Procurement Services

Data Access Questionnaire Instructions
Following Completion of DAQ Form

Send the questionnaire to end user department if the procurement is for:

(A) Any type of services; or
(B) IT, medical or scientific products; or
(C) Software.

1. Will the vendor receive, store, transmit, or have access to Institutional Data?
   If Yes, then:
   (A) Confirm that the appropriate Data Steward has approved the access.

2. Will the vendor receive, store, transmit or have access to any data that is individually identifiable health information?
   If Yes, then:
   (B) Refer the matter to ITS Security (security@unc.edu) so they can determine whether the vendor’s IT security practices are sufficient; and
   (C) Make sure the vendor signs the University’s BAA (not a vendor-supplied BAA). Send the vendor the appropriate BAA template in PDF format. (NOTE: Purchases involving the School of Medicine use a different BAA template than purchases involving the rest of the University.); and
   (D) Submit the completed BAA to the Institutional Privacy Office for recordkeeping purposes using the submission tool at privacy.unc.edu.
   (E) If the vendor is unable/unwilling to agree to the provisions of the BAA, refer the matter to the Institutional Privacy Office (privacy@unc.edu; ph: 962-6332).

3. Will the vendor receive, store, transmit, or have access to any data that is Personally Identifiable Information (PII)?
   If Yes, then:
(A) Refer the matter to ITS Security (security@unc.edu) so they can determine whether the vendor’s IT security practices are sufficient; and

(B) Revise the contract so it includes the provisions found in Exhibit A (Provisions for protection of Personally Identifiable Information and for contracts involving e-commerce services, including PCI compliance).

(C) If vendor is unable/unwilling to agree to the provisions of Exhibit A, refer the matter to the Office of University Counsel (Elizabeth Josephs ejosephs@email.unc.edu ph: 962-4349 or Will Tricomi will_tricomi@unc.edu ph: 919-843-5329).

4. Will the vendor receive, store, transmit, or have access to any data that is student information?

   If Yes, then:

   (A) Refer the matter to ITS Security (security@unc.edu) so they can determine whether the vendor’s IT security practices are sufficient; and

   (B) Revise the contract so it includes the provisions found in Exhibit B (Provisions for protection of student data). Skip this step if you already revised the contract to include Exhibit A.

   (C) If Vendor is unable/unwilling to agree to the provisions of Exhibit B, refer the matter to the Office of University Counsel (Elizabeth Josephs ejosephs@email.unc.edu ph: 962-4349 or Will Tricomi will_tricomi@unc.edu ph: 919-843-5329).

5. Will the vendor (i) receive, store, transmit, or have access to any bank account or payment card information; (ii) perform Automated Clearing House (ACH) or wire transfer transactions or electronic payments; (iii) collect credit/debit card numbers; (iv) process credit/debit card transactions; (v) remit funds to the University; or (vi) require use of TouchNet or any other University related payment portal?

   If Yes, then:

   (A) Refer the matter to ITS Security (security@unc.edu) so they can determine whether the vendor’s IT security practices are sufficient; and

   (B) Confirm with CERTFI (certifi@unc.edu) that CERTFI has issued a vendor approval letter; and

   (C) If you have not already done so, revise the contract so it includes the provisions found in Exhibit A.

6. Will the vendor be providing software-as-a-service (SaaS) or otherwise serving as an application service provider (ASP)? If so, will the vendor be working with, storing, or have access to sensitive University information? (Note: examples of SaaS include cloud hosting, off-site storage, etc.)

   If Yes, then:
(A) Refer the matter to ITS Security (security@unc.edu) so they can determine whether the vendor’s IT security practices are sufficient; and

(B) Revise the contract so it includes the provisions found in Exhibit C (Provisions for protections of University data hosted in vendor’s cloud environment (software-as-a-service contracts)).

(C) If vendor is unable/unwilling to agree to the provisions of Exhibit C, refer the matter to the Office of University Counsel (Elizabeth Josephs ejosephs@email.unc.edu ph: 962-4349 or Will Tricomi will_tricomi@unc.edu ph: 919-843-5329).

7. Will the service or product require integration or involve data sharing to or from existing campus information systems or finance systems? Note that integration includes, but is not limited to, use of Active Directory service, the campus single sign-on (SSO) service, or trusted/shared/federated sign-on services.

If Yes, then:

(A) Submit the matter to ITS Business Systems Analyst Jeanne Mesiano (Jeanne_Mesiano@unc.edu; ph: 919-962-3161).

8. Will the service or product require assistance from ITS, either for initial setup or ongoing maintenance?

If Yes, then:

(A) Submit the matter to ITS Business Systems Analyst Jeanne Mesiano (Jeanne_Mesiano@unc.edu; ph: 919-962-3161).

