

OFFICE OF COURT ADMINISTRATION VENDOR ACCESS POLICY

Date: 02/02/2004

Approved by: Alicia Key

Office of Court Administration

Vendor Access Policy

(Texas Administrative Code, Title 1, Part 10, Ch 202, Section 202.7)

Purpose The purpose of the OCA Vendor Access Policy is to establish the rules for vendor access to OCA Information Resources and certain facilities, vendor responsibilities, and protection of OCA information. Vendors play an important role in the support of hardware and software management, and operations for OCA. Setting rules for accessing OCA's Information Resources will enhance OCA's security of those resources.

Audience The OCA Vendor Access Policy and Vendor Access Procedure apply 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.

If a vendor is only providing facility or equipment maintenance, the individuals are required only to comply with the Vendor Access Procedure, and not this Vendor Access Policy.

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 assistant (PDA), pagers, distributed processing systems, 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.

Vendor: someone who exchanges goods or services for money.

Point of Contact: project manager or other OCA employee designated by the Information Services Division Director. The Point of Contact is responsible for the oversight of the vendor's activities during the contract period.

Vendor Access Policy

- Vendors must comply with all applicable OCA information services policies and practice standards, including but not limited to:
 - ❖ Computer Security Policy
 - ❖ Email and Internet Use Policy
 - ❖ Information Services (IS) Change Management Policy
 - ❖ Information Services (IS) Internal Security Policy
 - ❖ Software Policy
 - ❖ Vendor Access Procedure

- OCA's Director of Information Services will provide a 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.

- Each vendor must provide OCA with a list of all employees working on the contract who will be given access. The list must be updated and provided to OCA within 24 hours of staff changes.

- Each vendor employee with access to OCA or court information or data must agree in writing to abide by all applicable OCA policies and procedures.

- Vendor personnel must report all security incidents directly to the OCA Information Security Officer (ISO).

- Regular work hours and duties will be defined by the Point of Contact. Work outside of defined parameters must be pre-approved by the Point of Contact, who will make arrangements for necessary facility services and access to secure areas.

**Vendor Access
Policy, continued**

- Within 24 hours of termination of contract or the request of OCA, the vendor will return or destroy all OCA or court information and data and provide written certification of that return or destruction.
- Upon termination of contract or at the request of OCA, the vendor must surrender all OCA access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by the OCA Point of Contact.

**Acknowledgment – Receipt of Information
Concerning Office of Court Administration Vendor Access Policy**

I, _____, acknowledge by my signature below that I
(Printed Name)

received and read a copy of the Office of Court Administration Vendor Access Policy on

_____.
(Date)

(Employee Signature)

*******PLEASE RETURN A COPY OF THIS FORM TO*****
THE HUMAN RESOURCE OFFICER**

Office of Court Administration (OCA)
Vendor Access Procedure

The purpose of this document is to set out a procedure by which vendors may access an OCA server room or other area at OCA where Information Resources are secured.

1. Only authorized employees of the Information Services (IS) or Finance and Operations (FAO) divisions may provide entry for a vendor into an OCA server room or other area where information resources are secured.
2. Authorized employees are designated jointly by the Director of Information Services and the Chief Financial Officer of OCA. The names of authorized employees will be posted on or near the door of each server room or other secured area.
3. The Vendor Access Point of Contact or the Director of Information Services must provide advance, written notice to an authorized IS or FAO employee to provide entry for a vendor to a server room or other secured area. The notice must provide:
 - a. the approximate date/time of vendor access;
 - b. the approximate length of time vendor will remain in the server room or other secured area;
 - c. the name of the OCA employee who will oversee the vendor's activities in the server room or other secured area; and
 - d. the project for which access is required.

For vendors who need access to a server room or other secured area for facilities or equipment maintenance, advance notice is not required.

4. The OCA employee monitoring the vendor's activities will be responsible for scheduling entry to the secured area with the authorized IS or FAO employee providing the entry and must be present upon entry of the vendor.
5. The vendor must sign the server room log upon entry into and exit from the server room or other secured area. The OCA employee monitoring the activities must initial the log upon entry and exit of the vendor.
6. At no time may a vendor be in a server room without an OCA employee monitoring the activities of the vendor.
7. Unless agreed upon in advance, access to an OCA server room or other secured area shall take place during regular business hours.