



Services Order Form

6330 South 5000 East, Suite 700, Salt Lake City, UT 84121

Customer Contact Information

Customer	<u>UCLA EXTENSION</u>	Contact	<u>Vartan Adamian</u>
Address	<u>10925 Le Conte Ave</u>	Phone	<u>310.825.6437</u>
City	<u>Los Angeles</u>	email	<u>vadamian@uextor.ucla.edu</u>
State/Province	<u>CA</u>		
Zip/postal code	<u>90024</u>		

Description	Term	Metric	Quantity	Price	Total
Canvas Cloud Subscription	1/1/14 - 6/30/14	FTE	1,900	\$28.00	\$21,000
Canvas Cloud Subscription	7/1/14 - 6/30/15	FTE	1,900	\$28.00	\$42,000
Canvas Cloud Subscription	7/1/15 - 6/30/16	FTE	1,900	\$28.94	\$43,260
Canvas Cloud Subscription	7/1/16 - 6/30/17	FTE	3,900	\$25.46	\$89,110
Canvas Cloud Subscription	7/1/17 - 6/30/18	FTE	5,000	\$20.76	\$103,800
Canvas Cloud Subscription	7/1/18 - 6/30/19	FTE	5,000	\$21.38	\$106,900
Support Package					
Premium Support	1/1/14 - 6/30/14	20% of subscription (Min 250)	N/A	\$4,200	\$4,200
Premium Support	7/1/14 - 6/30/15	20% of subscription (Min 250)	N/A	\$8,400	\$8,400
Premium Support	7/1/15 - 6/30/16	20% of subscription (Min 250)	N/A	\$8,652	\$8,652
Premium Support	7/1/16 - 6/30/17	20% of subscription (Min 250)	N/A	\$17,822	\$17,822
Premium Support	7/1/17 - 6/30/18	20% of subscription (Min 250)	N/A	\$20,760	\$20,760
Premium Support	7/1/18 - 6/30/19	20% of subscription (Min 250)	N/A	\$21,380	\$21,380
Tier 1 Package					
Tier 1 Support	1/1/14 - 6/30/14	Per User (Min 1,500)	1,900	\$3.50	\$4,625
Tier 1 Support	7/1/14 - 6/30/15	Per User (Min 1,500)	1,900	\$3.50	\$43,250
Tier 1 Support	7/1/15 - 6/30/16	Per User (Min 1,500)	1,900	\$3.50	\$5,250
Tier 1 Support	7/1/16 - 6/30/17	Per User (Min 1,500)	3,900	\$3.50	\$12,250
Tier 1 Support	7/1/17 - 6/30/18	Per User (Min 1,500)	5,000	\$3.50	\$17,500
Tier 1 Support	7/1/18 - 6/30/19	Per User (Min 1,500)	5,000	\$3.50	\$17,500
Other Non-Recurring					
Guided Implementation	N/A	N/A	One Time	1	\$8,000
Tier 1 Setup	N/A	N/A	One Time	1	\$1,000
Total					\$499,689

Guided Implementation Package includes:

- Production account setup.
- Authentication integration assistance (for supported identity providers only, (i.e., LDAP, CAS or SAML 2.0).
- Starter training to be delivered online. Administrator Training, Support Training, User Training.
- Instructure will assist with Site Branding (school color header w/ logo).
- Basic SIS endpoint (We enable the Instructure bulk enrollment API which accepts updates provided in the Canvas SIS Import Format).
- Production Support Configuration for support ticketing system.
- Test Instance (Test instance that refreshes every three weeks) upon request.

FTE Definition
FTE means the number of full-time equivalent students calculated in accordance with the definition published by the Integrated Postsecondary Education Data System.

Customer must annually notify Instructure of its most recent reported FTE count within 30 days of the filing. If the reported FTE count for such year is different than the number of estimated FTEs in the Fee table above, then the reported FTE count will be used to calculate the Fees for the renewal Subscription Term directly following the filing date of the most recent reported FTE count.

Payment Terms: Customer agrees to pay to Instructure the applicable fees set forth on this order form.

For the initial term, Customer must pay such amount to Instructure on the date of this order.
For each subsequent term, Instructure will invoice Customer 30 days prior to the beginning of such term and customer must pay such invoice within 30 days of receipt.

Duration: This order begins on the initial date listed above under Term, and continues until the last date listed above, unless sooner terminated under the Agreement.

