively for the purposes for which such information, or access to it, is provided in order to perform Services.

(b) It will not share, sell, rent, or use Data with or to any third parties without the express written consent of Reed, and will not use Data for any purpose not directly related to the scope of Services.

2.2. Data provided by Reed, including but not limited to Protected Information, and other members of the Reed community, is confidential, and Contractor will treat it in accordance with Section 6 below and Reed's policies for the protection of confidential Data, provided at <http://web.reed.edu/cis/help/id-confidential.html>.

3. ACCESS AND PASSWORDS. Contractor and its employees who use computing resources provided by Reed or have Reed network access to Data must read and agree to the Reed College Computing User Agreement. Contractor and its employees will keep individual passwords secret and not share or disclose passwords to others, including other Contractor employees. A violation of this section by Contractor is a material breach of this Data Access Agreement, and both Contractor and the culpable individual(s) will be subject to termination of any rights to the Reed Network, as well as any and all remedies in law and equity.

4. CONTRACTOR OBLIGATIONS.

4.1. Contractor will not introduce or allow to be introduced into the Reed Network any viruses, worms, Trojan horses, spyware, or other code that is designed to disrupt, disable, erase, alter, harm, or otherwise impair any software or hardware in the Reed Network. Contractor represents and warrants that its equipment is regularly maintained to the standards provided by the operating system vendor, with the latest commercially available security patches, is running the latest, industry-standard, commercially-available antivirus software, and is configured with security measures appropriate for the storage and transmission of non-public data on public networks. Alternately, Contractor may limit its use of computing equipment to that which Reed has made available to Contractor for such purposes or instruct Reed to scan and patch Contractor's equipment, at Contractor's expense.

4.2. Contractor is and will remain in compliance with all applicable federal, state, and local laws and regulations governing its use and disclosure of Data, including but not limited to the Fair Credit Reporting Act, the Telephone Consumer Protection Act, the Fair Debt Collection Practices Act, the Gramm-Leach-Bliley Act, and FERPA.

4.3. Contractor is fully responsible and liable for all acts, omissions, and work performed by any of its representatives, including any subcontractor, and will require all subcontractors engaged in the provision of Services under this Agreement to comply with the terms and conditions of this Agreement and to require those individuals to cooperate with Contractor and Reed in connection with Contractor's obligations herein.

5. SECURITY NOTICE.

5.1. Contractor will notify Reed of a Security Breach within 24 hours after it becomes aware of it. Contractor will notify Reed of any Security Breaches by emailing Reed's Chief Technology Officer at cio@reed.edu.

5.2. Contractor will provide Reed with the name and contact information for a primary security contact who will be available to assist Reed 24 hours per day, seven days per week in resolving obligations associated with the Security Breach.

5.3. Immediately following such discovery and notification to Reed, the parties will coordinate with each other to investigate the Security Breach. Contractor agrees to fully cooperate with Reed in Reed's handling of the matter, including without limitation any investigation, providing Reed with physical access to the facilities and operations affected, facilitating interviews with Contractor's employees and others involved in the matter, and making available all relevant records, logs, files, and data reporting or other obligations required by applicable law, regulation, or standard, or as otherwise required by Reed.

5.4. Contractor will take immediate steps to remedy the Security Breach in accordance with applicable privacy rights, laws, and standards.

5.5. Except as required by law, Contractor agrees that it will not inform any third party of any Security Breach without first obtaining Reed's prior written consent. Further, Contractor agrees that Reed will have the sole right to determine (i) whether and how notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as may be required by law, regulation, or in Reed's discretion, and (ii) the contents of such notice.

5.6. Contractor agrees to cooperate with Reed in any litigation or other formal action against third parties deemed necessary by Reed to protect its rights.

5.7. Contractor will promptly use its best efforts to prevent a recurrence of any Security Breach.

6. STANDARD OF CARE FOR PROTECTED INFORMATION.

6.1. In connection with Protected Information, Contractor will implement and maintain commercially reasonable information safeguards that are no less rigorous than accepted industry practices and that comply with all applicable laws, regulations, and business guidance issued by the Department of Education and the Federal Trade Commission to protect Protected Information from unauthorized access, destruction, use, modification, or disclosure, and, to the extent that payment card information is stored or transmitted through Contractor's system, with the Payment Card Industry Data Security Standard ("PCI DSS") requirements.

6.2. Contractor will ensure that any Social Security numbers, driver's license numbers, full birth dates, financial account information, payment card information, customer lists, and other types of Protected Information that would reasonably be considered highly sensitive, and are maintained by Contractor, are encrypted (i) during transmission, whether sent by email, fax, or otherwise, and (ii) when stored on a mobile device, such as a portable computer, flash drive, personal digital assistant, or phone. If encryption is not feasible for mobile devices, Contractor will ensure that no sensitive Protected Information is stored on or transmitted through mobile devices. Further, all sensitive Protected Information stored on databases, servers, or other nonmobile devices will be protected against all reasonably anticipated forms of compromise, whether by use of encryption, logical access controls, or other robust safeguards.

6.3. Contractor will ensure that all software testing for systems or applications designed to handle Protected Information or other confidential information must be accomplished exclusively with "sanitized" production information. Sanitized information is production information that no longer contains specific details that might be valuable, sensitive, private, or confidential, and that can no longer be used to identify an individual.

7. INDEPENDENT CONTRACTOR. The parties intend to be independent contractors. Contractor will control its employees; provided, however, that Contractor and its employees and agents will be subject to the oversight and direction of Reed with respect to the use and maintenance of "education records" as that term is defined in FERPA. Contractor will be solely responsible for the compensation of its employees and all related withholding taxes, workers' compensation, insurance, and other obligations pertaining to Contractor's employees. Neither party will have any right or authority to incur or create any obligation for or legally bind the other party in any way.

8. OVERSIGHT AND VERIFICATION OF SECURITY COMPLIANCE.

8.1. If Contractor has payment card data (*i.e.*, anything more than truncated credit or debit card information), then Contractor will, upon Reed's request, submit a detailed summary to Reed or a third party on Reed's behalf of the PCI DSS assessment results and remediation efforts (if any).

8.2. If Contractor has other types of sensitive Protected Information, but not payment card data, then Contractor will, upon request, grant Reed or a third party on Reed's behalf permission to perform an assessment, audit, examination, or review of controls in Contractor's environment in relation to the Protected Information being handled and/or Services being provided to confirm compliance with this Data Access Agreement, as well as any applicable laws, regulations, and industry standards. In addition, upon request, Contractor will provide Reed with the results of any audit performed that assesses the effectiveness of Contractor's information security program as relevant to the security and confidentiality of Protected Information accessed during the course of this Data Access Agreement.

8.3. Upon request, Contractor will promptly and accurately complete an information security questionnaire provided by Reed or a third party on Reed's behalf regarding Contractor's environment in relation to the Protected Information being handled and/or Services being provided to confirm compliance with this Data Access Agreement, as well as any applicable laws, regulations, and industry standards. Contractor will fully cooperate with such inquiry.

9. **INDEMNITY.** Contractor will defend and indemnify Reed from and against any third-party claims, losses, liabilities, and expenses (including without limitation reasonable attorneys' fees and expenses) that relate to any failure by Contractor, Contractor's employees, agents, or subcontractors to comply with any obligation enumerated in this Data Access Agreement.

10. **LIMITATION ON LIABILITY.** EXCEPT FOR LIABILITIES ARISING OUT OF (A) A BREACH OF THE CONFIDENTIALITY OBLIGATIONS OF THIS DATA ACCESS AGREEMENT, (B) THE PRIVACY OBLIGATIONS OF SECTION 4, OR (C) THE INDEMNIFICATION OBLIGATION IN SECTION 9, NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS DATA ACCESS AGREEMENT, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE), EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

Signed:

THE REED INSTITUTE

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date: _____

Date: _____