THE UNIVERSITY OF TAMPA

INFORMATION TECHNOLOGY AND SECURITY

Supplemental Contract Language / Statements

Required by the University of Tampa Prior to Execution of Third-Party IT Solutions Contracts and Sales Agreements

Version 3 - November 2017

In order to ensure that institutional practices are followed when vendors engage in business with the University of Tampa, we require the following considerations be made prior to the execution of sales contracts. This is a university policy that must be adhered to by campus departments doing business with third party Information technology solutions vendors who provide software solutions accessible or made use of through internet web sites, portals, Software as a Service, et al.

Prior to Contracts Being Executed with third parties, the following information, if applicable, must be provided or added to vendor's contract language or provided to the ITS point of contact through email attachments/statements (vendor is to highlight each applicable area that is addressed in their contract):

ADA Accessibility

(Vendorxx) Will ensure accessibility of all web content and functionality produced or updated will be measured according to the accessibility standards of the World Wide Web Consortium's (W3C's) Web Content Accessibility Guidelines (WCAG) 2.0, Level AA and the Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.0 techniques for web content. Non-conforming web environments will be corrected in a timely manner.

Data Security and Best Practices

1. (Vendorxx) Will agree to fill out a security questionnaire and provide supplemental material as agreed upon that highlights data security methods and practices.
2. (Vendorxx) Will provide a statement in writing that data handled by their service or solution is encrypted in transmission and at rest on request, based on PII that will be stored on vendor's cloud service or storage facility, as well as written evidence of regulatory compliance if such claims are made by vendor (HIPAA, PCI, FERPA, et al).

3. (Vendorxx) agrees to provide a copy of recent certifications or audit results if applicable, that provide evidence of data security and regulatory compliance. We will agree to protect the confidentiality of said information.

Data Breach Notifications to Customer

4. (Vendorxx) agrees to notify the University when any (Vendorxx) system that may access, process, or store Institutional data is subject to unintended access. Unintended access includes compromise by malware (advanced persistent threats, SQL injection worms, et al), search engine web crawler, password compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures. (Vendor xx) further agrees to notify The University of Tampa Office of Information Security within twenty-four (24) hours of the discovery of the unintended access by providing notice via email to infosec@ut.edu.
5. [Vendorxx] agrees to notify the Institution within four hours if there is a threat to [Vendorxx]'s product as it pertains to the use, disclosure, and security of the Institution's data.
6. If an unauthorized use or disclosure of any Sensitive Data occurs, [Vendorxx] must provide: Written notice within one (1) business day after [Vendorxx]'s discovery of such use or disclosure and all information Institution requests concerning such unauthorized use or disclosure.
7. [Vendorxx], within one day of discovery, shall report to Institution any use or disclosure of sensitive data not authorized by this Addendum or in writing by Institution. [Vendorxx]'s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the [sensitive data] used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what [Vendorxx] has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action [Vendorxx] has taken or shall take to prevent future similar unauthorized use or disclosure. [Vendorxx] shall provide such other information, including a written report, as reasonably requested by Institution.
8. [Vendorxx] shall report, either orally or in writing, to Institution any use or disclosure of Covered Data not authorized by this Agreement or in writing by Institution, including any reasonable belief that an unauthorized individual has accessed Covered Data. [Vendorxx] shall make the report to Institution immediately upon discovery of the unauthorized disclosure, but in no event more than two (2) business days after [Vendorxx] reasonably believes there has been such unauthorized use or disclosure. [Vendorxx]'s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Institutional Covered Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what [Vendorxx] has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action [Vendorxx] has taken or shall take to prevent future similar unauthorized use or disclosure. [Vendorxx] shall provide such other information, including a written report, as reasonably requested by Institution.
9. [Vendorxx] agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of [Vendorxx]'s security obligations or other event requiring notification under applicable law ("Notification Event"), [Vendorxx] agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the Institution and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.
   End of Agreement Data Handling.

On Termination of Contract Agreement with Vendor

10. (Vendorxx) agrees that upon termination of this Agreement it shall erase, destroy, and render unrecoverable all client data and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the request of an agent of client, whichever shall come first. At a minimum, a "Clear" media sanitization is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization, SP800-88, Appendix A - see http://csrc.nist.gov/.

Tammy L. Clark

Tammy L. Clark, *CISSP, CISM, CISA, CRISC, PMP*

Chief Information Officer

Information Technology & Security