## ARTICLE 1. PURPOSE AND INTRODUCTION

A. In the course of providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to the University of California's (UC) Institutional Information and/or IT Resources (both defined below). In such an event, UC and Supplier desire to appropriately protect Institutional Information and IT Resources. The purpose of this Appendix-Data Security is to specify Supplier's cybersecurity and risk management responsibilities when Supplier has access to Institutional Information and/or IT Resources.

B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents.

C. Supplier must provide commercially acceptable cybersecurity and cyber risk management to protect Institutional Information and/or IT Resources. This must include, but is not limited to the Supplier:

1. Developing and documenting a plan that protects Institutional Information and IT Resources.
    - Supplier must responsibly execute this plan.
    - Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose.[1]
    - Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third-party review if approved by the responsible UC Information Security Officer.
2. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the Institutional Information and/or IT Resources. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect Institutional Information and/or IT Resources.
3. Updating its plan to effectively address new cybersecurity risks.
4. Complying with pertinent contractual and regulatory responsibilities.
5. Providing UC with evidence of compliance with Supplier's information security plan.
6. Keeping UC informed with timely updates on risks, vulnerabilities, Security Incidents, and Breaches.
7. Keeping UC informed of any measures UC must perform to ensure the security of Institutional Information and IT Resources.

[1] Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, IS0 27000 series, NIST SP 800-53 and NIST SP 800-171.

D. If, in the course of providing the Goods and/or Services under the Agreement, Supplier engages in transactions with UC affiliated individuals (including but not limited to: students, staff, faculty, customers, patients, guests, volunteers, visitors, research subjects, etc.), as a benefit and result of the Agreement, Supplier must treat any data about UC affiliated individuals that Supplier creates, receives, and/or collects in the course of those transactions with the same level of privacy and security protections and standards as required of Institutional Information by this Appendix.

E. 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 same terms and conditions contained in this Appendix on any sub-supplier retained by Supplier to provide or assist in providing the Goods and/or Services to UC.

F. To the extent that a requirement of this Appendix conflicts with those of any other UC Agreement or Incorporated Document, the most stringent requirement (including but not limited to: least risk to UC, shortest time, best practice, etc.) will apply.

## ARTICLE 2. DEFINED TERMS

A. **"Breach"** means: (1) Any disclosure of Institutional Information to an unauthorized party or in an unlawful manner; (2) Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of Institutional Information and/or IT Resources; or (3) The acquisition, access, use, or disclosure of protected health information (PHI) or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law.

B. **"Illicit Code"** means: (1) Any code UC would not reasonably expect to be present or operating; (2) Hidden software or functionality with adverse or undesired actions or consequences; (3) Code that replicates or transmits Institutional Information or activates operating systems or other similar services without the express knowledge and approval of UC; (4) Code that alters, damages, or erases any Institutional Information or software without the express knowledge and approval of UC; or (5) Code or apparatus that functions in any way as a: key lock, node lock, time-out, "back door," "trap door," "booby trap," "dead drop device," "data scrambling device," or other function, regardless of how it is implemented, which is intended to alter or restrict the use of or access to any Institutional Information and/or IT Resources.

C. **"Institutional Information"** means: Any information or data created, received, and/or collected by UC or on its behalf, including but not limited to: application logs, metadata, and data derived from such data.

D. **"IT Resource"** means: IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed or UC-owned, or a personally owned device that stores Institutional Information, is connected to UC systems, is connected to UC networks, or is used for UC business. IT Resources include, but are not limited to: personal and mobile computing systems and devices,

mobile phones, printers, network devices, industrial control systems (including but not limited to: SCADA, PLCs, DPC, Operational Technology, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, or Internet of Things (IoT).

E. **"Major Change"** means: The implementation of a change that could have an effect on the security of an IT Resource or Institutional Information. The scope includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. These include changes related to:

1. Technology upgrades or migrations.
2. Responses to Security Incidents.
3. Modifications of scope (data elements, features, location of Institutional Information, etc.).
4. Regulatory guidance.
5. Law and legal regulations.
6. Responses to risk assessments.
7. Addressing vulnerabilities.
8. Material updates or shifts in technologies used by Supplier.

F. **"Security Incident"** means: (1) A material compromise of the confidentiality, integrity, or availability of Institutional Information; (2) A single event or a series of unwanted or unexpected events that has a significant probability of compromising UC business operations or threatening Institutional Information and/or IT Resources; (3) Any event involving a cyber intrusion; or (4) A material failure of Supplier's administrative, technical, or physical controls that resulted or could have resulted in an adverse impact to the confidentiality, integrity, or availability of Institutional Information or IT Resources.