Terms: This order is governed by the terms of Master Subscription Services Agreement between the parties (Agreement), which terms are incorporated into this order for all purposes. If there is a conflict between the terms of this order and the Agreement, this order governs. This order and the Agreement are the entire agreement between the parties, and they supersede and replace all prior and contemporaneous negotiations, agreements, representations and discussions regarding this subject matter. Only a signed writing of the parties may amend this order. Any terms used in this order but not defined, will use the definitions in the Agreement.

The pricing includes 1 gigabyte of storage per FTE for UCLA Extension only.

*** Pro-rated First Term

Customer: UCLA EXTENSION

Signature: [Signature]
Name: Davis & Smith
Title: Buyer
Date: 01/10/2014

Instructure, Inc.

Signature: [Signature]
Name: Matthew Stark
Title: Sr. SA Analyst
Date: 1/10/14



Master Subscription Services Agreement

This agreement is between Instructure, Inc., a Delaware corporation (**Instructure**), and the entity or individual agreeing to these terms (**Customer**). It is effective as of the date of the last signature.

LEARNING MANAGEMENT SYSTEM SOFTWARE SERVICE. With a signed order, Instructure will provide its learning management system software as a service through a URL within a hosted server environment under the terms below (**Service**). This agreement contemplates one or more orders for the Service, which are governed by the terms of this agreement. **User** means a student, teacher, or administrator of Customer's educational institution, who is authorized by Customer to use the Service with an assigned login credential.

(1) USE OF SERVICE.

- a). **Customer Owned Content.** All information, data, results, plans, sketches, texts, files, links, images, photos, videos, audio files, notes, or other materials uploaded under Customer's account in the Service remains the sole property of Customer, as between Instructure and Customer (**Customer Content**). Customer grants Instructure the right to use the Customer Content solely for purposes of performing under this agreement. During the term of this agreement and for 3 months after expiration or termination, Customer may export the Customer Content through the API or by using the export feature within the Service. Instructure has no obligation to maintain the Customer Content 3 months after expiration or termination.
- b). **API Access.** Instructure provides access to its application-programming interface (**API**) as part of the Service for no additional fee. Subject to the other terms of this agreement, Instructure grants Customer a non-exclusive, nontransferable, terminable license to operate the API only for purposes of interfacing Customer's technology applications or services with the Service as allowed by the API. The Instructure **API Policy** is located at <http://www.instructure.com/policies/api-policy>
 - i. Customer may not use the API in a manner, as reasonably determined by Instructure, that exceeds reasonable request volume, constitutes excessive or abusive usage, or fails to comply with the API Policy or with any part of the API. If any of these occur, Instructure can suspend or terminate Customer's access to the API on a temporary or permanent basis.
 - ii. Instructure may change or remove existing endpoints or fields in API results upon at least 30 days notice to Customer, but Instructure will use commercially reasonable efforts to support the previous version of the API for at least 6 months. Instructure may add new endpoints or fields in API results without prior notice to Customer.
 - iii. Instructure will maintain and provide access to an API, unless it terminates the API for all customers with notice, as it is not technically feasible or economically viable to continue granting access to the API.
 - iv. The API is provided on an 'AS IS' and 'WHEN AVAILABLE' basis. Instructure has no liability to Customer as a result of any change, temporary unavailability, suspension, or termination of access to the API.
- c). **Customer Responsibilities.** Customer (i) is solely responsible for Customer Content (defined below), and User activity in its account in the Service, (ii) must keep its passwords secure and confidential, and notify Instructure promptly of any known unauthorized access, and (iii) may use the Service only in accordance with applicable law.
- d). **Customer Restrictions.** Customer may not, and will use reasonable means to ensure that each User does not,
 - i. sell, resell, rent or lease the Service or API (defined above);
 - ii. use the Service, for non-Customer educational purposes, to store or transmit infringing, unsolicited marketing emails, libelous, obscene, deceptive, defamatory, pornographic, racist, sexual, hateful, or otherwise objectionable, unlawful or tortious material, or any other material in violation of a third-party right;
 - iii. use the Service to harm or impersonate any person, or for any commercial purpose;
 - iv. interfere with or disrupt the integrity or performance of the Service; or
 - v. attempt to gain unauthorized access to the Service or their related systems or networks.
- e). **Disclosure of User Information.** Instructure may access, preserve, and disclose User's registration and any other information if required to do so by law or based on Instructure's good faith belief that such access preservation or disclosure is necessary to: (i) enforce this agreement; (ii) respond to claims of a violation of the rights of third parties, whether or not the third party is a User, individual, or government agency; (iii) respond to customer service inquiries; or (iv) protect the rights, property, or personal safety of Instructure, other users or the public.
- f). **Customer Support.** Instructure must provide customer support for the Service under the terms of Instructure's Customer Support (**Support**), which are located at <http://www.instructure.com/policies/support-terms>, and are incorporated into this agreement for all purposes.

(2) PAYMENT TERMS.

Customer must pay all fees as specified on the order, but if not specified then within 30 days of receipt of an invoice. Customer is responsible for the payment of all sales, use and other similar taxes. All orders are non-cancelable and the fees are non-refundable (except as expressly provided below).

(3) WARRANTY/SERVICE LEVEL AGREEMENT AND REMEDY.

- a). **Compliance with Laws.** Each party represents and warrants to the other party that it will comply with all applicable provisions of the Family Educational Rights and Privacy Act, as amended (FERPA), and other laws with respect to its activities under this agreement. Instructure will implement reasonable and typical administrative, technical, and physical safeguards to secure its facilities and systems from unauthorized access, and to secure the Customer Confidential Information (defined below) and data. Instructure agrees: to not use or disclose education records created or received from, by, or on behalf of Customer or its students for any purpose other than the purpose than providing the Services to students, except that Instructure may create, use, and disclose de-identified and aggregated data based upon education records; and to not use or disclose such education records except as permitted by this agreement, as required by law, or as authorized by Customer in writing.
- b). **Service Availability Warranty.** Instructure warrants to Customer, (i) that commercially reasonable efforts will be made to maintain the online availability of the Service for a minimum availability in a trailing 365-day period as provided below (excluding scheduled outages, force majeure, and outages that result from any Customer or User technology issue), (ii) the functionality or features of the Service may change but will not materially decrease during a paid term, and (iii) that Support may change but will not materially degrade during any paid term.

Annual Availability Warranty: 99.9% availability percentage

- If Customer has been using the Service for less than 365 days, the preceding 365 days will be used but any days prior to Customer's use of the Service will be deemed to have had 100% availability.
- Any unavailability occurring prior to a successful credit claim cannot be used for any future claims.

A Customer is eligible for a service credit if the annual availability percentage drops below 99.9% for the preceding 365 days from the date of a service credit claim. The maximum amount of the credit is 1/12 of the annual subscription fee for a twelve (12) month period. This service credit is calculated by taking the number of hours that the Service was unavailable below the warranty, and multiplying it by 3% of 1/12 the annual subscription fee. Customer's exclusive remedy and Instructure's sole obligation for breach of the warranty in b(i) will be for Instructure to provide a credit as provided above; provided that Customer notifies Instructure in writing of such claim within the applicable month Customer becomes eligible or 30 days after.

- c). **Third Party Links/Service Disclaimer.** The Service may contain links to third party web sites (including without limitation, links provided by instructors) or access third-party services (including without limitation, turnitin.com and Google docs). Such sites and services are not under the control of Instructure, and Instructure is not responsible for the content or any link on such sites or for the temporary or permanent unavailability of such third party sites or services.
- d). **Warranty Disclaimer.** INSTRUMENT DISCLAIMS ALL OTHER WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE AND FITNESS FOR A PARTICULAR PURPOSE. THE SERVICE MAY BE INTERRUPTED OR CONTAIN AN ERROR. WHILE INSTRUMENT TAKES REASONABLE MEASURES TO SECURE THE SERVICE, INSTRUMENT DOES NOT GUARANTY THAT THE SERVICE CANNOT BE COMPROMISED.

(4) MUTUAL CONFIDENTIALITY.

