SYRACUSE UNIVERSITY – Information Technology Services
Data Security Questionnaire for Access to SU Data by an External Party

Please submit completed form to **IT email address and arusso@syr.edu**

SU unit: **Purchasing** **Date:** _____

External party: _____

B. Information to be provided by the external party:

Please provide your information security plan, policy or security audit summary report. If any of the following items are addressed by your security plan, policy or audit report, please reference the appropriate section.

1. Provide your name and contact information.
2. Identify contact information for your Chief Privacy Officer, Information Security Officer or equivalent role.
3. To what structured security standard to you adhere, e.g. CIS Critical Security Controls, NIST 800-53 rev4, ISO 27002- 2013, or one of your own design? If the latter, provide a summary or list of your standards.
4. What positions in your organization have the ability to view SU data? Describe why they need access.
5. Employee Safeguards
    a. What safeguards are in place to ensure that your employees with access to confidential data are trustworthy (i.e. background investigations, bonding, etc.)?
    b. How are they trained regarding confidentiality and security of data?
    c. Does this training include FERPA training for access to student data?
    d. Do employees sign confidentiality agreements?
6. Describe your audit/assessment process in regards to information security.
7. Describe in detail your procedures for dealing with a data/system breach.
8. Have you had a breach in the past five years that has resulted in a compromise of customer data? If yes, what improvements have you put in place since then?
9. How will data be disposed of at the date to be specified by SU?
10. If relevant, how do end users authenticate?
11. If accessing payment card data, are you PCI DSS compliant?
12. Are your web based deliverables compliant with Web Content Accessibility Guidelines (WCAG) version 2.0 Level AA? Please provide your VPAT.

If you are responsible for hosting SU data:

13. If you outsource the hosting to a third party, indicate the provider name and address.
14. Data
    a. Identify where the data will reside, to include computer systems, back up media, offsite locations, paper printouts, etc.
    b. Is it possible to export data via automation with an API?
    c. Can data be imported from another cloud service? If so, identify the cloud service(s).
    d. If data will be self-reported by end users, provide links to your privacy policy and terms of use.
15. Backup/Disaster Recovery (DR)
    a. Identify the primary and secondary data site locations.
        1) What is the approximate distance between the primary site and secondary site for data center recovery purposes?

2) Are communications links with backup facility(ies) maintained and tested as part of the ongoing disaster recovery testing?

3) Will any data reside or be processed outside the US? If so, where?

b. For all of the systems/locations listed above, provide the backup and DR plans and include in detail how the data is safeguarded. Be sure to list both technical and physical protections, including protection against natural disasters.
   1) What are your recovery time objectives for SU data?

   2) What are your recovery point objectives for SU data?

c. If you have a DR plan:
   1) How does the DR service protect against a disaster?

   2) How often is the plan tested?

   3) Are communications links with backup facility(ies) maintained and tested as part of the ongoing disaster recovery testing?

   4) Does the backup facility(ies) use a different power grid and telecommunications grid from those at the primary site?

d. Have you had to respond to an incident which activated your DR plans?

e. If you are responsible for backup services:
   1) Where are the backups held once complete?

   2) How frequently is the data backed up?

   3) Detail the retention period for backup and any associated limits.

   4) How often is deleted data purged from backups?

   5) Is there a cost associated with data restoration?

   6) Are non-privileged users able to perform restoration of data using self-service?

   7) What is the service level agreement for restoration requests?

   8) Does restoration require downtime?

   9) Is the backup mechanism verified periodically?

   10) Are all backups encrypted?

f. If you are not responsible for backup service:
   1) If supported, what BaaS cloud solutions are available?

   2) Can data be backed up utilizing an on-premise solution such as Veeam?