## ARTICLE 3. ACCESS TO INSTITUTIONAL INFORMATION AND IT RESOURCES

A. Supplier must limit its access to, use of, and disclosure of Institutional Information and IT Resources to the least invasive degree necessary required to provide the Goods and/or Services.

1. Supplier may not access or use Institutional Information and IT Resources for any purpose except to provide the Goods and/or Services.
2. For the avoidance of doubt, Supplier may not access, use, or disclose Institutional Information and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by UC.

B. In the event that Goods and/or Services include the review of a specific Security Incident or a threat to or anomaly in Institutional Information or IT Resources, Supplier must limit inspection to the least invasive degree necessary required to perform the investigation.

## ARTICLE 4. SUPPLIER'S INFORMATION SECURITY PLAN AND RESPONSIBILITIES

A. Supplier acknowledges that UC must comply with information security standards as required by law, regulation, and regulatory guidance, as well as by UC's internal security program that protects Institutional Information and IT Resources.

B. Supplier must establish, maintain, comply with, and responsibly execute its information security plan.

C. Supplier's initial information security plan is attached as Exhibit 2 and incorporated by reference.

D. Updates to Exhibit 2 will occur as follows:

1. On an annual basis, Supplier will review its information security plan, update it as needed, and submit it upon written request by UC.

2. In the event of a Major Change, Supplier will review its information security plan, update it as needed, and submit it to UC as detailed herein.

E. If Supplier makes any material modifications to its information security plan that will affect the security of Institutional Information and IT Resources, Supplier must notify UC within seventy-two (72) calendar hours and identify the changes.

F. Supplier's Information Security Plan must:

1. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of Institutional Information and IT Resources through the use and maintenance of appropriate administrative, technical, and physical controls;

2. Protect against any reasonably anticipated threats or hazards to Institutional Information and IT Resources;

3. Address the risks associated with Supplier having access to Institutional Information and IT Resources;

4. Address applicable regulations and/or external obligations listed in Exhibit 1;

5. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy;

6. Clearly document the cybersecurity responsibilities of each party;

7. Follow UC records retention requirements outlined in the Statement of Work (SOW) or in UC's Terms and Conditions;

8. Prevent the sharing of passwords or authentication secrets that provide access to Institutional Information and/or IT Resources;

9. Prevent the use of passphrases (passwords) or other authentication secrets that are common across customers or multiple unrelated UC sites or units;

10. Prevent unauthorized access to Institutional Information and IT Resources;

11. Prevent unauthorized changes to IT Resources;

12. Prevent the reduction, removal, or turning off of any security control without express written approval from UC;

13. Prevent the creation of new Supplier accounts to access Institutional Information and IT Resources without express written approval from UC;

14. Prevent the storing, harvesting, or passing through of UC credentials (username, password, authentication secret, or other factor); and

15. Prevent the use or copying of Institutional Information for any purpose not authorized under the Agreement or any associated Statement of Work (SOW).

## ARTICLE 5. REQUESTS FROM UC AND EVIDENCE OF COMPLIANCE

A. Supplier must provide UC with evidence that demonstrates to UC's reasonable satisfaction Supplier's adherence to its information security plan (including but not limited to: third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent) upon execution of the Agreement, upon reasonable request (including but not limited to: annually, after Major Changes, and/or as a result of a Security Incident), or as required by any applicable regulatory or governmental authority.

B. Supplier must respond to UC's reasonable questions related to cybersecurity controls, Security Incidents, or Major Changes, newly published vulnerabilities, and/or risk assessments within ten (10) business days.

C. UC may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually or as a result of a Breach.

## ARTICLE 6. NOTIFICATION OF MAJOR CHANGES AND VULNERABILITY DISCLOSURES

A. Within twenty (20) business days, Supplier must notify UC regarding changes in Supplier's security posture or IT infrastructure. Such notices must occur:

1. When Major Changes happen.
2. When Supplier becomes aware of a vulnerability that warrants a CVE[2] rating of "High" or "Critical," based on the latest CVE version, for which a patch is not yet available or for which Supplier will delay application of an available patch.

B. Supplier must use commercially acceptable efforts to remediate, within twenty (20) business days, any vulnerability rated as CVE High or Critical.

C. In response to Major Changes, Supplier must update its information security plan no later than fifteen (15) days into the next calendar quarter and must provide updated evidence of compliance with the information security plan.

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures maintained by The MITRE Corporation. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. The CVE list can be found at: cve.mitre.org

## ARTICLE 7. RETURN AND DISPOSAL OF INSTITUTIONAL INFORMATION

A. Within thirty (30) calendar days of the termination, cancellation, expiration, or other conclusion of the Agreement, Supplier must return all Institutional Information to UC and then dispose of the Institutional Information in possession of Supplier as detailed herein. This provision also applies to all Institutional Information that is in the possession of sub-suppliers or agents of Supplier.