- a). **Definition of Confidential Information.** Confidential Information means all confidential information disclosed by a party (Discloser) to the other party (Recipient), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure (Confidential Information).
- b). **Protection of Confidential Information.** The Recipient must use the same degree of care that it uses to protect the confidentiality of its own Confidential Information (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this agreement. The Recipient must make commercially reasonable efforts to limit access to Confidential Information of Discloser to those of its employees and contractors who need such access for purposes consistent with this agreement and who have signed confidentiality agreements with Recipient no less restrictive than the confidentiality terms of this agreement.
- c). **Exclusions.** Confidential Information *excludes* information that: (i) is or becomes generally known to the public without breach of any obligation owed to Discloser, (ii) was known to the Recipient prior to its disclosure by the Discloser without breach of any obligation owed to the Discloser, (iii) is received from a third party without breach of any obligation owed to Discloser, or (iv) was independently developed by the Recipient without use or access to the Confidential Information. The Recipient may disclose Confidential Information to the extent required by law or court order, but will provide Discloser with advance notice to seek a protective order.

(5) PROPRIETARY RIGHTS.

- a). **Reservation of Rights by Instructure.** The software, workflow processes, user interface, designs, know-how, API information, third party technology and other technologies provided by Instructure as part of the Service are the proprietary property of Instructure and its licensors, and all right, title and interest in and to such items, including all associated intellectual property rights, remain only with Instructure. Instructure reserves all rights unless expressly granted in this agreement.
- b). **Customer Restrictions.** Customer *may not*:
 - i. reverse engineer the Service or the API;
 - ii. remove or modify any proprietary marking or restrictive legends in the Service; or
 - iii. access the Service to build a competitive service or product, or copy any feature, function or graphic for competitive purposes.
- c). **Feedback.** Instructure may contact each User (no more than once each year) for the *sole purpose* of seeking aggregate anonymous feedback regarding performance of the Service and suggestions for improvements. Customer, and each User (to the extent Customer has such right), hereby grants Instructure an irrevocable, royalty-free perpetual license to all feedback and suggestions regarding the Service.

(6) EXCLUSION OF DAMAGES AND LIMITATION OF LIABILITY.

- a). **EXCLUSION OF CERTAIN DAMAGES.** INSTRUMENT IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, COSTS OF DELAY, LOSS OF DATA, RECORDS OR INFORMATION, AND ANY FAILURE OF DELIVERY OF THE SERVICE).
- b). **LIMITATION OF LIABILITY.** EXCEPT FOR INSTRUMENT'S INDEMNITY OBLIGATIONS, INSTRUMENT'S LIABILITY FOR DIRECT DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT, TORT OR OTHERWISE) DOES NOT EXCEED THE AMOUNT PAID BY CUSTOMER WITHIN THE PRECEDING 12 MONTHS UNDER THIS AGREEMENT.

(7) TERM, TERMINATION, AND SUSPENSION OF SERVICE.

- a). **Term.** This agreement continues for the duration specified on the order (**Term**).
- b). **Termination for Lack of Funding.** Performance by Customer under this agreement may be dependent upon the appropriation and allotment of funds by the California State Legislature (the "Legislature") or through Federal Grant. If either body fails to appropriate or allot the necessary funds, or Customer fails to allocate the necessary funds, then Customer will issue written notice to Instructure and Customer may terminate this agreement without further duty or obligation hereunder. The Parties acknowledge that appropriation, allotment, and allocation of funds are beyond the control of Customer.
- c). **Mutual Termination for Material Breach.** If either party is in material breach of this agreement (including without limitation non-payment of any amounts owed Instructure), the other party may terminate this agreement at the end of a written 30-day notice/cure period, if the breach has not been cured.
- d). **Return or Destroy Upon Termination.** Upon termination or expiration of this agreement for any reason, Customer must pay Instructure all amounts owed, and destroy or return all property of Instructure. Customer will confirm this destruction or return requirement in writing upon request of Instructure.
- e). **Suspension of Service and Removal of Customer Content for Violations of Law or Policy.** Instructure may immediately suspend the Service and remove applicable Customer Content if it in good faith believes that, as part of using the Service, Customer may have violated a law or a restriction in this agreement. Instructure may try to contact Customer in advance, but it is not required to do so.

(8) GOVERNING LAW AND FORUM.

This agreement is governed by the laws of the State of California, without regard to conflict of law principles. Any dispute arising out of or related to this agreement may only be brought in the state and federal courts for CA. Both parties consent to the personal jurisdiction of such courts and waive any claim that it is an inconvenient forum. Nothing in this agreement prevents either party from seeking injunctive relief in a court of competent jurisdiction. The prevailing party in any litigation is entitled to recover its attorneys' fees and costs from the other party.

(9) INDEMNITY.

- a). **By Instructure for Infringement.** If a third-party claims that the Service (other than related to any Customer Content) infringes that party's patent, copyright or other proprietary right, Instructure will defend Customer against that claim at Instructure's expense and pay all costs, damages, and attorney's fees, that a court finally awards or that are included in a settlement approved by Instructure, provided that Customer:
 - i. promptly notifies Instructure in writing of the claim; and
 - ii. allows Instructure to control, and cooperates with Instructure in, the defense and any related settlement.

If such a claim is made, Instructure could continue to enable Customer to use the Service or to modify it. If Instructure determines that these alternatives are not reasonably available, Instructure may terminate the Service without any liability to Customer upon notice to Customer and with the return of any prepaid and unused fees. This indemnity does not apply to the extent of any technology not provided by Instructure, if the Service is used other than in accordance with this agreement, or with third party technology it is not designed to operate with.

- b). **By Customer.** If a third-party claims against Instructure that any part of the Customer Content infringes or violates a patent, copyright or other right, Customer will defend Instructure against that claim at Customer's expense and pay all costs, damages, and attorney's fees, that a court finally awards or that are included in a settlement approved by Customer, provided that Instructure:
 - i. promptly notifies Customer in writing of the claim; and
 - ii. allows Customer to control, and cooperates with Customer in, the defense and any related settlement.

The above indemnification By Customer shall only be in proportion to and to the extent of such claims and violations that are a result of customer's negligence or willful misconduct.

(10) MISCELLANEOUS OTHER TERMS.

- a). **Money Damages Insufficient.** Any breach by a party of this agreement or violation of the other party's intellectual property rights could cause irreparable injury or harm to the other party. The other party may seek a court order to stop any breach or avoid any future breach.
- b). **Entire Agreement and Changes.** This agreement and the order constitute the entire agreement between the parties, and supersede all prior or contemporaneous negotiations, agreements and representations, whether oral or written, related to this subject matter. No modification or waiver of any term of this agreement is effective unless both parties sign it.
- c). **Publicity.** Neither party shall use the other party's name, logo or any aspect of that party's brand without the express written consent of the other party.
- d). **No Assignment.** Neither party may assign or transfer this agreement or an order to a third party, except that this agreement with all orders may be assigned as part of a merger, or sale of all or substantially all of the business or assets, of a party.
- e). **Independent Contractors.** The parties are independent contractors with respect to each other.
- f). **Enforceability.** If any term of this agreement is invalid or unenforceable, the other terms remain in effect.
- g). **No Additional Terms.** Instructure rejects additional or conflicting terms of any Customer form-purchasing document.
- h). **Order of Precedence.** If there is an inconsistency between this agreement and an order, this agreement prevails.
- i). **Survival of Terms.** Any terms that by their nature survive termination or expiration of this agreement, will survive.
- j). **Notices.** For purposes of service messages and notices about the Service, Instructure may place a banner notice or send an email to an email address associated with an account.
- k). **CISG.** The Convention on Contracts for the International Sale of Goods does not apply.
- l). **Force Majeure.** Neither party is liable for force majeure events.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA,

on behalf of UCLA Extension (Customer)

[Signature]
Signature

FRANK G. SARRIS
Name

SUPERVISOR - FORMER
Title

01/10/2015
Date

Instructure, Inc.

[Signature]
Signature

Matthew Searle
Name

Sr. Bt. Analyst
Title

1/10/14
Date

6330 South 3000 East, Suite 700

Address

Salt Lake City, UT 84121

AMENDMENT No. 01
Master Subscription Services Agreement

Canvas Software:

The Following Terms and Conditions are amended as follows:

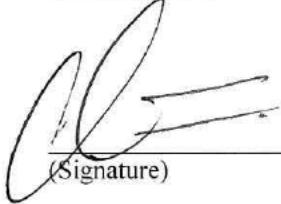
(10) MISCELLANEOUS OTHER TERMS

b). **Entire Agreement and Changes.** This Agreement and the **UC Appendix – Data Security and Privacy** and the order constitute the entire agreement between the parties, and supersede all prior or contemporaneous negotiations, agreement and representations, whether oral or written, related to this subject matter. No modification or waiver of any term of this agreement is effective unless both parties sign it.

All other terms and conditions of the Agreement remain unchanged and in full effect.

APPROVALS

Instructure, Inc.