9. Will the service or product replace or duplicate any existing campus information systems or finance systems?

If Yes, then:

(A) Submit the matter to ITS Business Systems Analyst Jeanne Mesiano (Jeanne_Mesiano@unc.edu; ph: 919-962-3161).
Exhibit A

[Provisions for protection of Personally Identifiable Information and for contracts involving e-commerce services, including PCI compliance]

1. GRANT OF ACCESS TO AND USE OF UNIVERSITY’S DATA.
   (a) Grant of Limited Right to Use University Data. Subject to the terms and conditions of this agreement, University grants to Vendor a non-exclusive, non-transferable, limited right to use University data received or accessed by Vendor in the course of performing the services under this agreement. All right, title and interest in the data shall remain with the University or end users, as applicable. Vendor may not access and/or duplicate the data for any reasons other than those stated herein without the prior written consent of University.
   (b) Limitations on Use of University Data. Vendor shall not collect, mine, save, disclose, or otherwise use any end user personal information or University data for any purpose other than to provision and support the services expressly contemplated under this agreement.

2. INFORMATION SECURITY CERTIFICATIONS. At all times during the term of this agreement, Vendor will (a) use information security best practices for transmitting and storing University data or end user data; (b) employ information security best practices with respect to network security techniques, including firewalls, intrusion detection, and authentication protocols; (c) comply with all applicable laws and regulations regarding privacy and data security to maintain database security on any online financial transactions conducted on University’s behalf through the use of Vendor’s Software or records belonging to University that contain sensitive and confidential information; (d) maintain SSAE 16 attestations, SHA-16 certificates, and ISO/IEC 27001:2005 certification with respect to its information security practices; and (e) in the event Vendor is providing merchant services, comply with the Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Application Data Security Standard (PA-DSS).

3. CONFIDENTIALITY; CARE OF INFORMATION.
   (a) Confidentiality. Any information, data, documents, studies and reports given to or prepared or assembled by the Vendor under this agreement shall be kept as confidential and not divulged or made available to any individual or organization without the prior written approval of the University.
   (b) Response to Third-party Requests for University Data. If Vendor is served with a subpoena related to University data, then, unless prohibited by law, Vendor will provide prior notice of such subpoena to the University to allow the University an opportunity to seek injunctive relief before disclosure of the information.
   (c) Protection of University’s Sensitive and Confidential Information. Vendor shall safeguard and protect Sensitive and Confidential Information of the University in accordance with all applicable laws and regulations and consistent with information security best practices. “Sensitive and Confidential Information” means any of the following: “Personal Information” under the North Carolina Identity Theft Protection Act of 2005, confidential “personnel information” under the North Carolina Human Resources Act, “Protected Health Information” under the Health Insurance Portability and Accountability Act (HIPAA), student “education records” under Family Educational Rights and Privacy Act (FERPA), “customer record information” under Gramm Leach Bliley Act (GLBA), “card holder data” under the Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Application Data Security Standard (PA-DSS), and any information protected from disclosure under the North Carolina Public Records Act. Sensitive and Confidential Information must be restricted by Vendor to those with a legitimate business need for access to such information. For purposes of illustration, Sensitive and Confidential Information may appear in research data, student data, financial donor information, system access passwords, information security records, and information file encryption keys. If Vendor becomes aware of a confirmed or suspected exposure of Sensitive and Confidential Information of the University,
Vendor shall notify as promptly as possible the University’s Information Security Office (tel: 919-445-9397) and the University’s Office of University Counsel (tel: 919-962-1219).

(d) **FERPA Acknowledgement.** If Vendor will be hosting or accessing student education records, Vendor acknowledges and agrees that (i) the University has outsourced to Vendor the performance of institutional services or functions for which the University would otherwise use its own employees, (ii) Vendor is considered to be a “school official” with “legitimate educational interests” in “personally identifiable information” from “education records” of University students, as those terms have been defined under FERPA (34 CFR 99), (iii) Vendor is under the direct control of the University with respect to Vendor’s use and maintenance of data in the education records, and (iv) Vendor will abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Vendor will use such data only for the purpose of fulfilling its duties under this agreement, and will not monitor or share such data with or disclose it to any third party except as required by law, or authorized in writing by the University.
EXHIBIT B
[Provisions for protection of student data]