B. Such disposal will be accomplished using the methods described in UC's Institutional Information Disposal Standard (https://security.ucop.edu/policies/institutional-information-disposal.html) or an alternative approved by UC.

C. Supplier will certify in writing to UC that such return and/or disposal has been completed.

D. If Supplier believes that return and/or disposal of Institutional Information is technically impossible or impractical, Supplier must provide UC with a written statement explaining the reason for this conclusion. If UC determines that return and/or disposal is technically impossible or impractical, Supplier will continue to protect the Institutional Information in accordance with the terms of this Appendix for as long as the Institutional Information is in Supplier's possession.

## ARTICLE 8. NOTIFICATION OF CORRESPONDENCE CONCERNING INSTITUTIONAL INFORMATION

A. Supplier agrees to notify UC promptly, both orally and in writing, but in no event more than seventy-two (72) calendar hours after Supplier receives correspondence or a complaint that relates to a regulation, contractual obligation, Breach, or material risk concerning Institutional Information. For purposes of this Article 8.A, a correspondence or complaint may include, but is not limited to, any communication that originates from law enforcement, regulatory or governmental agencies, government investigators, corporations, or an individual, but excludes normal customer service correspondence or inquiries.

## ARTICLE 9. COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS

A. **Reporting of Breach or Security Incident**: If Supplier reasonably suspects or confirms a Breach and/or a Security Incident impacting Institutional Information and/or IT Resources, Supplier must promptly notify UC both orally and in writing using the contacts in the Agreement. Supplier must provide such notifications no later than (1) seventy-two (72) calendar hours after the initial suspicion of a Security Incident and/or Breach and (2) seventy-two (72) calendar hours after the initial confirmation of a Security Incident and/or Breach, if Supplier is able to make such a confirmation. Supplier's notification must identify:

1. Contacts for both technical and management coordination;

2. Escalation and identifying information, such as ticket numbers, system identifiers, etc.;
3. The nature of the Breach and/or Security Incident;
4. The Institutional Information and/or IT Resources affected;
5. What Supplier has done or will do to mitigate any deleterious effect; and
6. What corrective action Supplier has taken or will take to prevent future Security Incidents.

B. Supplier will provide other information as reasonably requested by UC.

C. In the event of a suspected Breach and/or Security Incident, Supplier will keep UC informed regularly of the progress of its investigation until the incident is resolved.

D. Coordination of Breach Response or Security Incident Activities: Supplier will fully cooperate with UC's investigation of any Breach and/or Security Incident involving Supplier and/or Goods and/or Services. Supplier's full cooperation will include, but not be limited to, Supplier:

1. Promptly preserving any potential forensic evidence relating to the Breach and/or Security Incident;
2. Remedying the Breach and/or Security Incident as quickly as circumstances permit;
3. Promptly, but no more than seventy-two (72) calendar hours after the discovery of Breach and/or Security Incident, designating a contact person to whom UC will direct inquiries and who will communicate Supplier responses to UC inquiries;
4. As rapidly as circumstances permit, assigning/using appropriate resources to remedy, investigate, and document the Breach and/or Security Incident, to restore UC service(s) as directed by UC, and undertake appropriate response activities;
5. Providing status reports to UC regarding Breach and Security Incident response activities, either on a daily basis or a frequency approved by UC;
6. Coordinating all media, law enforcement, or other Breach and/or Security Incident notifications with UC in advance of such notification(s), unless expressly prohibited by law;
7. Ensuring that knowledgeable Supplier employees are available on short notice, if needed, to participate in UC and Supplier initiated meetings and/or conference calls regarding the Breach and/or Security Incident; and
8. Ensuring that knowledgeable Supplier employees and agents participate in after-action analysis, including root cause analysis and preventive action planning.

E. Breaches and Security Incidents – Corrective and Preventive Action: As a result of a Breach and/or Security Incident impacting Institutional Information and/or IT Resources, and upon UC's request, Supplier must prepare a report detailing corrective and preventive actions. The report must include:

1. A mutually agreed upon timeline for the corrective and preventive actions based on the nature of the Breach and/or Security Incident;
2. Identification and description of the root causes; and
3. Precise steps Supplier will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.

F. **Costs**: Supplier must reimburse UC for reasonable costs related to responding to Breaches impacting Institutional Information and IT Resources caused by Supplier. This includes all costs associated with notice and/or remediation of the Breach.

G. **Grounds for Termination:** Any Breach may be grounds for termination of the Agreement by UC. Agreement obligations to secure, dispose, and report continue through the resolution of the Breach and/or Security Incident.

