UTSA Institutional Compliance Office of Information Security

OIS 36 – Standard for Vendor Access

I. STANDARD STATEMENT

This standard applies to all persons or companies with whom UTSA enters into contracts to provide services involving IT resources and to those in the UTSA organization who sponsor a vendor or consultant.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. UTSA frequently relies on the services of outside vendors to support hardware and software management and operations for customers. In that role vendors might have the ability to view, copy or modify confidential data, raising concern about potential exposure or misuse of UTSA data.

B. Vendor Sponsorship
   1. A vendor account may be requested by a department or individual employee (sponsor) with justification and authorization by the department head.
   2. The sponsor must submit a request for vendor access to University Technology Solutions (UTS), specifying the reason for the request and noting confidential data that will be involved.
   3. UTS will contact the data owners for a determination of appropriate access, based on confidentiality.
   4. Access will be granted solely for the work contracted and for no other purposes. Access to additional resources requires written consent from the information owner as supported by the sponsor.

5. If physical access to the data center is required, the vendor must be accompanied at all times by the sponsor.
6. The sponsor is responsible for the handling the purchasing process, restrictions to be covered in contracts, non-disclosure agreements, and other provisions for protection of the data, as well and notification to the vendor of the university data security policies.
7. The sponsor must monitor closely the work/activities of the vendor report immediately any suspected violation of the agreement or data security policies.
8. Any vendor access to IT resources shall be granted for a defined and short duration. On completion the vendor must notify the sponsor of the completion of the task and access to the system(s) will be disabled.

C. Vendor Requirements
   1. The vendor shall be required to follow these steps in the event of unauthorized use or disclosure of confidential data:
      a. Provide written notice within one (1) day after the vendor's discovery of such use or disclosure; and all information that the university requests concerning such use or disclosure.
      b. Within thirty day after the termination or expiration of a Purchase Order, contract or other agreement, the vendor shall return or destroy, as applicable, all confidential data provided to the vendor by UTSA.

Title: OIS 36 – Standard for Vendor Access
Effective Date: August 1, 2011
Last Reviewed: August 13, 2020