

**THE TEXAS A&M UNIVERSITY SYSTEM  
HEALTH SCIENCE CENTER INTERNAL POLICIES**

---

---

**29.01.03.Z1.18 Vendor Access**

*Approved September 1, 2010*

**Supplements System Regulation 29.01.03**

---

---

**1. GENERAL**

1.1 Introduction

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors may:

- remotely view,
- copy and modify data and audit logs,
- 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 lost revenue, increased liability, loss of trust, and embarrassment to Texas A&M University System Health Science Center (HSC).

1.2 Audience

The HSC Vendor Access Policy applies to all individuals that are responsible for the installation of new information resources assets, and the operations and maintenance of existing information resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

## 1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.

## 1.5 Definitions

- **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Vendor:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

## 2. VENDOR ACCESS POLICY

2.1 Vendors must comply with all applicable HSC policies, practice standards and agreements, including, but not limited to:

- Safety Policies
- Privacy Policies
- Security Policies
- Auditing Policies
- Software Licensing Policies
- Acceptable Use Policies

- 2.2 Vendor agreements and contracts must specify:
- The HSC information the vendor is permitted to access.
  - How HSC information is to be protected by the vendor.
  - Acceptable methods for the return, destruction or disposal of HSC information in the vendor's possession at the end of the contract.
  - The vendor must only use HSC information and information resources for the purpose of the business agreement.
  - Any other HSC information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
  - HSC will provide an OIT point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
- 2.3 Each vendor must provide HSC with a list of all employees working on the contract. The list must be updated and provided to HSC within 24 hours of staff changes.
- 2.4 Each on-site vendor employee must acquire a HSC identification badge that will be displayed at all times while on HSC premises. The badge must be returned to HSC when the employee leaves the contract or at the end of the contract.
- 2.5 Each vendor employee with access to HSC sensitive information must be cleared to handle that information.
- 2.6 Vendor personnel must report all security incidents directly to the appropriate HSC personnel.
- 2.7 If vendor management is involved in HSC security incident management the responsibilities and details must be specified in the contract.
- 2.8 Vendor must follow all applicable HSC change control processes and procedures.
- 2.9 Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate HSC management.
- 2.10 All vendor maintenance equipment on the HSC network that connects to the outside world via the network, telephone line, or leased line, and all HSC IR vendor accounts will remain disabled except when in use for authorized maintenance.
- 2.11 Vendor access must be uniquely identifiable and password management must comply with the HSC Password Practice Standard and Administrative/Special Access Practice Standard. The vendor's major work activities must be entered into a log and available to HSC management upon request. Logs must include,

but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

- 2.12 Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to HSC or destroyed within 24 hours.
- 2.13 Upon termination of contract or at the request of HSC, the vendor will return or destroy all HSC information and provide written certification of that return or destruction within 24 hours.
- 2.14 Upon termination of contract or at the request of HSC, the vendor must surrender all HSC identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized HSC management.
- 2.15 Vendors are required to comply with all State and HSC auditing requirements, including the auditing of the vendor's work.
- 2.16 All software used by the vendor in providing service to HSC must be properly inventoried and licensed.

### **3. DISCIPLINARY ACTIONS**

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

### **OFFICE OF RESPONSIBILITY**

**Vice President for Information Technology and Chief Information Officer**