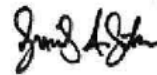


(Signature)

3/28/16
(Date)

Chris Tannen Assistant Counsel
(Print Name) (Title) Counsel

THE REGENTS OF THE
UNIVERSITY OF CALIFORNIA



(Signature)

Digitally signed by David
Smith
DN: dc=edu, dc=ucla,
dc=finance, ou=Finance,
cn=David Smith
Date: 2016.03.24 13:15:45
-07'00'

03/24/2016

(Date)

David A. Smith
Buyer – Purchasing Services
UCLA Campus Purchasing

UC APPENDIX – DATA SECURITY AND PRIVACY

ARTICLE 1 – PURPOSE AND SCOPE OF APPLICATION

- A. This Data Security and Privacy Appendix is designed to protect the University of California’s (UC) Protected Information and UC networks (defined below). This Appendix describes the data security and privacy obligations of all third parties (including individuals and entities) that connect to UC networks and/or gain access to Protected Information (Supplier).
- B. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this Appendix on any third party retained by Supplier to provide services for or on behalf of the UC.

ARTICLE 2 – PROTECTED INFORMATION

- A. Supplier acknowledges that its performance of Services under this Agreement may involve access to confidential UC information that identifies or is capable of identifying a specific individual, including, but not limited to, personally-identifiable information, student records, (collectively, “Protected Information”) that is subject to applicable 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 federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); the European Union Data Protection Directive and other state, federal and international laws.

ARTICLE 3 – ACCESS TO UC NETWORKS

“UC networks” means the set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information that is implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. Examples of networks include local area networks (LAN), wide area networks (WAN), Storage area networks (SAN), Enterprise private networks (EPN), Virtual private networks (VPN), Wireless local area networks (WLAN), or Campus area networks (CAN). UC networks include resources that are purchased, leased and/or otherwise obtained for use by UC, and may include personally owned devices. In any circumstance when Supplier has access to UC networks, it is the sole responsibility of Supplier to ensure that its access to the networks does not result in any access by unauthorized individuals to UC networks or Protected Information. This includes access to all types of UC network logins or credentials, as well as access to information contained on or transmitted through those networks. It is Supplier’s sole responsibility to protect the login and credential information, including through proper use, handling and destruction of such information. Consistent the requirements in Attachment 1, any technology and/or systems that gains access to UC networks must comply with the Computer System Security Requirements.

ARTICLE 4 – COMPLIANCE WITH APPLICABLE LAWS, FAIR INFORMATION PRACTICE PRINCIPLES AND UC POLICIES

Supplier agrees to comply with all applicable state, federal and international laws, as well as best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Protected Information. Additionally Supplier will comply as applicable with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission. Such principles would typically require Supplier to have a privacy policy, and, if collecting Protected Information electronically from individuals on behalf of UC, a prominently-posted privacy statement or notice in conformance with such principles (UC's sample Privacy Statement for websites is available at <http://www.ucop.edu/information-technology-services/policies/it-policies-and-guidelines/records-mgmt-and-privacy/files/sampleprivacystatement.doc>). Supplier also agrees, to the extent applicable, to comply with UC's Business and Finance Bulletin IS-2, *Inventory, Classification, and Release of UC Electronic Information* (<http://policy.ucop.edu/doc/7020447/BFB-IS-2>), and IS-3, *Electronic Information Security* (<https://www.google.com/url?q=http://policy.ucop.edu/doc/7000543&sa=U&ei=AegxU4KqNtCgogTZv4G4BQ&ved=0CAoQFjAC&client=internal-uds-cse&usq=AFQjCNFU3yBg9YoTU7TmBTGoJ2fDs2HHIA>).

ARTICLE 5 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Supplier agrees to hold UC's Protected Information, and any information derived from such information, in strictest confidence. Supplier will not access, use or disclose Protected Information other than to carry out the purposes for which UC disclosed the Protected Information to Supplier, except as permitted or required by applicable law, or as otherwise authorized in writing by UC. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Supplier will notify UC in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give UC 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 UC.

ARTICLE 6 – SAFEGUARD STANDARD

Supplier 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. Supplier will implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Protected Information. Supplier will ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Supplier has responsibility for the Protected Information under the terms of this Appendix. Prior to agreeing to the terms of this Appendix, and periodically thereafter (no more frequently than annually) at UC's request, Supplier will provide assurance, in the form of a third-party audit report or other documentation acceptable to UC (the Shared Assessments® tools <http://www.sharedassessments.org/>, or similar, are acceptable), demonstrating that appropriate information security safeguards and controls are in place.

