Appendix A – Checklist for Information Security in Agreements: Transfer of University Data to Third-Party Systems

Use this checklist when reviewing agreements to ensure all sections and subsections are covered.
Checklist key: ☑ = complete | ☐ = incomplete

- ☐ 1. Definitions
  - 1.1 Authorized Users
  - 1.2 Confidential Information
  - 1.3 University Data
  - 1.4 Data Compromise
  - 1.5 Information Security Incident

- ☐ 2. Concepts
  - 2.1 University Data Protection
    - 2.1.1 Access Control
    - 2.1.2 Patch Management
    - 2.1.3 Scanning and Penetration Testing
    - 2.1.4 Encryption
    - 2.1.5 Security Development
    - 2.1.6 Deterioration and Degradation

- ☐ 3. Notification
  - 3.1 Notification of Data Compromise
  - 3.2 Incident Reporting
  - 3.3 Third-Party Requests

- ☐ 4. Workforce Security and Location
  - 4.1 Offshore
  - 4.2 Background Checks

- ☐ 5. Audit
  - 5.1 Security Reviews
  - 5.2 Reports
  - 5.3 Additional Audits at University Request

- ☐ 6. Destruction and Return of University Data

Appendix B – Sample Addendum for Information Security in Agreements or RFPs: Transfer of University Data to Third-Party Systems

☐ 1. Definitions

- 1.1 Authorized Users

  "Authorized User" means and is limited to (1) Authorized Employees; and (2) Vendor's subcontractors, agents, and auditors who have a need-to-know or otherwise access data to enable the Vendor to comply with the Agreement, and who are bound in writing by confidentiality obligations sufficient to protect University Data in accordance with the terms hereof.

- 1.2 Confidential Information

  "Confidential Information" means any non-public information that is confidential or proprietary to a party and is disclosed or becomes known pursuant to this agreement. Except to the extent information is required to be kept private or confidential pursuant to other law, regulation, or policy, "Confidential Information" does not include information that is or becomes generally available or known to the public through no act of omission of the receiving party; was received lawfully from a third-party through no breach of any obligations of confidentiality owed to the disclosing party; or created by a party independently of its access to or use of other party's information.

- 1.3 University Data

  *"University Data" means any and all data, information, text, graphics, **images,** works and other materials that are collected, loaded, stored, accessible, transferred through and/or accessed by the University in the course of using the Vendor's services, including, but not limited to: (1) updates, modifications and/or deletions; (2) all of the results from the use of services; and (3) all information and materials that are developed or acquired prior to, or independently of, the Agreement. University Data is Confidential Information.*

- 1.4 Data Compromise

  "Data Compromise" means any actual or reasonably suspected unauthorized access to, or acquisition of, data that compromises the security, confidentiality or integrity of the data or the ability of the University to access the data.

- 1.5 Information Security Incident

  "Information Security Incident" means any actual or reasonably suspected incident, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of University Data; interference with information technology operations; or significant violation of the University's information security policy or the information security provisions of this Agreement.

☐ 2. Concepts

- 2.1 University Data Protection

  All facilities used by or on behalf of the Vendor to store and process University Data will implement and maintain administrative, physical, technical, and procedural safeguards in accordance with industry best practices at a level sufficient to secure such data from unauthorized access, destruction, use, modification or disclosure. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event, less than reasonable in view of the type and nature of the data involved. The Vendor must maintain the administrative, physical, technical and procedural infrastructure associated with the provision of services to the University in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than those specified by the parties to this Agreement.

  - 2.1.1 Access Control

    The Vendor will control access to the University's Data, limiting access to Authorized Users who have a legitimate need-to-know based on individual work assignment for the Vendor. The Vendor will trace approved access to ensure proper usage and accountability, and the Vendor will make such information available to the University for review, upon the University's request and not later than five (5) business days after the request is made in writing.

  - 2.1.2 Patch Management

    Vendor will carry out updates and patch management for all systems and devices in a timely manner, applying security patches within five (5) business days or less based on reported criticality. Updates and patch management must be deployed using an auditable process that can be reviewed by the University upon the University's request and not later than five (5) business days after the request is made in writing. An initial report of patch status must be provided to the University prior to the effective date of this Agreement.

  - 2.1.3 Scanning and Penetration Testing

    Prior to the Effective Date of this Agreement, and at regular intervals of no less than annually and whenever a change is made which may impact the confidentiality, integrity, or availability of University Data, and in accordance with

industry standards and best practices, Vendor will, at its expense, perform scans for unauthorized applications, services, code and system vulnerabilities on the networks and systems used to perform services related to this Agreement. An initial report must be provided to the University prior to the Effective Date of this Agreement. Vendor will provide the University the reports or other documentation resulting from the audits, certifications, scans and tests within five (5) business days of Vendor's generation or receipt of such results. The Vendor will, if such results so require, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement and provide the University with written evidence of remediation. The following audits, certifications, scans, and tests are required:

- *A vulnerability scan performed by a qualified and credible third-party of the Vendor's systems and facilities that are used in any way to deliver services under this Agreement;*
- *A formal penetration test performed by qualified personnel of the Vendor's systems and facilities in use in any way to deliver services under this Agreement; and*
- *The University may require the Vendor to perform additional audits and tests, the results of which will be provided to University within seven (7) business days of Vendor's receipt of such results.*

○ 2.1.4 Encryption

All systems and devices that store, process and/or transmit Confidential Information must use an industry standard encryption protocol for data in transit and at rest.