FERPA ACKNOWLEDGEMENT. If Vendor will be hosting or accessing student education records, Vendor acknowledges and agrees that (i) the University has outsourced to Vendor the performance of institutional services or functions for which the University would otherwise use its own employees, (ii) Vendor is considered to be a “school official” with “legitimate educational interests” in “personally identifiable information” from “education records” of University students, as those terms have been defined under FERPA (34 CFR 99), (iii) Vendor is under the direct control of the University with respect to Vendor’s use and maintenance of data in the education records, and (iv) Vendor will abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Vendor will use such data only for the purpose of fulfilling its duties under this agreement, and will not monitor or share such data with or disclose it to any third party except as required by law, or authorized in writing by the University.
Exhibit C

[Provisions for protections of University data hosted in vendor’s cloud environment (software-as-a-service contracts)]

1. INFORMATION SECURITY CERTIFICATIONS. At all times during the term of this agreement, Vendor shall (a) use information security best practices for transmitting and storing potentially sensitive information; (b) employ information security best practices with respect to network security techniques, including, but not limited to, firewalls, intrusion detection, and authentication protocols; (c) comply with all applicable laws and regulations regarding privacy and data security to maintain database security on any online financial transactions conducted on University’s behalf through the use of Vendor’s software or records belonging to University that contain sensitive and confidential information; (d) provide most current Statement on Standards for Attestation Engagements (SSAE) 16 attestation at least once every 2 years; (e) maintain ISO/IEC 27000 series information security best practices; and (f) in the event Vendor or is acting as a “service provider” as defined by the Payment Card Industry Data Security Standard (PCI-DSS), comply with the Payment Card Industry Data Security Standard (PCI-DSS) and provide appropriate PCI attestation documentation. The University reserves the right to conduct or request the Vendor to have an independent third party security audit performed.

2. LOCATION(S) OF HOSTING FACILITIES. Vendor certifies that for the duration of this agreement, all hosting facilities at which University data will be stored are located within the United States, unless otherwise agreed in a document signed by duly authorized officers of each of the Parties.

3. GRANT OF ACCESS TO AND USE OF UNIVERSITY’S DATA.

   (a) Grant of Limited Right to Use University Data. Subject to the terms and conditions of this agreement, University grants to Vendor a non-exclusive, non-transferable, limited right to use University data received or accessed by Vendor in the course of performing the services under this agreement. All right, title and interest in the data shall remain with the University or end users, as applicable. Vendor may not access and/or duplicate the data for any reasons other than those stated herein without the prior written consent of University.

   (b) Limitations on Use of University Data. Vendor shall not collect, mine, save, disclose, or otherwise use any end user personal information or University data for any purpose other than to provision and support the services expressly contemplated under this agreement.

4. SERVICE AVAILABILITY AND SUPPORT.

   (a) Vendor will ensure 99.9% availability of the hosted services to be provided under this agreement, excluding scheduled maintenance (“Availability Guarantee”). Vendor will reimburse the University for any reduction below this level of availability by granting the University a credit based on a sliding scale, as set forth in the table below, ranging from twenty percent (20%) to one-hundred percent (100%) of one-twelfth of the annual Service license fees for any single month in which the Availability Guarantee is not satisfied. Scheduled maintenance and events of force majeure shall not be counted in the calculation of any credit. All credits shall be calculated based on the total hours in a particular month. Any period of unavailability shall be counted from the time such unavailability commences until such time that access is restored.

<table>
<thead>
<tr>
<th>Service Access during Applicable Month (excluding Scheduled Maintenance and Events of Force Majeure)</th>
<th>Credit for such month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than or equal to 99.9%</td>
<td>0%</td>
</tr>
<tr>
<td>Less than 99.9% but greater than or equal to 98%</td>
<td>20%</td>
</tr>
<tr>
<td>Less than 98% but greater than or equal to 97%</td>
<td>29%</td>
</tr>
<tr>
<td>Less than 97% but greater than or equal to 96%</td>
<td>38%</td>
</tr>
<tr>
<td>Less than 96% but greater than or equal to 95%</td>
<td>47%</td>
</tr>
</tbody>
</table>
Less than 95% but greater than or equal to 94% | 56%
---|---
Less than 94% but greater than or equal to 93% | 65%
Less than 93% but greater than or equal to 92% | 74%
Less than 92% but greater than or equal to 91% | 83%
Less than 91% but greater than or equal to 90% | 92%
Less than 90% | 100%

(b) Vendor will provide to end users and University system administrators the same level of customer support that it then currently provides generally to its other end users and system administrators.

(c) In the event of a Major Incident, Vendor will promptly initiate and continue reasonable actions to limit the duration and scope of any Major Incident and will use commercially reasonable efforts to restore access to and functionality of the services as quickly as is reasonably possible after becoming aware of a Major Incident. “Major Incident” means a problem with a system, network, server, or critical application under Vendor’s control that prevents or unreasonably delays a majority of end users from using the services for more than fifteen (15) continuous minutes.

