

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.24 Vendor Access

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors may have the capability to remotely view, copy, and modify data and audit logs. They might remotely correct software and operating systems problems; monitor and fine tune system performance; monitor hardware performance and errors; modify environmental systems; and, reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of liability, embarrassment, and loss of revenue and/or loss of trust to the university.

2. APPLICABILITY

This university procedure applies to vendor-accessible university mission critical and confidential information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with vendor access. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources Security of Electronic Information Resources).

The procedures described herein apply to all departments, administrators, and vendors who are responsible for vendor supplied information resources.

These procedures apply to remote vendor access to systems, applications, or storage media containing university Sensitive Information over any medium to include, but not limited to, dial-up/modem, virtual private networking (VPN), virtual network computing technologies (e.g. RealVNC, GoToMyPC.com, PCAnywhere, etc), or communication applications (e.g. telnet, secure shell, etc). They also apply to direct vendor access to systems, applications, or storage media containing university Sensitive Information whether located on information resources owned and operated by the university or the vendor.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

- 4.1. The information resource owners must be informed of and, based on a risk assessment, may deny any vendor access to information resources containing Sensitive Information before vendor access is granted.
- 4.2. Personnel who provide vendor access to university resources containing Sensitive Information shall obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable system, university, and departmental rules and procedures pertaining, but not limited, to safety, privacy, information resource and physical security, auditing, software licensing, acceptable use, access/authorization, and nondisclosure as required by the university.
- 4.3. Vendors who are given access to Sensitive Information shall have written agreements and contracts that define:
 - (1) the university information to which the vendor should have access,
 - (2) how university information is to be protected by the vendor,
 - (3) acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract.
 - (4) that use of university information and information resources are only for the purpose of the business agreement; any other university information acquired by the vendor in the course of the contract cannot be used for the vendors' own purposes or divulged to others, and
 - (5) that vendors shall comply with terms of applicable non-disclosure agreements.
- 4.4. The providing entity shall assign an information resources point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with university policies.
- 4.5. Each vendor shall provide the providing entity with a list of all employees assigned to university contracts. The list shall be updated and provided to the providing entity within 24 hours of staff changes.
- 4.6. Appropriate access authorization for each on-site vendor employee (i.e., university affiliate) shall be specified by the resource owner according to the

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

criticality of the information resource. Where applicable, the university-issued identification may be required and all requirements associated with issue and return of the identification must be followed.

- 4.7. Vendor personnel shall report all security incidents directly to appropriate providing entity that will, in turn, follow the procedures outlined in University Procedure 21.01.06.C2.08 Incident Response.
- 4.8. The responsibilities and details of any vendor management involvement in university security incident management shall be specified in the contract.
- 4.9. The vendor must follow all applicable university change control processes and procedures. Regular work hours and duties shall be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate university management.
- 4.10. Upon termination of contract or at the request of university, the vendor shall return or destroy all university information and provide written certification of that return or destruction within 24 hours. Destruction of university information shall follow the guidelines set forth by the Texas Administrative Code Rule 202.78 Removal of Data from Data Processing Equipment.
- 4.11. Upon termination of contract or at the request of the university, the vendor must surrender all university identification badges, access cards, keys, software, equipment, and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by the providing entity.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 01.03 Appointing Power and Terms and Conditions of Employment
- 07.01 Ethics Policy, TAMUS Employees
- 32.02 Discipline and Dismissal of Employees
- 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
- 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
 - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
 - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration