



UNIVERSITY OF CALIFORNIA

APPENDIX DS

Additional Terms and Conditions – Data Security and Privacy

ARTICLE 1 – PROTECTED INFORMATION

Contractor acknowledges that its performance of Services under this Agreement may involve access to confidential University information including, but not limited to, personally-identifiable information, student records, protected health information, or individual financial information (collectively, “Protected Information”) that is subject to state or federal laws restricting the use and disclosure of such information, including, but not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 *et seq.*); the California Confidentiality of Medical Information Act (Civil Code § 56 *et seq.*); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164). Contractor agrees to comply with all applicable federal and state laws restricting the access, use and disclosure of Protected Information. Contractor agrees to include all of the terms and conditions contained in this Appendix in all subcontractor or agency contracts providing services under this Agreement.

ARTICLE 2 – COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

With respect to the University’s Protected Information, and in compliance with all applicable laws and regulations, Contractor shall comply in all respects reasonably pertinent to the Agreement with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission (<http://www.ftc.gov/reports/privacy3/fairinfo.shtm>). Such principles would typically require Contractor to have a privacy policy, and, if collecting Protected Information electronically from individuals on behalf of the University, a prominently-posted privacy statement or notice in conformance with such principles (the University’s sample Privacy Statement for websites is available at <http://www.ucop.edu/irc/services/documents/sampleprivacystatement.doc>). Contractor also agrees, to the extent applicable to the Agreement, to comply with the University’s Business and Finance Bulletin IS-2, *Inventory, Classification, and Release of University Electronic Information* (<http://www.ucop.edu/ucophome/policies/bfb/is2.pdf>), and IS-3, *Electronic Information Security* (<http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>).

ARTICLE 3 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Contractor agrees to hold the University’s Protected Information, and any information derived from such information, in strictest confidence. Contractor shall not access, use or disclose Protected Information except as permitted or required by the Agreement or as otherwise authorized in writing by University, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Contractor will notify University in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give University an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected Information outside the United States is prohibited except on prior written authorization by the University.

ARTICLE 4 – SAFEGUARD STANDARD

Contractor agrees to protect the privacy and security of Protected Information according to all applicable laws and regulations, by commercially-acceptable standards, and no less rigorously than it protects its own confidential information, but in no case less than reasonable care. Contractor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Protected Information. All Protected Information stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Contractor shall ensure that such security measures

are regularly reviewed and revised to address evolving threats and vulnerabilities while Contractor has responsibility for the Protected Information under the terms of this Appendix. Prior to execution of the Agreement, and periodically thereafter (no more frequently than annually) at the University's request, Contractor will provide assurance, in the form of a third-party audit report or other documentation acceptable to the University (the Shared Assessments® tools <http://www.sharedassessments.org/>, or similar, are acceptable), demonstrating that appropriate information security safeguards and controls are in place.

ARTICLE 5 – RETURN OR DESTRUCTION OF PROTECTED INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Contractor shall return the Protected Information to University unless University requests in writing that such data be destroyed. This provision shall also apply to all Protected Information that is in the possession of subcontractors or agents of Contractor. Such destruction shall be accomplished by “purging” or “physical destruction,” in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Contractor shall certify in writing to University that such return or destruction has been completed.

ARTICLE 6 – BREACHES OF PROTECTED INFORMATION

- A. **Definition.** For purposes of this article, a “Breach” has the meaning given to it under relevant California or federal law, for example, California Civil Code Section 1798.29, California Health and Safety Code Section 1280.15, etc.
- B. **Reporting of Breach:** Contractor shall report any confirmed or suspected Breach to University immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after Contractor reasonably believes a Breach has or may have occurred. Contractor's report shall identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Protected Information accessed, used or disclosed, (iii) the person(s) who accessed, used and disclosed and/or received Protected Information (if known), (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Contractor has taken or will take to prevent future unauthorized access, use or disclosure. Contractor shall provide such other information, including a written report, as reasonably requested by University. In the event of a suspected Breach, Contractor shall keep the University informed regularly of the progress of its investigation until the uncertainty is resolved.
- C. **Coordination of Breach Response Activities:** In the event of a Breach, Contractor will:
Immediately preserve any potential forensic evidence relating to the breach, and remedy the breach as quickly as circumstances permit;
 - 1. Promptly (within 2 business days) designate a contact person to whom the University will direct inquiries, and who will communicate Contractor responses to University inquiries;
 - 2. As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore University service(s) as directed by the University, and undertake appropriate response activities;
 - 3. Provide status reports to the University on Breach response activities, either on a daily basis or a frequency approved by the University;
 - 4. Coordinate all media, law enforcement, or other Breach notifications with the University in advance of such notification(s), unless expressly prohibited by law;
 - 5. Make all reasonable efforts to assist and cooperate with the University in its Breach response efforts; and
 - 6. Ensure that knowledgeable Contractor staff are available on short notice, if needed, to participate in University-initiated meetings and/or conference calls regarding the Breach.
- D. **Costs Arising from Breach.** In the event of a Breach, Contractor agrees to promptly reimburse all costs to the University arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of University personnel responding to Breach, civil or criminal penalties levied against the University, attorneys fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

ARTICLE 7 – EXAMINATION OF RECORDS

University and, if the applicable law, contract or grant so provides, the other contracting party or grantor (and if that be the United States, or an agency or instrumentality thereof, then the Controller General of the United States) shall have access to and the right to examine any pertinent books, documents, papers, and records of Contractor involving transactions and work related to this Appendix until the expiration of five years after final payment hereunder. Contractor shall retain project records for a period of five years from the date of final payment.

ARTICLE 8 – ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Contractor shall make itself and any employees, subcontractors, or agents assisting Contractor in the performance of its obligations under the Agreement available to University at no cost to University to testify as witnesses, or otherwise, in the event of an unauthorized disclosure caused by contractor that results in litigation or administrative proceedings against University, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy and arising out of this Appendix.

ARTICLE 9 – NO THIRD-PARTY RIGHTS

Nothing in this Appendix is intended to make any person or entity that is not signatory to the Agreement a third-party beneficiary of any right created by this Appendix or by operation of law.

ARTICLE 10 – ATTORNEY'S FEES

In any action brought by a party to enforce the terms of this Appendix, the prevailing party shall be entitled to reasonable attorney's fees and costs, including the reasonable value of any services provided by in-house counsel. The reasonable value of services provided by in-house counsel shall be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.

ARTICLE 11 – INDEMNITY

Contractor shall indemnify, defend and hold University (and its officers, directors, agents and employees) harmless from all lawsuits, claims, liabilities, damages, settlements, or judgments, including University's costs and attorney fees, which arise as a result of Contractor's negligent acts or omissions or willful misconduct.

ARTICLE 12 – SURVIVAL

The terms and conditions set forth in this Appendix shall survive termination of the Agreement between the parties. If Contractor is unable to return or destroy the University's Protected Information in accordance with Article 6, then this Appendix, in its entirety, shall survive the Agreement until such time as Contractor does return or destroy the Protected Information.