5. MANAGED BACK UP AND ARCHIVING. Vendor’s managed backup services must be designed to facilitate restoration of data to the server or device from which the data originated in the event the primary data is lost or corrupted. Vendor shall make available database duplications or “cloning” for restoration of lost or corrupted data at no cost to the University.

6. TRANSITION SERVICES; DESTRUCTION OF UNIVERSITY DATA.

(a) Transition Services. Upon the expiration or termination of the agreement for any reason, the University shall have the right, upon its request, to receive from Vendor for up to six (6) months all services reasonably necessary to effectuate an orderly transition to a successor vendor, including assistance in transferring University data to an industry-standard or other format requested by the University. Any fees charged by Vendor for such services should be at reasonable, fair market rates.

(b) Destruction of University Data. Upon the expiration or termination of the agreement, Vendor shall ask University in writing whether University wishes to exercise the transition services described in the subsection above, or whether University wishes for Vendor to destroy the University data in Vendor’s possession. If University responds that it wishes for Vendor to destroy the University data in Vendor’s possession. If University responds that it wishes for Vendor to destroy the University data in Vendor’s possession. If University notifies Vendor that it wishes for Vendor to destroy the University data, or if University does not respond to Vendor’s written inquiry within thirty (30) days of its receipt of the inquiry, or otherwise upon University’s written request, Vendor shall promptly destroy all University data it possesses in any form and provide University a written attestation to the destruction of the University data, specifying when it was destroyed and by what methods under NIST SP800-88 or other previously agreed upon destruction method.

7. CONFIDENTIALITY; CARE OF INFORMATION.

(a) Confidentiality. Any information, data, documents, studies and reports given to or prepared or assembled by the Vendor under this agreement shall be kept as confidential and not divulged or made available to any individual or organization without the prior written approval of the University.

(b) Response to Third-party Requests for University Data. If Vendor is served with a subpoena related to University data, then, unless prohibited by law, Vendor will provide prior notice of such subpoena to the University to allow the University an opportunity to seek injunctive relief before disclosure of the information.

(c) Protection of University's Sensitive and Confidential Information. Vendor shall safeguard and protect Sensitive and Confidential Information of the University in accordance with all applicable laws and regulations and consistent with ISO/IEC 27000 series information security best practices. “Sensitive and Confidential Information” means any, but not limited to, the following: “Personal Information” under the North Carolina Identity Theft Protection Act of 2005, confidential “personnel information” under the North Carolina Human Resources Act, “Protected Health Information” under the Health Insurance Portability and Accountability Act (HIPAA), student “education records” under Family Educational Rights and Privacy
Act (FERPA), “customer record information” under Gramm Leach Bliley Act (GLBA), “cardholder data” as defined by the Payment Card Industry Data Security Standard (PCI-DSS), and any information protected from disclosure under the North Carolina Public Records Act. Sensitive and Confidential Information must be restricted by Vendor to those with a legitimate business need for access to such information. For purposes of illustration, Sensitive and Confidential Information may appear in research data, public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

If Vendor becomes aware of a confirmed or suspected exposure of Sensitive and/or Confidential University Information, Vendor shall notify the UNC-Chapel Hill Help Desk (919-962-HELP) and ask that a “critical Remedy ticket” be created with the University’s Information Security Office. Vendor shall provide a telephone number at which the reporting party can be reached for more detail. The Help Desk takes calls 24x7x365. Vendor shall not provide any information regarding the risk to Sensitive Information or Confidential Information until contacted via telephone by a UNC-Chapel Hill incident handler. Upon being contacted by the incident handler, the Vendor agrees to provide UNC-Chapel Hill with access to any information that is pertinent to the investigation of the possible compromise of UNC-Chapel Hill’s sensitive information or mission critical system, including, but not limited to: log data, metadata and forensic images.

(d) FERPA Acknowledgement. If Vendor will be hosting or accessing student education records, Vendor acknowledges and agrees that (i) the University has outsourced to Vendor the performance of institutional services or functions for which the University would otherwise use its own employees, (ii) Vendor is considered to be a “school official” with “legitimate educational interests” in “personally identifiable information” from “education records” of University students, as those terms have been defined under FERPA (34 CFR 99), (iii) Vendor is under the direct control of the University with respect to Vendor’s use and maintenance of data in the education records, and (iv) Vendor will abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Vendor will use such data only for the purpose of fulfilling its duties under this agreement, and will not monitor or share such data with or disclose it to any third party except as required by law, or authorized in writing by the University.