## ARTICLE 10. ILLICIT CODE WARRANTY[3]

A. Supplier represents and warrants that the Goods and/or Services do not contain Illicit Code.

B. To the extent that any Goods and/or Services have Illicit Code written into them, Supplier will be in breach of this Agreement, and no cure period will apply.

C. Should Supplier learn of the presence of Illicit Code, Supplier will promptly provide UC with written notice explaining the scope and associated risk.

D. Supplier represents and warrants that it will take commercially reasonable steps to promptly remove Illicit Code.

## ARTICLE 11. BACKGROUND CHECKS

A. Before Supplier's employee, sub-supplier, or agent may access Institutional Information and/or IT Resources classified at Protection Level 3 or Protection Level 4[4], Supplier must conduct a thorough and pertinent background check. Supplier must evaluate the results prior to granting access in order to assure that there is no indication that the employee, sub-supplier, or agent presents a risk to Institutional Information and IT Resources.

B. Supplier must retain each employee's, sub-supplier's, or agent's background check documentation for a period of three (3) years following the termination of the Agreement.

[3] This provision does not relate to malware or viruses that attack the running IT Resource. These are covered under ARTICLE 9 - COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS.
[4] See Exhibit 1.

# Exhibit 1 – Institutional Information

This exhibit describes the Institutional Information for the benefit of both parties.

## 1. Protection Level Classification[5]:

| Protection Levels Needed | Anticipated Record Count |
|---|---|
| ☐ Protection Level 1 | |
| ☐ Protection Level 2 | |
| ☐ Protection Level 3 | ☐ Less than 70,000<br>☐ More than 70,000 |
| ☐ Protection Level 4 | ☐ Less than 70,000<br>☐ More than 70,000 |

| **Explanation**: | [Optional, add detail if needed, may be covered in SOW] |
|---|---|

The Protection Level and anticipated record count determines the applicable cyber security insurance requirement in the Terms and Conditions.

## 2. Institutional Information data element descriptors:

Select all data types that apply:

A. ☐ Animal Research Data.
B. ☐ Controlled Technical Information (CTI).
C. ☐ Controlled Unclassified Information (CUI) – 800-171/NARA.
D. ☐ Defense Department: Covered Defense Information (CDI).
E. ☐ Federal Acquisition Regulations (FARS/DFAR) other than CUI.
F. ☐ European Privacy Law (EEA and UK GDPR) personal data.
G. ☐ European Privacy Law (EEA and UK GDPR) special data.
H. ☐ Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
I. ☐ Health Records subject to HIPAA Privacy or Security Rule (PHI).
J. ☐ Human Subject Research Data.
    1. ☐ Identified.
    2. ☐ Anonymized.
K. ☐ Intellectual property (IP), such as patents, copyright, or trade secrets.
L. ☐ ITAR/EAR-controlled data.

[5] For more information about classification see: https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html.

M. ☐ Payment card data (PCI, PCI DSS).
N. ☐ Personally identifiable information – PII.
O. ☐ Student data, whether or not subject to FERPA.
P. ☐ Other: _____
Q. ☐ Other: _____

## 3. Regulation or Contracts Relating to the Institutional Information:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

**Privacy (* indicates data security requirements are also present)**

A. ☐ California Confidentiality of Medical Information Act (CMIA) *****.
B. ☐ California Consumer Privacy Act (CCPA).
C. ☐ California Information Practices Act (IPA).
D. ☐ European Privacy Laws Regulation (EEA and UK GDPR)*****.
E. ☐ Family Educational Rights and Privacy Act (FERPA) *****.
F. ☐ Federal Policy for the Protection of Human Subjects ("Common Rule").
G. ☐ Genetic Information Nondiscrimination Act (GINA).
H. ☐ Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) *****.
I. ☐ Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) *****.
J. ☐ Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
K. ☐ The Fair and Accurate Credit Transaction Act (FACTA).
L. ☐ The Fair Credit Reporting Act (FCRA).

Data Security

M. ☐ Chemical Facility Anti-Terrorism Standards (CFATS).
N. ☐ Defense Federal Acquisition Regulations (DFARS).
O. ☐ Export Administration Regulations (EAR).
P. ☐ Federal Acquisition Regulations (FARS).
Q. ☐ Federal Information Security Modernization Act (FISMA).
R. ☐ International Traffic in Arms Regulations (ITAR).
S. ☐ Payment card data (PCI, PCI DSS).
T. ☐ Toxic Substances Control Act (TSCA).
U. ☐ Other: _____
V. ☐ Other: _____

# Exhibit 2
# Supplier's Initial Information Security Plan

[Supplier to provide and update per the Appendix DS requirements.]