○ 2.1.5 Security Development

Vendor will use secure development and coding standards; including secure change management procedures in accordance with industry standards. The Vendor's web applications must meet OWASP Application Security Verification Standards (ASVS). The Vendor will perform penetration testing and/or scanning prior to releasing new software versions. Vendor will provide internal standards and procedures to the University for review upon the University's request.

○ 2.1.6 Deterioration and Degradation

Vendor will protect University Data against deterioration or degradation of quality and authenticity, including, but not limited to, annual data integrity audits performed by an independent, external organization.

☐ 3. Notification

Any notices or communications required or permitted to be given to the University under this Agreement must be (1) given in writing and (2) transmitted by electronic mail transmission (including PDF), to the University Information Security Office at security@arizona.edu. Any such notice or communication must be deemed to have been given on the day such notice or communication is sent electronically, provided that the sender has received a read receipt or other replied acknowledgement of such electronic transmission.

- ### 3.1 Notification of Data Compromise

  Unauthorized access or disclosure of nonpublic data is considered to be a breach. The Vendor will provide notification as soon as it is aware of the Data Compromise or breach to the University Information Security Office at security@arizona.edu. When the Vendor is liable for the loss, the Vendor must bear all costs associated with the investigation, response and recovery from the breach, including, but not limited to, credit monitoring services with a term of at least three (3) years; mailing costs; website; and toll-free telephone call center services. Any limitation on liability in this Agreement or elsewhere is void to the extent that it relieves a Vendor from its own negligence or to the extent that it creates an obligation on the University to hold the Vendor harmless.

- ### 3.2 Incident Reporting

  Vendor will report all other Information Security Incidents to the University within 24 hours of discovery.

- ### 3.3 Third-Party Requests

  The Vendor will notify the University immediately if the Vendor receives any third-party request for University Data, including but not limited to a subpoena, a court order, a public records request, a request directly from a data subject, or other type of inquiry or demand; or the location or method of transmission of University Data is changed. All notifications to the University required in this Information Security paragraph will be sent to the University Information Security Office at security@arizona.edu, in addition to any other notice addresses in this Agreement. In all such instances, to the extent legally feasible, the Vendor will not provide any University Data to such third-party and will instead direct the requestor to the University.

☐ 4. Workforce Security and Location

The Vendor will comply with workforce location and security clauses as outlined in this Agreement. Additionally, the Vendor will ensure their workforce is properly trained on information security and privacy practices of the University and on any information security or privacy regulations, as required by applicable rules. The Vendor must promote and maintain an awareness of the importance of securing the University Data to its employees and agents.

- ### 4.1 Offshore

  The University may select or restrict where University Data will be stored and where University Data can be processed, and the Vendor will store and/or process it there in accordance with the service terms. If a data location selection is not covered by the service terms (or a Data Location Selection is not made by the University with respect to any University Data), the Vendor will not be restricted in the selection of University storage or processing facilities. Any services that are described in this Agreement that directly serve the University and may involve access to sensitive University Data or development or modification of software

for the University will be performed within the borders of the United States. Unless stated otherwise in this Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Agreement. This provision applies to work performed by subcontractors at all tiers and to all University Data.

- 4.2 Background Checks

  The Vendor must conduct background checks and not utilize any individual to fulfill the obligations of this Agreement, including subcontractors, if such individual has been convicted of any crime involving dishonesty or false statement including, but not limited to fraud and theft, or otherwise convicted of any offense for which incarceration for a minimum of one (1) year is an authorized penalty. Any such individual may not be an "Authorized User" under this Agreement.

☐ 5. Audit

The Vendor will, at its expense, conduct or have conducted such audits and certifications as defined under this section at least annually, and immediately after any actual or reasonably suspected breach. The Vendor will provide the University the results of any such audits as defined under this section, along with the Vendor's plan for addressing or resolving any shortcomings identified by such audits, within seven (7) business days of the Vendor's receipt of such results.

- 5.1 Security Reviews

  The Vendor will complete one of the following audits at least annually and immediately after any actual or reasonably suspected Data Compromise: SOC 2 Type I or II, SOC for Cybersecurity, or an accepted Higher Education Cloud Vendor Assessment Tool (https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool). Evidence must be provided to the University prior to the Effective Date of this Agreement and at least annually thereafter.

- 5.2 Reports

  The University reserves the right to annual, at a minimum, review of: Vendor access reports related to access to University Data; Vendor patch management process, schedules, and logs; findings of vulnerability scans and/or penetration tests of Vendor systems; and Vendor development standards and processes.

- 5.3 Additional Audits at University Request

  The University may require the Vendor to perform additional audits and tests, the results of which will be provided to the University within five (5) business days of the Vendor's receipt of such results.

☐ 6. Destruction and Return of University Data

Except as permitted in other areas of the Agreement, the Vendor will promptly return the University's Confidential Information upon termination of this Agreement, the final performances of services under this Agreement, or upon the request of the University, whichever comes first. In the event the Vendor has non-unique copies of the University's Confidential Information that are also held by or returned to the University, the Vendor may, in lieu of returning such non-unique copies, destroy such Confidential Information in all forms and types of media and provide written confirmation or certification of such destruction.