ARTICLE 7 – SAFEGUARD STANDARD FOR PAYMENT CARD DATA

N/A

ARTICLE 8 - Information Security Plan

- A. Supplier acknowledges that UC is required to comply with information security standards for the protection of Protected Information as required by law, regulation and regulatory guidance, as well as UC's internal security program for information and systems protection.

- B. Supplier will establish, maintain and comply with an information security plan (“**Information Security Plan**”), which will contain, at a minimum, such elements as those set forth in Attachment 1 to this Appendix.
- C. Supplier’s Information Security Plan will be designed to:
 - i. Ensure the security, integrity and confidentiality of Protected Information;
 - ii. Protect against any anticipated threats or hazards to the security or integrity of such information;
 - iii. Protect against unauthorized access to or use of such information that could result in harm or inconvenience to the person that is the subject of such information;
 - iv. Reduce risks associated with Supplier having access to UC networks; and
 - v. Comply with all applicable legal and regulatory requirements for data protection.
- D. On at least an annual basis, Supplier will review its Information Security Plan, update and revise it as needed, and submit it to UC upon request. At UC’s request, Supplier will make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to UC’s security requirements as they exist from time to time.

ARTICLE 9 – RETURN OR DESTRUCTION OF PROTECTED INFORMATION

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

If Supplier is unable to return or destroy UC’s Protected Information because it is technically impossible or impractical to do so, Supplier will continue to protect such data in accordance with the terms of this Appendix. Supplier further agrees to provide verification, upon request by UC, that returning or destroying Protected Information is technically impossible or impractical.

ARTICLE 10 – BREACHES OF PROTECTED INFORMATION

- A. **Definition.** For purposes of this Appendix, a “Breach” means any information security event that violates UC Information Security policies and procedures, Supplier’s Information Security Plan, policies and procedures, and/or impacts or has the potential to impact the confidentiality, integrity, or availability of UC’s or Supplier’s information systems or Protected Information.
- B. **Reporting of Breach:** Supplier will report any confirmed or suspected Breach to UC immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after Supplier reasonably believes a Breach has or may have occurred. Supplier’s report will 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, disclosed and/or received Protected Information (if known), (iv) what Supplier has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Supplier has taken or will take to prevent future unauthorized access, use or disclosure. Supplier will provide such other information, including a written report, as reasonably requested by UC. In the event of a suspected Breach, Supplier will keep UC 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, Supplier will:
 - i. Immediately preserve any potential forensic evidence relating to the Breach, and remedy the Breach as quickly as circumstances permit
 - ii. Promptly (within 2 business days) designate a contact person to whom UC will direct inquiries, and who will communicate Supplier responses to UC inquiries;
 - iii. As rapidly as circumstances permit, apply appropriate resources to remedy the Breach condition, investigate, document, restore UC service(s) as directed by UC, and undertake appropriate response activities;
 - iv. Provide status reports to UC on Breach response activities, either on a daily basis or a frequency approved by UC;
 - v. Coordinate all media, law enforcement, or other Breach notifications with UC in advance of such notification(s), unless expressly prohibited by law;

- vi. Make all reasonable efforts to assist and cooperate with UC in its Breach response efforts; and
- vii. Ensure that knowledgeable Supplier staff is available on short notice, if needed, to participate in UC-initiated meetings and/or conference calls regarding the Breach.

D. **Grounds for Termination.** Any Breach may be grounds for immediate termination of the Agreement by UC.

E. **Assistance in Litigation or Administrative Proceedings.** Supplier will make itself and any employees, subcontractors, or agents assisting Supplier in the performance of its obligations available to UC at no cost to UC to testify as witnesses, or otherwise, in the event of a Breach or other unauthorized disclosure of Protected Information caused by Supplier that results in litigation or administrative proceedings against UC, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy or arising out of this Appendix.

ARTICLE 11 – EXAMINATION OF RECORDS

UC and, if an 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) will have access to and the right to examine any pertinent books, documents, papers, and records of Supplier involving transactions and work related to this Appendix until the expiration of five years after final payment hereunder. Supplier will retain project records for a period of five years from the date of final payment.

ARTICLE 12 – NO THIRD-PARTY RIGHTS

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

ARTICLE 13 – ATTORNEY'S FEES

In any action brought by a party to enforce the terms of this Appendix, the prevailing party will 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 will be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.

ARTICLE 14 – INDEMNITY

The Agreement includes an Indemnity provision, but for the avoidance of doubt regarding a Breach involving Protected Information, Supplier's indemnification obligations under the Agreement will include any and all costs associated with notification to individuals or remedial measures offered to individuals, whether or not required by law, including but not limited to costs of notification of individuals, establishment and operation of call center(s), credit monitoring and/or identity restoration services, time of UC personnel responding to Breach, civil or criminal penalties levied against UC, attorney's fees, and court costs, which arise as a result of Supplier's breach of this Appendix, negligent acts or omissions, or willful misconduct.

ARTICLE 15 – CYBER INSURANCE

In addition to the insurance required under the Agreement, Supplier at its sole cost and expense will obtain, keep in force, and maintain a cyber-insurance policy to insure its reasonable costs in investigating and responding to a cyber-incident or Breach with the following minimum limits: \$1,000,000 Each Occurrence and \$3,000,000 Aggregate.

ATTACHMENT 1 TO APPENDIX – DATA SECURITY AND PRIVACY

- A. Supplier will develop, implement, and maintain a comprehensive Information Security Plan that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards. The safeguards contained in such program must be consistent with the safeguards for protection of Protected Information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.
- B. Without limiting the generality of the foregoing, every comprehensive Information Security Plan will include, but not be limited to:
- i. Designating one or more employees to maintain the comprehensive Information Security Plan;
 - ii. Identifying and assessing internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Protected Information and of UC networks, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
 - a. Ongoing employee (including temporary and contract employee) training;
 - b. Employee compliance with policies and procedures; and
 - c. Means for detecting and preventing security system failures.
 - iii. Developing security policies for employees relating to the storage, access and transportation of records containing Protected Information outside of business premises.
 - iv. Imposing disciplinary measures for violations of the comprehensive Information Security Plan rules.
 - v. Preventing terminated employees from accessing records containing Protected Information and/or UC networks.
 - vi. Overseeing service providers, by:
 - a. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such Protected Information and UC networks consistent with all applicable laws and regulations; and
 - b. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for Protected Information.
 - vii. Placing reasonable restrictions upon physical access to records containing Protected Information and UC networks and requiring storage of such records and data in locked facilities, storage areas or containers.
 - viii. Restrict physical access to any network or data centers that may have access to Protected Information or UC networks.
 - ix. Requiring regular monitoring to ensure that the comprehensive Information Security Plan is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Protected Information and UC networks; and upgrading information safeguards as necessary to limit risks.
 - x. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Protected Information and of UC networks.
 - xi. Documenting responsive actions taken in connection with any incident involving a Breach, and mandating post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Protected Information and UC networks.

Computer System Security Requirements

To the extent that Supplier electronically stores or transmits Protected Information or has access to any UC networks, it will include in its written, comprehensive Information Security Plan the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, will have the following elements:

- A. Secure user authentication protocols including:
 - i. Control of user IDs and other identifiers;
 - ii. A secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - iii. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - iv. Restricting access to active users and active user accounts only; and
 - v. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
 - vi. Periodic review of user access, access rights and audit of user accounts.
- B. Secure access control measures that:
 - i. Restrict access to records and files containing Protected Information and systems that may have access to UC networks to those who need such information to perform their job duties; and
 - ii. Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, which are reasonably designed to maintain the integrity of the security of the access controls.
- C. Encryption of all transmitted records and files containing Protected Information.
- D. Adequate security of all networks that connect to UC networks or access Protected Information, including wireless networks.
- E. Reasonable monitoring of systems, for unauthorized use of or access to Protected Information and UC networks.
- F. Encryption of all Protected Information stored laptops or other portable storage devices.
- G. For files containing Protected Information on a system that is connected to the Internet or that may have access to UC networks, reasonably up-to-date firewall, router and switch protection and operating system security patches, reasonably designed to maintain the integrity of the Protected Information.
- H. Education and training of employees on the proper use of the computer security system and the importance of Protected Information and network security.

With reasonable notice to Supplier, UC may require additional security measures which may be identified in additional guidance, contracts, communications or requirements.