Secure Handling of UCF Data

Secure protection and handling of data by vendors and third parties

1. Network Security. Vendor agrees at all times to maintain network security that – at a minimum – includes: network firewall provisioning, intrusion detection, and regular third party penetration testing. Likewise Vendor agrees to maintain network security that conforms to one of the following:

    a. Those standards that UCF applies to its own network, as found at

        http://www.cst.ucf.edu/about/information-security-office/iso-policies-standards/

    b. Current standards set forth and maintained by the National Institute of Standards and Technology, including those at:

        http://web.nvd.nist.gov/view/ncp/repository

    c. Any generally recognized comparable standard (e.g., ISO/IEC 27001, etc.) that Vendor then applies to its own network.

2. Data Security. Vendor agrees to protect and maintain the security of UCF data based on the latest industry security standards and best practices. These security measures include, but are not limited to, maintaining secure segmented networks, maintaining systems that are up-to-date, and environments free of malware.

3. Data Transmission. Vendor agrees that any and all transmission or exchange of system application data with UCF and/or any other parties expressly designated by UCF – solely in accordance with Section 6 below – shall take place via secure means, e.g. HTTPS or FTPS with 128 bit key AES encryption or better.

4. Data Storage. Vendor agrees that any and all UCF data will be stored, processed, and maintained solely on designated target servers and that no UCF data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the Vendor's designated backup and recovery processes.

5. Data Encryption. Vendor agrees to store all UCF backup data as part of the its designated backup and recovery processes in encrypted form using 128 bit key AES encryption or better.

6. Data Re-Use. Vendor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Current Agreement. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of Vendor.

Vendor further agrees that no UCF data of any kind shall be transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by an agent of UCF.

7. End of Agreement Data Handling. Vendor agrees that upon termination of this Agreement or termination of the pertinent records retention period, whichever is later, it shall erase, destroy, and render unreadable all UCF data according to the standards enumerated in DOD 5220.22 or NIST 800-88 and certify in writing that these actions have been completed at a mutually predetermined date.

8. Data Breach. Vendor 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 Vendor's security obligations or other event requiring notification under applicable law ("Notification Event"), Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend UCF and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

9. FERPA. If Vendor is provided access to any student personally identifiable information (as defined under FERPA), Vendor acknowledges that it will comply with the privacy regulations outlined in the Family Educational Rights and Privacy Act ("FERPA"), for the handling of such information, to the extent such regulations apply to Vendor. Vendor will not disclose or use any student information except to the extent necessary to carry out its obligations under its agreement with UCF and as permitted by FERPA.

Related Documents:

- Third-Party Outsourcing (Cloud Computing) of University Data
- UCF Third Party Assurance Questionnaire
- 4-008 Data Classification and Protection

VENDOR Signature: